Notas de Aula - Fundamentos de matemática

Leandro F. Aurichi

ICMC-USP

Ou procure por aurichi icmc no google.

Aula 1 - Um primeiro problema

Numa república, moram 11 pessoas e só há uma geladeira.

Aula 1 - Um primeiro problema

Numa república, moram 11 pessoas e só há uma geladeira. Os moradores da república resolvem criar um método para a utilização da geladeira e, usando uma corrente e diversos cadeados, querem que ocorram duas coisas:

Aula 1 - Um primeiro problema

Numa república, moram 11 pessoas e só há uma geladeira. Os moradores da república resolvem criar um método para a utilização da geladeira e, usando uma corrente e diversos cadeados, querem que ocorram duas coisas:

- A geladeira só pode ser aberta quando houver pelo menos metade do moradores na casa;

Aula 1 - Um primeiro problema

Numa república, moram 11 pessoas e só há uma geladeira. Os moradores da república resolvem criar um método para a utilização da geladeira e, usando uma corrente e diversos cadeados, querem que ocorram duas coisas:

- A geladeira só pode ser aberta quando houver pelo menos metade do moradores na casa;
- Qualquer grupo de moradores que tenha pelo menos metade dos moradores, precisa conseguir abrir a geladeira.

Aula 1 - Um primeiro problema

Numa república, moram 11 pessoas e só há uma geladeira. Os moradores da república resolvem criar um método para a utilização da geladeira e, usando uma corrente e diversos cadeados, querem que ocorram duas coisas:

- A geladeira só pode ser aberta quando houver pelo menos metade do moradores na casa;
- Qualquer grupo de moradores que tenha pelo menos metade dos moradores, precisa conseguir abrir a geladeira.

Desta forma, quantos cadeados e quantas chaves são necessários no mínimo para satisfazer essas duas condições?

Aula 1 - Um caso simples

Aula 1 - Um caso simples

Antes de atacarmos o problema propriamente dito, vamos ver alguns casos mais simples:

Aula 1 - Um caso simples

Antes de atacarmos o problema propriamente dito, vamos ver alguns casos mais simples:

Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que qualquer morador da república pudesse abrir a geladeira?

Aula 1 - Um caso simples

Antes de atacarmos o problema propriamente dito, vamos ver alguns casos mais simples:

Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que qualquer morador da república pudesse abrir a geladeira?

Basta 1 cadeado e 11 chaves dele (uma cópia para cada morador).

Aula 1 - Outro caso simples

Aula 1 - Outro caso simples

Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que a geladeira só fosse aberta quando todos os moradores estivessem presentes?

Aula 1 - Outro caso simples

Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que a geladeira só fosse aberta quando todos os moradores estivessem presentes?

11 cadeados e 11 chaves (uma chave para cada cadeado, dando uma para cada morador).

Aula 1 - Funções

Aula 1 - Funções

Primeiramente, considere um grupo com 5 pessoas.

Primeiramente, considere um grupo com 5 pessoas. Note que 6 pessoas é o menor grupo com mais da metade do total de moradores, logo um grupo com 5 não pode conseguir abrir a geladeira.

Primeiramente, considere um grupo com 5 pessoas. Note que 6 pessoas é o menor grupo com mais da metade do total de moradores, logo um grupo com 5 não pode conseguir abrir a geladeira. Para que isso aconteça, precisa existir pelo menos um cadeado que esse grupo não consiga abrir.

Primeiramente, considere um grupo com 5 pessoas. Note que 6 pessoas é o menor grupo com mais da metade do total de moradores, logo um grupo com 5 não pode conseguir abrir a geladeira. Para que isso aconteça, precisa existir pelo menos um cadeado que esse grupo não consiga abrir. Assim, para cada grupo de 5 pessoas, precisa existir pelo menos um cadeado que esse grupo não abra.

Aula 1 - Criando uma função

Temos aqui uma associação entre diferentes conjuntos:

Aula 1 - Criando uma função

Temos aqui uma associação entre diferentes conjuntos: para cada grupo de 5 pessoas, fixe um cadeado que tal grupo não consegue abrir.

Aula 1 - Criando uma função

Temos aqui uma associação entre diferentes conjuntos: para cada grupo de 5 pessoas, fixe um cadeado que tal grupo não consegue abrir. Essa associação vai ser bastante importante, então precisamos deixá-la clara.

Aula 1 - Criando uma função

Temos aqui uma associação entre diferentes conjuntos: para cada grupo de 5 pessoas, fixe um cadeado que tal grupo não consegue abrir. Essa associação vai ser bastante importante, então precisamos deixá-la clara. Uma associação, em matemática, nada mais é que uma função, que denotamos da seguinte maneira:

$$f : A \to B$$

Aula 1 - Criando uma função

Temos aqui uma associação entre diferentes conjuntos: para cada grupo de 5 pessoas, fixe um cadeado que tal grupo não consegue abrir. Essa associação vai ser bastante importante, então precisamos deixá-la clara. Uma associação, em matemática, nada mais é que uma função, que denotamos da seguinte maneira:

$$f : A \to B$$

Isso quer dizer que a função f associa a cada elemento de A um elemento de B (em símbolos, f associa um elemento a com $f(a)$).

Aula 1 - Criando uma função

Aula 1 - Criando uma função

Neste caso, chamamos A de **domínio** de f

$$\text{dom}(f)$$

e B de **contradomínio** de f.

Aula 1 - Criando uma função

Neste caso, chamamos A de **domínio** de f

$$\text{dom}(f)$$

e B de **contradomínio** de f. O subconjunto de B formado pelos elementos que foram "atingidos" por f é chamado de **imagem** de f

$$\text{Im}(f).$$

Neste caso, chamamos A de **domínio** de f

$$\text{dom}(f)$$

e B de **contradomínio** de f. O subconjunto de B formado pelos elementos que foram "atingidos" por f é chamado de **imagem** de f

$$\text{Im}(f).$$

Isto é, são todos os elementos de B que são da forma $f(a)$ para algum elemento a de A.

Neste caso, chamamos A de **domínio** de f

$$\text{dom}(f)$$

e B de **contradomínio** de f. O subconjunto de B formado pelos elementos que foram "atingidos" por f é chamado de **imagem** de f

$$\text{Im}(f).$$

Isto é, são todos os elementos de B que são da forma $f(a)$ para algum elemento a de A.

Em símbolos

$$\text{Im}(f) = \{f(a) : a \in A\}.$$

Aula 1 - Voltando ao problema

Aula 1 - Voltando ao problema

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados.

Aula 1 - Voltando ao problema

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados. Essa associação será da seguinte forma: dado um grupo g, o cadeado $c(g)$ é um cadeado que o grupo g não consegue abrir.

Aula 1 - Voltando ao problema

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados. Essa associação será da seguinte forma: dado um grupo g, o cadeado $c(g)$ é um cadeado que o grupo g não consegue abrir.

Vejamos o que a gente consegue falar sobre essa função.

Aula 1 - Voltando ao problema

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados. Essa associação será da seguinte forma: dado um grupo g, o cadeado $c(g)$ é um cadeado que o grupo g não consegue abrir.

Vejamos o que a gente consegue falar sobre essa função. Note que a gente fez uma associação abstrata. Sabemos que a cada grupo, existe um cadeado associado tal que o grupo não consegue abri-lo.

Aula 1 - Voltando ao problema

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados. Essa associação será da seguinte forma: dado um grupo g, o cadeado $c(g)$ é um cadeado que o grupo g não consegue abrir.

Vejamos o que a gente consegue falar sobre essa função. Note que a gente fez uma associação abstrata. Sabemos que a cada grupo, existe um cadeado associado tal que o grupo não consegue abri-lo. Nem sabemos se existem outros cadeados nessa mesma situação.

Aula 1 - Voltando ao problema

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados. Essa associação será da seguinte forma: dado um grupo g, o cadeado $c(g)$ é um cadeado que o grupo g não consegue abrir.

Vejamos o que a gente consegue falar sobre essa função. Note que a gente fez uma associação abstrata. Sabemos que a cada grupo, existe um cadeado associado tal que o grupo não consegue abri-lo. Nem sabemos se existem outros cadeados nessa mesma situação. Mesmo com essa falta de informação, já podemos concluir algumas coisas.

Aula 1 - Cadeados diferentes

Aula 1 - Cadeados diferentes

Considere dois grupos diferentes, g_1 e g_2.

Aula 1 - Cadeados diferentes

Considere dois grupos diferentes, g_1 e g_2. Será que estes dois grupos podem estar associados ao mesmo cadeado?

Aula 1 - Cadeados diferentes

Considere dois grupos diferentes, g_1 e g_2. Será que estes dois grupos podem estar associados ao mesmo cadeado? Colocando em símbolos, pode acontecer $g_1 \neq g_2$ e $c(g_1) = c(g_2)$?

Aula 1 - Cadeados diferentes

Considere dois grupos diferentes, g_1 e g_2. Será que estes dois grupos podem estar associados ao mesmo cadeado? Colocando em símbolos, pode acontecer $g_1 \neq g_2$ e $c(g_1) = c(g_2)$? Essa é uma propriedade bastante importante sobre funções e que nos será bastante útil neste problema.

Aula 1 - Cadeados diferentes

Considere dois grupos diferentes, g_1 e g_2. Será que estes dois grupos podem estar associados ao mesmo cadeado? Colocando em símbolos, pode acontecer $g_1 \neq g_2$ e $c(g_1) = c(g_2)$? Essa é uma propriedade bastante importante sobre funções e que nos será bastante útil neste problema.

Dizemos que uma função $f : A \to B$ é **injetora** se, dados $a \neq b$, temos que $f(a) \neq f(b)$.

Aula 1 - Cadeados diferentes

Aula 1 - Cadeados diferentes

Ou seja, estamos nos perguntando se c é injetora ou não.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1. Juntando essa pessoa ao grupo g_1, temos um grupo de 6 pessoas.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1. Juntando essa pessoa ao grupo g_1, temos um grupo de 6 pessoas. Assim, tal grupo precisa conseguir abrir a geladeira.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1. Juntando essa pessoa ao grupo g_1, temos um grupo de 6 pessoas. Assim, tal grupo precisa conseguir abrir a geladeira. Desta forma, se $c(g_1) = c(g_2)$, o cadeado que o grupo g_1 não abre, também não seria aberto pela sexta pessoa acrescentada ao grupo (pois ela não abre $c(g_2)$, que é o mesmo cadeado $c(g_1)$).

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1. Juntando essa pessoa ao grupo g_1, temos um grupo de 6 pessoas. Assim, tal grupo precisa conseguir abrir a geladeira. Desta forma, se $c(g_1) = c(g_2)$, o cadeado que o grupo g_1 não abre, também não seria aberto pela sexta pessoa acrescentada ao grupo (pois ela não abre $c(g_2)$, que é o mesmo cadeado $c(g_1)$). Desta forma, os cadeados precisam ser diferentes.

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1. Juntando essa pessoa ao grupo g_1, temos um grupo de 6 pessoas. Assim, tal grupo precisa conseguir abrir a geladeira. Desta forma, se $c(g_1) = c(g_2)$, o cadeado que o grupo g_1 não abre, também não seria aberto pela sexta pessoa acrescentada ao grupo (pois ela não abre $c(g_2)$, que é o mesmo cadeado $c(g_1)$). Desta forma, os cadeados precisam ser diferentes. Ou seja, o argumento acima mostra que c é uma função injetora.

Aula 1 - Mais uma informação

Aula 1 - Mais uma informação

Com isso, já temos uma importante informação sobre o conjunto imagem da função c:

Aula 1 - Mais uma informação

Com isso, já temos uma importante informação sobre o conjunto imagem da função c: ele tem a mesma quantidade de elementos que o conjunto G (o conjunto de todos os grupos de 5 pessoas).

Aula 1 - Mais uma informação

Com isso, já temos uma importante informação sobre o conjunto imagem da função c: ele tem a mesma quantidade de elementos que o conjunto G (o conjunto de todos os grupos de 5 pessoas). Ou seja, a solução para o nosso problema requer uma quantidade de cadeados igual ou maior que a quantidade de grupos de 5 moradores da república.

Aula 1 - Mais uma informação

Com isso, já temos uma importante informação sobre o conjunto imagem da função c: ele tem a mesma quantidade de elementos que o conjunto G (o conjunto de todos os grupos de 5 pessoas). Ou seja, a solução para o nosso problema requer uma quantidade de cadeados igual ou maior que a quantidade de grupos de 5 moradores da república. Essa quantidade até poderia ser maior, pois ainda não sabemos se a tal associação fez aparecer todos os cadeados da solução.

Aula 1 - Chaves

Aula 1 - Chaves

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução.

Aula 1 - Chaves

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução. Imagine que você é um dos moradores da república e que só você esteja nela.

Aula 1 - Chaves

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução. Imagine que você é um dos moradores da república e que só você esteja nela. Agora suponha que chegou um grupo g de 5 moradores.

Aula 1 - Chaves

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução. Imagine que você é um dos moradores da república e que só você esteja nela. Agora suponha que chegou um grupo g de 5 moradores. Sabemos que o grupo não consegue abrir o cadeado $c(g)$.

Aula 1 - Chaves

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução. Imagine que você é um dos moradores da república e que só você esteja nela. Agora suponha que chegou um grupo g de 5 moradores. Sabemos que o grupo não consegue abrir o cadeado $c(g)$. Mas também sabemos que g junto com você forma um grupo de 6 pessoas.

Aula 1 - Chaves

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução. Imagine que você é um dos moradores da república e que só você esteja nela. Agora suponha que chegou um grupo g de 5 moradores. Sabemos que o grupo não consegue abrir o cadeado $c(g)$. Mas também sabemos que g junto com você forma um grupo de 6 pessoas. Logo, vocês conseguem abrir a geladeira.

Aula 1 - Chaves

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$.

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$. Mas se entrasse outro grupo, digamos h, pelo mesmo argumento, você teria que ter uma cópia da chave de $c(h)$.

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$. Mas se entrasse outro grupo, digamos h, pelo mesmo argumento, você teria que ter uma cópia da chave de $c(h)$. E já sabemos que, se $g \neq h$, então $c(g) \neq c(h)$.

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$. Mas se entrasse outro grupo, digamos h, pelo mesmo argumento, você teria que ter uma cópia da chave de $c(h)$. E já sabemos que, se $g \neq h$, então $c(g) \neq c(h)$. Ou seja, para cada grupo de 5 moradores (excluindo você), você precisa de uma chave diferente.

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$. Mas se entrasse outro grupo, digamos h, pelo mesmo argumento, você teria que ter uma cópia da chave de $c(h)$. E já sabemos que, se $g \neq h$, então $c(g) \neq c(h)$. Ou seja, para cada grupo de 5 moradores (excluindo você), você precisa de uma chave diferente. E o análogo vale para qualquer outro morador da casa.

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$. Mas se entrasse outro grupo, digamos h, pelo mesmo argumento, você teria que ter uma cópia da chave de $c(h)$. E já sabemos que, se $g \neq h$, então $c(g) \neq c(h)$. Ou seja, para cada grupo de 5 moradores (excluindo você), você precisa de uma chave diferente. E o análogo vale para qualquer outro morador da casa.

Resumindo, a quantidade de chaves que cada pessoa da casa precisa carregar é, pelo menos, a quantidade de grupos de 5 outras pessoas da república.

Aula 1 - Juntando tudo para resolver o problema

Aula 1 - Juntando tudo para resolver o problema

Já sabemos que, para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores.

Aula 1 - Juntando tudo para resolver o problema

Já sabemos que, para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores. Também sabemos que cada pessoa vai ter que carregar uma chave para cada grupo de outros 5 moradores (excluindo ela).

Aula 1 - Juntando tudo para resolver o problema

Já sabemos que, para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores. Também sabemos que cada pessoa vai ter que carregar uma chave para cada grupo de outros 5 moradores (excluindo ela).

Note que ainda não sabemos se uma solução com tais quantidades é possível.

Aula 1 - Juntando tudo para resolver o problema

Já sabemos que, para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores. Também sabemos que cada pessoa vai ter que carregar uma chave para cada grupo de outros 5 moradores (excluindo ela).

Note que ainda não sabemos se uma solução com tais quantidades é possível. Só sabemos, pela discussão acima, que uma solução vai ter que ter pelo menos tais quantidades.

Aula 1 - Juntando tudo para resolver o problema

Já sabemos que, para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores. Também sabemos que cada pessoa vai ter que carregar uma chave para cada grupo de outros 5 moradores (excluindo ela).

Note que ainda não sabemos se uma solução com tais quantidades é possível. Só sabemos, pela discussão acima, que uma solução vai ter que ter pelo menos tais quantidades. Ou seja, poderia ser que as quantidades mínimas fossem ainda maiores.

Aula 1 - É uma situação possível

Aula 1 - É uma situação possível

Vamos mostrar que existe uma solução com tais quantidades.

Aula 1 - É uma situação possível

Vamos mostrar que existe uma solução com tais quantidades.

Portanto, essa seria a melhor solução possível.

Aula 1 - É uma situação possível

Vamos mostrar que existe uma solução com tais quantidades.
Portanto, essa seria a melhor solução possível.

Para cada grupo de 5 pessoas, compre um cadeado.

Aula 1 - É uma situação possível

Vamos mostrar que existe uma solução com tais quantidades. Portanto, essa seria a melhor solução possível.

Para cada grupo de 5 pessoas, compre um cadeado. No cadeado, escreva o nome das 6 pessoas que não estão no tal grupo deste cadeado.

Aula 1 - É uma situação possível

Vamos mostrar que existe uma solução com tais quantidades. Portanto, essa seria a melhor solução possível.

Para cada grupo de 5 pessoas, compre um cadeado. No cadeado, escreva o nome das 6 pessoas que não estão no tal grupo deste cadeado. Para cada uma dessas pessoas cujo nome está no cadeado, dê uma cópia da chave deste cadeado.

Aula 1 - É uma situação possível

Vamos mostrar que existe uma solução com tais quantidades. Portanto, essa seria a melhor solução possível.

Para cada grupo de 5 pessoas, compre um cadeado. No cadeado, escreva o nome das 6 pessoas que não estão no tal grupo deste cadeado. Para cada uma dessas pessoas cujo nome está no cadeado, dê uma cópia da chave deste cadeado.

Primeiro, note que as quantidades batem: o número de cadeados é o mesmo da quantidade de grupos de 5 pessoas. Note também que cada pessoa tem o nome (e portanto a chave) de cada cadeado em cujo grupo ela não está.

Aula 1 - Funciona

Aula 1 - Funciona

Vejamos que isso é de fato uma solução.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas. Logo, uma das pessoas do grupo tem o nome escrito nele e, portanto, tal pessoa tem a chave do cadeado.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas. Logo, uma das pessoas do grupo tem o nome escrito nele e, portanto, tal pessoa tem a chave do cadeado. Isso vale para todos os cadeados, logo o grupo consegue abrir a geladeira.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas. Logo, uma das pessoas do grupo tem o nome escrito nele e, portanto, tal pessoa tem a chave do cadeado. Isso vale para todos os cadeados, logo o grupo consegue abrir a geladeira. Falta ver que grupos com menos de 6 pessoas não conseguem abrir.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas. Logo, uma das pessoas do grupo tem o nome escrito nele e, portanto, tal pessoa tem a chave do cadeado. Isso vale para todos os cadeados, logo o grupo consegue abrir a geladeira. Falta ver que grupos com menos de 6 pessoas não conseguem abrir. Se um grupo tiver 5 ou menos pessoas, vai haver um cadeado sem o nome de todos os integrantes do grupo.

Aula 1 - Funciona

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas. Logo, uma das pessoas do grupo tem o nome escrito nele e, portanto, tal pessoa tem a chave do cadeado. Isso vale para todos os cadeados, logo o grupo consegue abrir a geladeira. Falta ver que grupos com menos de 6 pessoas não conseguem abrir. Se um grupo tiver 5 ou menos pessoas, vai haver um cadeado sem o nome de todos os integrantes do grupo. Logo, tal cadeado não vai poder ser aberto.

Aula 1 - Colocando os números

Aula 1 - Colocando os números

Falta ver quais são as quantidades exatas.

Aula 1 - Colocando os números

Falta ver quais são as quantidades exatas. Para isso, vamos usar algumas fórmulas de contagem.

Aula 1 - Colocando os números

Falta ver quais são as quantidades exatas. Para isso, vamos usar algumas fórmulas de contagem. Essas fórmulas serão apresentadas formalmente mais adiante.

Aula 1 - Colocando os números

Falta ver quais são as quantidades exatas. Para isso, vamos usar algumas fórmulas de contagem. Essas fórmulas serão apresentadas formalmente mais adiante. Por equanto, vamos só aplicá-las aqui sem maiores discussões.

Aula 1 - Cadeados

Aula 1 - Cadeados

Para o número de cadeados, precisamos da quantidade de combinações de 11 5 a 5:

Aula 1 - Cadeados

Para o número de cadeados, precisamos da quantidade de combinações de 11 5 a 5:

$$\left(\begin{array}{c} 11 \\ 5 \end{array} \right) = \frac{11!}{5!6!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{5 \cdot 4 \cdot 3 \cdot 2} = 462$$

Aula 1 - Chaves

Aula 1 - Chaves

Já para as chaves, para cada morador é necessária a quantidade de combinações de 10 5 a 5:

Aula 1 - Chaves

Já para as chaves, para cada morador é necessária a quantidade de combinações de 10 5 a 5:

$$\left(\begin{array}{c} 10 \\ 5 \end{array} \right) = \frac{10!}{5!5!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252$$

Já para as chaves, para cada morador é necessária a quantidade de combinações de 10 5 a 5:

$$\left(\begin{array}{c} 10 \\ 5 \end{array} \right) = \frac{10!}{5!5!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252$$

Assim, somando as chaves de todos os moradores, temos um total de 2772 chaves.

Aula 2 - Conjuntos

Vamos ver um pouco sobre conjunto (mas só um pouco, por enquanto).

Aula 2 - Inclusão

Aula 2 - Inclusão

Podemos ter um subconjunto de um conjunto.

Aula 2 - Inclusão

Podemos ter um subconjunto de um conjunto. No sentido que todos os elementos do primeiro também são elementos do segundo.

Aula 2 - Inclusão

Podemos ter um subconjunto de um conjunto. No sentido que todos os elementos do primeiro também são elementos do segundo. Essa relação é denotada por

$$A \subset B$$

Lê-se A está contido em B.

Aula 2 - Inclusão

Podemos ter um subconjunto de um conjunto. No sentido que todos os elementos do primeiro também são elementos do segundo. Essa relação é denotada por

$$A \subset B$$

Lê-se A está contido em B. Como exemplo, temos que $\mathbb{N} \subset \mathbb{R}$, onde $\mathbb{R}$ é o conjunto dos números reais.

Aula 2 - Inclusão

Podemos ter um subconjunto de um conjunto. No sentido que todos os elementos do primeiro também são elementos do segundo. Essa relação é denotada por

$$A \subset B$$

Lê-se A está contido em B. Como exemplo, temos que $\mathbb{N} \subset \mathbb{R}$, onde $\mathbb{R}$ é o conjunto dos números reais. Afinal, todo número natural é também um número real.

Aula 2 - Algumas propriedades sobre a inclusão

Proposição

Sejam A, B, C conjuntos. Valem as seguintes propriedades:

Aula 2 - Algumas propriedades sobre a inclusão

Proposição

Sejam A, B, C conjuntos. Valem as seguintes propriedades:

- $A \subset A$;

Aula 2 - Algumas propriedades sobre a inclusão

Proposição

Sejam A, B, C conjuntos. Valem as seguintes propriedades:

- $A \subset A$;
- *Se* $A \subset B$ *e* $B \subset C$, *então* $A \subset C$;

Aula 2 - Algumas propriedades sobre a inclusão

Proposição

Sejam A, B, C conjuntos. Valem as seguintes propriedades:

- $A \subset A$;
- *Se* $A \subset B$ *e* $B \subset C$, *então* $A \subset C$;
- *Se* $A \subset B$ *e* $B \subset A$, *então* $A = B$.

Aula 2 - Provando

- $A \subset A$:

Aula 2 - Provando

- $A \subset A$:
  Teríamos só que verificar que todo elemento de A é um elemento de A.

- $A \subset A$:
  Teríamos só que verificar que todo elemento de A é um elemento de A. Mas isso é imediato (certo?). $\square$

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:
  Agora temos que verificar que todo elemento de A é também um elemento de C.

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:
  Agora temos que verificar que todo elemento de A é também um elemento de C. Isso fica mais fácil se fixarmos um elemento de A de começo.

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:
  Agora temos que verificar que todo elemento de A é também um elemento de C. Isso fica mais fácil se fixarmos um elemento de A de começo. Considere $a \in A$.

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:
  Agora temos que verificar que todo elemento de A é também um elemento de C. Isso fica mais fácil se fixarmos um elemento de A de começo. Considere $a \in A$. Como $A \subset B$, obtemos que $a \in B$.

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:
  Agora temos que verificar que todo elemento de A é também um elemento de C. Isso fica mais fácil se fixarmos um elemento de A de começo. Considere $a \in A$. Como $A \subset B$, obtemos que $a \in B$. Por sua vez, sabemos que $B \subset C$.

Aula 2 - Provando

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:
  Agora temos que verificar que todo elemento de A é também um elemento de C. Isso fica mais fácil se fixarmos um elemento de A de começo. Considere $a \in A$. Como $A \subset B$, obtemos que $a \in B$. Por sua vez, sabemos que $B \subset C$. Assim, $a \in C$, como queríamos. $\square$

Aula 2 - Provando

- Se $A \subset B$ e $B \subset A$, então $A = B$:

Aula 2 - Provando

- Se $A \subset B$ e $B \subset A$, então $A = B$:
  O grande truque aqui é: dois conjuntos são o mesmo conjunto se eles tem os mesmos elementos.

Aula 2 - Provando

- Se $A \subset B$ e $B \subset A$, então $A = B$:
  O grande truque aqui é: dois conjuntos são o mesmo conjunto se eles tem os mesmos elementos. Daí agora ficou simples: $A \subset B$ quer dizer que todos os elementos de A estão em B.

- Se $A \subset B$ e $B \subset A$, então $A = B$:
  O grande truque aqui é: dois conjuntos são o mesmo conjunto se eles tem os mesmos elementos. Daí agora ficou simples: $A \subset B$ quer dizer que todos os elementos de A estão em B. Por sua vez, todos os elementos de B estão em A (pois também temos que $B \subset A$). $\square$

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P.

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Um exemplo deixa isso mais claro.

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Um exemplo deixa isso mais claro. Imagine que queremos o conjunto P dos números pares.

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Um exemplo deixa isso mais claro. Imagine que queremos o conjunto P dos números pares. Podemos fazer isso a partir do conjunto dos números naturais:

$$P = \{n \in \mathbb{N} : n \text{ é par}\}.$$

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Um exemplo deixa isso mais claro. Imagine que queremos o conjunto P dos números pares. Podemos fazer isso a partir do conjunto dos números naturais:

$$P = \{n \in \mathbb{N} : n \text{ é par}\}.$$

Repare que sempre que fizermos algo do tipo temos uma inclusão automática.

Aula 2 - Subconjuntos especiais

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Um exemplo deixa isso mais claro. Imagine que queremos o conjunto P dos números pares. Podemos fazer isso a partir do conjunto dos números naturais:

$$P = \{n \in \mathbb{N} : n \text{ é par}\}.$$

Repare que sempre que fizermos algo do tipo temos uma inclusão automática. No caso deste último exemplo, $P \subset \mathbb{N}$.

Aula 2 - União

Aula 2 - União

Podemos “juntar” dois conjuntos.

Aula 2 - União

Podemos "juntar" dois conjuntos. Se A e B são dois conjuntos, podemos criar um novo conjunto que contém todos os elementos de A e de B.

Aula 2 - União

Podemos "juntar" dois conjuntos. Se A e B são dois conjuntos, podemos criar um novo conjunto que contém todos os elementos de A e de B. Chamamos tal conjunto de **união** de A e B e denotamos por $A \cup B$.

Aula 2 - União

Podemos "juntar" dois conjuntos. Se A e B são dois conjuntos, podemos criar um novo conjunto que contém todos os elementos de A e de B. Chamamos tal conjunto de **união** de A e B e denotamos por $A \cup B$.

Por exemplo, considere P o conjunto do números pares e I o conjunto dos números ímpares.

Aula 2 - União

Podemos "juntar" dois conjuntos. Se A e B são dois conjuntos, podemos criar um novo conjunto que contém todos os elementos de A e de B. Chamamos tal conjunto de **união** de A e B e denotamos por $A \cup B$.

Por exemplo, considere P o conjunto do números pares e I o conjunto dos números ímpares. Note que $\mathbb{N} = P \cup I$.

Aula 2 - Intersecção

Aula 2 - Intersecção

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B.

Aula 2 - Intersecção

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B. Chamamos tal conjunto de **intersecção** entre A e B e denotamos por $A \cap B$.

Aula 2 - Intersecção

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B. Chamamos tal conjunto de **intersecção** entre A e B e denotamos por $A \cap B$.

Por exemplo, considere P o conjunto dos números pares e T o conjunto dos números múltiplos de 3 (isto é, $T = \{0, 3, 6, 9, 12, ...\}$).

Aula 2 - Intersecção

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B. Chamamos tal conjunto de **intersecção** entre A e B e denotamos por $A \cap B$.

Por exemplo, considere P o conjunto dos números pares e T o conjunto dos números múltiplos de 3 (isto é, $T = \{0, 3, 6, 9, 12, ...\}$). Temos

$$P \cap T = \{0, 6, 12, 18, ...\}.$$

Aula 2 - Intersecção

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B. Chamamos tal conjunto de **intersecção** entre A e B e denotamos por $A \cap B$.

Por exemplo, considere P o conjunto dos números pares e T o conjunto dos números múltiplos de 3 (isto é, $T = \{0, 3, 6, 9, 12, ...\}$). Temos

$$P \cap T = \{0, 6, 12, 18, ...\}.$$

Por outro lado, se tomarmos P (conjunto dos pares) e I (conjunto dos ímpares), temos que $P \cap I$ não tem qualquer elemento, já que P e I não tem elementos em comum.

Aula 2 - Intersecção

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B. Chamamos tal conjunto de **intersecção** entre A e B e denotamos por $A \cap B$.

Por exemplo, considere P o conjunto dos números pares e T o conjunto dos números múltiplos de 3 (isto é, $T = \{0, 3, 6, 9, 12, ...\}$). Temos

$$P \cap T = \{0, 6, 12, 18, ...\}.$$

Por outro lado, se tomarmos P (conjunto dos pares) e I (conjunto dos ímpares), temos que $P \cap I$ não tem qualquer elemento, já que P e I não tem elementos em comum. Ao conjunto que não tem elementos damos o nome de **conjunto vazio** e denotamos por $\emptyset$. Assim, $P \cap I = \emptyset$.

Aula 2 - Vacuidade

Aqui há algo que causa estranhamento:

Aula 2 - Vacuidade

Aqui há algo que causa estranhamento: $\emptyset \subset A$, para qualquer conjunto A.

Aula 2 - Vacuidade

Aqui há algo que causa estranhamento: $\emptyset \subset A$, para qualquer conjunto A. Para tentar aceitar isso, pense da seguinte forma: para que não fosse verdade que $\emptyset \subset A$, deveria existir algum elemento em $\emptyset$ que não estivesse em A.

Aula 2 - Uma igualdade

Aula 2 - Uma igualdade

Vamos apresentar uma igualdade bastante útil (Nos alongamentos das notas de aula tem outras.).

Aula 2 - Uma igualdade

Vamos apresentar uma igualdade bastante útil (Nos alongamentos das notas de aula tem outras.).

Proposição
Sejam A, B e C conjuntos. Então vale a seguinte igualdade:

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

Demonstração. Essa demonstração fica muito mais fácil se tentarmos mostrá-la em dois pedaços.

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

Demonstração. Essa demonstração fica muito mais fácil se tentarmos mostrá-la em dois pedaços. Primeiro, vamos mostrar que o conjunto da esquerda é subconjunto do da direita. Depois fazemos o contrário e, portanto, teremos a igualdade.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$:

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$. Neste caso é imediato que $x \in A \cup (B \cap C)$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$. Neste caso é imediato que $x \in A \cup (B \cap C)$. Agora suponha que $x \notin A$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$. Neste caso é imediato que $x \in A \cup (B \cap C)$. Agora suponha que $x \notin A$. Então, como $x \in A \cup B$, $x \in B$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$. Neste caso é imediato que $x \in A \cup (B \cap C)$. Agora suponha que $x \notin A$. Então, como $x \in A \cup B$, $x \in B$. Analogamente, como $x \in A \cup C$, temos que $x \in C$. Ou seja, $x \in B \cap C$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$. Neste caso é imediato que $x \in A \cup (B \cap C)$. Agora suponha que $x \notin A$. Então, como $x \in A \cup B$, $x \in B$. Analogamente, como $x \in A \cup C$, temos que $x \in C$. Ou seja, $x \in B \cap C$. Logo, temos o que queríamos.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\supset$:

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\supset$: Seja $x \in A \cup (B \cap C)$.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\supset$: Seja $x \in A \cup (B \cap C)$. Novamente, fazemos dois casos.

Aula 2 - Provando

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\supset$: Seja $x \in A \cup (B \cap C)$. Novamente, fazemos dois casos. Se $x \in A$, então claramente $x \in (A \cup B) \cap (A \cup C)$.

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\supset$: Seja $x \in A \cup (B \cap C)$. Novamente, fazemos dois casos. Se $x \in A$, então claramente $x \in (A \cup B) \cap (A \cup C)$. Por outro lado, se $x \notin A$, então $x \in B \cap C$.

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

- $\supset$: Seja $x \in A \cup (B \cap C)$. Novamente, fazemos dois casos. Se $x \in A$, então claramente $x \in (A \cup B) \cap (A \cup C)$. Por outro lado, se $x \notin A$, então $x \in B \cap C$. Neste caso, novamente temos que $x \in A \cup B$ e $x \in A \cup C$ como queríamos.

□

Aula 2 - Conjuntos de conjuntos

Não há problema em um conjunto pertencer a outro.

Não há problema em um conjunto pertencer a outro. Na verdade, no exemplo da geladeira, fizemos exatamente isso: tínhamos um conjunto que cada elemento era um conjunto de 5 moradores.

Não há problema em um conjunto pertencer a outro. Na verdade, no exemplo da geladeira, fizemos exatamente isso: tínhamos um conjunto que cada elemento era um conjunto de 5 moradores. Podemos então ter um conjunto

$$A = \{1, 2, 4\}$$

e depois ter um outro conjunto que contém A como elemento:

$$B = \{7, 9, A\}.$$

Um outro jeito de representar B seria não usando a notação de A:

$$B = \{7, 9, \{1, 2, 4\}\}.$$

Não há problema em um conjunto pertencer a outro. Na verdade, no exemplo da geladeira, fizemos exatamente isso: tínhamos um conjunto que cada elemento era um conjunto de 5 moradores. Podemos então ter um conjunto

$$A = \{1, 2, 4\}$$

e depois ter um outro conjunto que contém A como elemento:

$$B = \{7, 9, A\}.$$

Um outro jeito de representar B seria não usando a notação de A:

$$B = \{7, 9, \{1, 2, 4\}\}.$$

Que é muito diferente de

$$\{7, 9, 1, 2, 4\}.$$

Aula 2 - É só contar

Note, por exemplo, que o conjunto $\{7, 9, \{1, 2, 4\}\}$ tem 3 elementos, enquanto que o conjunto $\{7, 9, 1, 2, 4\}$ tem 5.

Note, por exemplo, que o conjunto $\{7, 9, \{1, 2, 4\}\}$ tem 3 elementos, enquanto que o conjunto $\{7, 9, 1, 2, 4\}$ tem 5.

Se você estiver com dúvidas com relação a isso, tente se convencer primeiramente que 2 não é um elemento de $\{7, 9, \{1, 2, 4\}\}$.

Aula 2 - Conjunto das partes

Aula 2 - Conjunto das partes

Dado um conjunto A, existe um conjunto especial, chamado de **conjunto das partes** de A, denotado por $\wp(A)$ que nada mais é que o conjunto de todos os subconjuntos de A.

Aula 2 - Conjunto das partes

Dado um conjunto A, existe um conjunto especial, chamado de **conjunto das partes** de A, denotado por $\wp(A)$ que nada mais é que o conjunto de todos os subconjuntos de A.

Por exemplo, considere $A = \{a, b, c\}$.

Aula 2 - Conjunto das partes

Dado um conjunto A, existe um conjunto especial, chamado de **conjunto das partes** de A, denotado por $\wp(A)$ que nada mais é que o conjunto de todos os subconjuntos de A.

Por exemplo, considere $A = \{a, b, c\}$. Assim

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Aula 2 - Conjunto das partes

Dado um conjunto A, existe um conjunto especial, chamado de **conjunto das partes** de A, denotado por $\wp(A)$ que nada mais é que o conjunto de todos os subconjuntos de A.

Por exemplo, considere $A = \{a, b, c\}$. Assim

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Observe que, não importa quem seja o conjunto A, sempre teremos que $\emptyset \in \wp(A)$ e também que $A \in \wp(A)$.

Aula 2 - Mais estranhezas

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$?

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez.

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A.

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A).

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$?

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$? A resposta, depois de pensarmos um pouco, é não.

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$? A resposta, depois de pensarmos um pouco, é não. Ou seja

$$\wp(\emptyset) = \{\emptyset\}.$$

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$? A resposta, depois de pensarmos um pouco, é não. Ou seja

$$\wp(\emptyset) = \{\emptyset\}.$$

Um erro comum aqui é achar que $\emptyset = \{\emptyset\}$.

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$? A resposta, depois de pensarmos um pouco, é não. Ou seja

$$\wp(\emptyset) = \{\emptyset\}.$$

Um erro comum aqui é achar que $\emptyset = \{\emptyset\}$. Mas tem um argumento simples para ver que tais conjuntos são diferentes.

Aula 2 - Mais estranhezas

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$? A resposta, depois de pensarmos um pouco, é não. Ou seja

$$\wp(\emptyset) = \{\emptyset\}.$$

Um erro comum aqui é achar que $\emptyset = \{\emptyset\}$. Mas tem um argumento simples para ver que tais conjuntos são diferentes. Por exemplo, $\emptyset$ tem 0 elementos, enquanto que $\{\emptyset\}$ tem um elemento (chamamos um conjunto com um único elemento de **conjunto unitário**) que é o próprio conjunto $\emptyset$.

Aula 2 - Uniões e intersecções múltiplas

Aula 2 - Uniões e intersecções múltiplas

Podemos fazer uniões de infinitos conjuntos de uma vez.

Aula 2 - Uniões e intersecções múltiplas

Podemos fazer uniões de infinitos conjuntos de uma vez. Por exemplo, se para cada $n \in \mathbb{N}$ temos um conjunto A_n, denotamos por $\bigcup_{n\in\mathbb{N}} A_n$ o conjunto com todos os elementos que pertençam a algum dos A_n's.

Aula 2 - Uniões e intersecções múltiplas

Podemos fazer uniões de infinitos conjuntos de uma vez. Por exemplo, se para cada $n \in \mathbb{N}$ temos um conjunto A_n, denotamos por $\bigcup_{n\in\mathbb{N}} A_n$ o conjunto com todos os elementos que pertençam a algum dos A_n's.

Analogamente, denotamos por $\bigcap_{n\in\mathbb{N}} A_n$ o conjunto que contém todos os elementos que pertençam a todos os A_n's.

Aula 2 - Também serve para finitos

Aula 2 - Também serve para finitos

Essa notação também serve para finitos conjuntos.

Aula 2 - Também serve para finitos

Essa notação também serve para finitos conjuntos. Por exemplo, se A_1, A_2 e A_3 são conjuntos, podemos usar a notação

$$\bigcup_{n=1}^{3} A_n$$

em vez de $A_1 \cup A_2 \cup A_3$.

Aula 2 - Também serve para finitos

Essa notação também serve para finitos conjuntos. Por exemplo, se A_1, A_2 e A_3 são conjuntos, podemos usar a notação

$$\bigcup_{n=1}^{3} A_n$$

em vez de $A_1 \cup A_2 \cup A_3$. O análogo serve para a intersecção.

Aula 2 - Um pequeno resultado

Aula 2 - Um pequeno resultado

Como exemplo, vamos provar um resultado para ver essa notação em uso:

Aula 2 - Um pequeno resultado

Como exemplo, vamos provar um resultado para ver essa notação em uso:

Proposição
Seja I um conjunto de índices. Para cada $i \in I$, considere A_i um conjunto. Se existe um conjunto X tal que cada $A_i \subset X$, então $\bigcup_{i \in I} A_i \subset X$.

Aula 2 - Um pequeno resultado

Como exemplo, vamos provar um resultado para ver essa notação em uso:

Proposição
Seja I um conjunto de índices. Para cada $i \in I$, considere A_i um conjunto. Se existe um conjunto X tal que cada $A_i \subset X$, então $\bigcup_{i \in I} A_i \subset X$.

Demonstração.
Precisamos tomar um elemento de $\bigcup_{i \in I} A_i$ e mostrar que ele pertence a X.

Aula 2 - Um pequeno resultado

Como exemplo, vamos provar um resultado para ver essa notação em uso:

Proposição
Seja I um conjunto de índices. Para cada $i \in I$, considere A_i um conjunto. Se existe um conjunto X tal que cada $A_i \subset X$, então $\bigcup_{i \in I} A_i \subset X$.

Demonstração.
Precisamos tomar um elemento de $\bigcup_{i \in I} A_i$ e mostrar que ele pertence a X.

Seja $x \in \bigcup_{i \in I} A_i$. Isso quer dizer que existem um $i \in I$ tal que $x \in A_i$. Mas, por hipótese, temos que $A_i \subset X$.

Aula 2 - Um pequeno resultado

Como exemplo, vamos provar um resultado para ver essa notação em uso:

Proposição
Seja I um conjunto de índices. Para cada $i \in I$, considere A_i um conjunto. Se existe um conjunto X tal que cada $A_i \subset X$, então $\bigcup_{i \in I} A_i \subset X$.

Demonstração.
Precisamos tomar um elemento de $\bigcup_{i \in I} A_i$ e mostrar que ele pertence a X.

Seja $x \in \bigcup_{i \in I} A_i$. Isso quer dizer que existem um $i \in I$ tal que $x \in A_i$. Mas, por hipótese, temos que $A_i \subset X$. Assim, $x \in X$, como queríamos. □

Aula 2 - Um exemplo de união infinita

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$.

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$.

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$. Note que já temos que $\bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{N}$.

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$. Note que já temos que $\bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{N}$. Assim, só precisamos mostrar que $\mathbb{N} \subset \bigcup_{n\in\mathbb{N}} A_n$.

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$. Note que já temos que $\bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{N}$. Assim, só precisamos mostrar que $\mathbb{N} \subset \bigcup_{n\in\mathbb{N}} A_n$. De fato, seja $n \in \mathbb{N}$.

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$. Note que já temos que $\bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{N}$. Assim, só precisamos mostrar que $\mathbb{N} \subset \bigcup_{n\in\mathbb{N}} A_n$. De fato, seja $n \in \mathbb{N}$. Note que $n \in A_n$ (pois $A_n = \{0, 1, ..., n\}$).

Aula 2 - Um exemplo de união infinita

Exemplo
Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$. Note que já temos que $\bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{N}$. Assim, só precisamos mostrar que $\mathbb{N} \subset \bigcup_{n\in\mathbb{N}} A_n$. De fato, seja $n \in \mathbb{N}$. Note que $n \in A_n$ (pois $A_n = \{0, 1, ..., n\}$). Assim, $n \in \bigcup_{n\in\mathbb{N}} A_n$.

Aula 2 - Diferença entre conjuntos

Aula 2 - Diferença entre conjuntos

Dados A e B conjuntos, muitas vezes é útil o conjunto formado pelos elementos que estão em A mas não estão em B.

Aula 2 - Diferença entre conjuntos

Dados A e B conjuntos, muitas vezes é útil o conjunto formado pelos elementos que estão em A mas não estão em B. Ou seja, o seguinte conjunto:

$$A \setminus B = \{a \in A : a \notin B\}$$

Aula 2 - Diferença entre conjuntos

Dados A e B conjuntos, muitas vezes é útil o conjunto formado pelos elementos que estão em A mas não estão em B. Ou seja, o seguinte conjunto:

$$A \setminus B = \{a \in A : a \notin B\}$$

Uma coisa "estranha" aqui é que B não precisa estar contido em A (Veja um alongamento nas notas de aula.).

Aula 2 - Intervalos

Aula 2 - Intervalos

Um tipo de conjunto bastante importante é o **intervalo** de números reais.

Aula 2 - Intervalos

Um tipo de conjunto bastante importante é o **intervalo** de números reais. Formalmente, um subconjunto A dos reais é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in \mathbb{R}$ é tal que $a < c < b$, então $c \in A$.

Aula 2 - Intervalos

Um tipo de conjunto bastante importante é o **intervalo** de números reais. Formalmente, um subconjunto A dos reais é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in \mathbb{R}$ é tal que $a < c < b$, então $c \in A$. Isso quer dizer o seguinte: se um número c estrá entre dois números do intervalo, então c também está no intervalo.

Aula 2 - Intervalos

Um tipo de conjunto bastante importante é o **intervalo** de números reais. Formalmente, um subconjunto A dos reais é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in \mathbb{R}$ é tal que $a < c < b$, então $c \in A$. Isso quer dizer o seguinte: se um número c estrá entre dois números do intervalo, então c também está no intervalo. As notações para intervalos são as usuais:

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

Aula 2 - Intervalos

Um tipo de conjunto bastante importante é o **intervalo** de números reais. Formalmente, um subconjunto A dos reais é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in \mathbb{R}$ é tal que $a < c < b$, então $c \in A$. Isso quer dizer o seguinte: se um número c estrá entre dois números do intervalo, então c também está no intervalo. As notações para intervalos são as usuais:

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\}$$

Aula 2 - Intervalos

Um tipo de conjunto bastante importante é o **intervalo** de números reais. Formalmente, um subconjunto A dos reais é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in \mathbb{R}$ é tal que $a < c < b$, então $c \in A$. Isso quer dizer o seguinte: se um número c estrá entre dois números do intervalo, então c também está no intervalo. As notações para intervalos são as usuais:

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\}$$

$$[a, \infty[= \{x \in \mathbb{R} : a \leq x\}.$$

Aula 2 - $[a, \infty[$

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição.

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados.

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados. Para deixar isso mais claro, vejamos que $[1, +\infty[$ é de fato um intervalo (segundo a nossa definição).

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados. Para deixar isso mais claro, vejamos que $[1, +\infty[$ é de fato um intervalo (segundo a nossa definição). Ou seja, precisamos tomar $a, b \in [1, +\infty[$ e $c \in \mathbb{R}$ de forma que $a < c < b$ e provar que $c \in [1, +\infty[$.

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados. Para deixar isso mais claro, vejamos que $[1, +\infty[$ é de fato um intervalo (segundo a nossa definição). Ou seja, precisamos tomar $a, b \in [1, +\infty[$ e $c \in \mathbb{R}$ de forma que $a < c < b$ e provar que $c \in [1, +\infty[$. Note que, como $a \in [1, +\infty[$, temos que $1 \leq a$.

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados. Para deixar isso mais claro, vejamos que $[1, +\infty[$ é de fato um intervalo (segundo a nossa definição). Ou seja, precisamos tomar $a, b \in [1, +\infty[$ e $c \in \mathbb{R}$ de forma que $a < c < b$ e provar que $c \in [1, +\infty[$. Note que, como $a \in [1, +\infty[$, temos que $1 \leq a$. Como $a < c$, temos que $1 < c$.

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados. Para deixar isso mais claro, vejamos que $[1, +\infty[$ é de fato um intervalo (segundo a nossa definição). Ou seja, precisamos tomar $a, b \in [1, +\infty[$ e $c \in \mathbb{R}$ de forma que $a < c < b$ e provar que $c \in [1, +\infty[$. Note que, como $a \in [1, +\infty[$, temos que $1 \leq a$. Como $a < c$, temos que $1 < c$. Ou seja, $c \in [1, +\infty[$.

Aula 2 - Nem tudo é intervalo

Aula 2 - Nem tudo é intervalo

O seguinte conjunto não é um intervalo:

Aula 2 - Nem tudo é intervalo

O seguinte conjunto não é um intervalo:

$$A = \{x \in \mathbb{R} : x \neq 0\}.$$

Aula 2 - Nem tudo é intervalo

O seguinte conjunto não é um intervalo:

$$A = \{x \in \mathbb{R} : x \neq 0\}.$$

Um motivo para que ele não seja um intervalo: note que $-1, 1 \in A$.

Aula 2 - Nem tudo é intervalo

O seguinte conjunto não é um intervalo:

$$A = \{x \in \mathbb{R} : x \neq 0\}.$$

Um motivo para que ele não seja um intervalo: note que $-1, 1 \in A$. Note também que $-1 < 0 < 1$.

Aula 2 - Nem tudo é intervalo

O seguinte conjunto não é um intervalo:

$$A = \{x \in \mathbb{R} : x \neq 0\}.$$

Um motivo para que ele não seja um intervalo: note que $-1, 1 \in A$. Note também que $-1 < 0 < 1$. Mas, $0 \notin A$.

Aula 2 - Nem tudo é intervalo

O seguinte conjunto não é um intervalo:

$$A = \{x \in \mathbb{R} : x \neq 0\}.$$

Um motivo para que ele não seja um intervalo: note que $-1, 1 \in A$. Note também que $-1 < 0 < 1$. Mas, $0 \notin A$. Ou seja, 0 está entre dois elementos de A mas não está em A.

Aula 2 - Uniões e intersecções

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.).

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$.
Temos que mostrar que $c \in I \cap J$.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$. Temos que mostrar que $c \in I \cap J$. Mas, como $a, b \in I \cap J$, então $a, b \in I$.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$. Temos que mostrar que $c \in I \cap J$. Mas, como $a, b \in I \cap J$, então $a, b \in I$. Logo, como I é intervalo, $c \in I$.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$. Temos que mostrar que $c \in I \cap J$. Mas, como $a, b \in I \cap J$, então $a, b \in I$. Logo, como I é intervalo, $c \in I$. Analogamente, $c \in J$.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (Ver alongamento nas notas de aula.). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição
Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.

Demonstração.
Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$. Temos que mostrar que $c \in I \cap J$. Mas, como $a, b \in I \cap J$, então $a, b \in I$. Logo, como I é intervalo, $c \in I$. Analogamente, $c \in J$. Ou seja, $c \in I \cap J$. □

Aula 2 - Qualquer intersecção funciona

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja um exercício nas notas de aula).

Aula 2 - Qualquer intersecção funciona

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja um exercício nas notas de aula).

Mais um fato estranho: tanto o vazio, como os conjuntos unitários são intervalos.

Aula 2 - Qualquer intersecção funciona

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja um exercício nas notas de aula).

Mais um fato estranho: tanto o vazio, como os conjuntos unitários são intervalos. Talvez o mais fácil seja pensar qual seria o motivo para eles não serem (teria que existir a, b, c etc.).

Aula 2 - Qualquer intersecção funciona

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja um exercício nas notas de aula).

Mais um fato estranho: tanto o vazio, como os conjuntos unitários são intervalos. Talvez o mais fácil seja pensar qual seria o motivo para eles não serem (teria que existir a, b, c etc.). Outro motivo é ver o que acabamos de provar e notar que:

Aula 2 - Qualquer intersecção funciona

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja um exercício nas notas de aula).

Mais um fato estranho: tanto o vazio, como os conjuntos unitários são intervalos. Talvez o mais fácil seja pensar qual seria o motivo para eles não serem (teria que existir a, b, c etc.). Outro motivo é ver o que acabamos de provar e notar que:

- $\emptyset = [1, 2] \cap [3, 4]$;

Aula 2 - Qualquer intersecção funciona

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja um exercício nas notas de aula).

Mais um fato estranho: tanto o vazio, como os conjuntos unitários são intervalos. Talvez o mais fácil seja pensar qual seria o motivo para eles não serem (teria que existir a, b, c etc.). Outro motivo é ver o que acabamos de provar e notar que:

- $\emptyset = [1, 2] \cap [3, 4]$;
- $\{1\} = [0, 1] \cap [1, 2]$.

Aula 3 - Indução

Aula 3 - Indução

Uma maneira de se provar coisas que valem para todos os naturais é o processo conhecido como **indução**.

Aula 3 - Indução

Uma maneira de se provar coisas que valem para todos os naturais é o processo conhecido como **indução**. Basicamente, uma demonstração por indução funciona da seguinte forma:

Uma maneira de se provar coisas que valem para todos os naturais é o processo conhecido como **indução**. Basicamente, uma demonstração por indução funciona da seguinte forma:

- Provamos que certa propriedade vale para 0.

Aula 3 - Indução

Uma maneira de se provar coisas que valem para todos os naturais é o processo conhecido como **indução**. Basicamente, uma demonstração por indução funciona da seguinte forma:

- Provamos que certa propriedade vale para 0.
- Provamos que se a tal propriedade vale para algum $n \in \mathbb{N}$, ela precisa valer para $n + 1$.

Aula 3 - Indução

Uma maneira de se provar coisas que valem para todos os naturais é o processo conhecido como **indução**. Basicamente, uma demonstração por indução funciona da seguinte forma:

- Provamos que certa propriedade vale para 0.
- Provamos que se a tal propriedade vale para algum $n \in \mathbb{N}$, ela precisa valer para $n + 1$.

Com essas duas verificações, provamos que ela vale para todos os naturais.

Aula 3 - Porque isso vale?

Aula 3 - Porque isso vale?

Pense nisso como uma sequência de peças de dominó, de forma que a primeira peça cai e que, se uma peça cair, a seguinte cai também.

Aula 3 - Porque isso vale?

Pense nisso como uma sequência de peças de dominó, de forma que a primeira peça cai e que, se uma peça cair, a seguinte cai também. No final, teremos que todas as peças caem.

Aula 3 - Porque isso vale?

Pense nisso como uma sequência de peças de dominó, de forma que a primeira peça cai e que, se uma peça cair, a seguinte cai também. No final, teremos que todas as peças caem.

Um jeito formal para ver que isso vale de fato, é o uso do seguinte fato sobre os naturais:

Aula 3 - Porque isso vale?

Pense nisso como uma sequência de peças de dominó, de forma que a primeira peça cai e que, se uma peça cair, a seguinte cai também. No final, teremos que todas as peças caem.

Um jeito formal para ver que isso vale de fato, é o uso do seguinte fato sobre os naturais:

Todo subconjunto não vazio de $\mathbb{N}$ admite mínimo.

Aula 3 - Usando o fato para provar

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio. Assim, pelo fato, tal conjunto admite mínimo.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio. Assim, pelo fato, tal conjunto admite mínimo. Seja m tal mínimo.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio. Assim, pelo fato, tal conjunto admite mínimo. Seja m tal mínimo. Note que $m \neq 0$, já que temos que vale $P(0)$.

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio. Assim, pelo fato, tal conjunto admite mínimo. Seja m tal mínimo. Note que $m \neq 0$, já que temos que vale $P(0)$. Então $m-1 \in \mathbb{N}$ (pois $m > 0$).

Aula 3 - Usando o fato para provar

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio. Assim, pelo fato, tal conjunto admite mínimo. Seja m tal mínimo. Note que $m \neq 0$, já que temos que vale $P(0)$. Então $m-1 \in \mathbb{N}$ (pois $m > 0$). Note que $m-1$ não pertence ao conjunto, já que é menor que o mínimo.

Aula 3 - Continuando

Assim, pela definição do conjunto, vale $P(m-1)$.

Assim, pela definição do conjunto, vale $P(m-1)$. Mas, se vale $P(m-1)$, vale para $P((m-1)+1)$.

Assim, pela definição do conjunto, vale $P(m-1)$. Mas, se vale $P(m-1)$, vale para $P((m-1)+1)$. Mas $(m-1)+1 = m$.

Assim, pela definição do conjunto, vale $P(m-1)$. Mas, se vale $P(m-1)$, vale para $P((m-1)+1)$. Mas $(m-1)+1=m$. Ou seja, vale $P(m)$, contradição.

Aula 3 - Um exemplo

Aula 3 - Um exemplo

Vamos ver como isso funciona na prática:

Aula 3 - Um exemplo

Vamos ver como isso funciona na prática:

Proposição

Para todo $n \in \mathbb{N}$, *vale* $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$

Aula 3 - Um exemplo

Vamos ver como isso funciona na prática:

Proposição

Para todo $n \in \mathbb{N}$, *vale* $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$

Demonstração. Precisamos verificar a igualdade para o caso $n = 0$.

Aula 3 - Um exemplo

Vamos ver como isso funciona na prática:

Proposição

Para todo $n \in \mathbb{N}$, *vale* $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$

Demonstração. Precisamos verificar a igualdade para o caso $n = 0$. Nela, só temos que calcular ambos os lados.

Aula 3 - Um exemplo

Vamos ver como isso funciona na prática:

Proposição

Para todo $n \in \mathbb{N}$, *vale* $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$

Demonstração. Precisamos verificar a igualdade para o caso $n = 0$. Nela, só temos que calcular ambos os lados. Mas, de fato, temos $2^0 = 1 = 2^{0+1} - 1$.

Aula 3 - Provando

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n + 1$.

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Vamos começar pelo lado esquerdo e chegar no direito:

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Vamos começar pelo lado esquerdo e chegar no direito:

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} \quad = \quad (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1}$$

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Vamos começar pelo lado esquerdo e chegar no direito:

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^n + 2^{n+1} &= (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} \\ &\overset{HI}{=} (2^{n+1} - 1) + 2^{n+1} \end{aligned}$$

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Vamos começar pelo lado esquerdo e chegar no direito:

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^n + 2^{n+1} &= (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} \\ &\overset{HI}{=} (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \end{aligned}$$

Aula 3 - Provando

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Vamos começar pelo lado esquerdo e chegar no direito:

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^n + 2^{n+1} &= (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} \\ &\overset{HI}{=} (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{n+2} - 1 \end{aligned}$$

□

Aula 3 - Mais um exemplo

Aula 3 - Mais um exemplo

Vejamos uma fórmula para somar os primeiros números ímpares.

Aula 3 - Mais um exemplo

Vejamos uma fórmula para somar os primeiros números ímpares.

Proposição
Dado $N \in \mathbb{N}$, *temos* $\sum_{k=0}^{N}(2k+1) = (N+1)^2$.

Aula 3 - Mais um exemplo

Vejamos uma fórmula para somar os primeiros números ímpares.

Proposição
Dado $N \in \mathbb{N}$, temos $\sum_{k=0}^{N}(2k+1) = (N+1)^2$.

Demonstração.

Para o caso $N = 0$, temos que a fórmula vale (basta verificar ambos os lados).

Aula 3 - Provando

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N + 1$.

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

e temos que provar que

$$\sum_{k=0}^{N+1}(2k+1) = (N+2)^2.$$

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

e temos que provar que

$$\sum_{k=0}^{N+1}(2k+1) = (N+2)^2.$$

Temos

$$\sum_{k=0}^{N+1}(2k+1) \quad = \quad (\sum_{k=0}^{N} 2k+1) + 2(N+1) + 1$$

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

e temos que provar que

$$\sum_{k=0}^{N+1}(2k+1) = (N+2)^2.$$

Temos

$$\begin{array}{rcl} \sum_{k=0}^{N+1}(2k+1) & = & (\sum_{k=0}^{N} 2k+1) + 2(N+1)+1 \\ & \stackrel{HI}{=} & (N+1)^2 + 2N + 3 \end{array}$$

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

e temos que provar que

$$\sum_{k=0}^{N+1}(2k+1) = (N+2)^2.$$

Temos

$$\begin{array}{rcl} \sum_{k=0}^{N+1}(2k+1) & = & (\sum_{k=0}^{N} 2k+1) + 2(N+1)+1 \\ & \stackrel{HI}{=} & (N+1)^2 + 2N + 3 \\ & = & N^2 + 2N + 1 + 2N + 3 \end{array}$$

Aula 3 - Provando

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

e temos que provar que

$$\sum_{k=0}^{N+1}(2k+1) = (N+2)^2.$$

Temos

$$\begin{aligned}
\textstyle\sum_{k=0}^{N+1}(2k+1) &= (\textstyle\sum_{k=0}^{N} 2k+1) + 2(N+1)+1 \\
&\overset{HI}{=} (N+1)^2 + 2N + 3 \\
&= N^2 + 2N + 1 + 2N + 3 \\
&= (N+2)^2
\end{aligned}$$

□

Aula 3 - Generalizando

Note que pelo argumento anterior, se a gente prova que vale para $n = 3$ e depois que se vale para n, então vale para $n + 1$, conseguimos garantir que a propriedade vale para qualquer $k \geq 3$ (e não para todo $\mathbb{N}$).

Note que pelo argumento anterior, se a gente prova que vale para $n = 3$ e depois que se vale para n, então vale para $n + 1$, conseguimos garantir que a propriedade vale para qualquer $k \geq 3$ (e não para todo $\mathbb{N}$). Obviamente, o análogo vale para qualquer k_0 que seja o primeiro que a gente prova que vale.

Aula 3 - Exemplo

Aula 3 - Exemplo

Isso é útil em alguns casos, como por exemplo:

Aula 3 - Exemplo

Isso é útil em alguns casos, como por exemplo:

Proposição
Se $n \geq 5$, *então* $4n < 2^n$.

Aula 3 - Exemplo

Isso é útil em alguns casos, como por exemplo:

Proposição
Se $n \geq 5$, *então* $4n < 2^n$.

Demonstração.
Vamos provar o primeiro caso, que aqui é quando $n = 5$.

Aula 3 - Exemplo

Isso é útil em alguns casos, como por exemplo:

Proposição
Se $n \geq 5$, *então* $4n < 2^n$.

Demonstração.
Vamos provar o primeiro caso, que aqui é quando $n = 5$. De fato, temos que $4n = 20 < 32 = 2^5$.

Aula 3 - Exemplo

Isso é útil em alguns casos, como por exemplo:

Proposição
Se $n \geq 5$, *então* $4n < 2^n$.

Demonstração.
Vamos provar o primeiro caso, que aqui é quando $n = 5$. De fato, temos que $4n = 20 < 32 = 2^5$.

Agora suponha que vale para n e vamos provar para $n + 1$.

Aula 3 - Exemplo

Isso é útil em alguns casos, como por exemplo:

Proposição
Se $n \geq 5$, *então* $4n < 2^n$.

Demonstração.
Vamos provar o primeiro caso, que aqui é quando $n = 5$. De fato, temos que $4n = 20 < 32 = 2^5$.

Agora suponha que vale para n e vamos provar para $n + 1$. Temos

$$4(n+1) = 4n + 4 \overset{HI}{<} 2^n + 2^2 \overset{2<n}{<} 2^n + 2^n = 2^{n+1}.$$

□

Aula 3 - Misturando um pouco

Aula 3 - Misturando um pouco

Nem sempre as afirmações envolvem só naturais:

Aula 3 - Misturando um pouco

Nem sempre as afirmações envolvem só naturais:

Proposição

Se X tem n elementos, $\wp(X)$ tem 2^n elementos.

Nem sempre as afirmações envolvem só naturais:

Proposição

Se X tem n elementos, $\wp(X)$ tem 2^n elementos.

Demonstração. De fato, se $n = 0$, temos que $X = \emptyset$ e $\wp(X) = \{\emptyset\}$ que tem um elemento.

Aula 3 - Provando

Aula 3 - Provando

Agora suponha que vale para n e vamos provar para $n+1$.

Aula 3 - Provando

Agora suponha que vale para n e vamos provar para $n+1$.

Então $X = \{x_1, ..., x_{n+1}\}$.

Aula 3 - Provando

Agora suponha que vale para n e vamos provar para $n+1$.

Então $X = \{x_1, ..., x_{n+1}\}$. Note que

$$\wp(X) = \{A \subset X : x_{n+1} \notin A\} \cup \{A \subset X : x_{n+1} \in A\}.$$

Aula 3 - Provando

Agora suponha que vale para n e vamos provar para $n+1$.

Então $X = \{x_1, ..., x_{n+1}\}$. Note que

$$\wp(X) = \{A \subset X : x_{n+1} \notin A\} \cup \{A \subset X : x_{n+1} \in A\}.$$

Note que os dois conjuntos acima são disjuntos e que eles têm a mesma quantidade de elementos (voce consegue fazer uma bijeção entre eles?).

Aula 3 - Provando

Agora suponha que vale para n e vamos provar para $n+1$.

Então $X = \{x_1, ..., x_{n+1}\}$. Note que

$$\wp(X) = \{A \subset X : x_{n+1} \notin A\} \cup \{A \subset X : x_{n+1} \in A\}.$$

Note que os dois conjuntos acima são disjuntos e que eles têm a mesma quantidade de elementos (voce consegue fazer uma bijeção entre eles?).

Note também que $\{A \subset X : x_{n+1} \notin A\} = \wp(Y)$, onde $Y = \{x_1, ..., x_n\}$.

Aula 3 - Provando

Agora suponha que vale para n e vamos provar para $n+1$.

Então $X = \{x_1, ..., x_{n+1}\}$. Note que

$$\wp(X) = \{A \subset X : x_{n+1} \notin A\} \cup \{A \subset X : x_{n+1} \in A\}.$$

Note que os dois conjuntos acima são disjuntos e que eles têm a mesma quantidade de elementos (voce consegue fazer uma bijeção entre eles?).

Note também que $\{A \subset X : x_{n+1} \notin A\} = \wp(Y)$, onde $Y = \{x_1, ..., x_n\}$. Ou seja, por hipótese de indução, tal conjunto tem 2^n elementos.

Agora suponha que vale para n e vamos provar para $n+1$.

Então $X = \{x_1, ..., x_{n+1}\}$. Note que

$$\wp(X) = \{A \subset X : x_{n+1} \notin A\} \cup \{A \subset X : x_{n+1} \in A\}.$$

Note que os dois conjuntos acima são disjuntos e que eles têm a mesma quantidade de elementos (voce consegue fazer uma bijeção entre eles?).

Note também que $\{A \subset X : x_{n+1} \notin A\} = \wp(Y)$, onde $Y = \{x_1, ..., x_n\}$. Ou seja, por hipótese de indução, tal conjunto tem 2^n elementos. Assim, $\wp(X)$ tem $2^n + 2^n = 2^{n+1}$ elementos. □

Aula 3 - Apertos de mão

Aula 3 - Apertos de mão

Numa festa, havia $2n$ pessoas e algumas se cumprimentaram com apertos de mão.

Aula 3 - Apertos de mão

Numa festa, havia $2n$ pessoas e algumas se cumprimentaram com apertos de mão. Sabe-se que a cada 3 pessoas, alguma delas não cumprimentou alguma das outras (ou seja, não tem 3 que se cumprimentaram mutuamente).

Aula 3 - Apertos de mão

Numa festa, havia $2n$ pessoas e algumas se cumprimentaram com apertos de mão. Sabe-se que a cada 3 pessoas, alguma delas não cumprimentou alguma das outras (ou seja, não tem 3 que se cumprimentaram mutuamente). Podemos concluir que houve no máximo n^2 cumprimentos.

Aula 3 - Apertos de mão

Numa festa, havia $2n$ pessoas e algumas se cumprimentaram com apertos de mão. Sabe-se que a cada 3 pessoas, alguma delas não cumprimentou alguma das outras (ou seja, não tem 3 que se cumprimentaram mutuamente). Podemos concluir que houve no máximo n^2 cumprimentos.

Vamo fazer isso por indução. Se $n = 1$, o resultado é claro (tem no máximo 1 cumprimento).

Aula 3 - Dando as mãos

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Aula 3 - Dando as mãos

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Note que temos $2n+2$ pessoas.

Aula 3 - Dando as mãos

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Note que temos $2n+2$ pessoas. Dessas, separe duas que se cumprimentaram (podemos supor que elas existem, caso contrário o resultado vale). Vamos chamá-las de A e B.

Aula 3 - Dando as mãos

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Note que temos $2n+2$ pessoas. Dessas, separe duas que se cumprimentaram (podemos supor que elas existem, caso contrário o resultado vale). Vamos chamá-las de A e B.

Por (HI), existe no máximo n^2 apertos de mão entre as outras pessoas.

Aula 3 - Dando as mãos

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Note que temos $2n+2$ pessoas. Dessas, separe duas que se cumprimentaram (podemos supor que elas existem, caso contrário o resultado vale). Vamos chamá-las de A e B.

Por (HI), existe no máximo n^2 apertos de mão entre as outras pessoas. E, pela hipótese do problema, nenhuma das outras pessoas cumprimentou tanto A como B.

Aula 3 - Dando as mãos

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Note que temos $2n+2$ pessoas. Dessas, separe duas que se cumprimentaram (podemos supor que elas existem, caso contrário o resultado vale). Vamos chamá-las de A e B.

Por (HI), existe no máximo n^2 apertos de mão entre as outras pessoas. E, pela hipótese do problema, nenhuma das outras pessoas cumprimentou tanto A como B. Ou seja, existem no máximo $2n$ cumprimentos envolvendo alguma das outras pessoas com A ou B.

Agora suponha que vale o resultado para n e vamos provar para $n+1$.

Note que temos $2n+2$ pessoas. Dessas, separe duas que se cumprimentaram (podemos supor que elas existem, caso contrário o resultado vale). Vamos chamá-las de A e B.

Por (HI), existe no máximo n^2 apertos de mão entre as outras pessoas. E, pela hipótese do problema, nenhuma das outras pessoas cumprimentou tanto A como B. Ou seja, existem no máximo $2n$ cumprimentos envolvendo alguma das outras pessoas com A ou B. Assim, a quantidade de apertos de mão é limitada por

$$n^2 + 2n + 1 = (n+1)^2$$

como queríamos.

Aula 4 - Palavras

Aula 4 - Palavras

Fixe um conjunto A que vamos chamar de **alfabeto**.

Aula 4 - Palavras

Fixe um conjunto A que vamos chamar de **alfabeto**. Uma **palavra** de n letras neste alfabeto nada mais é do que uma sequência de n elementos de A.

Aula 4 - Palavras

Fixe um conjunto A que vamos chamar de **alfabeto**. Uma **palavra** de n letras neste alfabeto nada mais é do que uma sequência de n elementos de A. Por exemplo, se $A = \{1, 2, 3, 4\}$, temos que 113 e 345 são duas palavras de 3 letras de A.

Aula 4 - Palavras

Fixe um conjunto A que vamos chamar de **alfabeto**. Uma **palavra** de n letras neste alfabeto nada mais é do que uma sequência de n elementos de A. Por exemplo, se $A = \{1, 2, 3, 4\}$, temos que 113 e 345 são duas palavras de 3 letras de A. Note também que a ordem *importa*: $212 \neq 122$.

Aula 4 - Palavras

Aula 4 - Palavras

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Aula 4 - Palavras

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples.

Aula 4 - Palavras

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples. Por exemplo, se $|A| = k$, existem $k \cdots k = k^n$ palavras de n letras.

Aula 4 - Palavras

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples. Por exemplo, se $|A| = k$, existem $k \cdots k = k^n$ palavras de n letras.

Mas muitas vezes não queremos *qualquer* palavra possível feita com o alfabeto.

Aula 4 - Palavras

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples. Por exemplo, se $|A| = k$, existem $k \cdots k = k^n$ palavras de n letras.

Mas muitas vezes não queremos *qualquer* palavra possível feita com o alfabeto. Uma restrição bastante popular é exigir que as letras sejam todas distintas.

Aula 4 - Palavras

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples. Por exemplo, se $|A| = k$, existem $k \cdots k = k^n$ palavras de n letras.

Mas muitas vezes não queremos *qualquer* palavra possível feita com o alfabeto. Uma restrição bastante popular é exigir que as letras sejam todas distintas. Ou seja, neste caso, temos que uma palavra $p = a_1 \cdots a_n$ é tal que cada $a_i \in A$ como antes mas, além disso, $a_i \neq a_j$ se $i \neq j$.

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples. Por exemplo, se $|A| = k$, existem $k \cdots k = k^n$ palavras de n letras.

Mas muitas vezes não queremos *qualquer* palavra possível feita com o alfabeto. Uma restrição bastante popular é exigir que as letras sejam todas distintas. Ou seja, neste caso, temos que uma palavra $p = a_1 \cdots a_n$ é tal que cada $a_i \in A$ como antes mas, além disso, $a_i \neq a_j$ se $i \neq j$. Desta forma, voltando ao nosso exemplo inicial, temos que 123 é uma palavra válida, enquanto que 141 não é.

Aula 4 - Um exemplo

Vejamos uma situação mais concreta.

Aula 4 - Um exemplo

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas.

Aula 4 - Um exemplo

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas. De quantas maneiras podemos fazer isso?

Aula 4 - Um exemplo

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas. De quantas maneiras podemos fazer isso? Vamos usar a ideia de alfabeto e de palavras para nos ajudar.

Aula 4 - Um exemplo

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas. De quantas maneiras podemos fazer isso? Vamos usar a ideia de alfabeto e de palavras para nos ajudar. Podemos fixar como alfabeto o conjunto dos livros $\{A, B, C, D, E\}$ e associar a cada distribuição uma palavra com letras distintas (e vice e versa) da seguinte maneira: a primeira letra indica o livro da primeira criança.

Aula 4 - Um exemplo

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas. De quantas maneiras podemos fazer isso? Vamos usar a ideia de alfabeto e de palavras para nos ajudar. Podemos fixar como alfabeto o conjunto dos livros $\{A, B, C, D, E\}$ e associar a cada distribuição uma palavra com letras distintas (e vice e versa) da seguinte maneira: a primeira letra indica o livro da primeira criança. A segunda, o da segunda e a terceira o da terceira.

Aula 4 - Um exemplo

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas. De quantas maneiras podemos fazer isso? Vamos usar a ideia de alfabeto e de palavras para nos ajudar. Podemos fixar como alfabeto o conjunto dos livros $\{A, B, C, D, E\}$ e associar a cada distribuição uma palavra com letras distintas (e vice e versa) da seguinte maneira: a primeira letra indica o livro da primeira criança. A segunda, o da segunda e a terceira o da terceira. Ou seja, desta forma, basta contarmos apenas quantas palavras de 3 letras *sem repetição* são possíveis.

Aula 4 - Exibindo todas

Aula 4 - Exibindo todas

Podemos tentar exibir todas:

ABC ABD ABE ACB ACE ADE BAC BAD...

Aula 4 - Exibindo todas

Podemos tentar exibir todas:

ABC ABD ABE ACB ACE ADE BAC BAD...

Mas note que já deu uma quantidade razoável.

Aula 4 - Permutações

O exemplo anterior indica que pode ser interessante sabermos contar quantas palavras de k letras sem repetição são possíveis de ser feitas com um alfabeto de n letras.

O exemplo anterior indica que pode ser interessante sabermos contar quantas palavras de k letras sem repetição são possíveis de ser feitas com um alfabeto de n letras. Vamos denotar tal quantidade por $P(n, k)$.

O exemplo anterior indica que pode ser interessante sabermos contar quantas palavras de k letras sem repetição são possíveis de ser feitas com um alfabeto de n letras. Vamos denotar tal quantidade por $P(n, k)$. Lê-se permutações de n k a k.

O exemplo anterior indica que pode ser interessante sabermos contar quantas palavras de k letras sem repetição são possíveis de ser feitas com um alfabeto de n letras. Vamos denotar tal quantidade por $P(n, k)$. Lê-se permutações de n k a k. Alguns lugares chamam isso de k-permutações.

O exemplo anterior indica que pode ser interessante sabermos contar quantas palavras de k letras sem repetição são possíveis de ser feitas com um alfabeto de n letras. Vamos denotar tal quantidade por $P(n, k)$. Lê-se permutações de n k a k. Alguns lugares chamam isso de k-permutações. Outros ainda dizem que é permutação só se $k = n$ - os outros casos são chamados de arranjos.

Aula 4 - A fórmula

Aula 4 - A fórmula

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$. Ou seja, estamos supondo que vale $P(n,q) = \frac{n!}{(n-q)!}$ e queremos mostrar que vale $P(n,q+1) = \frac{n!}{(n-q-1)!}$.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$. Ou seja, estamos supondo que vale $P(n,q) = \frac{n!}{(n-q)!}$ e queremos mostrar que vale $P(n,q+1) = \frac{n!}{(n-q-1)!}$. Sabemos que com q letras, temos $P(n,q)$ palavras.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$. Ou seja, estamos supondo que vale $P(n,q) = \frac{n!}{(n-q)!}$ e queremos mostrar que vale $P(n,q+1) = \frac{n!}{(n-q-1)!}$. Sabemos que com q letras, temos $P(n,q)$ palavras. Podemos pensar que uma palavra de $q+1$ letras é simplesmente uma palavra de q letras seguida de mais uma letra no final.

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$. Ou seja, estamos supondo que vale $P(n,q) = \frac{n!}{(n-q)!}$ e queremos mostrar que vale $P(n,q+1) = \frac{n!}{(n-q-1)!}$. Sabemos que com q letras, temos $P(n,q)$ palavras. Podemos pensar que uma palavra de $q+1$ letras é simplesmente uma palavra de q letras seguida de mais uma letra no final. Para cada início de q letras, temos mais quantas possibilidades para o final?

Proposição
Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$. Ou seja, estamos supondo que vale $P(n,q) = \frac{n!}{(n-q)!}$ e queremos mostrar que vale $P(n,q+1) = \frac{n!}{(n-q-1)!}$. Sabemos que com q letras, temos $P(n,q)$ palavras. Podemos pensar que uma palavra de $q+1$ letras é simplesmente uma palavra de q letras seguida de mais uma letra no final. Para cada início de q letras, temos mais quantas possibilidades para o final? Já "gastamos" q letras, então ainda nos sobram $n-q$ possibilidades para esta última.

Aula 4 - Finalizando

Ou seja:

$$P(n, q+1) \quad = \quad P(n, q)(n-q)$$

Ou seja:

$$\begin{aligned} P(n, q+1) &= P(n, q)(n-q) \\ &\overset{HI}{=} \frac{n!}{(n-q)!}(n-q) \end{aligned}$$

Aula 4 - Finalizando

Ou seja:

$$\begin{aligned} P(n, q+1) &= P(n, q)(n-q) \\ &\overset{HI}{=} \frac{n!}{(n-q)!}(n-q) \\ &= \frac{n!}{(n-q)(n-q-1)!}(n-q) \end{aligned}$$

Aula 4 - Finalizando

Ou seja:

$$\begin{aligned} P(n, q+1) &= P(n, q)(n-q) \\ &\overset{HI}{=} \frac{n!}{(n-q)!}(n-q) \\ &= \frac{n!}{(n-q)(n-q-1)!}(n-q) \\ &= \frac{n!}{(n-q-1)!} \end{aligned}$$

Ou seja:

$$\begin{aligned} P(n, q+1) &= P(n, q)(n-q) \\ &\overset{HI}{=} \frac{n!}{(n-q)!}(n-q) \\ &= \frac{n!}{(n-q)(n-q-1)!}(n-q) \\ &= \frac{n!}{(n-q-1)!} \end{aligned}$$

□

Aula 4 - Uma convenção

Se $k > n$, é conveniente definir $P(n, k) = 0$ (note que isso fica coerente com a contagem de palavras).

Aula 4 - Finalizando o exemplo dos livros

Aula 4 - Finalizando o exemplo dos livros

No nosso exemplo dos livros, temos que existem $P(5,3) = 60$ formas diferentes de distribuir os livros.

Aula 4 - Mais um exemplo

Aula 4 - Mais um exemplo

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Aula 4 - Mais um exemplo

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Vamos ter que supor vários fatos aqui: todo mundo só faz aniversário num dos 365 dias do ano (ou seja, sem 29 de fevereiro) e que todos os dias são equiprováveis.

Aula 4 - Mais um exemplo

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Vamos ter que supor vários fatos aqui: todo mundo só faz aniversário num dos 365 dias do ano (ou seja, sem 29 de fevereiro) e que todos os dias são equiprováveis.

Se são 50 pessoas, há 365^{50} possibilidades de aniversários.

Aula 4 - Mais um exemplo

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Vamos ter que supor vários fatos aqui: todo mundo só faz aniversário num dos 365 dias do ano (ou seja, sem 29 de fevereiro) e que todos os dias são equiprováveis.

Se são 50 pessoas, há 365^{50} possibilidades de aniversários. Mas, estamos interessados em saber se há duas pessoas que fazem aniversário no mesmo dia.

Aula 4 - Mais um exemplo

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Vamos ter que supor vários fatos aqui: todo mundo só faz aniversário num dos 365 dias do ano (ou seja, sem 29 de fevereiro) e que todos os dias são equiprováveis.

Se são 50 pessoas, há 365^{50} possibilidades de aniversários. Mas, estamos interessados em saber se há duas pessoas que fazem aniversário no mesmo dia. Ou seja, podemos contar quantas palavras de comprimento 50 existem, formadas com os dias do ano como alfabeto sem repetição: as que repetem são justamente os casos que não estamos interessados.

Aula 4 - Mais um exemplo

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Vamos ter que supor vários fatos aqui: todo mundo só faz aniversário num dos 365 dias do ano (ou seja, sem 29 de fevereiro) e que todos os dias são equiprováveis.

Se são 50 pessoas, há 365^{50} possibilidades de aniversários. Mas, estamos interessados em saber se há duas pessoas que fazem aniversário no mesmo dia. Ou seja, podemos contar quantas palavras de comprimento 50 existem, formadas com os dias do ano como alfabeto sem repetição: as que repetem são justamente os casos que não estamos interessados. Assim

$$P = 1 - \frac{P(365, 50)}{365^{50}}$$

esse resultado é aproximadamente $0,97$.

Aula 4 - Combinações

Aula 4 - Combinações

Imagine que temos que montar um grupo de 4 pessoas para uma comissão de forma que uma seja a presidente, um seja a vice, uma seja a tesoureira e o última seja a estagiária.

Aula 4 - Combinações

Imagine que temos que montar um grupo de 4 pessoas para uma comissão de forma que uma seja a presidente, um seja a vice, uma seja a tesoureira e o última seja a estagiária. Se temos 50 pessoas para dividir nestes 4 cargos, de quantas maneiras podemos fazer isso?

Imagine que temos que montar um grupo de 4 pessoas para uma comissão de forma que uma seja a presidente, um seja a vice, uma seja a tesoureira e o última seja a estagiária. Se temos 50 pessoas para dividir nestes 4 cargos, de quantas maneiras podemos fazer isso?

Já sabemos que isso pode ser feito através de
$P(50,4) = \frac{50!}{46!} = 50 \cdot 49 \cdot 48 \cdot 47 = 5527200$.

Aula 4 - Combinações

Mas e se quisermos simplesmente montar uma chapa com 4 pessoas, depois elas que decidam quem faz o quê?

Mas e se quisermos simplesmente montar uma chapa com 4 pessoas, depois elas que decidam quem faz o quê? Podemos pensar nisso como sendo uma palavra de 4 letras (cada letra uma pessoa diferente) mas que não importa qual a posição de cada letra (por exemplo, a palavra $ABCD = DBCA$).

Mas e se quisermos simplesmente montar uma chapa com 4 pessoas, depois elas que decidam quem faz o quê? Podemos pensar nisso como sendo uma palavra de 4 letras (cada letra uma pessoa diferente) mas que não importa qual a posição de cada letra (por exemplo, a palavra $ABCD = DBCA$). Vamos denotar tal quantidade da seguinte maneira: $\binom{n}{k}$.

Aula 4 - A fórmula

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente.

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas.

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas. Quantas palavras de comprimento k podemos escrever com elas?

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas. Quantas palavras de comprimento k podemos escrever com elas? $k!$.

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas. Quantas palavras de comprimento k podemos escrever com elas? $k!$. Assim, para cada conjunto de k letras, temos $k!$ palavras distintas.

Aula 4 - A fórmula

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas. Quantas palavras de comprimento k podemos escrever com elas? $k!$. Assim, para cada conjunto de k letras, temos $k!$ palavras distintas. Note que se tomamos dois conjuntos diferentes de k letras cada, formamos palavras distintas - e variando sobre todos os conjuntos de k letras, obtemos todas as palavras.

Proposição

Sejam $n \geq k \geq 0$. *Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração.
Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas. Quantas palavras de comprimento k podemos escrever com elas? $k!$. Assim, para cada conjunto de k letras, temos $k!$ palavras distintas. Note que se tomamos dois conjuntos diferentes de k letras cada, formamos palavras distintas - e variando sobre todos os conjuntos de k letras, obtemos todas as palavras. Assim

$$k! \left(\begin{array}{c} n \\ k \end{array} \right) = P(n, k)$$

e portanto temos o resultado desejado. □

Aula 4 - Finalizando a comissão

Aula 4 - Finalizando a comissão

Assim, para a mesma escolha da comissão, agora não importando como as pessoas se organizam, temos $\binom{50}{4} = \frac{50!}{46!4!} = 230300$.

Aula 4 - Simetria

Pela simetria da fórmula, pode-se notar que $\binom{n}{k} = \binom{n}{n-k}$.

Pela simetria da fórmula, pode-se notar que $\binom{n}{k} = \binom{n}{n-k}$.

Mas também podemos notar essa igualdade de outra forma: o primeiro conta como escolher k, dentre n, o segundo, conta como escolher $n - k$, dentre n.

Pela simetria da fórmula, pode-se notar que $\binom{n}{k} = \binom{n}{n-k}$.

Mas também podemos notar essa igualdade de outra forma: o primeiro conta como escolher k, dentre n, o segundo, conta como escolher $n-k$, dentre n. Claramente, quando se escolhe k, se escolhe $n-k$ (os não escolhidos).

Pela simetria da fórmula, pode-se notar que $\binom{n}{k} = \binom{n}{n-k}$.

Mas também podemos notar essa igualdade de outra forma: o primeiro conta como escolher k, dentre n, o segundo, conta como escolher $n-k$, dentre n. Claramente, quando se escolhe k, se escolhe $n-k$ (os não escolhidos). Logo, essas duas quantidades deveriam ser mesmo iguais.

Aula 4 - Subconjuntos

Proposição

Considere o conjunto $A = \{a_1, ..., a_n\}$. *Então existem* $\binom{n}{k}$ *subconjuntos* A *com* k *elementos.*

Proposição

Considere o conjunto $A = \{a_1, ..., a_n\}$. *Então existem* $\binom{n}{k}$ *subconjuntos* A *com* k *elementos.*

Demonstração.
Basta notar que é o mesmo que montar palavras de comprimento k, sem repetição e não importando a ordem. □

Proposição

Considere o conjunto $A = \{a_1, ..., a_n\}$. *Então existem* $\binom{n}{k}$ *subconjuntos* A *com* k *elementos.*

Demonstração.
Basta notar que é o mesmo que montar palavras de comprimento k, sem repetição e não importando a ordem. □

Proposição

Seja $n \geq 1$. *Então* $\sum_{i=1}^{n} \binom{n}{k} = 2^n - 1$.

Proposição

Considere o conjunto $A = \{a_1, ..., a_n\}$. *Então existem* $\binom{n}{k}$ *subconjuntos* A *com* k *elementos.*

Demonstração.
Basta notar que é o mesmo que montar palavras de comprimento k, sem repetição e não importando a ordem. □

Proposição

Seja $n \geq 1$. *Então* $\sum_{i=1}^{n} \binom{n}{k} = 2^n - 1$.

Demonstração.
É só ver que o lado esquerdo contou quantos subconjuntos de um conjunto de n elementos existem, com exceção do vazio. □

Proposição

Considere o conjunto $A = \{a_1, ..., a_n\}$. *Então existem* $\binom{n}{k}$ *subconjuntos* A *com* k *elementos.*

Demonstração.
Basta notar que é o mesmo que montar palavras de comprimento k, sem repetição e não importando a ordem. □

Proposição

Seja $n \geq 1$. *Então* $\sum_{i=1}^{n} \binom{n}{k} = 2^n - 1$.

Demonstração.
É só ver que o lado esquerdo contou quantos subconjuntos de um conjunto de n elementos existem, com exceção do vazio. □

Já vimos isso antes, não?

Aula 4 - Um exemplo

Aula 4 - Um exemplo

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60.

Aula 4 - Um exemplo

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e quem acertar os 6 vence.

Aula 4 - Um exemplo

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e quem acertar os 6 vence.

Vejamos qual a chance de alguém vencer.

Aula 4 - Um exemplo

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e quem acertar os 6 vence.

Vejamos qual a chance de alguém vencer. Quem jogar vai escolher uma palavra de comprimento 6 com todos os símbolos distintos e precisa que essa seja a palavra sorteada.

Aula 4 - Um exemplo

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e quem acertar os 6 vence.

Vejamos qual a chance de alguém vencer. Quem jogar vai escolher uma palavra de comprimento 6 com todos os símbolos distintos e precisa que essa seja a palavra sorteada. Então a chance de acertar é uma entre todas as palavras de comprimento 6, sem repetição e sem importar a ordem.

Aula 4 - Um exemplo

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e quem acertar os 6 vence.

Vejamos qual a chance de alguém vencer. Quem jogar vai escolher uma palavra de comprimento 6 com todos os símbolos distintos e precisa que essa seja a palavra sorteada. Então a chance de acertar é uma entre todas as palavras de comprimento 6, sem repetição e sem importar a ordem. Ou seja, 1 em

$$\binom{60}{6} = \frac{60!}{54!6!} = 50.063.860$$

Aula 4 - Bilhetes múltiplos

Aula 4 - Bilhetes múltiplos

Pode-se fazer uma aposta com 10 números (e se vence se os 6 sorteados estiverem entre eles).

Aula 4 - Bilhetes múltiplos

Pode-se fazer uma aposta com 10 números (e se vence se os 6 sorteados estiverem entre eles). Isso equivale a quantos bilhetes "simples"?

Aula 4 - Bilhetes múltiplos

Pode-se fazer uma aposta com 10 números (e se vence se os 6 sorteados estiverem entre eles). Isso equivale a quantos bilhetes "simples"?

Para isso basta contarmos quantos bilhetes simples estão nesta jogada: cada grupo de 6 é uma.

Aula 4 - Bilhetes múltiplos

Pode-se fazer uma aposta com 10 números (e se vence se os 6 sorteados estiverem entre eles). Isso equivale a quantos bilhetes "simples"?

Para isso basta contarmos quantos bilhetes simples estão nesta jogada: cada grupo de 6 é uma. Ou seja, na verdade se está fazendo a seguinte quantidade de jogadas simples:

$$\binom{10}{6} = \frac{10!}{6!4!} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2} = 210$$

Aula 4 - Bilhetes múltiplos

Pode-se fazer uma aposta com 10 números (e se vence se os 6 sorteados estiverem entre eles). Isso equivale a quantos bilhetes "simples"?

Para isso basta contarmos quantos bilhetes simples estão nesta jogada: cada grupo de 6 é uma. Ou seja, na verdade se está fazendo a seguinte quantidade de jogadas simples:

$$\left(\begin{array}{c} 10 \\ 6 \end{array} \right) = \frac{10!}{6!4!} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2} = 210$$

Se o valor de uma aposta simples for $R\$4,50$, então isso equivaleria a apostar $R\$945$.

Aula 4 - Ganhando menos

Mas também se ganha (menos) se acertar 5 números.

Aula 4 - Ganhando menos

Mas também se ganha (menos) se acertar 5 números. Qual a chance de se ganhar tal prêmio? (e não ganhar o prêmio total dos 6)

Aula 4 - Ganhando menos

Mas também se ganha (menos) se acertar 5 números. Qual a chance de se ganhar tal prêmio? (e não ganhar o prêmio total dos 6)

Suponha que alguém escolheu 6 números.

Aula 4 - Ganhando menos

Mas também se ganha (menos) se acertar 5 números. Qual a chance de se ganhar tal prêmio? (e não ganhar o prêmio total dos 6)

Suponha que alguém escolheu 6 números. Vejamos quantos sorteios possíveis existem de forma que exatamente 5 destes números apareçam.

Aula 4 - Ganhando menos

Mas também se ganha (menos) se acertar 5 números. Qual a chance de se ganhar tal prêmio? (e não ganhar o prêmio total dos 6)

Suponha que alguém escolheu 6 números. Vejamos quantos sorteios possíveis existem de forma que exatamente 5 destes números apareçam. Para cada grupo de 5 números jogados, existem $60 - 6 = 54$ possíveis sorteios nessas condições (montamos o sorteio com 5 dos números jogados mais um dos não escolhidos).

Aula 4 - Ganhando menos

Aula 4 - Ganhando menos

Assim, a quantidade de sorteios possíveis é

$$\begin{pmatrix} 6 \\ 5 \end{pmatrix} 54$$

Aula 4 - Ganhando menos

Assim, a quantidade de sorteios possíveis é

$$\binom{6}{5}54$$

Ou seja, comparando isso com todos os sorteios possíveis, obtemos que a chance de se vencer é 1 em:

$$\frac{\binom{60}{6}}{\binom{6}{5}54}$$

que é aproximadamente 154.518.

Aula 4 - Ganhando menos ainda

Aula 4 - Ganhando menos ainda

Analogamente, se quisermos acertar apenas 4, obtemos uma em

$$\frac{\binom{60}{6}}{\binom{6}{4}\binom{54}{2}}$$

que é aproximadamente 2.332

Aula 4 - Ganhando menos ainda

Analogamente, se quisermos acertar apenas 4, obtemos uma em

$$\frac{\binom{60}{6}}{\binom{6}{4}\binom{54}{2}}$$

que é aproximadamente 2.332 (para justificar o denominador: para cada jogo de 4 entre 6, devemos "completar" o sorteio com 2 números entre os restantes).

Aula 4 - Ganhando menos ainda

Aula 4 - Ganhando menos ainda

Finalmente, jogando-se 10 números, qual a chance de se acertar exatamente 4?

Aula 4 - Ganhando menos ainda

Finalmente, jogando-se 10 números, qual a chance de se acertar exatamente 4?

Novamente, podemos fazer

$$\frac{\binom{60}{6}}{\binom{10}{4}\binom{50}{2}}$$

que dá aproximadamente 1 em 195.

Aula 4 - Mas ganha mais coisas

Aula 4 - Mas ganha mais coisas

Se são jogados 10 números e se acerta 5, ganha-se diversos prêmios de bilhetes de 5 números.

Aula 4 - Mas ganha mais coisas

Se são jogados 10 números e se acerta 5, ganha-se diversos prêmios de bilhetes de 5 números. Basicamente, para cada bilhete simples (6 números) possível entre os 10 jogados que contenha os 5 sorteados, ganha-se o correspondente valor.

Aula 4 - Mas ganha mais coisas

Se são jogados 10 números e se acerta 5, ganha-se diversos prêmios de bilhetes de 5 números. Basicamente, para cada bilhete simples (6 números) possível entre os 10 jogados que contenha os 5 sorteados, ganha-se o correspondente valor.

Como são 5 números fixados, para completar o bilhete, falta só um, escolhido entre os cinco não sorteados.

Aula 4 - Mas ganha mais coisas

Se são jogados 10 números e se acerta 5, ganha-se diversos prêmios de bilhetes de 5 números. Basicamente, para cada bilhete simples (6 números) possível entre os 10 jogados que contenha os 5 sorteados, ganha-se o correspondente valor.

Como são 5 números fixados, para completar o bilhete, falta só um, escolhido entre os cinco não sorteados. Ou seja, são 5 prêmios desse tipo.

Aula 4 - Mas ganha mais coisas

Mas há prêmios para acertos de 4 números.

Aula 4 - Mas ganha mais coisas

Mas há prêmios para acertos de 4 números. Então, na mesma jogada que se jogam 10 números e se acertam 5, precisamos ver quantos bilhetes simples são possíveis de serem feitos com 4 sorteados e 2 não, dentre os 10.

Aula 4 - Mas ganha mais coisas

Mas há prêmios para acertos de 4 números. Então, na mesma jogada que se jogam 10 números e se acertam 5, precisamos ver quantos bilhetes simples são possíveis de serem feitos com 4 sorteados e 2 não, dentre os 10.

Começamos escolhendo 4 entre os 5 sorteados e, para cada grupo desses, há $\begin{pmatrix} 5 \\ 2 \end{pmatrix}$ formas de se completar o bilhete, pegando 2 dentre os não sorteados.

Aula 4 - Mas ganha mais coisas

Mas há prêmios para acertos de 4 números. Então, na mesma jogada que se jogam 10 números e se acertam 5, precisamos ver quantos bilhetes simples são possíveis de serem feitos com 4 sorteados e 2 não, dentre os 10.

Começamos escolhendo 4 entre os 5 sorteados e, para cada grupo desses, há $\begin{pmatrix} 5 \\ 2 \end{pmatrix}$ formas de se completar o bilhete, pegando 2 dentre os não sorteados. Ou seja, temos

$$\begin{pmatrix} 5 \\ 4 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \end{pmatrix} = 50$$

prêmios desse tipo.

Aula 4 - Veja também

Aqui você pode encontrar diversos resultados sobre esse jogo (de forma oficial).

Aula 4 - Veja também

Aqui você pode encontrar diversos resultados sobre esse jogo (de forma oficial). Você consegue calcular todas as formas?

`https://loterias.caixa.gov.br/Paginas/Mega-Sena.aspx`

Aula 4 - Veja também

Aqui você tem uma história interessante sobre um jogo de loteria

https://www.bbc.com/portuguese/geral-62133938

Aula 5 - Princípio da inclusão-exclusão

Aula 5 - Princípio da inclusão-exclusão

Considere um grupo X de indivíduos e suponha que tenhamos propriedades $P_1, ..., P_n$.

Aula 5 - Princípio da inclusão-exclusão

Considere um grupo X de indivíduos e suponha que tenhamos propriedades $P_1, ..., P_n$. Dado $S \subset \{P_1, ..., P_n\}$, denote por $N(S)$ a quantidade de indivíduos que satisfazem todas as P_i's em S.

Aula 5 - Princípio da inclusão-exclusão

Considere um grupo X de indivíduos e suponha que tenhamos propriedades $P_1, ..., P_n$. Dado $S \subset \{P_1, ..., P_n\}$, denote por $N(S)$ a quantidade de indivíduos que satisfazem todas as P_i's em S. Note que $N(\emptyset) = |X|$.

Aula 5 - Um exemplo

Aula 5 - Um exemplo

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Aula 5 - Um exemplo

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Num total de 63 alunos, temos que 47 fazem matemática pura, 51 são homens, 45 homens fazem matemática pura.

Aula 5 - Um exemplo

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Num total de 63 alunos, temos que 47 fazem matemática pura, 51 são homens, 45 homens fazem matemática pura. Quantas mulheres não fazem matemática pura?

Aula 5 - Um exemplo

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Num total de 63 alunos, temos que 47 fazem matemática pura, 51 são homens, 45 homens fazem matemática pura. Quantas mulheres não fazem matemática pura?

Neste caso, temos $|X| = 63$.

Aula 5 - Um exemplo

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Num total de 63 alunos, temos que 47 fazem matemática pura, 51 são homens, 45 homens fazem matemática pura. Quantas mulheres não fazem matemática pura?

Neste caso, temos $|X| = 63$. Vamos chamar de P_1 ser homem, P_2 fazer matemática pura.

Aula 5 - Um exemplo

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Num total de 63 alunos, temos que 47 fazem matemática pura, 51 são homens, 45 homens fazem matemática pura. Quantas mulheres não fazem matemática pura?

Neste caso, temos $|X| = 63$. Vamos chamar de P_1 ser homem, P_2 fazer matemática pura. Desta maneira, podemos notar que a quantidade de mulheres que não fazem matemática pura é dada por

Aula 5 - Mulheres que não fazem matemática pura

Aula 5 - Mulheres que não fazem matemática pura

- Adicionamos todos os indivíduos ($N(\emptyset)$);

Aula 5 - Mulheres que não fazem matemática pura

- Adicionamos todos os indivíduos ($N(\emptyset)$);
- Tiramos os homens ($N(P_1)$);

Aula 5 - Mulheres que não fazem matemática pura

- Adicionamos todos os indivíduos ($N(\emptyset)$);
- Tiramos os homens ($N(P_1)$);
- Tiramos quem faz matemática pura ($N(P_2)$);

Aula 5 - Mulheres que não fazem matemática pura

- Adicionamos todos os indivíduos ($N(\emptyset)$);
- Tiramos os homens ($N(P_1)$);
- Tiramos quem faz matemática pura ($N(P_2)$);
- Note que nas subtrações acima, tiramos cada "homem que faz matemática pura" duas vezes, então precisamos acrescentar eles uma vez ($N(P_1, P_2)$).

Aula 5 - Mulheres que não fazem matemática pura

- Adicionamos todos os indivíduos ($N(\emptyset)$);
- Tiramos os homens ($N(P_1)$);
- Tiramos quem faz matemática pura ($N(P_2)$);
- Note que nas subtrações acima, tiramos cada "homem que faz matemática pura" duas vezes, então precisamos acrescentar eles uma vez ($N(P_1, P_2)$).

$$N(\emptyset) - N(P_1) - N(P_2) + N(P_1, P_2)$$

Aula 5 - Mulheres que não fazem matemática pura

- Adicionamos todos os indivíduos ($N(\emptyset)$);
- Tiramos os homens ($N(P_1)$);
- Tiramos quem faz matemática pura ($N(P_2)$);
- Note que nas subtrações acima, tiramos cada "homem que faz matemática pura" duas vezes, então precisamos acrescentar eles uma vez ($N(P_1, P_2)$).

$$N(\emptyset) - N(P_1) - N(P_2) + N(P_1, P_2)$$

Ou seja, $63 - 51 - 47 + 45 = 10$.

Aula 5 - O teorema

Aula 5 - O teorema

Teorema (Princípio da inclusão exclusão)
A quantidade de indivíduos que não satisfazem nenhuma $P_1, ..., P_n$ *é dada por*

$$\sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S).$$

Teorema (Princípio da inclusão exclusão)
A quantidade de indivíduos que não satisfazem nenhuma $P_1, ..., P_n$ *é dada por*

$$\sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S).$$

Assim, a quantidade de elementos que satisfaz alguma das propriedades é dada por

$$N(\emptyset) - \sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S)$$

Teorema (Princípio da inclusão exclusão)
A quantidade de indivíduos que não satisfazem nenhuma $P_1, ..., P_n$ é dada por

$$\sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S).$$

Assim, a quantidade de elementos que satisfaz alguma das propriedades é dada por

$$N(\emptyset) - \sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S)$$

que, por sua vez, pode ser reduzida para

$$\sum_{S \subset \{1,...,n\}, S \neq \emptyset} (-1)^{|S|+1} N(S).$$

Aula 5 - Exemplo de múltiplos

Aula 5 - Exemplo de múltiplos

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Aula 5 - Exemplo de múltiplos

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Chame de P_i ser múltiplo de i.

Aula 5 - Exemplo de múltiplos

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Chame de P_i ser múltiplo de i. Assim, temos $N(P_2) = 50$, $N(P_3) = 33$, $N(P_5) = 20$.

Aula 5 - Exemplo de múltiplos

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Chame de P_i ser múltiplo de i. Assim, temos $N(P_2) = 50$, $N(P_3) = 33$, $N(P_5) = 20$. Também temos que $N(P_2, P_3) = N(P_6) = 16$, $N(P_2, P_5) = N(P_{10}) = 10$ e $N(P_3, P_5) = N(P_{15}) = 6$.

Aula 5 - Exemplo de múltiplos

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Chame de P_i ser múltiplo de i. Assim, temos $N(P_2) = 50$, $N(P_3) = 33$, $N(P_5) = 20$. Também temos que $N(P_2, P_3) = N(P_6) = 16$, $N(P_2, P_5) = N(P_{10}) = 10$ e $N(P_3, P_5) = N(P_{15}) = 6$. Finalmente, $N(P_2, P_3, P_5) = N(P_{30}) = 3$.

Aula 5 - Exemplo de múltiplos

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Chame de P_i ser múltiplo de i. Assim, temos $N(P_2) = 50$, $N(P_3) = 33$, $N(P_5) = 20$. Também temos que $N(P_2, P_3) = N(P_6) = 16$, $N(P_2, P_5) = N(P_{10}) = 10$ e $N(P_3, P_5) = N(P_{15}) = 6$. Finalmente, $N(P_2, P_3, P_5) = N(P_{30}) = 3$.

Assim, a quantidade desejada é

$$50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$$

Aula 5 - Exemplo de almoço

Aula 5 - Exemplo de almoço

Uma pessoa almoçou 34 vezes durante certo período.

Aula 5 - Exemplo de almoço

Uma pessoa almoçou 34 vezes durante certo período. Sabemos que essa pessoa tem 4 amigos e que, nestes almoços, ela almoçou com cada amigo 20 vezes, com cada dupla de amigos 11 vezes, com cada trio de amigos 5 vezes e com todos os 4 amigos uma única vez.

Aula 5 - Exemplo de almoço

Uma pessoa almoçou 34 vezes durante certo período. Sabemos que essa pessoa tem 4 amigos e que, nestes almoços, ela almoçou com cada amigo 20 vezes, com cada dupla de amigos 11 vezes, com cada trio de amigos 5 vezes e com todos os 4 amigos uma única vez. Alguma vez a pessoa almoçou sozinha?

Aula 5 - Continuando

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d.

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x.

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x. Note que pelo enunciado, $N(\emptyset) = 34$, $N(P_a) = N(P_b) = N(P_c) = N(P_d) = 20$.

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x. Note que pelo enunciado, $N(\emptyset) = 34$, $N(P_a) = N(P_b) = N(P_c) = N(P_d) = 20$. Note também que $N(P_a, P_b) = N(P_a, P_c) = ... = 11$,
$N(P_a, P_b, P_c) = N(P_a, P_b, P_d) = ... = 5$ e $N(P_a, P_b, P_c, P_d) = 1$.

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x. Note que pelo enunciado, $N(\emptyset) = 34$, $N(P_a) = N(P_b) = N(P_c) = N(P_d) = 20$. Note também que $N(P_a, P_b) = N(P_a, P_c) = ... = 11$,
$N(P_a, P_b, P_c) = N(P_a, P_b, P_d) = ... = 5$ e $N(P_a, P_b, P_c, P_d) = 1$.
Assim

$$\sum_{S \subset \{a,b,c,d\}} (-1)^{|S|} N(S) = 34 - \binom{4}{1} 20 + \binom{4}{2} 11 - \binom{4}{3} 5 + \binom{4}{4} 1$$

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x. Note que pelo enunciado, $N(\emptyset) = 34$, $N(P_a) = N(P_b) = N(P_c) = N(P_d) = 20$. Note também que $N(P_a, P_b) = N(P_a, P_c) = ... = 11$, $N(P_a, P_b, P_c) = N(P_a, P_b, P_d) = ... = 5$ e $N(P_a, P_b, P_c, P_d) = 1$. Assim

$$\begin{aligned} \sum_{S \subset \{a,b,c,d\}} (-1)^{|S|} N(S) &= 34 - \binom{4}{1} 20 + \binom{4}{2} 11 - \binom{4}{3} 5 + \binom{4}{4} 1 \\ &= 34 - 80 + 66 - 20 + 1 \end{aligned}$$

Aula 5 - Continuando

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x. Note que pelo enunciado, $N(\emptyset) = 34$, $N(P_a) = N(P_b) = N(P_c) = N(P_d) = 20$. Note também que $N(P_a, P_b) = N(P_a, P_c) = ... = 11$, $N(P_a, P_b, P_c) = N(P_a, P_b, P_d) = ... = 5$ e $N(P_a, P_b, P_c, P_d) = 1$. Assim

$$\begin{aligned}
\sum_{S \subset \{a,b,c,d\}} (-1)^{|S|} N(S) &= 34 - \binom{4}{1} 20 + \binom{4}{2} 11 - \binom{4}{3} 5 + \binom{4}{4} 1 \\
&= 34 - 80 + 66 - 20 + 1 \\
&= 1
\end{aligned}$$

Aula 5 - Sobrejeções

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete.

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete. De quantas maneira ele pode fazer isso?

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete. De quantas maneira ele pode fazer isso?

Se chamamos de X o conjunto dos bilhetes e de Y o conjunto dos netos, podemos definir $f(x) = y$ como sendo "bilhete x vai para o neto y" e, desta maneira, as distribuições que estamos interessados são as sobrejetoras.

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete. De quantas maneira ele pode fazer isso?

Se chamamos de X o conjunto dos bilhetes e de Y o conjunto dos netos, podemos definir $f(x) = y$ como sendo "bilhete x vai para o neto y" e, desta maneira, as distribuições que estamos interessados são as sobrejetoras. Agora basta contá-las.

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete. De quantas maneira ele pode fazer isso?

Se chamamos de X o conjunto dos bilhetes e de Y o conjunto dos netos, podemos definir $f(x) = y$ como sendo "bilhete x vai para o neto y" e, desta maneira, as distribuições que estamos interessados são as sobrejetoras. Agora basta contá-las.

Considere P_i apropriedade "i não pertence à imagem de f".

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete. De quantas maneira ele pode fazer isso?

Se chamamos de X o conjunto dos bilhetes e de Y o conjunto dos netos, podemos definir $f(x) = y$ como sendo "bilhete x vai para o neto y" e, desta maneira, as distribuições que estamos interessados são as sobrejetoras. Agora basta contá-las.

Considere P_i apropriedade "i não pertence à imagem de f". Assim, só precisamos contar quantas funções não satisfazem nenhuma das P_i's.

Aula 5 - Um resultado auxiliar

Aula 5 - Um resultado auxiliar

Lema
Sejam $n \geq m > 0$. Considere P_i como acima, trabalhando com domínio das f's como $\{1, ..., n\}$ e contradomínio $\{1, ..., m\}$. Seja $S \subset \{P_1, ..., P_m\}$. Então

$$N(S) = (m - |S|)^n.$$

Aula 5 - Um resultado auxiliar

Lema
Sejam $n \geq m > 0$. Considere P_i como acima, trabalhando com domínio das f's como $\{1, ..., n\}$ e contradomínio $\{1, ..., m\}$. Seja $S \subset \{P_1, ..., P_m\}$. Então

$$N(S) = (m - |S|)^n.$$

Demonstração.
Dada uma $f : \{1, ..., n\} \to \{1, ..., m\}$ satisfazendo toda $P_i \in S$, temos que ela é uma palavra de comprimento n num alfabeto com $m - |S|$ letras com repetição.

Aula 5 - Um resultado auxiliar

Lema
Sejam $n \geq m > 0$. Considere P_i como acima, trabalhando com domínio das f's como $\{1, ..., n\}$ e contradomínio $\{1, ..., m\}$. Seja $S \subset \{P_1, ..., P_m\}$. Então

$$N(S) = (m - |S|)^n.$$

Demonstração.
Dada uma $f : \{1, ..., n\} \to \{1, ..., m\}$ satisfazendo toda $P_i \in S$, temos que ela é uma palavra de comprimento n num alfabeto com $m - |S|$ letras com repetição. Assim, $N(S) = (m - |S|)^n$. □

Aula 5 - Quantidade de sobrejeções

Aula 5 - Quantidade de sobrejeções

Denote por $S(n, m)$ como sendo a quantidade de funções da forma $f : \{1, ..., n\} \to \{1, ..., m\}$ sobrejetoras.

Aula 5 - Quantidade de sobrejeções

Denote por $S(n, m)$ como sendo a quantidade de funções da forma $f : \{1, ..., n\} \to \{1, ..., m\}$ sobrejetoras. Temos

Teorema

$S(n, m) = \sum_{k=0}^{m} (-1)^k \begin{pmatrix} m \\ k \end{pmatrix} (m - k)^n.$

Aula 5 - Quantidade de sobrejeções

Denote por $S(n, m)$ como sendo a quantidade de funções da forma $f : \{1, ..., n\} \to \{1, ..., m\}$ sobrejetoras. Temos

Teorema

$$S(n, m) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m - k)^n.$$

Demonstração.
Temos

$$S(n, m) = \sum_{S \subset \{P_1, ..., P_m\}} (-1)^{|S|} N(S)$$

Aula 5 - Quantidade de sobrejeções

Denote por $S(n, m)$ como sendo a quantidade de funções da forma $f : \{1, ..., n\} \to \{1, ..., m\}$ sobrejetoras. Temos

Teorema

$$S(n, m) = \sum_{k=0}^{m} (-1)^k \begin{pmatrix} m \\ k \end{pmatrix} (m - k)^n.$$

Demonstração.
Temos

$$\begin{aligned} S(n, m) &= \sum_{S \subset \{P_1, ..., P_m\}} (-1)^{|S|} N(S) \\ &= \sum_{S \subset \{P_1, ..., P_m\}} (-1)^{|S|} (m - |S|)^n \end{aligned}$$

Aula 5 - Quantidade de sobrejeções

Denote por $S(n,m)$ como sendo a quantidade de funções da forma $f : \{1,...,n\} \to \{1,...,m\}$ sobrejetoras. Temos

Teorema

$$S(n,m) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n.$$

Demonstração.
Temos

$$\begin{aligned} S(n,m) &= \sum_{S \subset \{P_1,...,P_m\}} (-1)^{|S|} N(S) \\ &= \sum_{S \subset \{P_1,...,P_m\}} (-1)^{|S|} (m - |S|)^n \\ &= \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n \end{aligned}$$

□

Aula 5 - Voltando ao avô

Aula 5 - Voltando ao avô

De curiosidade, aplicando esta fórmula, temos que o problema do avô tem como resposta $S(15, 4) = 1.016.542.800$.

Aula 5 - Amigo secreto

Aula 5 - Amigo secreto

Vejamos agora o sorteio de um amigo secreto.

Aula 5 - Amigo secreto

Vejamos agora o sorteio de um amigo secreto. Esse sorteio nada mais é que uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora (ou bijetora, é equivalente neste caso) e tal que $f(x) \neq x$ (ninguém sorteia a si mesmo).

Aula 5 - Um resultado auxiliar

Aula 5 - Um resultado auxiliar

Considere P_i a propriedade de uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora ser tal que $f(i) = i$.

Aula 5 - Um resultado auxiliar

Considere P_i a propriedade de uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora ser tal que $f(i) = i$. Desta forma, temos:

Lema
Seja $S \subset \{P_1, ..., P_n\}$. *Temos que*

$$N(S) = (n - |S|)!$$

Aula 5 - Um resultado auxiliar

Considere P_i a propriedade de uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora ser tal que $f(i) = i$. Desta forma, temos:

Lema
Seja $S \subset \{P_1, ..., P_n\}$. *Temos que*

$$N(S) = (n - |S|)!$$

Demonstração.
Note que cada f nada mais é que uma palavra de comprimento n sem repetição e com essa restrição para a i-ésima casa.

Aula 5 - Um resultado auxiliar

Considere P_i a propriedade de uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora ser tal que $f(i) = i$. Desta forma, temos:

Lema
Seja $S \subset \{P_1, ..., P_n\}$. Temos que

$$N(S) = (n - |S|)!$$

Demonstração.
Note que cada f nada mais é que uma palavra de comprimento n sem repetição e com essa restrição para a i-ésima casa. Assim, fixadas as posições que aparecem em S, temos que restam $(n - |S|)!$ possibilidades. □

Aula 5 - Desarranjos

Aula 5 - Desarranjos

Uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo.

Aula 5 - Desarranjos

Uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo. Denotamos por d_n a quantidade de desarranjos.

Uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo. Denotamos por d_n a quantidade de desarranjos.

Teorema

$d_n = \sum_{k=0}^{n} (-1)^k \begin{pmatrix} n \\ k \end{pmatrix} (n-k)!$

Uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo. Denotamos por d_n a quantidade de desarranjos.

Teorema

$$d_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!$$

Demonstração.
De fato

$$d_n = \sum_{S \subset \{P_1, ..., P_n\}} (-1)^{|S|} N(S)$$

Uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo. Denotamos por d_n a quantidade de desarranjos.

Teorema

$$d_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!$$

Demonstração.
De fato

$$\begin{aligned} d_n &= \sum_{S \subset \{P_1, ..., P_n\}} (-1)^{|S|} N(S) \\ &= \sum_{S \subset \{P_1, ..., P_n\}} (-1)^{|S|} (n - |S|)! \end{aligned}$$

Uma função $f : \{1, ..., n\} \to \{1, ..., n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo. Denotamos por d_n a quantidade de desarranjos.

Teorema

$$d_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!$$

Demonstração.
De fato

$$\begin{aligned} d_n &= \sum_{S \subset \{P_1, ..., P_n\}} (-1)^{|S|} N(S) \\ &= \sum_{S \subset \{P_1, ..., P_n\}} (-1)^{|S|} (n - |S|)! \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \end{aligned}$$

□

Aula 5 - Voltando ao amigo secreto

Aula 5 - Voltando ao amigo secreto

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$.

Aula 5 - Voltando ao amigo secreto

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$. Temos:

Teorema
$\frac{d_n}{n!} = \sum_{k=0}^{n} (-1)^k \frac{1}{k!}$.

Aula 5 - Voltando ao amigo secreto

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$. Temos:

Teorema
$\frac{d_n}{n!} = \sum_{k=0}^{n} (-1)^k \frac{1}{k!}$. *Que, no limite quando* $n \to +\infty$, *temos que vale* $\frac{1}{e}$.

Aula 5 - Voltando ao amigo secreto

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$. Temos:

Teorema
$\frac{d_n}{n!} = \sum_{k=0}^{n}(-1)^k \frac{1}{k!}$. *Que, no limite quando* $n \to +\infty$, *temos que vale* $\frac{1}{e}$.

Demonstração.
Temos

$$\frac{d_n}{n!} = \frac{\sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)!}{n!}$$

Aula 5 - Voltando ao amigo secreto

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$. Temos:

Teorema
$\frac{d_n}{n!} = \sum_{k=0}^{n}(-1)^k \frac{1}{k!}$. *Que, no limite quando* $n \to +\infty$, *temos que vale* $\frac{1}{e}$.

Demonstração.
Temos

$$\begin{aligned} \frac{d_n}{n!} &= \frac{\sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)!}{n!} \\ &= \frac{\sum_{k=0}^{n}(-1)^k \frac{n!}{(n-k)!k!}(n-k)!}{n!} \end{aligned}$$

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$. Temos:

Teorema
$\frac{d_n}{n!} = \sum_{k=0}^{n}(-1)^k \frac{1}{k!}$. *Que, no limite quando* $n \to +\infty$, *temos que vale* $\frac{1}{e}$.

Demonstração.
Temos

$$\begin{aligned} \frac{d_n}{n!} &= \frac{\sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)!}{n!} \\ &= \frac{\sum_{k=0}^{n}(-1)^k \frac{n!}{(n-k)!k!}(n-k)!}{n!} \\ &= \sum_{k=0}^{n}(-1)^k \frac{1}{k!} \end{aligned}$$

□

Aula 6 - Listas Circulares

Exemplo
De quantas maneiras podemos acomodar 5 pessoas numa mesa de 5 lugares? (pensando que qualquer alteração de lugar é uma configuração diferente)

Exemplo
De quantas maneiras podemos acomodar 5 pessoas numa mesa de 5 lugares? (pensando que qualquer alteração de lugar é uma configuração diferente)

5!

Aula 6 - Mais um exemplo

Aula 6 - Mais um exemplo

Exemplo
De quantas maneiras podemos acomodar 5 pessoas numa mesa circular (de 5 cadeiras)? (Só importa a posição relativa entre elas).

Aula 6 - Mais um exemplo

Exemplo
De quantas maneiras podemos acomodar 5 pessoas numa mesa circular (de 5 cadeiras)? (Só importa a posição relativa entre elas).

Uma maneira de se pensar é a seguinte: fixe uma das pessoas.

Aula 6 - Mais um exemplo

Exemplo
De quantas maneiras podemos acomodar 5 pessoas numa mesa circular (de 5 cadeiras)? (Só importa a posição relativa entre elas).

Uma maneira de se pensar é a seguinte: fixe uma das pessoas. Distribua nos lugares restantes (no sentido horário). Assim, temos como resposta 4!.

Aula 6 - Aumentando a mesa

Aula 6 - Aumentando a mesa

Exemplo
Mesmo problema anterior, mas temos 8 pessoas e a mesa continua com 5 lugares.

Aula 6 - Aumentando a mesa

Exemplo
Mesmo problema anterior, mas temos 8 pessoas e a mesa continua com 5 lugares.

Escolhidas as 5 pessoas que vão se sentar, já temos quantas posições possíveis.

Aula 6 - Aumentando a mesa

Exemplo
Mesmo problema anterior, mas temos 8 pessoas e a mesa continua com 5 lugares.

Escolhidas as 5 pessoas que vão se sentar, já temos quantas posições possíveis. Assim, só falta ver quantos grupos de 5 vão se sentar:

Exemplo
Mesmo problema anterior, mas temos 8 pessoas e a mesa continua com 5 lugares.

Escolhidas as 5 pessoas que vão se sentar, já temos quantas posições possíveis. Assim, só falta ver quantos grupos de 5 vão se sentar:

$$\left(\begin{array}{c} 8 \\ 5 \end{array} \right) 4! = \frac{8!}{5!3!} 4! = 8 \cdot 7 \cdot 6 \cdot 4 = 1.344$$

Aula 6 - Alternando

Exemplo
Para sentar numa mesa circular com 10 lugares, temos 5 homens e 5 mulheres.

Exemplo
Para sentar numa mesa circular com 10 lugares, temos 5 homens e 5 mulheres. De quantas de quantas maneiras podemos acomodá-los (posições relativas) de forma que se alternem entre homens e mulheres?

Exemplo
Para sentar numa mesa circular com 10 lugares, temos 5 homens e 5 mulheres. De quantas de quantas maneiras podemos acomodá-los (posições relativas) de forma que se alternem entre homens e mulheres?

Fixamos, por exemplo, um homem. Daí para o seu lado temos 5 alternativas.

Exemplo
Para sentar numa mesa circular com 10 lugares, temos 5 homens e 5 mulheres. De quantas de quantas maneiras podemos acomodá-los (posições relativas) de forma que se alternem entre homens e mulheres?

Fixamos, por exemplo, um homem. Daí para o seu lado temos 5 alternativas. Depois, 4 para os outros homens, depois 4 para as outras mulheres etc.

Exemplo
Para sentar numa mesa circular com 10 lugares, temos 5 homens e 5 mulheres. De quantas de quantas maneiras podemos acomodá-los (posições relativas) de forma que se alternem entre homens e mulheres?

Fixamos, por exemplo, um homem. Daí para o seu lado temos 5 alternativas. Depois, 4 para os outros homens, depois 4 para as outras mulheres etc. Ou seja, temos

$$5 \cdot 4 \cdot 4 \cdot 3 \cdots 1 = 5!4!$$

Aula 6 - Repetições

Aula 6 - Repetições

Vamos ver agora algumas contagens onde alguns elementos se repetem.

Vamos ver agora algumas contagens onde alguns elementos se repetem.

Exemplo
Temos n bolinhas brancas e 1 bolinha preta para colocar em fila. De quantas maneiras podemos fazer isso?

Vamos ver agora algumas contagens onde alguns elementos se repetem.

Exemplo
Temos n bolinhas brancas e 1 bolinha preta para colocar em fila. De quantas maneiras podemos fazer isso?

Basta notar que temos $n+1$ lugares para a bolinha preta.

Aula 6 - Mais bolinhas

Aula 6 - Mais bolinhas

Exemplo
Temos n bolinhas brancas e 2 bolinhas pretas para colocar em fila.

Aula 6 - Mais bolinhas

Exemplo
Temos n bolinhas brancas e 2 bolinhas pretas para colocar em fila.

De quantas maneiras podemos fazer isso?

Exemplo
Temos n bolinhas brancas e 2 bolinhas pretas para colocar em fila.

De quantas maneiras podemos fazer isso?

Podemos pensar que a primeira bolinha preta tem $n+2$ posições possíveis, enquanto que a segunda tem $n+1$.

Exemplo
Temos n bolinhas brancas e 2 bolinhas pretas para colocar em fila. De quantas maneiras podemos fazer isso?

Podemos pensar que a primeira bolinha preta tem $n+2$ posições possíveis, enquanto que a segunda tem $n+1$. Mas note que não devemos contar como diferentes onde cada uma das bolinhas pretas parou.

Exemplo
Temos n bolinhas brancas e 2 bolinhas pretas para colocar em fila. De quantas maneiras podemos fazer isso?

Podemos pensar que a primeira bolinha preta tem $n+2$ posições possíveis, enquanto que a segunda tem $n+1$. Mas note que não devemos contar como diferentes onde cada uma das bolinhas pretas parou. Assim, temos:

$$\frac{(n+2)(n+1)}{2}$$

Aula 6 - Ainda mais bolinhas

Aula 6 - Ainda mais bolinhas

Exemplo
Temos n bolinhas brancas e k bolinhas pretas.

Aula 6 - Ainda mais bolinhas

Exemplo
Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Aula 6 - Ainda mais bolinhas

Exemplo
Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Agora começa a ficar um pouco mais complicado, então vamos apelar para alguma regra mais geral.

Aula 6 - Ainda mais bolinhas

Exemplo
Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Agora começa a ficar um pouco mais complicado, então vamos apelar para alguma regra mais geral. Podemos pensar que temos $n + k$ casas, uma para cada bolinha.

Aula 6 - Ainda mais bolinhas

Exemplo
Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Agora começa a ficar um pouco mais complicado, então vamos apelar para alguma regra mais geral. Podemos pensar que temos $n + k$ casas, uma para cada bolinha. Daí só precisamos selecionar k dessas casas para colocarmos bolinhas pretas.

Exemplo
Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Agora começa a ficar um pouco mais complicado, então vamos apelar para alguma regra mais geral. Podemos pensar que temos $n + k$ casas, uma para cada bolinha. Daí só precisamos selecionar k dessas casas para colocarmos bolinhas pretas. Mas isso é simplesmente contar quantos subconjuntos de tamanho k existem em $n + k$

Exemplo
Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Agora começa a ficar um pouco mais complicado, então vamos apelar para alguma regra mais geral. Podemos pensar que temos $n+k$ casas, uma para cada bolinha. Daí só precisamos selecionar k dessas casas para colocarmos bolinhas pretas. Mas isso é simplesmente contar quantos subconjuntos de tamanho k existem em $n+k$

$$\binom{n+k}{k} = \frac{(n+k)!}{n!k!}$$

Aula 6 - Voltando ao anterior

Exemplo
Se o último exemplo está certo, deveríamos poder aplicá-lo no segundo exemplo:

$$\binom{n+2}{2} = \frac{(n+2)!}{2!n!} = \frac{(n+2)(n+1)}{2}$$

Aula 6 - Misturando

Exemplo
Mesma situação anterior, mas agora com k bolinhas pretas e n bolinhas brancas, sendo que as brancas são numeradas de forma que elas fiquem distintas.

Exemplo
Mesma situação anterior, mas agora com k bolinhas pretas e n bolinhas brancas, sendo que as brancas são numeradas de forma que elas fiquem distintas.

Podemos simplesmente contar as distribuições das pretas e depois, para cada uma desta, temos as distribuições das brancas:

Exemplo
Mesma situação anterior, mas agora com k bolinhas pretas e n bolinhas brancas, sendo que as brancas são numeradas de forma que elas fiquem distintas.

Podemos simplesmente contar as distribuições das pretas e depois, para cada uma desta, temos as distribuições das brancas:

$$\begin{pmatrix} n+k \\ k \end{pmatrix} P(n,n)$$

Aula 6 - Estrelas e barras

Aula 6 - Estrelas e barras

Vamos apresentar uma nova técnica de contagem na demonstração do seguinte resultado:

Vamos apresentar uma nova técnica de contagem na demonstração do seguinte resultado:

Proposição
Sejam $k \leq n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$ com $a_i \in \mathbb{N}_{>0}$ é dada por $\binom{n-1}{k-1}$.

Aula 6 - Provando

Demonstração.
Desenhe n $*$'s.

Demonstração.
Desenhe n $*$'s. Coloque $k-1$ $|$'s, cada uma entre dois $*$.

Demonstração.
Desenhe n $*$'s. Coloque $k-1$ $|$'s, cada uma entre dois $*$. Por exemplo, com $n=6$ e $k=3$, uma possível maneira é

$$*|**|**$$

Demonstração.
Desenhe n $*$'s. Coloque $k-1$ $|$'s, cada uma entre dois $*$. Por exemplo, com $n=6$ e $k=3$, uma possível maneira é

$$*|***|**$$

Pense que a_1 indica a quantidade de $*$'s antes da primeira $|$, a_2 a quantidade entre a primeira e a segunda $|$ etc.

Demonstração.
Desenhe n $*$'s. Coloque $k-1$ $|$'s, cada uma entre dois $*$. Por exemplo, com $n=6$ e $k=3$, uma possível maneira é

$$*|***|**$$

Pense que a_1 indica a quantidade de $*$'s antes da primeira $|$, a_2 a quantidade entre a primeira e a segunda $|$ etc.

Note que a quantidade de locais possíveis para as $|$'s é $n-1$ e

precisamos escolher $k-1$ delas.

Demonstração.
Desenhe n $*$'s. Coloque $k-1$ $|$'s, cada uma entre dois $*$. Por exemplo, com $n=6$ e $k=3$, uma possível maneira é

$$*|***|**$$

Pense que a_1 indica a quantidade de $*$'s antes da primeira $|$, a_2 a quantidade entre a primeira e a segunda $|$ etc.

Note que a quantidade de locais possíveis para as $|$'s é $n-1$ e precisamos escolher $k-1$ delas. Ou seja, existem $\binom{n-1}{k-1}$ maneiras de se fazer isso. □

Aula 6 - Podendo zerar

Aula 6 - Podendo zerar

Proposição
Sejam $k, n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$, com $a_i \in \mathbb{N}$ é dada por

$$\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix} = \begin{pmatrix} n+k-1 \\ n \end{pmatrix}.$$

Aula 6 - Podendo zerar

Proposição
Sejam $k, n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$, com $a_i \in \mathbb{N}$ é dada por
$$\left(\begin{array}{c} n+k-1 \\ k-1 \end{array} \right) = \left(\begin{array}{c} n+k-1 \\ n \end{array} \right).$$

Demonstração.
Note que agora podemos colocar $|$ em qualquer lugar, incluindo no começo, no fim ou mesmo colocar duas consecutivas (sem $*$ entre elas).

Aula 6 - Podendo zerar

Proposição
Sejam $k, n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$, com $a_i \in \mathbb{N}$ é dada por
$$\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix} = \begin{pmatrix} n+k-1 \\ n \end{pmatrix}.$$

Demonstração.
Note que agora podemos colocar $|$ em qualquer lugar, incluindo no começo, no fim ou mesmo colocar duas consecutivas (sem $*$ entre elas). Mas no total, entre $*$'s e $|$'s, temos espaço para $n + k - 1$ símbolos.

Aula 6 - Podendo zerar

Proposição
Sejam $k, n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$, com $a_i \in \mathbb{N}$ é dada por
$$\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix} = \begin{pmatrix} n+k-1 \\ n \end{pmatrix}.$$

Demonstração.
Note que agora podemos colocar $|$ em qualquer lugar, incluindo no começo, no fim ou mesmo colocar duas consecutivas (sem $*$ entre elas). Mas no total, entre $*$'s e $|$'s, temos espaço para $n+k-1$ símbolos. Se quisermos ver onde colocar as $|$'s, temos simplesmente $\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix}$ lugares.

Proposição
Sejam $k, n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$, com $a_i \in \mathbb{N}$ é dada por
$$\left(\begin{array}{c} n+k-1 \\ k-1 \end{array} \right) = \left(\begin{array}{c} n+k-1 \\ n \end{array} \right).$$

Demonstração.
Note que agora podemos colocar $|$ em qualquer lugar, incluindo no começo, no fim ou mesmo colocar duas consecutivas (sem $*$ entre elas). Mas no total, entre $*$'s e $|$'s, temos espaço para $n+k-1$ símbolos. Se quisermos ver onde colocar as $|$'s, temos simplesmente $\left(\begin{array}{c} n+k-1 \\ k-1 \end{array} \right)$ lugares. Se quisermos simplesmente contar onde colocar $*$, temos $\left(\begin{array}{c} n+k-1 \\ n \end{array} \right)$. □

Aula 7 - Pinos e elásticos

Aula 7 - Pinos e elásticos

Considere $2n$ pinos numerados de 1 a $2n$, colocados em formato circular.

Aula 7 - Pinos e elásticos

Considere $2n$ pinos numerados de 1 a $2n$, colocados em formato circular. Tendo j elásticos idênticos ($j \leq n$), de quantas formas podemos prender os elásticos nos pinos, sendo que um elástico prende dois pinos consecutivos e não queremos colocar 2 elásticos num mesmo pino?

Aula 7 - Organizando

Podemos representar cada elástico preso com um $*$ e cada pino sem elástico como $|$.

Aula 7 - Organizando

Podemos representar cada elástico preso com um $*$ e cada pino sem elástico como $|$. Desta forma, temos j $*$'s e $2n - 2j$ $|$'s para dispor.

Aula 7 - Continuando

Ou seja, como fizemos antes, temos
$\begin{pmatrix} 2n-2j+j \\ j \end{pmatrix} = \begin{pmatrix} 2n-j \\ j \end{pmatrix}$ maneiras de fazer isso.

Ou seja, como fizemos antes, temos $\binom{2n-2j+j}{j} = \binom{2n-j}{j}$ maneiras de fazer isso. Mas note que isso só conta configurações que começam com um elástico ou com um pino solto.

Ou seja, como fizemos antes, temos $\begin{pmatrix} 2n-2j+j \\ j \end{pmatrix} = \begin{pmatrix} 2n-j \\ j \end{pmatrix}$ maneiras de fazer isso. Mas note que isso só conta configurações que começam com um elástico ou com um pino solto. Faltam as que há um elástico entre o último pino e o primeiro.

Ou seja, como fizemos antes, temos $\binom{2n-2j+j}{j} = \binom{2n-j}{j}$ maneiras de fazer isso. Mas note que isso só conta configurações que começam com um elástico ou com um pino solto. Faltam as que há um elástico entre o último pino e o primeiro. Para contar essas, temos $j-1$ $*$'s e as mesmas $2n-2j$ $|$'s.

Ou seja, como fizemos antes, temos $\begin{pmatrix} 2n-2j+j \\ j \end{pmatrix} = \begin{pmatrix} 2n-j \\ j \end{pmatrix}$ maneiras de fazer isso. Mas note que isso só conta configurações que começam com um elástico ou com um pino solto. Faltam as que há um elástico entre o último pino e o primeiro. Para contar essas, temos $j-1$ $*$'s e as mesmas $2n-2j$ $|$'s. Assim, temos mais $\begin{pmatrix} 2n-2j+j-1 \\ j-1 \end{pmatrix} = \begin{pmatrix} 2n-j-1 \\ j-1 \end{pmatrix}$ configurações.

Aula 7 - Fazendo as contas

Aula 7 - Fazendo as contas

Dá para simplificar essa fórmula:

$$\binom{2n-j}{j} + \binom{2n-j-1}{j-1} = \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!}{(j-1)!(2n-2j)!}$$

Aula 7 - Fazendo as contas

Dá para simplificar essa fórmula:

$$\begin{aligned}\binom{2n-j}{j} + \binom{2n-j-1}{j-1} &= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!}{(j-1)!(2n-2j)!} \\ &= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!j}{j!(2n-2j)!}\end{aligned}$$

Aula 7 - Fazendo as contas

Dá para simplificar essa fórmula:

$$\begin{aligned}
\binom{2n-j}{j} + \binom{2n-j-1}{j-1} &= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!}{(j-1)!(2n-2j)!} \\
&= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!j}{j!(2n-2j)!} \\
&= \frac{(2n-j)!+(2n-j-1)!j}{j!(2n-2j)!}
\end{aligned}$$

Aula 7 - Fazendo as contas

Dá para simplificar essa fórmula:

$$\begin{aligned}
\binom{2n-j}{j} + \binom{2n-j-1}{j-1} &= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!}{(j-1)!(2n-2j)!} \\
&= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!j}{j!(2n-2j)!} \\
&= \frac{(2n-j)!+(2n-j-1)!j}{j!(2n-2j)!} \\
&= \frac{1}{(2n-j)} \frac{(2n-j)(2n-j)!+(2n-j)!j}{j!(2n-2j)!}
\end{aligned}$$

Aula 7 - Fazendo as contas

Dá para simplificar essa fórmula:

$$
\begin{aligned}
\binom{2n-j}{j} + \binom{2n-j-1}{j-1} &= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!}{(j-1)!(2n-2j)!} \\
&= \frac{(2n-j)!}{j!(2n-2j)!} + \frac{(2n-j-1)!j}{j!(2n-2j)!} \\
&= \frac{(2n-j)!+(2n-j-1)!j}{j!(2n-2j)!} \\
&= \frac{1}{(2n-j)} \frac{(2n-j)(2n-j)!+(2n-j)!j}{j!(2n-2j)!} \\
&= \frac{2n}{2n-j} \binom{2n-j}{j}
\end{aligned}
$$

Aula 7 - Mãos de poker

Aula 7 - Mãos de poker

Vamos mostrar como calcular as chances de certas mãos saírem num jogo de poker.

Aula 7 - Mãos de poker

Vamos mostrar como calcular as chances de certas mãos saírem num jogo de poker. Um baralho consiste em 52 cartas, divididas em 4 naipes (♢, ♠, ♡, ♣), sendo que cada naipe tem 13 cartas listadas a seguir em ordem crescente:

2 3 4 5 6 7 8 9 10 J Q K A

Aula 7 - Mãos de poker

Vamos mostrar como calcular as chances de certas mãos saírem num jogo de poker. Um baralho consiste em 52 cartas, divididas em 4 naipes (♢, ♠, ♡, ♣), sendo que cada naipe tem 13 cartas listadas a seguir em ordem crescente:

2 3 4 5 6 7 8 9 10 J Q K A

Um sorteio no poker tipicamente é a escolha de 5 cartas, dentre as 52.

Aula 7 - Mãos de poker

Vamos mostrar como calcular as chances de certas mãos saírem num jogo de poker. Um baralho consiste em 52 cartas, divididas em 4 naipes ($\diamondsuit$, $\spadesuit$, $\heartsuit$, $\clubsuit$), sendo que cada naipe tem 13 cartas listadas a seguir em ordem crescente:

$$2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ J\ Q\ K\ A$$

Um sorteio no poker tipicamente é a escolha de 5 cartas, dentre as 52. Ou seja, temos $\binom{52}{5}$ possíveis sorteios (2.598.960).

Aula 7 - Mãos de poker

Vamos mostrar como calcular as chances de certas mãos saírem num jogo de poker. Um baralho consiste em 52 cartas, divididas em 4 naipes (♢, ♠, ♡, ♣), sendo que cada naipe tem 13 cartas listadas a seguir em ordem crescente:

2 3 4 5 6 7 8 9 10 J Q K A

Um sorteio no poker tipicamente é a escolha de 5 cartas, dentre as 52. Ou seja, temos $\binom{52}{5}$ possíveis sorteios (2.598.960). A seguir vamos calcular quantos sorteios são possíveis contendo cada um dos itens pontuáveis.

Aula 7 - Dupla

Aula 7 - Dupla

Uma dupla consiste de duas cartas de mesmo valor (e, portanto, naipes diferentes).

Aula 7 - Dupla

Uma dupla consiste de duas cartas de mesmo valor (e, portanto, naipes diferentes). Cuidado que aqui queremos que o sorteio tenha apenas uma dupla (e não duas, nem um trio etc).

Aula 7 - Dupla

Uma dupla consiste de duas cartas de mesmo valor (e, portanto, naipes diferentes). Cuidado que aqui queremos que o sorteio tenha apenas uma dupla (e não duas, nem um trio etc). Uma maneira de organizar o cálculo é a seguinte: contamos quantas são as duplas possíveis, vezes as distribuições dos naipes nesta dupla, como juntar mais 3 valores distintos ao sorteio (e diferentes da dupla) e, finalmente, como distribuir os naipes para os tais valores.

Aula 7 - Dupla

Uma dupla consiste de duas cartas de mesmo valor (e, portanto, naipes diferentes). Cuidado que aqui queremos que o sorteio tenha apenas uma dupla (e não duas, nem um trio etc). Uma maneira de organizar o cálculo é a seguinte: contamos quantas são as duplas possíveis, vezes as distribuições dos naipes nesta dupla, como juntar mais 3 valores distintos ao sorteio (e diferentes da dupla) e, finalmente, como distribuir os naipes para os tais valores. Desta forma, a expressão fica

$$\binom{13}{1}\binom{4}{2}\binom{12}{3}\binom{4}{1}^3$$

Aula 7 - Dupla

Uma dupla consiste de duas cartas de mesmo valor (e, portanto, naipes diferentes). Cuidado que aqui queremos que o sorteio tenha apenas uma dupla (e não duas, nem um trio etc). Uma maneira de organizar o cálculo é a seguinte: contamos quantas são as duplas possíveis, vezes as distribuições dos naipes nesta dupla, como juntar mais 3 valores distintos ao sorteio (e diferentes da dupla) e, finalmente, como distribuir os naipes para os tais valores. Desta forma, a expressão fica

$$\binom{13}{1}\binom{4}{2}\binom{12}{3}\binom{4}{1}^3$$

dando um total de 1.098.240 possibilidades.

Aula 7 - Duas duplas

Aula 7 - Duas duplas

Sorteio de duas duplas que não formem quatro cartas de mesmo valor (e que a última seja de valor distinto ao das duplas).

Aula 7 - Duas duplas

Sorteio de duas duplas que não formem quatro cartas de mesmo valor (e que a última seja de valor distinto ao das duplas).
Seguindo o raciocínio acima, temos:

$$\binom{13}{2}\binom{4}{2}^2\binom{11}{1}\binom{4}{1}$$

Aula 7 - Duas duplas

Sorteio de duas duplas que não formem quatro cartas de mesmo valor (e que a última seja de valor distinto ao das duplas). Seguindo o raciocínio acima, temos:

$$\binom{13}{2}\binom{4}{2}^2\binom{11}{1}\binom{4}{1}$$

dando um total de 123.552 possibilidades.

Aula 7 - Trio

Aula 7 - Trio

Sorteio de 3 cartas de mesmo valor, com as duas últimas com valores distintos (entre si e do trio).

Aula 7 - Trio

Sorteio de 3 cartas de mesmo valor, com as duas últimas com valores distintos (entre si e do trio).

$$\binom{13}{1}\binom{4}{3}\binom{12}{2}\binom{4}{1}^2$$

dando um total de 54.912 possibilidades.

Aula 7 - Quadra

Aula 7 - Quadra

Sorteio de 4 cartas de mesmo valor.

Aula 7 - Quadra

Sorteio de 4 cartas de mesmo valor.

$$\binom{13}{1}\binom{12}{1}\binom{4}{1}$$

dando um total de 624 possibilidades.

Aula 7 - Full house

Aula 7 - Full house

Sorteio de um trio e uma dupla.

Aula 7 - Full house

Sorteio de um trio e uma dupla.

$$\binom{13}{1}\binom{4}{3}\binom{12}{1}\binom{4}{2}$$

dando um total de 3.744 possibilidades.

Aula 7 - Straight

Aula 7 - Straight

Todas as 5 cartas do sorteio são consecutivas entre si, mas não do mesmo naipe.

Aula 7 - Straight

Todas as 5 cartas do sorteio são consecutivas entre si, mas não do mesmo naipe. Podemos escolher onde a sequência começa (cuidado que aqui a sequência pode ser $A2345$ ou $10JQKA$, mas não coisas do tipo $QKA23$), daí escolher qual o naipe de cada carta e descontar os casos em que todas são do mesmo naipe.

Aula 7 - Straight

Todas as 5 cartas do sorteio são consecutivas entre si, mas não do mesmo naipe. Podemos escolher onde a sequência começa (cuidado que aqui a sequência pode ser $A2345$ ou $10JQKA$, mas não coisas do tipo $QKA23$), daí escolher qual o naipe de cada carta e descontar os casos em que todas são do mesmo naipe.

$$\binom{10}{1}\binom{4}{1}^5 - \binom{10}{1}\binom{4}{1}$$

dando um total de 10.200 possibilidades.

Aula 7 - Flush

Aula 7 - Flush

Todas as 5 cartas do mesmo naipe, mas não em sequência.

Aula 7 - Flush

Todas as 5 cartas do mesmo naipe, mas não em sequência. Só precisamos fazer o sorteio dos valores e daí escolher um dos naipes, mas descontar as que estiverem em sequência.

Aula 7 - Flush

Todas as 5 cartas do mesmo naipe, mas não em sequência. Só precisamos fazer o sorteio dos valores e daí escolher um dos naipes, mas descontar as que estiverem em sequência.

$$(\binom{13}{5} - \binom{10}{1})\binom{4}{1}$$

dando um total de 5.108 possibilidades.

Aula 7 - Straight flush

Aula 7 - Straight flush

Todas as cartas consecutivas e do mesmo naipe. Mas exclui-se o caso em que termina em A.

Aula 7 - Straight flush

Todas as cartas consecutivas e do mesmo naipe. Mas exclui-se o caso em que termina em A.

$$\binom{9}{1}\binom{4}{1}$$

dando um total de 36 possibilidades.

Aula 7 - Royal straight flush

Aula 7 - Royal straight flush

Todas as cartas consecutivas, do mesmo naipe e terminando em A.

Aula 7 - Royal straight flush

Todas as cartas consecutivas, do mesmo naipe e terminando em A.

$$\binom{4}{1}$$

dando um total de 4 possibilidades.

Aula 8 - Rudimentos de lógica

Exemplo

- Todo homem é mortal;

Exemplo

- Todo homem é mortal;
- Sócrates é um homem;

Exemplo

- Todo homem é mortal;
- Sócrates é um homem;
- Logo, Sócrates é mortal.

Aula 8 - Mais um exemplo

Aula 8 - Mais um exemplo

Exemplo

- Nenhum cachorro voa;

Aula 8 - Mais um exemplo

Exemplo

- Nenhum cachorro voa;
- Snoopy é um cachorro;

Aula 8 - Mais um exemplo

Exemplo

- Nenhum cachorro voa;
- Snoopy é um cachorro;
- Logo, Snoopy não voa.

Aula 8 - Último

Aula 8 - Último

Exemplo

- Todo pássaro é amarelo;

Aula 8 - Último

Exemplo

- Todo pássaro é amarelo;
- Todo papagaio é um pássaro;

Aula 8 - Último

Exemplo

- Todo pássaro é amarelo;
- Todo papagaio é um pássaro;
- Todo papagaio é amarelo.

Aula 8 - Não exemplos

Aula 8 - Não exemplos

Exemplo

- Alguns cachorros são pretos;

Aula 8 - Não exemplos

Exemplo

- Alguns cachorros são pretos;
- Snoopy é um cachorro;

Aula 8 - Não exemplos

Exemplo

- Alguns cachorros são pretos;
- Snoopy é um cachorro;
- Logo, Snoopy é preto.

Aula 8 - Mais um

Exemplo

- Algumas flores são vermelhas;

Exemplo

- Algumas flores são vermelhas;
- Sócrates é um homem;

Exemplo

- Algumas flores são vermelhas;
- Sócrates é um homem;
- Logo, Snoopy é um cachorro.

Aula 8 - Imprecisão

Exemplo

- Quanto mais queijo suíço, mais buracos há nele;

Exemplo

- Quanto mais queijo suíço, mais buracos há nele;
- Quanto mais buracos houver num pedaço de queijo, menos queijo há em tal pedaço;

Exemplo

- Quanto mais queijo suíço, mais buracos há nele;
- Quanto mais buracos houver num pedaço de queijo, menos queijo há em tal pedaço;
- Logo, quanto mais queijo, menos queijo.

Aula 8 - Mais um

Aula 8 - Mais um

Exemplo

- Todo cavalo raro é caro;

Aula 8 - Mais um

Exemplo

- Todo cavalo raro é caro;
- Um cavalo barato é raro;

Aula 8 - Mais um

Exemplo

- Todo cavalo raro é caro;
- Um cavalo barato é raro;
- Logo, um cavalo barato é caro.

Aula 8 - Paradoxo

Aula 8 - Paradoxo

"Esta afirmação é falsa"

Aula 8 - Autorreferência

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita.

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português.

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso).

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta.

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito.

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito. Ou seja, o conjunto N claramente é finito e, portanto, diferente de $\mathbb{N}$ - o conjunto de todos os naturais.

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito. Ou seja, o conjunto N claramente é finito e, portanto, diferente de $\mathbb{N}$ - o conjunto de todos os naturais. Dessa forma, podemos tomar n como "o menor elemento que não está em N".

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito. Ou seja, o conjunto N claramente é finito e, portanto, diferente de $\mathbb{N}$ - o conjunto de todos os naturais. Dessa forma, podemos tomar n como "o menor elemento que não está em N". O que, traduzindo, pode ser escrito como "o menor elemento que não pode ser descrito com menos de 100 palavras".

Aula 8 - Autorreferência

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito. Ou seja, o conjunto N claramente é finito e, portanto, diferente de $\mathbb{N}$ - o conjunto de todos os naturais. Dessa forma, podemos tomar n como "o menor elemento que não está em N". O que, traduzindo, pode ser escrito como "o menor elemento que não pode ser descrito com menos de 100 palavras". Note que, desta forma, acabamos de descrever n com menos de 100 palavras e portanto ele está em N.

Aula 8 - Proposições

Aula 8 - Proposições

Vamos começar com o que vem a ser uma **proposição simples**. Intuitivamente, ela é uma afirmação qualquer que possui sentido por si só. O melhor é explicar por exemplos:

Aula 8 - Proposições

Vamos começar com o que vem a ser uma **proposição simples**. Intuitivamente, ela é uma afirmação qualquer que possui sentido por si só. O melhor é explicar por exemplos:

Exemplo
"Existe um cachorro branco" é uma proposição simples, assim como "$7 > 4$", "o Sol é uma estrela" ou mesmo "$5 > 10$".

Vamos começar com o que vem a ser uma **proposição simples**. Intuitivamente, ela é uma afirmação qualquer que possui sentido por si só. O melhor é explicar por exemplos:

Exemplo
"Existe um cachorro branco" é uma proposição simples, assim como "$7 > 4$", "o Sol é uma estrela" ou mesmo "$5 > 10$". Note que não pedimos que uma proposição seja verdadeira.

Vamos começar com o que vem a ser uma **proposição simples**. Intuitivamente, ela é uma afirmação qualquer que possui sentido por si só. O melhor é explicar por exemplos:

Exemplo
"Existe um cachorro branco" é uma proposição simples, assim como "$7 > 4$", "o Sol é uma estrela" ou mesmo "$5 > 10$". Note que não pedimos que uma proposição seja verdadeira.

Por outro lado, "camisa" não é uma proposição simples, já que ela não afirma nada sobre coisa alguma.

Aula 8 - Representando

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**.

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**.

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\neg$ (negação);

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\neg$ (negação);
- $\wedge$ (e);

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\neg$ (negação);
- $\wedge$ (e);
- $\vee$ (ou);

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\neg$ (negação);
- $\wedge$ (e);
- $\vee$ (ou);
- $\rightarrow$ (implicação);

Aula 8 - Representando

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\neg$ (negação);
- $\wedge$ (e);
- $\vee$ (ou);
- $\rightarrow$ (implicação);
- $\leftrightarrow$ (bi-implicação).

Aula 8 - Representando

Por exemplo, se p e q são proposições, então $p \vee q$ também é.

Por exemplo, se p e q são proposições, então $p \vee q$ também é.
Assim como $p \rightarrow q$ ou $\neg q$.

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades.

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\neg s)$.

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\neg s)$. Mas qual a interpretação que devemos dar a esses conectivos?

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\neg s)$. Mas qual a interpretação que devemos dar a esses conectivos? A negação serve para quando queremos o contrário de uma afirmação.

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\neg s)$. Mas qual a interpretação que devemos dar a esses conectivos? A negação serve para quando queremos o contrário de uma afirmação. Isto é, $\neg p$ é verdadeira se, e somente se, p é falsa. O conectivo $\wedge$ serve para indicar que ambas as proposições devem ser verdadeiras.

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\neg s)$. Mas qual a interpretação que devemos dar a esses conectivos? A negação serve para quando queremos o contrário de uma afirmação. Isto é, $\neg p$ é verdadeira se, e somente se, p é falsa. O conectivo $\wedge$ serve para indicar que ambas as proposições devem ser verdadeiras. Isto é, $p \wedge q$ é verdadeira se, e somente se, p e q são verdadeiras simultaneamente.

Aula 8 - Tabela verdade

Aula 8 - Tabela verdade

Um jeito fácil de definir um conectivo é por meio de uma **tabela verdade**.

Um jeito fácil de definir um conectivo é por meio de uma **tabela verdade**. Vejamos os dois exemplos anteriores:

p	$\neg p$
V	F
F	V

Aula 8 - E

Aula 8 - E

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Aula 8 - Ou

Aula 8 - Ou

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Aula 8 - Bi-implicação

Aula 8 - Bi-implicação

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Aula 8 - Implicação

Aula 8 - Implicação

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Aula 8 - Combinando

Aula 8 - Combinando

Tabelas verdade não precisam conter apenas um conectivo, nem precisam ter apenas 3 colunas.

Aula 8 - Combinando

Tabelas verdade não precisam conter apenas um conectivo, nem precisam ter apenas 3 colunas. Muitas vezes diversas colunas nos ajudam a encontrar quando uma certa proposição composta é verdadeira ou não.

Tabelas verdade não precisam conter apenas um conectivo, nem precisam ter apenas 3 colunas. Muitas vezes diversas colunas nos ajudam a encontrar quando uma certa proposição composta é verdadeira ou não. Por exemplo:

p	q	$\neg q$	$p \wedge (\neg q)$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	V	F

Aula 8 - Mais exemplos

Aula 8 - Mais exemplos

p	q	$p \to q$	$(\neg q) \to (\neg p)$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Aula 8 - Mais exemplos

Aula 8 - Mais exemplos

p	q	$p \to q$	$(\neg p) \vee q$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Aula 8 - Mais exemplos

Aula 8 - Mais exemplos

p	$\neg p$	$p \vee (\neg p)$
V	F	V
F	V	V

Aula 8 - Mais exemplos

p	$\neg p$	$p \vee (\neg p)$
V	F	V
F	V	V

Note a última coluna.

Aula 8 - Mais exemplos

p	$\neg p$	$p \vee (\neg p)$
V	F	V
F	V	V

Note a última coluna. Não importa se p é verdade ou não, $p \vee (\neg p)$ é sempre verdade.

p	$\neg p$	$p \vee (\neg p)$
V	F	V
F	V	V

Note a última coluna. Não importa se p é verdade ou não, $p \vee (\neg p)$ é sempre verdade. Proposições que são sempre verdadeiras, independente de seus significados, são ditas **tautologias**.

Aula 9 - Quantificando

Vamos a um exemplo para mostrar um dos possíveis problemas.

Vamos a um exemplo para mostrar um dos possíveis problemas. Suponha que numa fazenda só existam vacas pretas e vacas brancas.

Vamos a um exemplo para mostrar um dos possíveis problemas. Suponha que numa fazenda só existam vacas pretas e vacas brancas. Suponha que temos duas proposições:

- p: "todas as vacas são pretas";
- q: "todas as vacas são brancas".

Vamos a um exemplo para mostrar um dos possíveis problemas. Suponha que numa fazenda só existam vacas pretas e vacas brancas. Suponha que temos duas proposições:

- p: "todas as vacas são pretas";
- q: "todas as vacas são brancas".

Como construir uma proposição que indique o que há na fazenda a partir destas duas?

Aula 9 - Quantificadores

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;
- $(\exists x\ A(x))$ quer dizer que há pelo menos um valor para x de forma que $A(x)$ seja verdadeira.

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;
- $(\exists x\ A(x))$ quer dizer que há pelo menos um valor para x de forma que $A(x)$ seja verdadeira.

Note que o $A(x)$ pode ser algo "composto" como $(B(x) \vee P(x))$.

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;
- $(\exists x\ A(x))$ quer dizer que há pelo menos um valor para x de forma que $A(x)$ seja verdadeira.

Note que o $A(x)$ pode ser algo "composto" como $(B(x) \vee P(x))$.

No caso das vacas, se indicarmos por $B(x)$ a propriedade "x é branca" e por $P(x)$ a propriedade "x ser preta", temos que a frase que reflete a fazenda é

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;
- $(\exists x\ A(x))$ quer dizer que há pelo menos um valor para x de forma que $A(x)$ seja verdadeira.

Note que o $A(x)$ pode ser algo "composto" como $(B(x) \vee P(x))$.

No caso das vacas, se indicarmos por $B(x)$ a propriedade "x é branca" e por $P(x)$ a propriedade "x ser preta", temos que a frase que reflete a fazenda é

$$\forall x\ (B(x) \vee P(x))$$

Aula 9 - Exemplo

Aula 9 - Exemplo

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";

Aula 9 - Exemplo

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Aula 9 - Exemplo

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Se queremos dizer que há um número real positivo (não estrito), podemos simplesmente escrever $(\exists x\ P(x))$.

Aula 9 - Exemplo

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Se queremos dizer que há um número real positivo (não estrito), podemos simplesmente escrever $(\exists x\ P(x))$. Se queremos dizer que todo número real é positivo ou negativo, podemos dizer $(\forall x\ (P(x) \vee N(x)))$.

Aula 9 - Exemplo

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Se queremos dizer que há um número real positivo (não estrito), podemos simplesmente escrever $(\exists x\ P(x))$. Se queremos dizer que todo número real é positivo ou negativo, podemos dizer $(\forall x\ (P(x) \vee N(x)))$. Se quisermos dizer que existe um que é positivo e negativo ao mesmo tempo (o 0 tem essa propriedade), podemos dizer $(\exists x(P(x) \wedge N(x)))$.

Aula 9 - Exemplo

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Se queremos dizer que há um número real positivo (não estrito), podemos simplesmente escrever $(\exists x\ P(x))$. Se queremos dizer que todo número real é positivo ou negativo, podemos dizer $(\forall x\ (P(x) \vee N(x)))$. Se quisermos dizer que existe um que é positivo e negativo ao mesmo tempo (o 0 tem essa propriedade), podemos dizer $(\exists x(P(x) \wedge N(x)))$. Podemos também dizer que todo número que não for negativo é positivo: $(\forall x((\neg N(x)) \rightarrow P(x)))$.

Aula 9 - Mais de um quantificador

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas.

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável.

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo.

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significando $x > y$.

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significando $x > y$. Se x, y vão simbolizar números reais, precisamos dizer quais exatamente: se algum, se todos etc.

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significando $x > y$. Se x, y vão simbolizar números reais, precisamos dizer quais exatamente: se algum, se todos etc. Começamos com a seguinte fórmula $(\exists x M(x, y))$. Com isso que queremos dizer que algum x é maior que y.

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significando $x > y$. Se x, y vão simbolizar números reais, precisamos dizer quais exatamente: se algum, se todos etc. Começamos com a seguinte fórmula $(\exists x M(x, y))$. Com isso que queremos dizer que algum x é maior que y. Mas qual o valor de y?

Aula 9 - Mais de um quantificador

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significando $x > y$. Se x, y vão simbolizar números reais, precisamos dizer quais exatamente: se algum, se todos etc. Começamos com a seguinte fórmula $(\exists x M(x, y))$. Com isso que queremos dizer que algum x é maior que y. Mas qual o valor de y? Resolvemos isso com o uso de outro quantificador.

Aula 9 - Mais de um quantificador

Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x, y)))$;

Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x, y)))$;

(b) $(\forall y(\forall x M(x, y)))$;

Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x, y)))$;

(b) $(\forall y(\forall x M(x, y)))$;

(c) $(\exists y(\forall x M(x, y)))$;

Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x,y)))$;

(b) $(\forall y(\forall x M(x,y)))$;

(c) $(\exists y(\forall x M(x,y)))$;

(d) $(\forall y(\exists x M(x,y)))$;

Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x,y)))$;

(b) $(\forall y(\forall x M(x,y)))$;

(c) $(\exists y(\forall x M(x,y)))$;

(d) $(\forall y(\exists x M(x,y)))$;

(e) $(\forall x(\exists y M(x,y)))$.

Aula 9 - Negando quantificadores

Aula 9 - Negando quantificadores

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Aula 9 - Negando quantificadores

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Estamos afirmando que todo x satisfaz a propriedade P.

Aula 9 - Negando quantificadores

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Estamos afirmando que todo x satisfaz a propriedade P. Então o que significa

$$\neg(\forall x P(x))?$$

Aula 9 - Negando quantificadores

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Estamos afirmando que todo x satisfaz a propriedade P. Então o que significa

$$\neg(\forall x P(x))?$$

Simplesmente ela quer dizer que não é verdade que todo x satisfaz a propriedade P.

Aula 9 - Negando quantificadores

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Estamos afirmando que todo x satisfaz a propriedade P. Então o que significa

$$\neg(\forall x P(x))?$$

Simplesmente ela quer dizer que não é verdade que todo x satisfaz a propriedade P. Isto é, que é verdade que

$$(\exists x(\neg P(x))).$$

Aula 9 - Negando quantificadores

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Estamos afirmando que todo x satisfaz a propriedade P. Então o que significa

$$\neg(\forall x P(x))?$$

Simplesmente ela quer dizer que não é verdade que todo x satisfaz a propriedade P. Isto é, que é verdade que

$$(\exists x(\neg P(x))).$$

O que é muito diferente de

$$(\forall x(\neg P(x)))$$

que simplesmente diz que todos os valores de x não satisfazem P.

Aula 9 - Negando quantificadores

Por outro lado, dizer que

$$\neg(\exists x P(x))$$

é o mesmo que afirmar que não é verdade que algum x satisfaz a propriedade P.

Por outro lado, dizer que

$$\neg(\exists x P(x))$$

é o mesmo que afirmar que não é verdade que algum x satisfaz a propriedade P. Isto é, para qualquer valor de x, $P(x)$ não é satisfeito.

Por outro lado, dizer que

$$\neg(\exists x P(x))$$

é o mesmo que afirmar que não é verdade que algum x satisfaz a propriedade P. Isto é, para qualquer valor de x, $P(x)$ não é satisfeito. Isto é, tal afirmação é equivalente a

$$(\forall x(\neg(P(x)))).$$

Por outro lado, dizer que

$$\neg(\exists x P(x))$$

é o mesmo que afirmar que não é verdade que algum x satisfaz a propriedade P. Isto é, para qualquer valor de x, $P(x)$ não é satisfeito. Isto é, tal afirmação é equivalente a

$$(\forall x(\neg(P(x)))).$$

Ou seja, para negar um quantificador basta "trocar o mesmo e negar o que vem depois".

Aula 9 - Exemplo

Aula 9 - Exemplo

Comecemos com a negação a da seguinte fórmula

$$(\forall x(\exists y(x < y))).$$

Aula 9 - Exemplo

Comecemos com a negação a da seguinte fórmula

$$(\forall x(\exists y(x < y))).$$

Vamos utilizar o método descrito acima, sem nos preocupar com o sinificado.

Aula 9 - Exemplo

Comecemos com a negação a da seguinte fórmula

$$(\forall x(\exists y(x < y))).$$

Vamos utilizar o método descrito acima, sem nos preocupar com o sinificado. Ou seja, começamos escrevendo a negação da fórmula:

$$\neg(\forall x(\exists y(x < y))).$$

Aula 9 - Exemplo

Comecemos com a negação a da seguinte fórmula

$$(\forall x(\exists y(x < y))).$$

Vamos utilizar o método descrito acima, sem nos preocupar com o sinificado. Ou seja, começamos escrevendo a negação da fórmula:

$$\neg(\forall x(\exists y(x < y))).$$

Daí negamos o primeiro quantificador (o segundo fica "aguardando"):

$$(\exists x(\neg(\exists y(x < y)))).$$

Aula 9 - Exemplo

Comecemos com a negação a da seguinte fórmula

$$(\forall x(\exists y(x < y))).$$

Vamos utilizar o método descrito acima, sem nos preocupar com o sinificado. Ou seja, começamos escrevendo a negação da fórmula:

$$\neg(\forall x(\exists y(x < y))).$$

Daí negamos o primeiro quantificador (o segundo fica "aguardando"):

$$(\exists x(\neg(\exists y(x < y)))).$$

Agora negamos o segundo:

$$(\exists x(\forall y\ \neg(x < y)))$$

.

Aula 9 - Demonstrações

Aula 9 - Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro.

Aula 9 - Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto.

Aula 9 - Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto.
Como dizer que algo é consequência de outras coisas?

Aula 9 - Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto. Como dizer que algo é consequência de outras coisas? Para não deixar dúvidas, deixaremos claro o que entendemos por isso.

Aula 9 - Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto. Como dizer que algo é consequência de outras coisas? Para não deixar dúvidas, deixaremos claro o que entendemos por isso. Diremos que B é consequência de afirmações anteriores se dentre as anteriores tivermos uma afirmação do tipo A e uma do tipo $A \to B$.

Aula 9 - Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto. Como dizer que algo é consequência de outras coisas? Para não deixar dúvidas, deixaremos claro o que entendemos por isso. Diremos que B é consequência de afirmações anteriores se dentre as anteriores tivermos uma afirmação do tipo A e uma do tipo $A \to B$. Tal regra é comumente resumida da seguinte forma:

Aula 9 - Demonstrações

$$\frac{A \qquad A \to B}{B}$$

$$\frac{A \qquad A \to B}{B}$$

A interpretação disso é "se sabemos que A vale e que toda vez que A vale, B vale, então B vale".

Aula 9 - Axiomas

Aula 9 - Axiomas

Mas e a parte do "sabidamente verdadeiro"?

Mas e a parte do “sabidamente verdadeiro”? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é.

Mas e a parte do “sabidamente verdadeiro”? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não.

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa.

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto?

Aula 9 - Axiomas

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto? O resto é o que vamos chamar de axiomas.

Aula 9 - Axiomas

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto? O resto é o que vamos chamar de axiomas.

Um **axioma** é uma afirmação que vamos supor verdadeira.

Aula 9 - Axiomas

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto? O resto é o que vamos chamar de axiomas.

Um **axioma** é uma afirmação que vamos supor verdadeira. O uso disso em geral é o seguinte: queremos definir uma determinada coisa, dizemos quais os axiomas que isso satisfaz e daí deduzimos tudo o que podemos a partir de tais axiomas.

Aula 9 - Axiomas

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto? O resto é o que vamos chamar de axiomas.

Um **axioma** é uma afirmação que vamos supor verdadeira. O uso disso em geral é o seguinte: queremos definir uma determinada coisa, dizemos quais os axiomas que isso satisfaz e daí deduzimos tudo o que podemos a partir de tais axiomas. Ou seja, tudo aquilo que satisfizer tais axiomas, vai satisfazer suas consequências também.

Aula 9 - Exemplo

Definição

Aula 9 - Exemplo

Definição

Dizemos que uma relação $\preceq$ é uma **relação de ordem** sobre um conjunto A se são satisfeitas as seguintes condições:

Aula 9 - Exemplo

Definição

Dizemos que uma relação $\preceq$ é uma **relação de ordem** sobre um conjunto A se são satisfeitas as seguintes condições:

(a) $\forall a \in A \ (a \preceq a)$ (reflexiva);

Aula 9 - Exemplo

Definição

Dizemos que uma relação $\preceq$ é uma **relação de ordem** sobre um conjunto A se são satisfeitas as seguintes condições:

(a) $\forall a \in A \ (a \preceq a)$ (reflexiva);

(b) $\forall a \in A \ \forall b \in A \ (a \preceq b \wedge b \preceq a) \rightarrow a = b$ (antissimétrica);

Aula 9 - Exemplo

Definição

Dizemos que uma relação $\preceq$ é uma **relação de ordem** sobre um conjunto A se são satisfeitas as seguintes condições:

(a) $\forall a \in A \ (a \preceq a)$ (reflexiva);

(b) $\forall a \in A \ \forall b \in A \ (a \preceq b \wedge b \preceq a) \rightarrow a = b$ (antissimétrica);

(c) $\forall a \in A \ \forall b \in A \ \forall c \in A((a \preceq b \wedge b \preceq c) \rightarrow a \preceq c)$ (transitiva).

Aula 9 - Exemplo

Aula 9 - Exemplo

Um exemplo de uma ordem sobre um conjunto é a relação $\leq$ sobre os números reais.

Aula 9 - Exemplo

Um exemplo de uma ordem sobre um conjunto é a relação $\leq$ sobre os números reais. Verificamos isso simplesmente notando que para qualquer $x \in \mathbb{R}$, temos $x \leq x$;

Aula 9 - Exemplo

Um exemplo de uma ordem sobre um conjunto é a relação $\leq$ sobre os números reais. Verificamos isso simplesmente notando que para qualquer $x \in \mathbb{R}$, temos $x \leq x$; que para todo $x \in \mathbb{R}$ e todo $y \in \mathbb{R}$, se $x \leq y$ e $y \leq x$, então $x = y$;

Aula 9 - Exemplo

Um exemplo de uma ordem sobre um conjunto é a relação $\leq$ sobre os números reais. Verificamos isso simplesmente notando que para qualquer $x \in \mathbb{R}$, temos $x \leq x$; que para todo $x \in \mathbb{R}$ e todo $y \in \mathbb{R}$, se $x \leq y$ e $y \leq x$, então $x = y$; e, por fim, que para qualquer $x \in \mathbb{R}$, qualquer $y \in \mathbb{R}$ e qualquer $z \in \mathbb{R}$, temos que $x \leq y$ e $y \leq z$, então $x \leq z$.

Aula 9 - Outro exemplo

Aula 9 - Outro exemplo

Um outro exemplo de ordem, um tanto diferente, é o seguinte:

Exemplo
Considere a relação $|$ sobre os números naturais maiores que 0 dada por $m|n$ se "m divide n".

Aula 9 - Outro exemplo

Um outro exemplo de ordem, um tanto diferente, é o seguinte:

Exemplo
Considere a relação $|$ sobre os números naturais maiores que 0 dada por $m|n$ se "m divide n". Note que tal relação também é uma relação de ordem.

Aula 9 - Outro exemplo

Um outro exemplo de ordem, um tanto diferente, é o seguinte:

Exemplo
Considere a relação $|$ sobre os números naturais maiores que 0 dada por $m|n$ se "m divide n". Note que tal relação também é uma relação de ordem. De fato:

(a) $m|m$ para todo $m \in \{k \in \mathbb{N} : k > 0\}$, já que m divide m se $m \neq 0$;

(b) Se m divide n e n divide m, temos que, necessariamente, $m = n$;

(c) Se m divide n e n divide k, então m divide k.

Aula 9 - Outro exemplo

Um outro exemplo de ordem, um tanto diferente, é o seguinte:

Exemplo
Considere a relação $|$ sobre os números naturais maiores que 0 dada por $m|n$ se "m divide n". Note que tal relação também é uma relação de ordem. De fato:

(a) $m|m$ para todo $m \in \{k \in \mathbb{N} : k > 0\}$, já que m divide m se $m \neq 0$;

(b) Se m divide n e n divide m, temos que, necessariamente, $m = n$;

(c) Se m divide n e n divide k, então m divide k.

Na verdade, voltaremos a este exemplo mais tarde e poderemos provar a última afirmação.

Aula 9 - Mínimo

Aula 9 - Mínimo

Considere a seguinte definição:

Definição
Seja $\preceq$ uma ordem sobre A. Dizemos que $a \in A$ é um **mínimo** de A se vale $a \preceq b$ para todo $b \in A$.

Aula 9 - Mínimo

Considere a seguinte definição:

Definição
Seja $\preceq$ uma ordem sobre A. Dizemos que $a \in A$ é um **mínimo** de A se vale $a \preceq b$ para todo $b \in A$.

Poderíamos nos perguntar se a existência de um mínimo é consequência dos axiomas de ordem.

Aula 9 - Mínimo

Considere a seguinte definição:

Definição
Seja $\preceq$ uma ordem sobre A. Dizemos que $a \in A$ é um **mínimo** de A se vale $a \preceq b$ para todo $b \in A$.

Poderíamos nos perguntar se a existência de um mínimo é consequência dos axiomas de ordem. Isto é, se podemos provar a partir de tais axiomas a seguinte proposição:

$$\exists a \in A \; \forall b \in A \; a \preceq b.$$

Aula 9 - Independência

Exemplo

Note que 1 é um mínimo na ordem $|$ sobre $\{n \in \mathbb{N} : n > 0\}$ já que $1|b$ para todo $b \in \mathbb{N} \setminus \{0\}$.

Exemplo

Note que 1 é um mínimo na ordem $|$ sobre $\{n \in \mathbb{N} : n > 0\}$ já que $1|b$ para todo $b \in \mathbb{N} \setminus \{0\}$. Ou seja, $|$ é uma ordem que admite mínimo.

Exemplo

Note que 1 é um mínimo na ordem $|$ sobre $\{n \in \mathbb{N} : n > 0\}$ já que $1|b$ para todo $b \in \mathbb{N} \setminus \{0\}$. Ou seja, $|$ é uma ordem que admite mínimo. Por outro lado, $\leq$ é uma ordem sobre $\mathbb{R}$ que não admite mínimo.

Exemplo

Note que 1 é um mínimo na ordem $|$ sobre $\{n \in \mathbb{N} : n > 0\}$ já que $1|b$ para todo $b \in \mathbb{N} \setminus \{0\}$. Ou seja, $|$ é uma ordem que admite mínimo. Por outro lado, $\leq$ é uma ordem sobre $\mathbb{R}$ que não admite mínimo. Basta notar que, para qualquer $x \in \mathbb{R}$, $\neg(x \leq (x-1))$.

Aula 10 - Números naturais

Aula 10 - Números naturais

Vamos começar dando uma definição axiomática para os números naturais.

Aula 10 - Números naturais

Vamos começar dando uma definição axiomática para os números naturais. Posteriormente, mostraremos como definir em tal conjunto as operações básicas, como a soma e a multiplicação.

Aula 10 - Números naturais

Vamos começar dando uma definição axiomática para os números naturais. Posteriormente, mostraremos como definir em tal conjunto as operações básicas, como a soma e a multiplicação.

Depois, mostraremos como usar os naturais para definir outros conjuntos importantes em matemática, como os inteiros e os racionais.

Aula 10 - Números naturais

Vamos começar dando uma definição axiomática para os números naturais. Posteriormente, mostraremos como definir em tal conjunto as operações básicas, como a soma e a multiplicação.

Depois, mostraremos como usar os naturais para definir outros conjuntos importantes em matemática, como os inteiros e os racionais. Ou seja, de certa forma, vamos mostrar como fundamentar parte da matemática assumindo apenas algumas afirmações sobre números naturais.

Aula 10 - Axiomas de Peano

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

(a) $0 \in \mathbb{N}$;

Aula 10 - Axiomas de Peano

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

(c) $\forall n \in \mathbb{N}\ s(n) \neq 0$;

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

(c) $\forall n \in \mathbb{N}\ s(n) \neq 0$;

(d) $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ s(n) = s(m) \rightarrow n = m$;

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

(c) $\forall n \in \mathbb{N}\ s(n) \neq 0$;

(d) $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ s(n) = s(m) \rightarrow n = m$;

(e) Seja $P(x)$ uma propriedade sobre elementos de $\mathbb{N}$. Se valem

  (i) $P(0)$;

  (ii) $\forall n \in \mathbb{N}\ P(n) \rightarrow P(s(n))$;

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

(c) $\forall n \in \mathbb{N}\ s(n) \neq 0$;

(d) $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ s(n) = s(m) \rightarrow n = m$;

(e) Seja $P(x)$ uma propriedade sobre elementos de $\mathbb{N}$. Se valem

(i) $P(0)$;

(ii) $\forall n \in \mathbb{N}\ P(n) \rightarrow P(s(n))$;

Então vale $P(n)$ para todo $n \in \mathbb{N}$.

Aula 10 - Consequências

Proposição
Temos que $s(n) \neq n$ *para todo* $n \in \mathbb{N}$.

Proposição
Temos que $s(n) \neq n$ *para todo* $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução.

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$".

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$.

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Agora suponha que vale $P(n)$ para algum n.

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Agora suponha que vale $P(n)$ para algum n. Ou seja, vale $n \neq s(n)$.

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Agora suponha que vale $P(n)$ para algum n. Ou seja, vale $n \neq s(n)$. Vamos mostrar que vale $P(s(n))$, isto é, $s(n) \neq s(s(n))$.

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Agora suponha que vale $P(n)$ para algum n. Ou seja, vale $n \neq s(n)$. Vamos mostrar que vale $P(s(n))$, isto é, $s(n) \neq s(s(n))$. Suponha que não, isto é, que vale $s(n) = s(s(n))$.

Proposição
Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.

Demonstração.
Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Agora suponha que vale $P(n)$ para algum n. Ou seja, vale $n \neq s(n)$. Vamos mostrar que vale $P(s(n))$, isto é, $s(n) \neq s(s(n))$. Suponha que não, isto é, que vale $s(n) = s(s(n))$. Por (d), temos que $n = s(n)$, contrariando nossa hipótese. □

Aula 10 - Consequências

Proposição
Se $n \in \mathbb{N}$ *e* $n \neq 0$, *então existe* $m \in \mathbb{N}$ *tal que* $n = s(m)$.

Proposição
Se $n \in \mathbb{N}$ e $n \neq 0$, então existe $m \in \mathbb{N}$ tal que $n = s(m)$.

Demonstração. Novamente, vamos mostrar por indução.

Proposição
Se $n \in \mathbb{N}$ e $n \neq 0$, então existe $m \in \mathbb{N}$ tal que $n = s(m)$.

Demonstração. Novamente, vamos mostrar por indução. Ou seja, vamos mostrar que vale a fórmula $P(x)$ para todo $x \in \mathbb{N}$ onde $P(x)$ é a fórmula

$$x \neq 0 \to \exists m\ x = s(m).$$

Proposição
Se $n \in \mathbb{N}$ e $n \neq 0$, então existe $m \in \mathbb{N}$ tal que $n = s(m)$.

Demonstração. Novamente, vamos mostrar por indução. Ou seja, vamos mostrar que vale a fórmula $P(x)$ para todo $x \in \mathbb{N}$ onde $P(x)$ é a fórmula

$$x \neq 0 \to \exists m\ x = s(m).$$

Note que $0 \neq 0 \to \exists m\ 0 = s(m)$ simplesmente porque não vale $0 \neq 0$ (não importa que também não valha o lado direito da implicação).

Aula 10 - Provando

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale:

$$n \neq 0 \rightarrow \exists m \; n = s(m).$$

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale:

$$n \neq 0 \rightarrow \exists m \; n = s(m).$$

Precisamos mostrar então que vale $P(s(n))$.

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale:

$$n \neq 0 \rightarrow \exists m \; n = s(m).$$

Precisamos mostrar então que vale $P(s(n))$. Isto é, precisamos mostrar que, se vale $s(n) \neq 0$ (o que vale!), então vale que existe m tal que $s(n) = s(m)$.

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale:

$$n \neq 0 \rightarrow \exists m \; n = s(m).$$

Precisamos mostrar então que vale $P(s(n))$. Isto é, precisamos mostrar que, se vale $s(n) \neq 0$ (o que vale!), então vale que existe m tal que $s(n) = s(m)$. Considere $m = n$.

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale:

$$n \neq 0 \rightarrow \exists m \; n = s(m).$$

Precisamos mostrar então que vale $P(s(n))$. Isto é, precisamos mostrar que, se vale $s(n) \neq 0$ (o que vale!), então vale que existe m tal que $s(n) = s(m)$. Considere $m = n$. Note que, então $s(n) = s(m)$ como queríamos. $\square$

Aula 10 - A soma nos naturais

Aula 10 - A soma nos naturais

Vejamos agora como definir a operação de soma $(+)$ sobre os naturais:

Aula 10 - A soma nos naturais

Vejamos agora como definir a operação de soma $(+)$ sobre os naturais:

Definição
Chamamos de **soma** nos naturais (ou **adição**) uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que sejam satisfeitas:

Vejamos agora como definir a operação de soma $(+)$ sobre os naturais:

Definição
Chamamos de **soma** nos naturais (ou **adição**) uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que sejam satisfeitas:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = a$;

Vejamos agora como definir a operação de soma $(+)$ sobre os naturais:

Definição
Chamamos de **soma** nos naturais (ou **adição**) uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que sejam satisfeitas:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = a$;

(b) $\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ f(a, s(b)) = s(f(a, b))$.

Aula 10 - Consequências

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dado* $a \in \mathbb{N}$, *temos que* $f(0, a) = a$.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dado* $a \in \mathbb{N}$, *temos que* $f(0, a) = a$.

Demonstração.
Vamos mostrar a afirmação $P(x)$ dada por

$$f(0, x) = x$$

por indução.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dado* $a \in \mathbb{N}$, *temos que* $f(0, a) = a$.

Demonstração.
Vamos mostrar a afirmação $P(x)$ dada por

$$f(0, x) = x$$

por indução.

$P(0)$**:** Temos que $f(0, 0) = 0$ pelo axioma (a) de adição.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dado* $a \in \mathbb{N}$, *temos que* $f(0, a) = a$.

Demonstração.
Vamos mostrar a afirmação $P(x)$ dada por

$$f(0, x) = x$$

por indução.

$P(0)$**:** Temos que $f(0, 0) = 0$ pelo axioma (a) de adição.

$P(n) \to P(s(n))$**:** Suponha que $f(0, n) = n$ e vamos provar que $f(0, s(n)) = s(n)$.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dado* $a \in \mathbb{N}$, *temos que* $f(0, a) = a$.

Demonstração.
Vamos mostrar a afirmação $P(x)$ dada por

$$f(0, x) = x$$

por indução.

$P(0)$**:** Temos que $f(0, 0) = 0$ pelo axioma (a) de adição.

$P(n) \to P(s(n))$**:** Suponha que $f(0, n) = n$ e vamos provar que $f(0, s(n)) = s(n)$. Temos, por (b), que

$$f(0, s(n)) = s(f(0, n)) = s(n).$$

□

Aula 10 - Consequências

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Demonstração. Seja $a \in \mathbb{N}$.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x).$$

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x).$$

Note que se $P(x)$ for verdadeira para todo $x \in \mathbb{N}$, temos o resultado desejado (já que o a é qualquer).

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x).$$

Note que se $P(x)$ for verdadeira para todo $x \in \mathbb{N}$, temos o resultado desejado (já que o a é qualquer). Vamos mostrar $P(x)$ por indução.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x).$$

Note que se $P(x)$ for verdadeira para todo $x \in \mathbb{N}$, temos o resultado desejado (já que o a é qualquer). Vamos mostrar $P(x)$ por indução.

$P(0)$: Temos $f(a, s(0)) = s(f(a, 0)) = s(a)$.

Lema

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, s(b)) = f(s(a), b)$

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x).$$

Note que se $P(x)$ for verdadeira para todo $x \in \mathbb{N}$, temos o resultado desejado (já que o a é qualquer). Vamos mostrar $P(x)$ por indução.

$P(0)$: Temos $f(a, s(0)) = s(f(a, 0)) = s(a)$. Por outro lado, $f(s(a), 0) = s(a)$. Logo, temos $P(0)$.

Aula 10 - Provando

$P(n) \to P(s(n))$: Suponha que vale $f(a, s(n)) = f(s(a), n)$ e vamos mostrar $f(a, s(s(n))) = f(s(a), s(n))$.

$P(n) \to P(s(n))$: Suponha que vale $f(a, s(n)) = f(s(a), n)$ e vamos mostrar $f(a, s(s(n))) = f(s(a), s(n))$. Temos

$$f(a, s(s(n))) \quad = \quad s(f(a, s(n)))$$

$P(n) \to P(s(n))$: Suponha que vale $f(a, s(n)) = f(s(a), n)$ e vamos mostrar $f(a, s(s(n))) = f(s(a), s(n))$. Temos

$$\begin{aligned} f(a, s(s(n))) &= s(f(a, s(n))) \\ &= s(f(s(a), n)) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $f(a, s(n)) = f(s(a), n)$ e vamos mostrar $f(a, s(s(n))) = f(s(a), s(n))$. Temos

$$\begin{aligned} f(a, s(s(n))) &= s(f(a, s(n))) \\ &= s(f(s(a), n)) \\ &= f(s(a), s(n)) \end{aligned}$$

□

Aula 10 - Consequências

Aula 10 - Consequências

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = f(b, a)$.

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = f(b, a)$.

Demonstração. Seja $a \in \mathbb{N}$.

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = f(b, a)$.

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação sobre $x \in \mathbb{N}$:

$$f(x, a) = f(a, x).$$

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = f(b, a)$.

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação sobre $x \in \mathbb{N}$:

$$f(x, a) = f(a, x).$$

Vamos chamar tal afirmação de $P(x)$.

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *uma soma sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = f(b, a)$.

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação sobre $x \in \mathbb{N}$:

$$f(x, a) = f(a, x).$$

Vamos chamar tal afirmação de $P(x)$. Note que se mostrarmos $P(x)$ para todos os $x \in \mathbb{N}$, teremos o resultado desejado (já que o a é qualquer).

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, b) = f(b, a)$.

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação sobre $x \in \mathbb{N}$:

$$f(x, a) = f(a, x).$$

Vamos chamar tal afirmação de $P(x)$. Note que se mostrarmos $P(x)$ para todos os $x \in \mathbb{N}$, teremos o resultado desejado (já que o a é qualquer). Assim, vamos mostrar $P(n)$ por indução sobre $n \in \mathbb{N}$.

Aula 10 - Provando

$P(0)$: Temos que $f(x, 0) = x$, pelo axioma (a) da definição de soma.

$P(0)$: Temos que $f(x, 0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0, x) = x$ também (pelo Lema 10.4).

$P(0)$: Temos que $f(x, 0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0, x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$:

$P(0)$: Temos que $f(x, 0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0, x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$: Suponha que vale $f(n, a) = f(a, n)$ e vamos mostrar que $f(s(n), a) = f(a, s(n))$.

$P(0)$: Temos que $f(x,0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0,x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$: Suponha que vale $f(n,a) = f(a,n)$ e vamos mostrar que $f(s(n),a) = f(a,s(n))$. Temos:

$$f(s(n),a) \overset{10.5}{=} f(n,s(a))$$

$P(0)$: Temos que $f(x,0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0,x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$: Suponha que vale $f(n,a) = f(a,n)$ e vamos mostrar que $f(s(n),a) = f(a,s(n))$. Temos:

$$\begin{aligned} f(s(n),a) &\overset{10.5}{=} f(n,s(a)) \\ &= s(f(n,a)) \end{aligned}$$

$P(0)$: Temos que $f(x,0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0,x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$: Suponha que vale $f(n,a) = f(a,n)$ e vamos mostrar que $f(s(n),a) = f(a,s(n))$. Temos:

$$\begin{aligned} f(s(n),a) &\overset{10.5}{=} f(n,s(a)) \\ &= s(f(n,a)) \\ &= s(f(a,n)) \end{aligned}$$

$P(0)$: Temos que $f(x,0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0,x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$: Suponha que vale $f(n,a) = f(a,n)$ e vamos mostrar que $f(s(n),a) = f(a,s(n))$. Temos:

$$\begin{aligned} f(s(n),a) &\overset{10.5}{=} f(n,s(a)) \\ &= s(f(n,a)) \\ &= s(f(a,n)) \\ &= f(a,s(n)) \end{aligned}$$

□

Aula 10 - Unicidade

Proposição

Suponha que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *sejam duas adições sobre* $\mathbb{N}$. *Então, para quaisquer* $a, b \in \mathbb{N}$ *temos que* $f(a, b) = g(a, b)$.

Proposição

Suponha que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *sejam duas adições sobre* $\mathbb{N}$. *Então, para quaisquer* $a, b \in \mathbb{N}$ *temos que* $f(a, b) = g(a, b)$.

Demonstração. Seja $a \in \mathbb{N}$.

Proposição

Suponha que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *sejam duas adições sobre* $\mathbb{N}$. *Então, para quaisquer* $a, b \in \mathbb{N}$ *temos que* $f(a, b) = g(a, b)$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$f(a, x) = g(a, x).$$

Proposição

Suponha que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *sejam duas adições sobre* $\mathbb{N}$. *Então, para quaisquer* $a, b \in \mathbb{N}$ *temos que* $f(a, b) = g(a, b)$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$f(a, x) = g(a, x).$$

Vamos mostrar tal afirmação por indução (note que isso é suficiente para o que queremos).

Aula 10 - Provando

$P(0)$: Pelo axioma (a) da soma, temos que $f(a,0) = a = g(a,0)$.

$P(0)$: Pelo axioma (a) da soma, temos que $f(a,0) = a = g(a,0)$.

$P(n) \to P(s(n))$: Vamos supor que vale $f(a,n) = g(a,n)$ e mostrar que vale $f(a,s(n)) = g(a,s(n))$.

$P(0)$: Pelo axioma (a) da soma, temos que $f(a,0) = a = g(a,0)$.

$P(n) \to P(s(n))$: Vamos supor que vale $f(a,n) = g(a,n)$ e mostrar que vale $f(a,s(n)) = g(a,s(n))$. Temos $f(a,s(n)) = s(f(a,n)) = s(g(a,n)) = g(a,s(n))$. $\square$

Aula 10 - Notação

Assim, não há outra função sobre os naturais que satisfaça as condições impostas, além da soma usual que conhecemos.

Assim, não há outra função sobre os naturais que satisfaça as condições impostas, além da soma usual que conhecemos.

Para manter a coerência com a notação usual, a partir deste momento adotaremos a notação $a + b$ no lugar da $f(a, b)$.

Aula 10 - Mais consequências

Vejamos mais algumas propriedades sobre a soma:

Proposição
Valem as seguintes propriedades:

(a) *Dados* $a, b \in \mathbb{N}$, *temos* $a + b = b + a$; *(***comutativa***)*

(b) *Dados* $a, b, c \in \mathbb{N}$, *temos que* $(a + b) + c = a + (b + c)$; *(***associativa***)*

Vejamos mais algumas propriedades sobre a soma:

Proposição
Valem as seguintes propriedades:

(a) *Dados* $a, b \in \mathbb{N}$, *temos* $a + b = b + a$; *(***comutativa***)*

(b) *Dados* $a, b, c \in \mathbb{N}$, *temos que* $(a + b) + c = a + (b + c)$; *(***associativa***)*

Demonstração. Note que o item (a) é simplesmente o que foi provado na Proposição 10.6.

Aula 10 - Provando

Aula 10 - Provando

Para o item (b), sejam $a, b \in \mathbb{N}$.

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

$P(n) \to P(s(n))$: Vamos supor que vale $(a + b) + n = a + (b + n)$ e vamos mostrar que $(a + b) + s(n) = a + (b + s(n))$.

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

$P(n) \to P(s(n))$: Vamos supor que vale $(a + b) + n = a + (b + n)$ e vamos mostrar que $(a + b) + s(n) = a + (b + s(n))$. Temos

$$(a + b) + s(n) \quad = \quad s((a + b) + n)$$

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

$P(n) \to P(s(n))$: Vamos supor que vale $(a + b) + n = a + (b + n)$ e vamos mostrar que $(a + b) + s(n) = a + (b + s(n))$. Temos

$$\begin{aligned} (a + b) + s(n) &= s((a + b) + n) \\ &= s(a + (b + n)) \end{aligned}$$

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

$P(n) \to P(s(n))$: Vamos supor que vale $(a + b) + n = a + (b + n)$ e vamos mostrar que $(a + b) + s(n) = a + (b + s(n))$. Temos

$$\begin{aligned} (a + b) + s(n) &= s((a + b) + n) \\ &= s(a + (b + n)) \\ &= a + s(b + n) \end{aligned}$$

Para o item (b), sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x).$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

$P(n) \to P(s(n))$: Vamos supor que vale $(a + b) + n = a + (b + n)$ e vamos mostrar que $(a + b) + s(n) = a + (b + s(n))$. Temos

$$\begin{aligned} (a + b) + s(n) &= s((a + b) + n) \\ &= s(a + (b + n)) \\ &= a + s(b + n) \\ &= a + (b + s(n)) \end{aligned}$$

Aula 10 - Mais consequencias

Proposição (Lei do Cancelamento)
Sejam $a, b, c \in \mathbb{N}$. *Se* $a + b = a + c$, *então* $b = c$.

Proposição (Lei do Cancelamento)
Sejam $a, b, c \in \mathbb{N}$. *Se* $a + b = a + c$, *então* $b = c$.

Demonstração. Sejam $b, c \in \mathbb{N}$.

Proposição (Lei do Cancelamento)
Sejam $a, b, c \in \mathbb{N}$. Se $a + b = a + c$, então $b = c$.

Demonstração. Sejam $b, c \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$(x + b = x + c) \to b = c.$$

Proposição (Lei do Cancelamento)
Sejam $a, b, c \in \mathbb{N}$. Se $a + b = a + c$, então $b = c$.

Demonstração. Sejam $b, c \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$(x + b = x + c) \to b = c.$$

Vamos mostrá-la por indução (note que isso é suficiente).

Proposição (Lei do Cancelamento)
Sejam $a, b, c \in \mathbb{N}$. Se $a + b = a + c$, então $b = c$.

Demonstração. Sejam $b, c \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$(x + b = x + c) \to b = c.$$

Vamos mostrá-la por indução (note que isso é suficiente).

$P(0)$: Suponha que $0 + b = 0 + c$. Note que $0 + b = b$ e que $0 + c = c$. Logo, temos que $b = c$ como queríamos.

Aula 10 - Provando

Aula 10 - Provando

$P(n) \to P(s(n)$: Suponha que vale $(n + b = n + c) \to b = c$.

$P(n) \to P(s(n)$: Suponha que vale $(n + b = n + c) \to b = c$.
Suponha que vale $s(n) + b = s(n) + c$.

$P(n) \rightarrow P(s(n)$: Suponha que vale $(n + b = n + c) \rightarrow b = c$.
Suponha que vale $s(n) + b = s(n) + c$. Logo, temos
$b + s(n) = c + s(n)$.

$P(n) \to P(s(n)$: Suponha que vale $(n + b = n + c) \to b = c$.
Suponha que vale $s(n) + b = s(n) + c$. Logo, temos
$b + s(n) = c + s(n)$. Pela axioma (b) da adição, temos
$s(b + n) = s(c + n)$.

$P(n) \rightarrow P(s(n)$: Suponha que vale $(n + b = n + c) \rightarrow b = c$. Suponha que vale $s(n) + b = s(n) + c$. Logo, temos $b + s(n) = c + s(n)$. Pela axioma (b) da adição, temos $s(b + n) = s(c + n)$. Pelo axioma (d) dos naturais, temos que $b + n = c + n$.

$P(n) \rightarrow P(s(n)$: Suponha que vale $(n + b = n + c) \rightarrow b = c$.
Suponha que vale $s(n) + b = s(n) + c$. Logo, temos
$b + s(n) = c + s(n)$. Pela axioma (b) da adição, temos
$s(b + n) = s(c + n)$. Pelo axioma (d) dos naturais, temos que
$b + n = c + n$. Logo, $n + b = n + c$ e, portanto, $b = c$. $\square$

Aula 10 - Mais notações

Aula 10 - Mais notações

Finalmente, podemos passar a usar algumas notações mais usuais:

Definição
Vamos chamar de 1 o elemento $s(0)$ de $\mathbb{N}$. Também usaremos a notação usual para $s(1) = 2$, $s(2) = 3$...

Aula 10 - Mais algumas consequências

Proposição
Seja $a \in \mathbb{N}$. *Então* $s(a) = a + 1$.

Proposição
Seja $a \in \mathbb{N}$. *Então* $s(a) = a + 1$.

Demonstração. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$s(x) = x + 1.$$

Proposição
Seja $a \in \mathbb{N}$. *Então* $s(a) = a + 1$.

Demonstração. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$s(x) = x + 1.$$

Vamos mostrá-la por indução.

Proposição
Seja $a \in \mathbb{N}$. Então $s(a) = a + 1$.

Demonstração. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$s(x) = x + 1.$$

Vamos mostrá-la por indução.

$P(0)$: Temos $s(0) = 1$ por definição.

Proposição
Seja $a \in \mathbb{N}$. *Então* $s(a) = a + 1$.

Demonstração. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$s(x) = x + 1.$$

Vamos mostrá-la por indução.

$P(0)$: Temos $s(0) = 1$ por definição. Por outro lado,
$0 + 1 = 1 + 0 = 1$.

Aula 10 - Provando

Aula 10 - Provando

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$.

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$. Temos

$$s(s(n)) \quad = \quad s(n+1)$$

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$. Temos

$$\begin{aligned} s(s(n)) &= s(n+1) \\ &= s(1+n) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$. Temos

$$\begin{aligned} s(s(n)) &= s(n+1) \\ &= s(1+n) \\ &= 1 + s(n) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$. Temos

$$\begin{aligned} s(s(n)) &= s(n+1) \\ &= s(1+n) \\ &= 1 + s(n) \\ &= s(n) + 1 \end{aligned}$$

□

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$. Temos

$$\begin{aligned} s(s(n)) &= s(n+1) \\ &= s(1+n) \\ &= 1 + s(n) \\ &= s(n) + 1 \end{aligned}$$

□

Dado o último resultado, daqui em diante muitas vezes utilizaremos a notação $n + 1$ no lugar da $s(n)$.

Aula 11 - O produto nos naturais

Aula 11 - O produto nos naturais

Vamos agora, de forma semelhante ao que fizemos com a soma, definir o produto de naturais.

Aula 11 - O produto nos naturais

Vamos agora, de forma semelhante ao que fizemos com a soma, definir o produto de naturais.

Definição
Chamamos de **produto** (ou de **multiplicação**) uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que satisfaz:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = 0$;

(b) $\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ f(a, s(b)) = a + f(a, b)$.

Aula 11 - Unicidade

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, n) = g(a, n)$ e vamos mostrar que vale $f(a, s(n)) = g(a, s(n))$.

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, n) = g(a, n)$ e vamos mostrar que vale $f(a, s(n)) = g(a, s(n))$. Temos

$$f(a, s(n)) \quad = \quad a + f(a, n)$$

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, n) = g(a, n)$ e vamos mostrar que vale $f(a, s(n)) = g(a, s(n))$. Temos

$$\begin{aligned} f(a, s(n)) &= a + f(a, n) \\ &= a + g(a, n) \end{aligned}$$

Proposição

Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *e* $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *dois produtos sobre* $\mathbb{N}$. *Então, dados* $a, b \in \mathbb{N}$, *temos que* $f(a, b) = g(a, b)$.

Demonstração.

Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, n) = g(a, n)$ e vamos mostrar que vale $f(a, s(n)) = g(a, s(n))$. Temos

$$\begin{aligned} f(a, s(n)) &= a + f(a, n) \\ &= a + g(a, n) \\ &= g(a, s(n)) \end{aligned}$$

□

Aula 11 - Notação

Aula 11 - Notação

Dada a unicidade, denotaremos o único produto sobre os naturais por $\cdot$. Isto é, em vez de usarmos $f(a, b)$ usaremos $a \cdot b$.

Aula 11 - Notação

Dada a unicidade, denotaremos o único produto sobre os naturais por $\cdot$. Isto é, em vez de usarmos $f(a, b)$ usaremos $a \cdot b$. Muitas vezes omitiremos o $\cdot$ e usaremos simplesmente ab.

Aula 11 - Consequências

Lema

Seja $a \in \mathbb{N}$. *Então* $0 \cdot a = 0$.

Lema

Seja $a \in \mathbb{N}$. *Então* $0 \cdot a = 0$.

Demonstração.
Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

Lema

Seja $a \in \mathbb{N}$. *Então* $0 \cdot a = 0$.

Demonstração.
Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

$P(0)$**:** $0 \cdot 0 = 0$, pelo axioma (a).

Lema

Seja $a \in \mathbb{N}$. *Então* $0 \cdot a = 0$.

Demonstração.
Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

$P(0)$**:** $0 \cdot 0 = 0$, pelo axioma (a).

$P(n) \to P(s(n))$**:** Suponha $0 \cdot n = 0$. Temos

$$0 \cdot s(n) \quad = \quad 0 + (0 \cdot n)$$

Lema

Seja $a \in \mathbb{N}$. *Então* $0 \cdot a = 0$.

Demonstração.
Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

$P(0)$**:** $0 \cdot 0 = 0$, pelo axioma (a).

$P(n) \to P(s(n))$**:** Suponha $0 \cdot n = 0$. Temos

$$\begin{aligned} 0 \cdot s(n) &= 0 + (0 \cdot n) \\ &= 0 + 0 \end{aligned}$$

Lema

Seja $a \in \mathbb{N}$. *Então* $0 \cdot a = 0$.

Demonstração.
Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

$P(0)$**:** $0 \cdot 0 = 0$, pelo axioma (a).

$P(n) \to P(s(n))$**:** Suponha $0 \cdot n = 0$. Temos

$$\begin{aligned} 0 \cdot s(n) &= 0 + (0 \cdot n) \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

□

Aula 11 - Consequências

Lema

Sejam $a, b \in \mathbb{N}$. *Então vale* $s(b) \cdot a = a + (b \cdot a)$.

Lema

Sejam $a, b \in \mathbb{N}$. *Então vale* $s(b) \cdot a = a + (b \cdot a)$.

Demonstração. Seja $b \in \mathbb{N}$. Considere $P(x)$ sendo $s(b) \cdot x = x + (b \cdot x)$.

Lema

Sejam $a, b \in \mathbb{N}$. *Então vale* $s(b) \cdot a = a + (b \cdot a)$.

Demonstração. Seja $b \in \mathbb{N}$. Considere $P(x)$ sendo $s(b) \cdot x = x + (b \cdot x)$. Vamos mostrar por indução.

Lema

Sejam $a, b \in \mathbb{N}$. *Então vale* $s(b) \cdot a = a + (b \cdot a)$.

Demonstração. Seja $b \in \mathbb{N}$. Considere $P(x)$ sendo $s(b) \cdot x = x + (b \cdot x)$. Vamos mostrar por indução. Temos:

$P(0)$: $s(b) \cdot 0 = 0$.

Lema

Sejam $a, b \in \mathbb{N}$. *Então vale* $s(b) \cdot a = a + (b \cdot a)$.

Demonstração. Seja $b \in \mathbb{N}$. Considere $P(x)$ sendo $s(b) \cdot x = x + (b \cdot x)$. Vamos mostrar por indução. Temos:

$P(0)$: $s(b) \cdot 0 = 0$. Por outro lado, $0 + (c \cdot 0) = 0 + 0 = 0$.

Aula 11 - Provando

Aula 11 - Provando

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$.

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$s(b) \cdot s(n) \quad = \quad s(b) + (s(b) \cdot n)$$

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{aligned} s(b) \cdot s(n) &= s(b) + (s(b) \cdot n) \\ &= s(b) + (n + (b \cdot n)) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{aligned} s(b) \cdot s(n) &= s(b) + (s(b) \cdot n) \\ &= s(b) + (n + (b \cdot n)) \\ &= (s(b) + n) + (b \cdot n) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{aligned} s(b) \cdot s(n) &= s(b) + (s(b) \cdot n) \\ &= s(b) + (n + (b \cdot n)) \\ &= (s(b) + n) + (b \cdot n) \\ &= (b + s(n)) + (b \cdot n) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{aligned} s(b) \cdot s(n) &= s(b) + (s(b) \cdot n) \\ &= s(b) + (n + (b \cdot n)) \\ &= (s(b) + n) + (b \cdot n) \\ &= (b + s(n)) + (b \cdot n) \\ &= s(n) + (b + (b \cdot n)) \end{aligned}$$

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{aligned} s(b) \cdot s(n) &= s(b) + (s(b) \cdot n) \\ &= s(b) + (n + (b \cdot n)) \\ &= (s(b) + n) + (b \cdot n) \\ &= (b + s(n)) + (b \cdot n) \\ &= s(n) + (b + (b \cdot n)) \\ &= s(n) + (b \cdot s(n)) \end{aligned}$$

□

Aula 11 - Consequências

Proposição
Valem as seguintes propriedades:

(a) *Dados* $a, b \in \mathbb{N}$, $a \cdot b = b \cdot a$; *(***comutativa***)*

(b) *Dados* $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; *(***distributiva***).*

(c) *Dados* $a, b, c \in \mathbb{N}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; *(***associativa***)*

Aula 11 - Comutativa

Demonstração. Seja $a \in \mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$**:** Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema 11.3).

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$**:** Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema 11.3).

$P(n) \to P(s(n))$**:** Suponha $a \cdot n = n \cdot a$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$**:** Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema 11.3).

$P(n) \to P(s(n))$**:** Suponha $a \cdot n = n \cdot a$. Temos

$$a \cdot s(n) \quad = \quad a + (a \cdot n)$$

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$**:** Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema 11.3).

$P(n) \to P(s(n))$**:** Suponha $a \cdot n = n \cdot a$. Temos

$$\begin{aligned} a \cdot s(n) &= a + (a \cdot n) \\ &= a + (n \cdot a) \end{aligned}$$

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$**:** Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema 11.3).

$P(n) \to P(s(n))$**:** Suponha $a \cdot n = n \cdot a$. Temos

$$\begin{aligned} a \cdot s(n) &= a + (a \cdot n) \\ &= a + (n \cdot a) \\ &\overset{11.4}{=} s(n) \cdot a \end{aligned}$$

Aula 11 - Distributiva

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$.

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$.

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.
Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$.

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.
Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$.
Temos:

$$a \cdot (b + s(n)) \quad = \quad a \cdot (s(b + n))$$

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.
Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$.
Temos:

$$\begin{aligned} a \cdot (b + s(n)) &= a \cdot (s(b + n)) \\ &= a + (a \cdot (b + n)) \end{aligned}$$

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.
Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$.
Temos:

$$\begin{aligned} a \cdot (b + s(n)) &= a \cdot (s(b + n)) \\ &= a + (a \cdot (b + n)) \\ &= a + ((a \cdot b) + (a \cdot n)) \end{aligned}$$

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.
Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$.
Temos:

$$\begin{aligned} a \cdot (b + s(n)) &= a \cdot (s(b + n)) \\ &= a + (a \cdot (b + n)) \\ &= a + ((a \cdot b) + (a \cdot n)) \\ &= (a \cdot b) + (a + (a \cdot n)) \end{aligned}$$

Aula 11 - Distributiva

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado,
$a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$.
Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$.
Temos:

$$\begin{aligned} a \cdot (b + s(n)) &= a \cdot (s(b + n)) \\ &= a + (a \cdot (b + n)) \\ &= a + ((a \cdot b) + (a \cdot n)) \\ &= (a \cdot b) + (a + (a \cdot n)) \\ &= (a \cdot b) + (a \cdot s(n)) \end{aligned}$$

Aula 11 - Associativa

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$.

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.
Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$.

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$. Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado, $a \cdot (b \cdot 0) = a \cdot 0 = 0$.

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.
Vamos mostrar por indução.

$P(0)$**:** Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado,
$a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$**:** Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$.

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.
Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado,
$a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$: Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Temos

$$(a \cdot b) \cdot s(n) \quad = \quad (a \cdot b) + ((a \cdot b) \cdot n)$$

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.
Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado,
$a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$: Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Temos

$$\begin{aligned} (a \cdot b) \cdot s(n) &= (a \cdot b) + ((a \cdot b) \cdot n) \\ &= (a \cdot b) + (a \cdot (b \cdot n)) \end{aligned}$$

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$. Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado, $a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$: Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Temos

$$\begin{aligned} (a \cdot b) \cdot s(n) &= (a \cdot b) + ((a \cdot b) \cdot n) \\ &= (a \cdot b) + (a \cdot (b \cdot n)) \\ &\overset{(dist.)}{=} a \cdot (b + (b \cdot n)) \end{aligned}$$

Aula 11 - Associativa

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$. Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado, $a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$: Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Temos

$$\begin{aligned} (a \cdot b) \cdot s(n) &= (a \cdot b) + ((a \cdot b) \cdot n) \\ &= (a \cdot b) + (a \cdot (b \cdot n)) \\ &\overset{(dist.)}{=} a \cdot (b + (b \cdot n)) \\ &= a \cdot (b \cdot s(n)) \quad \square \end{aligned}$$

Aula 11 - Consequências

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente).

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$. Por outro lado, temos que $a \cdot s(m) = a + (a \cdot m)$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$. Por outro lado, temos que $a \cdot s(m) = a + (a \cdot m)$. Assim, temos que $a + (a \cdot m) = 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$. Por outro lado, temos que $a \cdot s(m) = a + (a \cdot m)$. Assim, temos que $a + (a \cdot m) = 0$. Logo, $a = 0$ e $a \cdot m = 0$.

Proposição
Sejam $a, b \in \mathbb{N}$. *Se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Demonstração.
Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$. Por outro lado, temos que $a \cdot s(m) = a + (a \cdot m)$. Assim, temos que $a + (a \cdot m) = 0$. Logo, $a = 0$ e $a \cdot m = 0$. Em particular, temos que $a = 0$ como queríamos. □

Aula 11 - Consequências

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Demonstração.
Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Demonstração.
Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Demonstração.
Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

$P(n) \to P(s(n))$**:** Suponha que vale $1 \cdot n = n$.

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Demonstração.
Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

$P(n) \to P(s(n))$**:** Suponha que vale $1 \cdot n = n$. Temos:

$$1 \cdot s(n) \quad = \quad 1 + (1 \cdot n)$$

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Demonstração.
Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

$P(n) \to P(s(n))$**:** Suponha que vale $1 \cdot n = n$. Temos:

$$\begin{aligned} 1 \cdot s(n) &= 1 + (1 \cdot n) \\ &= 1 + n \end{aligned}$$

Proposição
Seja $a \in \mathbb{N}$. *Então* $1 \cdot a = a$.

Demonstração.
Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

$P(n) \to P(s(n))$**:** Suponha que vale $1 \cdot n = n$. Temos:

$$\begin{aligned} 1 \cdot s(n) &= 1 + (1 \cdot n) \\ &= 1 + n \\ &= s(n) \end{aligned}$$

□

Aula 11 - Convenção

Aula 11 - Convenção

Para evitar o uso excessivo de parênteses, vamos utilizar as convenções usuais.

Aula 11 - Convenção

Para evitar o uso excessivo de parênteses, vamos utilizar as convenções usuais. Por exemplo, em vez de escrevermos $(a + b) + c$, escreveremos $a + b + c$ (já que pela associativa, não importa como interpretamos a última notação).

Aula 11 - Convenção

Para evitar o uso excessivo de parênteses, vamos utilizar as convenções usuais. Por exemplo, em vez de escrevermos $(a + b) + c$, escreveremos $a + b + c$ (já que pela associativa, não importa como interpretamos a última notação). Também usaremos o "critério de prioridade" do produto sobre a soma.

Aula 11 - Convenção

Para evitar o uso excessivo de parênteses, vamos utilizar as convenções usuais. Por exemplo, em vez de escrevermos $(a + b) + c$, escreveremos $a + b + c$ (já que pela associativa, não importa como interpretamos a última notação). Também usaremos o "critério de prioridade" do produto sobre a soma. Por exemplo, $ab + c$ deverá ser interpretado como $(a \cdot b) + c$.

Aula 11 - A ordem nos naturais

Aula 11 - A ordem nos naturais

Vamos agora definir a ordem sobre os naturais.

Aula 11 - A ordem nos naturais

Vamos agora definir a ordem sobre os naturais.

Definição
Dados $a, b \in \mathbb{N}$, vamos denotar por $a \leq b$ se existe $m \in \mathbb{N}$ tal que $a + m = b$. Esta é a **ordem** usual sobre $\mathbb{N}$.

Aula 11 - De fato é ordem

Aula 11 - De fato é ordem

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$. Assim $b + (k + m) = b + 0$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$. Assim $b + (k + m) = b + 0$. Logo, $k + m = 0$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$. Assim $b + (k + m) = b + 0$. Logo, $k + m = 0$. Temos que $k = m = 0$.

Proposição
A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$. Assim $b + (k + m) = b + 0$. Logo, $k + m = 0$. Temos que $k = m = 0$. Assim, de $a + m = b$ temos que $a = b$ como queríamos.

Aula 11 - Provando

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$.

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$.

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$.

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$a + t \quad = \quad a + (m + k)$$

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$\begin{aligned} a + t &= a + (m + k) \\ &= (a + m) + k \end{aligned}$$

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$\begin{aligned} a + t &= a + (m + k) \\ &= (a + m) + k \\ &= b + k \end{aligned}$$

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$\begin{aligned} a + t &= a + (m + k) \\ &= (a + m) + k \\ &= b + k \\ &= c \end{aligned}$$

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$\begin{aligned} a + t &= a + (m + k) \\ &= (a + m) + k \\ &= b + k \\ &= c \end{aligned}$$

Logo, $a \leq c$. □

Aula 11 - Consequências

Aula 11 - Consequências

Os axiomas de ordem não implicam que, dados dois elementos quaisquer, eles precisam ser comparáveis.

Aula 11 - Consequências

Os axiomas de ordem não implicam que, dados dois elementos quaisquer, eles precisam ser comparáveis. Mas, no caso desta ordem específica que apresentamos, isso vale:

Os axiomas de ordem não implicam que, dados dois elementos quaisquer, eles precisam ser comparáveis. Mas, no caso desta ordem específica que apresentamos, isso vale:

Definição
Dizemos que uma ordem $\preceq$ sobre X é uma **ordem total** sobre X se, dados $a, b \in X$, temos que $a \preceq b$ ou $b \preceq a$.

Aula 11 - Consequências

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \rightarrow a + 1 \leq b$.

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \to a + 1 \leq b$.

Demonstração.

(a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$.

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \to a + 1 \leq b$.

Demonstração.

(a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \to a + 1 \leq b$.

Demonstração.

(a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

(b) Temos que existe $m \in \mathbb{N}$ tal que $a + m = b$, com $m \neq 0$ (pois, se $m = 0$, teríamos $a = b$).

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \to a + 1 \leq b$.

Demonstração.

(a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

(b) Temos que existe $m \in \mathbb{N}$ tal que $a + m = b$, com $m \neq 0$ (pois, se $m = 0$, teríamos $a = b$). Assim, $m = s(n)$.

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \to a + 1 \leq b$.

Demonstração.

(a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

(b) Temos que existe $m \in \mathbb{N}$ tal que $a + m = b$, com $m \neq 0$ (pois, se $m = 0$, teríamos $a = b$). Assim, $m = s(n)$. Logo, $a + s(n) = b$ e, portanto $(a + 1) + n = b$.

Lema

Valem as seguintes afirmações:

(a) *Seja* $a \in \mathbb{N}$. *Então* $a < a + 1$;

(b) *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b \to a + 1 \leq b$.

Demonstração.

(a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

(b) Temos que existe $m \in \mathbb{N}$ tal que $a + m = b$, com $m \neq 0$ (pois, se $m = 0$, teríamos $a = b$). Assim, $m = s(n)$. Logo, $a + s(n) = b$ e, portanto $(a + 1) + n = b$. Isto é, $a + 1 \leq b$.

□

Aula 11 - Consequências

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$.

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a").

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$.

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$).

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$). Vamos mostrar isso por indução.

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$). Vamos mostrar isso por indução. Isto é, considere $P(x)$ a afirmação $C_x = \mathbb{N}$.

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$). Vamos mostrar isso por indução. Isto é, considere $P(x)$ a afirmação $C_x = \mathbb{N}$.

$P(0)$: Note que dado qualquer $m \in \mathbb{N}$, temos que $0 \leq m$ (pois $0 + m = m$).

Proposição
A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$). Vamos mostrar isso por indução. Isto é, considere $P(x)$ a afirmação $C_x = \mathbb{N}$.

$P(0)$: Note que dado qualquer $m \in \mathbb{N}$, temos que $0 \leq m$ (pois $0 + m = m$). Assim, $C_0 = \mathbb{N}$.

Aula 11 - Provando

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$.

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$.

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução).

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução). Assim, temos dois casos:

- Caso $m \leq n$: Como $m \leq n$ e $n < n+1$, temos que $m \leq n+1$ e, portanto, $m \in C_{n+1}$ como queríamos.

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução). Assim, temos dois casos:

- Caso $m \leq n$: Como $m \leq n$ e $n < n+1$, temos que $m \leq n+1$ e, portanto, $m \in C_{n+1}$ como queríamos.
- Caso $n \leq m$: Vamos dividir esse caso em dois.

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução). Assim, temos dois casos:

- Caso $m \leq n$: Como $m \leq n$ e $n < n+1$, temos que $m \leq n+1$ e, portanto, $m \in C_{n+1}$ como queríamos.
- Caso $n \leq m$: Vamos dividir esse caso em dois. Se $n < m$, então $n+1 \leq m$ e, portanto, $m \in C_{n+1}$.

$P(n) \to P(n+1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução). Assim, temos dois casos:

- Caso $m \leq n$: Como $m \leq n$ e $n < n+1$, temos que $m \leq n+1$ e, portanto, $m \in C_{n+1}$ como queríamos.
- Caso $n \leq m$: Vamos dividir esse caso em dois. Se $n < m$, então $n+1 \leq m$ e, portanto, $m \in C_{n+1}$. Se $n = m$, então $m \leq n+1$ e, portanto, $m \in C_{n+1}$.

□

Aula 11 - Consequências

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição
Sejam $a, b, c \in \mathbb{N}$ com $c \neq 0$. Se $ac = bc$, então $a = b$.

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição
Sejam $a, b, c \in \mathbb{N}$ *com* $c \neq 0$. *Se* $ac = bc$, *então* $a = b$.

Demonstração.
Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo).

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição
Sejam $a, b, c \in \mathbb{N}$ com $c \neq 0$. Se $ac = bc$, então $a = b$.

Demonstração.
Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo). Então existem $m \in \mathbb{N}$ tal que $a + m = b$.

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição
Sejam $a, b, c \in \mathbb{N}$ *com* $c \neq 0$. *Se* $ac = bc$, *então* $a = b$.

Demonstração.
Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo). Então existem $m \in \mathbb{N}$ tal que $a + m = b$. Assim, de $ac = bc$, temos que $ac = (a + m)c$.

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição
Sejam $a, b, c \in \mathbb{N}$ *com* $c \neq 0$. *Se* $ac = bc$, *então* $a = b$.

Demonstração.
Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo). Então existem $m \in \mathbb{N}$ tal que $a + m = b$. Assim, de $ac = bc$, temos que $ac = (a + m)c$. Ou seja, $ac = ac + mc$ e, portanto, $mc = 0$.

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição
Sejam $a, b, c \in \mathbb{N}$ com $c \neq 0$. Se $ac = bc$, então $a = b$.

Demonstração.
Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo). Então existem $m \in \mathbb{N}$ tal que $a + m = b$. Assim, de $ac = bc$, temos que $ac = (a + m)c$. Ou seja, $ac = ac + mc$ e, portanto, $mc = 0$. Como $c \neq 0$, temos que $m = 0$ e, portanto, $a = b$ como queríamos. □

Aula 11 - Curiosidade

Aula 11 - Curiosidade

Dizemos que um número $n \in \mathbb{N}$ está escrito recursivamente na base b se n está escrito na base b, cada expoente também está escrito na base b, cada expoente de cada expoente também etc.

Aula 11 - Curiosidade

Dizemos que um número $n \in \mathbb{N}$ está escrito recursivamente na base b se n está escrito na base b, cada expoente também está escrito na base b, cada expoente de cada expoente também etc. Por exemplo, considere o número 521.

Aula 11 - Curiosidade

Dizemos que um número $n \in \mathbb{N}$ está escrito recursivamente na base b se n está escrito na base b, cada expoente também está escrito na base b, cada expoente de cada expoente também etc. Por exemplo, considere o número 521. Ele escrito na base 2 fica

$$521 = 2^9 + 2^3 + 2^0$$

Aula 11 - Curiosidade

Dizemos que um número $n \in \mathbb{N}$ está escrito recursivamente na base b se n está escrito na base b, cada expoente também está escrito na base b, cada expoente de cada expoente também etc. Por exemplo, considere o número 521. Ele escrito na base 2 fica

$$521 = 2^9 + 2^3 + 2^0$$

Mas os expoentes 9 e 3 não estão escritos na base 2, assim, arrumamos:

$$521 = 2^{2^3+2^0} + 2^{2^1+2^0} + 2^0$$

Aula 11 - Curiosidade

Dizemos que um número $n \in \mathbb{N}$ está escrito recursivamente na base b se n está escrito na base b, cada expoente também está escrito na base b, cada expoente de cada expoente também etc. Por exemplo, considere o número 521. Ele escrito na base 2 fica

$$521 = 2^9 + 2^3 + 2^0$$

Mas os expoentes 9 e 3 não estão escritos na base 2, assim, arrumamos:

$$521 = 2^{2^3+2^0} + 2^{2^1+2^0} + 2^0$$

Apareceu um novo 3, daí fazemos:

$$521 = 2^{2^{2^{2^0}+2^0}+2^0} + 2^{2^{2^0}+2^0} + 2^0$$

Agora o processo terminou.

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada.

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;
- a função p_b retorna o valor obtido na conta acima.

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;
- a função p_b retorna o valor obtido na conta acima.

Por exemplo, lembrando que já fizemos a expansão acima,

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;
- a função p_b retorna o valor obtido na conta acima.

Por exemplo, lembrando que já fizemos a expansão acima,

$$p_2(521) = 3^{3^{3^1+3^0}+3^0} + 3^{3^1+3^0} + 3^0$$

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;
- a função p_b retorna o valor obtido na conta acima.

Por exemplo, lembrando que já fizemos a expansão acima,

$$\begin{aligned} p_2(521) &= 3^{3^{3^1+3^0}+3^0} + 3^{3^1+3^0} + 3^0 \\ &= 1.330.279.464.729.113.309.844.748.891.857.449.678.491 \end{aligned}$$

Aula 11 - Generalizando

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;
- a função p_b retorna o valor obtido na conta acima.

Por exemplo, lembrando que já fizemos a expansão acima,

$$\begin{aligned} p_2(521) &= 3^{3^{3^1+3^0}+3^0} + 3^{3^1+3^0} + 3^0 \\ &= 1.330.279.464.729.113.309.844.748.891.857.449.678.491 \\ &\approx 13 \cdot 10^{38} \end{aligned}$$

Aula 11 - Definindo

Aula 11 - Definindo

Essa função pode ser definida formalmente por recursão.

Essa função pode ser definida formalmente por recursão. De posse de tal função (na verdade, de posse de cada p_b), podemos definir a seguinte sequência, dado $k \in \mathbb{N}$:

Essa função pode ser definida formalmente por recursão. De posse de tal função (na verdade, de posse de cada p_b), podemos definir a seguinte sequência, dado $k \in \mathbb{N}$:

- $g_k(1) = k$;

Aula 11 - Definindo

Essa função pode ser definida formalmente por recursão. De posse de tal função (na verdade, de posse de cada p_b), podemos definir a seguinte sequência, dado $k \in \mathbb{N}$:

- $g_k(1) = k$;
- $g_k(n+1) = \begin{cases} p_{n+1}(g_k(n)) - 1 & \text{se } g_k(n) > 0; \\ 0 & \text{caso contrário} \end{cases}$

Essa função pode ser definida formalmente por recursão. De posse de tal função (na verdade, de posse de cada p_b), podemos definir a seguinte sequência, dado $k \in \mathbb{N}$:

- $g_k(1) = k$;
- $g_k(n+1) = \begin{cases} p_{n+1}(g_k(n)) - 1 & \text{se } g_k(n) > 0; \\ 0 & \text{caso contrário} \end{cases}$

Chamamos $g_k(1), g_k(2), g_k(3), \ldots$ de **sequência de Goodstein** de k.

Aula 11 - Exemplos

Vejamos alguns exemplos:

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;
- $g_3(4) = 3$;

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;
- $g_3(4) = 3$;
- $g_3(5) = 2$;

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;
- $g_3(4) = 3$;
- $g_3(5) = 2$;
- $g_3(6) = 1$;

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;
- $g_3(4) = 3$;
- $g_3(5) = 2$;
- $g_3(6) = 1$;
- $g_3(7) = 0$.

Aula 11 - Exemplos

Vejamos alguns exemplos:

Exemplo
Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;
- $g_3(4) = 3$;
- $g_3(5) = 2$;
- $g_3(6) = 1$;
- $g_3(7) = 0$.

Note que uma vez que o valor 0 é atingido, a sequência fica constante.

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;
- $g_4(6) = 83$;

Aula 11 - Exemplos

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;
- $g_4(6) = 83$;
- $g_4(7) = 109$;

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;
- $g_4(6) = 83$;
- $g_4(7) = 109$;
- $g_4(24) = 1151$;

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;
- $g_4(6) = 83$;
- $g_4(7) = 109$;
- $g_4(24) = 1151$;
- $g_4(3 \cdot 2^{402\ 653\ 209}) = 3 \cdot 2^{402\ 653\ 210} - 1$

Exemplo
Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;
- $g_4(6) = 83$;
- $g_4(7) = 109$;
- $g_4(24) = 1151$;
- $g_4(3 \cdot 2^{402\ 653\ 209}) = 3 \cdot 2^{402\ 653\ 210} - 1$
- $g_4(3 \cdot 2^{402\ 653\ 211}) = 0$ (essa é a primeira vez que tal função dá 0)

Aula 11 - Desfecho

Aula 11 - Desfecho

Na verdade, pode-se provar:

Na verdade, pode-se provar:

Teorema (Goodstein)
Dado $k \geq 1$, existe $n \in \mathbb{N}$ tal que $g_k(n) = 0$.

Na verdade, pode-se provar:

Teorema (Goodstein)
Dado $k \geq 1$, existe $n \in \mathbb{N}$ tal que $g_k(n) = 0$.

Talvez o mais interessante aqui é que o teorema acima é impossível de ser provado só com o uso dos axiomas de Peano aqui apresentados - ou seja, sua afirmação é uma afirmação independente de tais axiomas (ver, por exemplo, Seção 10.2 de [**?**]).

Aula 12 - Números inteiros

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7).

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$. Veremos no que se segue que fazer essa representação nos facilita muitos casos.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$. Veremos no que se segue que fazer essa representação nos facilita muitos casos. Mas ela tem um incoveniente: por exemplo, os pares $(4, 1)$ e $(7, 4)$ representam ambos o número 3.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$. Veremos no que se segue que fazer essa representação nos facilita muitos casos. Mas ela tem um incoveniente: por exemplo, os pares $(4, 1)$ e $(7, 4)$ representam ambos o número 3. Veremos em seguida uma maneira de lidar com essa repetição.

Aula 12 - Números inteiros

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$. Veremos no que se segue que fazer essa representação nos facilita muitos casos. Mas ela tem um incoveniente: por exemplo, os pares $(4, 1)$ e $(7, 4)$ representam ambos o número 3. Veremos em seguida uma maneira de lidar com essa repetição. Tal método nos será útil em muitas outras situações.

Aula 12 - Relações de equivalência

Definição
Seja X um conjunto. Dizemos que uma relação $\sim$ é uma **relação de equivalência** se são satisfeitas:

(a) Para todo $x \in X$, temos que $x \sim x$; (**reflexiva**)

(b) Para todos $x, y \in X$, temos que $x \sim y \to y \sim x$; (**simétrica**)

(c) Para todos $x, y, z \in X$, temos que $(x \sim y \wedge y \sim z) \to x \sim z$. (**transitiva**)

Aula 12 - Exemplos

Exemplo
A igualdade é uma relação de equivalência sobre um conjunto X, já que, para todo $x \in X$ temos que $x = x$.

Exemplo
A igualdade é uma relação de equivalência sobre um conjunto X, já que, para todo $x \in X$ temos que $x = x$. Também temos que se $x = y$ então $y = x$ para quaisquer $x, y \in X$.

Exemplo
A igualdade é uma relação de equivalência sobre um conjunto X, já que, para todo $x \in X$ temos que $x = x$. Também temos que se $x = y$ então $y = x$ para quaisquer $x, y \in X$. E, por último, temos que se $x = y$ e $y = z$, então $x = z$ para todo $x, y, z \in X$.

Aula 12 - Exemplos

Exemplo
Dados $a, b \in \mathbb{N}$, dizemos que $a \sim b$ se o conjunto dos divisores primos de a e de b são iguais.

Exemplo
Dados $a, b \in \mathbb{N}$, dizemos que $a \sim b$ se o conjunto dos divisores primos de a e de b são iguais. Por exemplo, temos que $6 \sim 12$ já que os divisores primos de ambos são $\{2, 3\}$.

Exemplo
Dados $a, b \in \mathbb{N}$, dizemos que $a \sim b$ se o conjunto dos divisores primos de a e de b são iguais. Por exemplo, temos que $6 \sim 12$ já que os divisores primos de ambos são $\{2, 3\}$. Note que tal relação é uma relação de equivalência (exercício).

Aula 12 - Exemplos

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

(c) Sejam $a, b, c \in X$.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

(c) Sejam $a, b, c \in X$. Suponha $a \sim b$ e $b \sim c$.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

(c) Sejam $a, b, c \in X$. Suponha $a \sim b$ e $b \sim c$. Então $f(a) = f(b)$ e $f(b) = f(c)$.

Proposição

Seja $f : X \to Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.

Demonstração.
Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

(c) Sejam $a, b, c \in X$. Suponha $a \sim b$ e $b \sim c$. Então $f(a) = f(b)$ e $f(b) = f(c)$. Assim $f(a) = f(c)$ e, portanto, $a \sim c$ como queríamos.

Aula 12 - Classe de equivalência

Definição
Seja X um conjunto e $\sim$ uma relação de equivalência sobre X. Dado $x \in X$, denotamos por $[x]$ (ou $\overline{x}$) o conjunto $\{y \in X : y \sim x\}$ (**classe de equivalência** de x). Denotamos por $X/\sim$ o conjunto de todas as classes de equivalência, isto é, $X/\sim = \{[x] : x \in X\}$.

Aula 12 - Consequências

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$. Como $x \sim b$, temos que $y \sim b$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$. Como $x \sim b$, temos que $y \sim b$. Logo, $y \in [b]$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$. Como $x \sim b$, temos que $y \sim b$. Logo, $y \in [b]$. Assim mostramos que $[a] \subset [b]$.

Lema

Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.

Demonstração.
Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$. Como $x \sim b$, temos que $y \sim b$. Logo, $y \in [b]$. Assim mostramos que $[a] \subset [b]$. Analogamente, mostramos que $[b] \subset [a]$ (exercício). $\square$

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que isso não ocorre.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que isso não ocorre. Seja $b \in [a]$.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que isso não ocorre. Seja $b \in [a]$. Então $b \sim a$.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que isso não ocorre. Seja $b \in [a]$. Então $b \sim a$. Logo, $f(b) = f(a)$.

Proposição

Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que isso não ocorre. Seja $b \in [a]$. Então $b \sim a$. Logo, $f(b) = f(a)$. Assim, dado qualquer representante b da classe $[a]$, $\tilde{f}([a]) = f(a) = f(b)$.

Vamos agora mostrar que tal função é, de fato, injetora.

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$.

Aula 12 - Provando

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$.

Aula 12 - Provando

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$. Vamos mostrar que $[a] = [b]$.

Aula 12 - Provando

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$. Vamos mostrar que $[a] = [b]$. Note que temos $f(a) = f(b)$.

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$. Vamos mostrar que $[a] = [b]$. Note que temos $f(a) = f(b)$. Logo, $a \sim b$ e, portanto, $b \in [a]$.

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$. Vamos mostrar que $[a] = [b]$. Note que temos $f(a) = f(b)$. Logo, $a \sim b$ e, portanto, $b \in [a]$. Pelo Lema 12.6, temos que $[a] = [b]$. $\square$

Aula 12 - Partições

Definição
Seja X um conjunto. Chamamos uma família $\mathcal{F}$ de subconjuntos de X de uma **partição** de X se são satisfeitas:

(a) $\bigcup_{F \in \mathcal{F}} F = X$;

(b) Se $A, B \in \mathcal{F}$ são distintos, então $A \cap B = \emptyset$.

Aula 12 - Relacionando

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$.

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$.

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$. Logo, $x \sim x$ (pois $x \in F$).

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$. Logo, $x \sim x$ (pois $x \in F$).
- Sejam $x, y \in X$ tais que $x \sim y$.

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$. Logo, $x \sim x$ (pois $x \in F$).
- Sejam $x, y \in X$ tais que $x \sim y$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$.

Proposição

Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de **relação de equivalência induzida** *por $\mathcal{F}$.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$. Logo, $x \sim x$ (pois $x \in F$).
- Sejam $x, y \in X$ tais que $x \sim y$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$. Logo, $y \sim x$.

Aula 12 - Provando

Aula 12 - Provando

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$.

Aula 12 - Provando

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$.

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$. Note que $y \in F \cap G$.

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$. Note que $y \in F \cap G$. Pelo axioma (b) de partição, se F e G fossem distintos, teríamos $F \cap G = \emptyset$.

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$. Note que $y \in F \cap G$. Pelo axioma (b) de partição, se F e G fossem distintos, teríamos $F \cap G = \emptyset$. Logo, $F = G$.

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$. Note que $y \in F \cap G$. Pelo axioma (b) de partição, se F e G fossem distintos, teríamos $F \cap G = \emptyset$. Logo, $F = G$. Assim, $x, y, z \in F$ e, portanto, $x \sim z$.

□

Aula 12 - Números inteiros

Proposição

Considere a relação $\sim$ *sobre* $\mathbb{N}^2$ *dada por*

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. *Então* $\sim$ *é uma relação de equivalência sobre* $\mathbb{N}^2$.

Proposição
Considere a relação $\sim$ *sobre* $\mathbb{N}^2$ *dada por*

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. *Então* $\sim$ *é uma relação de equivalência sobre* $\mathbb{N}^2$.

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

Proposição
Considere a relação $\sim$ sobre $\mathbb{N}^2$ dada por

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. Então $\sim$ é uma relação de equivalência sobre $\mathbb{N}^2$.

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

- Seja $(a, b) \in \mathbb{N}^2$.

Proposição
Considere a relação $\sim$ *sobre* $\mathbb{N}^2$ *dada por*

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. *Então* $\sim$ *é uma relação de equivalência sobre* $\mathbb{N}^2$.

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

- Seja $(a, b) \in \mathbb{N}^2$. Temos que $a + b = a + b$, logo $(a, b) \sim (a, b)$.

Proposição
Considere a relação $\sim$ sobre $\mathbb{N}^2$ dada por

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. Então $\sim$ é uma relação de equivalência sobre $\mathbb{N}^2$.

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

- Seja $(a, b) \in \mathbb{N}^2$. Temos que $a + b = a + b$, logo $(a, b) \sim (a, b)$.
- Sejam $(a, b), (c, d) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$.

Proposição
Considere a relação $\sim$ sobre $\mathbb{N}^2$ dada por

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. Então $\sim$ é uma relação de equivalência sobre $\mathbb{N}^2$.

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

- Seja $(a, b) \in \mathbb{N}^2$. Temos que $a + b = a + b$, logo $(a, b) \sim (a, b)$.
- Sejam $(a, b), (c, d) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$. Temos que $c + b = a + d$, logo $(c, d) \sim (a, b)$.

Aula 12 - Provando

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$.

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$.

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$.

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$. Também temos que $c + f = e + d$.

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$. Também temos que $c + f = e + d$. Logo, temos $c + f + b = e + d + b$.

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$. Também temos que $c + f = e + d$. Logo, temos $c + f + b = e + d + b$. Desta forma obtemos $a + d + f = e + d + b$ e, portanto, $a + f = e + b$.

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$. Também temos que $c + f = e + d$. Logo, temos $c + f + b = e + d + b$. Desta forma obtemos $a + d + f = e + d + b$ e, portanto, $a + f = e + b$. Isto é, $(a, b) \sim (e, f)$.

□

Aula 12 - Números inteiros

Definição
Chamamos de $\mathbb{Z}$ o conjunto $\mathbb{N}^2/\sim$ onde $\sim$ é a relação de equivalência definida no item anterior. Cada elemento de $\mathbb{Z}$ é chamado de **número inteiro**.

Aula 12 - Somando

Definição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$. Definimos
$[(a,b)] + [(c,d)] = [(a+c, b+d)]$ (**soma nos inteiros**).

Aula 12 - Somando

Proposição

A operação de soma está bem definida.

Proposição

A operação de soma está bem definida.

Demonstração.
Precisamos mostrar que tal definição independe dos representantes de classe tomados.

Proposição

A operação de soma está bem definida.

Demonstração.
Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$ então $(a + c, b + d) \sim (x + w, y + z)$.

Proposição

A operação de soma está bem definida.

Demonstração.
Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$ então $(a + c, b + d) \sim (x + w, y + z)$. Temos que $a + y = b + x$ e que $c + z = d + w$.

Proposição

A operação de soma está bem definida.

Demonstração.
Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$ então $(a + c, b + d) \sim (x + w, y + z)$. Temos que $a + y = b + x$ e que $c + z = d + w$. Assim

$$(a + c) + (y + z) \quad = \quad (a + y) + (c + z)$$

Proposição

A operação de soma está bem definida.

Demonstração.
Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$ então $(a + c, b + d) \sim (x + w, y + z)$. Temos que $a + y = b + x$ e que $c + z = d + w$. Assim

$$\begin{aligned} (a + c) + (y + z) &= (a + y) + (c + z) \\ &= (b + x) + (d + w) \end{aligned}$$

Proposição

A operação de soma está bem definida.

Demonstração.
Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$ então $(a + c, b + d) \sim (x + w, y + z)$. Temos que $a + y = b + x$ e que $c + z = d + w$. Assim

$$\begin{aligned}(a + c) + (y + z) &= (a + y) + (c + z) \\ &= (b + x) + (d + w) \\ &= (b + d) + (x + w)\end{aligned}$$

□

Aula 12 - Propriedades básicas

Aula 12 - Propriedades básicas

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Demonstração.
Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício.

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Demonstração.
Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício. Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Demonstração.
Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Vamos mostrar que $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$.

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Demonstração.
Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Vamos mostrar que $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$. Temos

$$[(a,b)] + [(c,d)] \quad = \quad [(a+c, b+d)]$$

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Demonstração.
Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Vamos mostrar que $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$. Temos

$$\begin{aligned} [(a,b)] + [(c,d)] &= [(a+c, b+d)] \\ &= [(c+a, d+b)] \end{aligned}$$

Proposição
Temos que a soma satisfaz as seguintes propriedades:

(a) *Comutativa;*

(b) *Associativa;*

Demonstração.
Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Vamos mostrar que $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$. Temos

$$\begin{aligned} [(a,b)] + [(c,d)] &= [(a+c, b+d)] \\ &= [(c+a, d+b)] \\ &= [(c,d)] + [(a,b)] \end{aligned}$$

□

Aula 12 - Propriedades básicas

Proposição
Para qualquer $[(a, b)] \in \mathbb{Z}$, *temos que* $[(a, b)] + [(0, 0)] = [(a, b)]$

Proposição
Para qualquer $[(a,b)] \in \mathbb{Z}$*, temos que* $[(a,b)] + [(0,0)] = [(a,b)]$

Demonstração.
Basta notar que $(a+0, b+0) \sim (a,b)$, já que
$a+0+b = b+0+a$. $\square$

Aula 12 - Propriedades básicas

Proposição (Lei do Cancelamento)
Sejam $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$. *Se*
$[(a,b)]+[(x,y)] = [(c,d)]+[(x,y)]$, *então* $[(a,b)] = [(c,d)]$.

Proposição (Lei do Cancelamento)
Sejam $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$. *Se*
$[(a,b)]+[(x,y)] = [(c,d)]+[(x,y)]$, *então* $[(a,b)] = [(c,d)]$.

Demonstração.
Temos que $[(a+x, b+y)] = [(c+x, d+y]]$.

Proposição (Lei do Cancelamento)
Sejam $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$. *Se*
$[(a,b)]+[(x,y)] = [(c,d)]+[(x,y)]$, *então* $[(a,b)] = [(c,d)]$.

Demonstração.
Temos que $[(a+x, b+y)] = [(c+x, d+y]]$. Assim,
$a+x+d+y = b+y+c+x$.

Proposição (Lei do Cancelamento)
Sejam $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$. *Se*
$[(a,b)]+[(x,y)]=[(c,d)]+[(x,y)]$, *então* $[(a,b)]=[(c,d)]$.

Demonstração.
Temos que $[(a+x,b+y)]=[(c+x,d+y]]$. Assim,
$a+x+d+y=b+y+c+x$. Assim, cancelando $x+y$, temos
$a+d=b+c$, isto é, $(a,b)\sim(c,d)$. □

Aula 12 - Multiplicando

Definição
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Definimos $[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$. Este é o **produto nos inteiros**. Assim como fizemos com $\mathbb{N}$, omitiremos o sinal $\cdot$ normalmente.

Aula 12 - Consequências

Proposição
A operação de produto está bem definida.

Aula 12 - Propriedades básicas

Proposição
Valem as seguintes propriedades para o produto.

(a) *Associativa;*

(b) *Comutativa;*

Aula 12 - Propriedades básicas

Proposição

Vale a propriedade distributiva entre a soma e o produto em $\mathbb{Z}$.

Isto é, dados $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$, *temos que*

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

Proposição
Vale a propriedade distributiva entre a soma e o produto em $\mathbb{Z}$.
Isto é, dados $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$, temos que

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

Demonstração.
Temos

$$[(x,y)]([(a,b)+(c,d)]) \quad = \quad [(x,y)][(a+c,b+d)]$$

Proposição
Vale a propriedade distributiva entre a soma e o produto em $\mathbb{Z}$.
Isto é, dados $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$, temos que

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

Demonstração.
Temos

$$\begin{aligned} [(x,y)]([(a,b)+(c,d)]) &= [(x,y)][(a+c,b+d)] \\ &= [(x(a+c)+y(b+d), x(b+d)+y(a+c \end{aligned}$$

Proposição
Vale a propriedade distributiva entre a soma e o produto em $\mathbb{Z}$.
Isto é, dados $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$, *temos que*

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

Demonstração.
Temos

$$\begin{aligned}
[(x,y)]([(a,b)+(c,d)]) &= [(x,y)][(a+c,b+d)] \\
&= [(x(a+c)+y(b+d), x(b+d)+y(a+c)] \\
&= [(xa+xc+yb+yd, xb+xd+ya+yc)] \\
&= [(xa+yb, xb+ya)] + [(xc+yd, xd+yc)]
\end{aligned}$$

Proposição
Vale a propriedade distributiva entre a soma e o produto em $\mathbb{Z}$.
Isto é, dados $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$, temos que

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

Demonstração.
Temos

$$\begin{aligned}
[(x,y)]([(a,b)+(c,d)]) &= [(x,y)][(a+c,b+d)] \\
&= [(x(a+c)+y(b+d), x(b+d)+y(a+c)] \\
&= [(xa+xc+yb+yd, xb+xd+ya+yc)] \\
&= [(xa+yb, xb+ya)] + [(xc+yd, xd+yc)] \\
&= ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])
\end{aligned}$$

□

Aula 12 - Propriedades básicas

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então* $[(1,0)][(a,b)] = [(a,b)]$.

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então* $[(1,0)][(a,b)] = [(a,b)]$.

Demonstração.
Temos $[(a,b)][(1,0)] = [(a1 + b0, a0 + b1)] = [(a,b)]$. $\square$

Aula 13 - Forma canônica

Proposição
Seja $[(a, b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a, b)] = [(x, 0)]$ *ou* $[(a, b)] = [(0, x)]$.

Proposição
Seja $[(a, b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a, b)] = [(x, 0)]$ *ou* $[(a, b)] = [(0, x)]$.

Demonstração.
Vamos separar em 3 casos:

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração.
Vamos separar em 3 casos:

$a = b$**:** Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração.
Vamos separar em 3 casos:

- $a = b$**:** Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$
- $a < b$**:** Seja $m \in \mathbb{N}$ tal que $a + m = b$. Vamos mostrar que $(a,b) \sim (0,m)$. De fato, temos que $a + m = b + 0$.

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração.
Vamos separar em 3 casos:

- $a = b$**:** Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$
- $a < b$**:** Seja $m \in \mathbb{N}$ tal que $a + m = b$. Vamos mostrar que $(a,b) \sim (0,m)$. De fato, temos que $a + m = b + 0$.
- $b < a$**:** Seja $m \in \mathbb{N}$ tal que $b + m = 0$.

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração.
Vamos separar em 3 casos:

- $a = b$**:** Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$
- $a < b$**:** Seja $m \in \mathbb{N}$ tal que $a + m = b$. Vamos mostrar que $(a,b) \sim (0,m)$. De fato, temos que $a + m = b + 0$.
- $b < a$**:** Seja $m \in \mathbb{N}$ tal que $b + m = 0$. Vamos mostrar que $(a,b) \sim (m,0)$.

Proposição
Seja $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração.
Vamos separar em 3 casos:

- $a = b$: Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$
- $a < b$: Seja $m \in \mathbb{N}$ tal que $a + m = b$. Vamos mostrar que $(a,b) \sim (0,m)$. De fato, temos que $a + m = b + 0$.
- $b < a$: Seja $m \in \mathbb{N}$ tal que $b + m = 0$. Vamos mostrar que $(a,b) \sim (m,0)$. De fato, temos que $a + 0 = b + m$.

□

Aula 13 - Forma canônica

Definição
Dizemos que um elemento de $\mathbb{Z}$ está escrito na **forma canônica** se ele está escrito na forma $[(x, 0)]$ ou $[(0, x)]$. Pelo resultado anterior, temos que todo elemento pode ser escrito na forma canônica. Note que tal representação é única .

Aula 13 - Aplicando

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$.

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos.

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos. Vamos mostrar 2, deixando os outros dois como exercício:

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos. Vamos mostrar 2, deixando os outros dois como exercício:

- Pela definição do produto, temos $[(x,0)][(y,0)] = [(xy,0)]$.

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos. Vamos mostrar 2, deixando os outros dois como exercício:

- Pela definição do produto, temos $[(x,0)][(y,0)] = [(xy,0)]$. De $[(xy,0)] = [(0,0)]$, temos que $xy = 0$.

Aula 13 - Aplicando

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos. Vamos mostrar 2, deixando os outros dois como exercício:

- Pela definição do produto, temos $[(x,0)][(y,0)] = [(xy,0)]$. De $[(xy,0)] = [(0,0)]$, temos que $xy = 0$. Logo, $x = 0$ ou $y = 0$ e, portanto, $[(a,b)] = [(0,0)]$ ou $[(c,d)] = [(0,0)]$.

Aula 13 - Provando

- Pela definição do produto, temos que $[(x, 0)][(0, y)] = [(0, xy)]$.

- Pela definição do produto, temos que $[(x, 0)][(0, y)] = [(0, xy)]$. Como no caso anterior, temos que $xy = 0$ e, portanto, $x = 0$ ou $y = 0$.

- Pela definição do produto, temos que $[(x,0)][(0,y)] = [(0,xy)]$. Como no caso anterior, temos que $xy = 0$ e, portanto, $x = 0$ ou $y = 0$. Assim $[(a,b)] = [(0,0)]$ ou $[(c,d)] = [(0,0)]$.

□

Aula 13 - Ordem

Definição
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Dizemos que $[(a,b)] \leq [(c,d)]$ se, e somente se, ocorre um dos seguintes casos:

- $[(a,b)] = [(x,0)]$, $[(c,d)] = [(y,0)]$ e $x \leq y$;
- $[(a,b)] = [(0,x)]$, $[(c,d)] = [(y,0)]$;
- $[(a,b)] = [(0,x)]$, $[(c,d)] = [(0,y)]$ e $y \leq x$.

Esta é a **ordem usual sobre os inteiros**.

Aula 13 - É total

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$. Temos que mostrar que $[(a, b)] \leq [(c, d)]$ ou $[(c, d)] \leq [(a, b)]$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$. Se $x \leq y$, temos que $[(x,0)] \leq [(y,0)]$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$. Se $x \leq y$, temos que $[(x,0)] \leq [(y,0)]$. Caso contrário, temos que $y \leq x$ e, portanto, $[(y,0)] \leq [(x,0)]$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$. Se $x \leq y$, temos que $[(x,0)] \leq [(y,0)]$. Caso contrário, temos que $y \leq x$ e, portanto, $[(y,0)] \leq [(x,0)]$.
- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(0,y)]$, então $[(0,y)] \leq [(x,0)]$.

Aula 13 - É total

Proposição
A ordem sobre os inteiros é total.

Demonstração.
Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$. Se $x \leq y$, temos que $[(x,0)] \leq [(y,0)]$. Caso contrário, temos que $y \leq x$ e, portanto, $[(y,0)] \leq [(x,0)]$.
- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(0,y)]$, então $[(0,y)] \leq [(x,0)]$.

Os outros casos são análogos. □

Aula 13 - Notações

Definição
Denotamos por x o elemento $[(x, 0)]$. Denotamos por $-x$ o elemento $[(0, x)]$. Assim, denotamos por $x + (-y)$ o elemento $[(x, 0)] + [(0, y)]$. Muitas vezes, omitimos o $+$, ficando apenas $x - y$. Chamamos de **positivo** um elemento da forma $[(x, 0)]$ e de **negativo** um da forma $[(0, y)]$.

Aula 13 - Regras de sinal

Aula 13 - Regras de sinal

Proposição

(a) *O produto de dois positivos é positivo;*

(b) *O produto de dois negativos é positivo;*

(c) *O produto de um positivo com um negativo é negativo;*

Aula 13 - Regras de sinal

Proposição

(a) *O produto de dois positivos é positivo;*

(b) *O produto de dois negativos é positivo;*

(c) *O produto de um positivo com um negativo é negativo;*

Demonstração.
Sejam $a, b \in \mathbb{N}$.

Aula 13 - Regras de sinal

Proposição

(a) *O produto de dois positivos é positivo;*

(b) *O produto de dois negativos é positivo;*

(c) *O produto de um positivo com um negativo é negativo;*

Demonstração.
Sejam $a, b \in \mathbb{N}$.

(a) Temos que $[(a,0)][(b,0)] = [(ab,0)]$;

Aula 13 - Regras de sinal

Proposição

(a) *O produto de dois positivos é positivo;*

(b) *O produto de dois negativos é positivo;*

(c) *O produto de um positivo com um negativo é negativo;*

Demonstração.
Sejam $a, b \in \mathbb{N}$.

(a) Temos que $[(a,0)][(b,0)] = [(ab,0)]$;

(b) Temos que $[(0,a)][(0,b)] = [(ab,0)]$;

Proposição

(a) *O produto de dois positivos é positivo;*

(b) *O produto de dois negativos é positivo;*

(c) *O produto de um positivo com um negativo é negativo;*

Demonstração.
Sejam $a, b \in \mathbb{N}$.

(a) Temos que $[(a,0)][(b,0)] = [(ab,0)]$;

(b) Temos que $[(0,a)][(0,b)] = [(ab,0)]$;

(c) Temos que $[(a,0)][(0,b)] = [(0,ab)]$.

□

Aula 13 - Notação

Aula 13 - Notação

Definição
Dado $[(a, b)] \in \mathbb{Z}$, denotamos por $-[(a, b)]$ o elemento $[(b, a)]$.

Aula 13 - Propriedades básicas

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. *Temos:*

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$. Temos

$$a(-b) \quad = \quad [(x, y)](-([w, z]))$$

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$. Temos

$$\begin{aligned} a(-b) &= [(x, y)](-([w, z])) \\ &= [(x, y)][(z, w)] \end{aligned}$$

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$. Temos

$$\begin{aligned} a(-b) &= [(x, y)](-([w, z])) \\ &= [(x, y)][(z, w)] \\ &= [(xz + yw, xw + yz)] \end{aligned}$$

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$. Temos

$$\begin{aligned} a(-b) &= [(x, y)](-([w, z])) \\ &= [(x, y)][(z, w)] \\ &= [(xz + yw, xw + yz)] \\ &= -[(xw + yz, xz + yw)] \end{aligned}$$

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos:

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração.

(a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$. Temos

$$\begin{aligned} a(-b) &= [(x, y)](-([w, z])) \\ &= [(x, y)][(z, w)] \\ &= [(xz + yw, xw + yz)] \\ &= -[(xw + yz, xz + yw)] \\ &= -([(x, y)][(w, z)]) \end{aligned}$$

□

Aula 13 - Propriedades básicas

Proposição
Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.

Proposição
Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.

Demonstração.
Suponha z positivo.

Proposição
Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.

Demonstração.
Suponha z positivo. Então existe $a \in \mathbb{N}$ tal que $z = [(a, 0)]$.

Proposição
Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.

Demonstração.
Suponha z positivo. Então existe $a \in \mathbb{N}$ tal que $z = [(a, 0)]$.
Assim, $-z = -[(a, 0)] = [(0, a)]$ e, portanto, é negativo.

Proposição
Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.

Demonstração.
Suponha z positivo. Então existe $a \in \mathbb{N}$ tal que $z = [(a, 0)]$.
Assim, $-z = -[(a, 0)] = [(0, a)]$ e, portanto, é negativo.

Por outro lado, se $-z$ é negativo, existe $a \in \mathbb{N}$ tal que $-z = [(0, a)]$.

Proposição
Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.

Demonstração.
Suponha z positivo. Então existe $a \in \mathbb{N}$ tal que $z = [(a, 0)]$.
Assim, $-z = -[(a, 0)] = [(0, a)]$ e, portanto, é negativo.

Por outro lado, se $-z$ é negativo, existe $a \in \mathbb{N}$ tal que $-z = [(0, a)]$. Logo, $z = -(-z) = -[(0, a)] = [(a, 0)]$ é positivo. □

Aula 13 - Notação

Aula 13 - Notação

Vamos identificar $\mathbb{N} = \{z \in \mathbb{Z} : z \geq 0\}$ da maneira usual.

Aula 13 - Divisibilidade

Definição
Dados $a, b \in \mathbb{Z}$, dizemos que a **divide** b (e denotamos por $a|b$) se existe $m \in \mathbb{Z}$ tal que $am = b$.

Aula 13 - Propriedades básicas

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b, c \in \mathbb{Z}$. *Temos:*

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

(a) Basta notar que $1a = a$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

(a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

(a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

(c) Basta notar que $a1 = a$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

(a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

(c) Basta notar que $a1 = a$.

(d) Seja $m \in \mathbb{Z}$ tal que $am = b$.

Proposição
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

(a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

(c) Basta notar que $a1 = a$.

(d) Seja $m \in \mathbb{Z}$ tal que $am = b$. Seja $n \in \mathbb{Z}$ tal que $bn = c$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) *Se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração.

(a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

(c) Basta notar que $a1 = a$.

(d) Seja $m \in \mathbb{Z}$ tal que $am = b$. Seja $n \in \mathbb{Z}$ tal que $bn = c$.
Vamos provar que $a(mn) = c$. De fato,
$a(mn) = (am)n = bn = c$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. *Então* $ab = (-a)(-b)$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Então $ab = (-a)(-b)$.

Demonstração.
Temos $(-a)(-b) = (-1a)(-1b) = (-1)(-1)(a)(b) = ab$. □

Aula 13 - Diferenças entre casos

Aula 13 - Diferenças entre casos

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$).

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$. Assim, temos que $a \leq 1$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$, *então* $a = b = 1$.

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$. Assim, temos que $a \leq 1$. Como $a \in \mathbb{N}$, temos $a = 0$ ou $a = 1$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$*, então* $a = b = 1$*.*

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$. Assim, temos que $a \leq 1$. Como $a \in \mathbb{N}$, temos $a = 0$ ou $a = 1$. Como $a \neq 0$ (pois $0b = 0 \neq 1$), temos que $a = 1$.

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema
Se $a, b \in \mathbb{N}$ *são tais que* $ab = 1$*, então* $a = b = 1$*.*

Demonstração.
Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$. Assim, temos que $a \leq 1$. Como $a \in \mathbb{N}$, temos $a = 0$ ou $a = 1$. Como $a \neq 0$ (pois $0b = 0 \neq 1$), temos que $a = 1$. Como $1b = 1 \cdot 1$, temos, pela lei do cancelamento, que $b = 1$. □

Aula 13 - Diferenças entre casos

Aula 13 - Diferenças entre casos

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Aula 13 - Diferenças entre casos

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema
Se $a, b \in \mathbb{Z}$ *são tais que* $ab = 1$, *então* $a = b = 1$ *ou* $a = b = -1$.

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema
Se $a, b \in \mathbb{Z}$ *são tais que* $ab = 1$, *então* $a = b = 1$ *ou* $a = b = -1$.

Demonstração. Temos 3 casos: a, b são positivos, a, b são negativos e o terceiro caso é o que um é positivo e o outro é negativo (neste último caso, podemos supor sem problemas que a é positivo e b é negativo).

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema
Se $a, b \in \mathbb{Z}$ *são tais que* $ab = 1$, *então* $a = b = 1$ *ou* $a = b = -1$.

Demonstração. Temos 3 casos: a, b são positivos, a, b são negativos e o terceiro caso é o que um é positivo e o outro é negativo (neste último caso, podemos supor sem problemas que a é positivo e b é negativo). Note também que, claramente, a, $b \neq 0$.

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema
Se $a, b \in \mathbb{Z}$ são tais que $ab = 1$, então $a = b = 1$ ou $a = b = -1$.

Demonstração. Temos 3 casos: a, b são positivos, a, b são negativos e o terceiro caso é o que um é positivo e o outro é negativo (neste último caso, podemos supor sem problemas que a é positivo e b é negativo). Note também que, claramente, a, $b \neq 0$.

- $a, b > 0$.

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema
Se $a, b \in \mathbb{Z}$ *são tais que* $ab = 1$, *então* $a = b = 1$ *ou* $a = b = -1$.

Demonstração. Temos 3 casos: a, b são positivos, a, b são negativos e o terceiro caso é o que um é positivo e o outro é negativo (neste último caso, podemos supor sem problemas que a é positivo e b é negativo). Note também que, claramente, a, $b \neq 0$.

- $a, b > 0$. Neste caso, pelo lema anterior, temos que $a, b = 1$.

Aula 13 - Provando

Aula 13 - Provando

- $a, b < 0$.

- $a, b < 0$. Note que

$$1 = ab$$

- $a, b < 0$. Note que

$$\begin{aligned} 1 &= ab \\ &= (-a)(-b) \end{aligned}$$

- $a, b < 0$. Note que

$$\begin{aligned} 1 &= ab \\ &= (-a)(-b) \end{aligned}$$

Como $(-a), (-b)$ são positivos, temos que $-a, -b = 1$ e, portanto, $a, b = -1$.

- $a, b < 0$. Note que

$$\begin{aligned} 1 &= ab \\ &= (-a)(-b) \end{aligned}$$

  Como $(-a), (-b)$ são positivos, temos que $-a, -b = 1$ e, portanto, $a, b = -1$.

- $a > 0$ e $b < 0$.

- $a, b < 0$. Note que

$$\begin{aligned} 1 &= ab \\ &= (-a)(-b) \end{aligned}$$

  Como $(-a), (-b)$ são positivos, temos que $-a, -b = 1$ e, portanto, $a, b = -1$.

- $a > 0$ e $b < 0$. Note que, neste caso, $ab < 0$ e, portanto, não pode ser 1 (ou seja, esse caso era impossível de ocorrer).

□

Aula 13 - Diferenças entre casos

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$. De $b|a$, temos que existe n tal que $bn = a$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$. De $b|a$, temos que existe n tal que $bn = a$. Assim, de $am = b$, temos que $(bn)m = b$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$. De $b|a$, temos que existe n tal que $bn = a$. Assim, de $am = b$, temos que $(bn)m = b$. Como $b \neq 0$, pela lei do cancelamento, temos que $nm = 1$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.

Demonstração.
Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$. De $b|a$, temos que existe n tal que $bn = a$. Assim, de $am = b$, temos que $(bn)m = b$. Como $b \neq 0$, pela lei do cancelamento, temos que $nm = 1$. Pelo lema anterior, $n = m = 1$ ou $n = m = -1$ e temos o resultado. □

Aula 13 - Menor elemento

Aula 13 - Menor elemento

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$.

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$. Como $S \neq \emptyset$, temos que existe $s \in S$.

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$. Como $S \neq \emptyset$, temos que existe $s \in S$. Note que $s + 1 \notin M$.

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$. Como $S \neq \emptyset$, temos que existe $s \in S$. Note que $s + 1 \notin M$. Logo, $M \neq \mathbb{N}$.

Teorema (Princípio do menor elemento)
Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$. Como $S \neq \emptyset$, temos que existe $s \in S$. Note que $s + 1 \notin M$. Logo, $M \neq \mathbb{N}$. Considere a propriedade $P(x)$ como

$$x \in M.$$

Aula 13 - Provando

Note que temos $P(0)$.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer).

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$. Suponha que não.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$. Suponha que não. Então vale que, para qualquer $s \in S$, $n < s$.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$. Suponha que não. Então vale que, para qualquer $s \in S$, $n < s$. Logo, $n+1 \leq s$ (pelo Lema 11.11) para qualquer $s \in S$.

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$. Suponha que não. Então vale que, para qualquer $s \in S$, $n < s$. Logo, $n+1 \leq s$ (pelo Lema 11.11) para qualquer $s \in S$. Assim, $n+1 \in M$ e, portanto, $P(n+1)$, contradição. $\square$

Aula 13 - Divisão

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ *tais que* $a \geq 0$ *e* $b > 0$. *Então existem inteiros* q *e* r *tais que* $a = bq + r$ *com* $0 \leq r < b$.

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$.

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$. Seja r o menor elemento de S.

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$. Seja r o menor elemento de S. Assim, para algum $q \in \mathbb{Z}$, temos que $r = a - bq$.

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$. Seja r o menor elemento de S. Assim, para algum $q \in \mathbb{Z}$, temos que $r = a - bq$. Logo, $r + bq = a$.

Teorema (Algoritmo da divisão de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$. Seja r o menor elemento de S. Assim, para algum $q \in \mathbb{Z}$, temos que $r = a - bq$. Logo, $r + bq = a$. Note que, como $r \in S$, $r \geq 0$.

Aula 13 - Provando

Aula 13 - Provando

Se mostrarmos que $r < b$ terminamos.

Aula 13 - Provando

Se mostrarmos que $r < b$ terminamos. Suponha que não.

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$0 \quad \leq \quad r - b$$

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{aligned} 0 &\leq r - b \\ &= (a - bq) - b \end{aligned}$$

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{aligned} 0 &\leq r - b \\ &= (a - bq) - b \\ &= a - b(q + 1) \end{aligned}$$

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{aligned} 0 &\leq r - b \\ &= (a - bq) - b \\ &= a - b(q + 1) \end{aligned}$$

Note então que $a - b(q + 1) \in S$.

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{aligned} 0 &\leq r - b \\ &= (a - bq) - b \\ &= a - b(q+1) \end{aligned}$$

Note então que $a - b(q+1) \in S$. E note que
$a - b(q+1) = a - bq - b < a - bq = r$, já que $b > 0$.

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{aligned} 0 &\leq r - b \\ &= (a - bq) - b \\ &= a - b(q+1) \end{aligned}$$

Note então que $a - b(q+1) \in S$. E note que $a - b(q+1) = a - bq - b < a - bq = r$, já que $b > 0$. Mas isso contradiz a minimalidade de r. $\square$

Aula 13 - Valor absoluto

Definição
Dado $z \in \mathbb{Z}$, definimos o valor absoluto de z (denotado por $|z|$) da seguinte maneira:

$$|z| = \begin{cases} z & \text{se } z \geq 0 \\ -z & \text{se } z < 0 \end{cases}$$

Aula 13 - Propriedades básicas

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$. Se $a > 0$, temos que $|a| = a > 0$ e, portanto $|a| \neq 0$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$. Se $a > 0$, temos que $|a| = a > 0$ e, portanto $|a| \neq 0$. Se $a < 0$, temos que $|a| = -a > 0$ e novamente temos que $|a| \neq 0$.

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$. Se $a > 0$, temos que $|a| = a > 0$ e, portanto $|a| \neq 0$. Se $a < 0$, temos que $|a| = -a > 0$ e novamente temos que $|a| \neq 0$.

(c) se $a \geq 0$, temos que $|a| = a$ e, portanto, $a \leq |a|$.

Aula 13 - Propriedades básicas

Proposição
Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:

(a) $|a| \geq 0$;

(b) $|a| = 0 \rightarrow a = 0$;

(c) $a \leq |a|$;

Demonstração.

(a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$. Se $a > 0$, temos que $|a| = a > 0$ e, portanto $|a| \neq 0$. Se $a < 0$, temos que $|a| = -a > 0$ e novamente temos que $|a| \neq 0$.

(c) se $a \geq 0$, temos que $|a| = a$ e, portanto, $a \leq |a|$. Se $a < 0$, temos que $a < |a|$ pelo item (a).

Aula 14 - Números primos

Aula 14 - Números primos

Um conceito bastante útil é o de número primo:

Aula 14 - Números primos

Um conceito bastante útil é o de número primo:

Definição
Dado um $p \in \mathbb{N}$, dizemos que p é **primo** se $p > 1$ e se $a \in \mathbb{N}$ é tal que $a|p$, então $a = p$ ou $a = 1$.

Aula 14 - Relação com a ordem

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$.

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$.

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$.

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$. Temos

$$b = an$$

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$. Temos

$$\begin{aligned} b &= an \\ &= a(m+1) \end{aligned}$$

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$. Temos

$$\begin{aligned} b &= an \\ &= a(m+1) \\ &= am + a \end{aligned}$$

Aula 14 - Relação com a ordem

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição

Sejam $a, b \in \mathbb{N}$ *tais que* $a, b > 1$. *Se* $a|b$, *então* $a \leq b$.

Demonstração.
Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$. Temos

$$\begin{aligned} b &= an \\ &= a(m+1) \\ &= am + a \end{aligned}$$

Logo, $a \leq b$. □

Aula 14 - Algum primo divide

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$.
Seja p o mínimo de D.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$.
Seja p o mínimo de D. Vamos mostrar que p é primo.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não. Então existe d tal que $d > 1$, $d \neq p$ e $d|p$.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não. Então existe d tal que $d > 1$, $d \neq p$ e $d|p$. Pela Proposição 14.2, temos que $d < p$.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não. Então existe d tal que $d > 1$, $d \neq p$ e $d|p$. Pela Proposição 14.2, temos que $d < p$. Note que, como $d|p$ e $p|a$, temos que $d|a$.

Aula 14 - Algum primo divide

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.

Demonstração.
Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não. Então existe d tal que $d > 1$, $d \neq p$ e $d|p$. Pela Proposição 14.2, temos que $d < p$. Note que, como $d|p$ e $p|a$, temos que $d|a$. Logo, $d \in D$ contrariando a minimalidade de p. □

Aula 14 - Decomposição

Aula 14 - Decomposição

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$.

Aula 14 - Decomposição

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio. Seja m o mínimo de tal conjunto. Note que $m > 1$.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio. Seja m o mínimo de tal conjunto. Note que $m > 1$. Pela Proposição 14.3, existe p primo tal que $p|m$.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio. Seja m o mínimo de tal conjunto. Note que $m > 1$. Pela Proposição 14.3, existe p primo tal que $p|m$. Pela Proposição 14.2, temos dois casos $p = m$ ou $p < m$.

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição

Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1$ e existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio. Seja m o mínimo de tal conjunto. Note que $m > 1$. Pela Proposição 14.3, existe p primo tal que $p|m$. Pela Proposição 14.2, temos dois casos $p = m$ ou $p < m$. Se $p = m$, temos uma contradição com a definição de m (pois $m \notin A$).

Aula 14 - Provando

Se $p < m$, note que existe k tal que $pk = m$ e tal que $k > 1$ (se $k = 0$, teríamos $m = 0$ e se $k = 1$, teríamos $m = p$).

Se $p < m$, note que existe k tal que $pk = m$ e tal que $k > 1$ (se $k = 0$, teríamos $m = 0$ e se $k = 1$, teríamos $m = p$). Assim, pela minimalidade m, temos que existem $p_1, ..., p_n$ tais que $k = p_1 \cdots p_n$.

Se $p < m$, note que existe k tal que $pk = m$ e tal que $k > 1$ (se $k = 0$, teríamos $m = 0$ e se $k = 1$, teríamos $m = p$). Assim, pela minimalidade m, temos que existem $p_1, ..., p_n$ tais que $k = p_1 \cdots p_n$. Logo, $m = (p_1 \cdot \cdots \cdot p_n)p$, contrariando a definição de m. $\square$

Aula 14 - mdc

Definição
Sejam $a, b \in \mathbb{Z}$. Dizemos que d é um **máximo divisor comum** de a e b se

(a) $d \geq 0$;

(b) $d|a$ e $d|b$;

(c) Se e satisfaz (a) e (b), então $e|d$.

Aula 14 - Unicidade

Proposição

Se d e e são máximos divisores comuns de a e b, então $d = e$.

Proposição

Se d e e são máximos divisores comuns de a e b, então $d = e$.

Demonstração.
Basta notar que $d|e$ e $e|d$.

Proposição

Se d e e são máximos divisores comuns de a e b, então $d = e$.

Demonstração.
Basta notar que $d|e$ e $e|d$. Logo, como ambos são positivos, temos que $d = e$. □

Aula 14 - Encontrando o mdc

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício).

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não. Aplique o algoritmo da divisão de Euclides e tome $a = dq + r$ com $0 < r < d$.

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não. Aplique o algoritmo da divisão de Euclides e tome $a = dq + r$ com $0 < r < d$. Note que

$$r = a - dq$$

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não. Aplique o algoritmo da divisão de Euclides e tome $a = dq + r$ com $0 < r < d$. Note que

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \end{aligned}$$

Proposição
Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não. Aplique o algoritmo da divisão de Euclides e tome $a = dq + r$ com $0 < r < d$. Note que

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \\ &= a(1 - xq) - b(yq) \end{aligned}$$

Aula 14 - Provando

Logo $r \in A$, contrariando a minimalidade de d.

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$.

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$.

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$.

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$.

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$. Assim, temos

$$d = ax + by$$

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$. Assim, temos

$$\begin{aligned} d &= ax + by \\ &= emx + eny \end{aligned}$$

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$. Assim, temos

$$\begin{aligned} d &= ax + by \\ &= emx + eny \\ &= e(mx + ny) \end{aligned}$$

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$. Assim, temos

$$\begin{aligned} d &= ax + by \\ &= emx + eny \\ &= e(mx + ny) \end{aligned}$$

Logo, $d|e$ como queríamos. □

Aula 14 - Forma usual

Definição
Dados $a, b \in \mathbb{Z}_{\neq 0}$, chamamos de $mdc(a, b)$ o máximo divisor comum de a e b.

Aula 14 - Finalmente

Proposição
Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.

Proposição
Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.

Demonstração. Suponha que M é o máximo divisor comum entre a, b.

Proposição
Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.

Demonstração. Suponha que M é o máximo divisor comum entre a, b. Pela definição, já temos que $M|a$ e $M|b$.

Proposição
Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.

Demonstração. Suponha que M é o máximo divisor comum entre a, b. Pela definição, já temos que $M|a$ e $M|b$. Assim, dado n tal que $n|a$ e $n|b$, resta mostrar que $n \leq M$.

Proposição
Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.

Demonstração. Suponha que M é o máximo divisor comum entre a, b. Pela definição, já temos que $M|a$ e $M|b$. Assim, dado n tal que $n|a$ e $n|b$, resta mostrar que $n \leq M$. Temos dois casos:

- Se $n < 0$, então $n < M$, já que $M \geq 0$.

Proposição
Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.

Demonstração. Suponha que M é o máximo divisor comum entre a, b. Pela definição, já temos que $M|a$ e $M|b$. Assim, dado n tal que $n|a$ e $n|b$, resta mostrar que $n \leq M$. Temos dois casos:

- Se $n < 0$, então $n < M$, já que $M \geq 0$.
- Se $n \geq 0$, então pela definição de máximo divisor comum entre a e b, temos que $n|M$. Logo, como $M, n \in \mathbb{N}$, pela Proposição 14.2, temos que $n \leq M$ como queríamos.

Aula 14 - Provando

Aula 14 - Provando

Agora suponha M como no enunciado.

Aula 14 - Provando

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$. Pela definição de d, temos que $M|d$.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$. Pela definição de d, temos que $M|d$. Ou seja, $M \leq d$.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$. Pela definição de d, temos que $M|d$. Ou seja, $M \leq d$. Por outro lado, temos que $d \leq M$ pela definição de M.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$. Pela definição de d, temos que $M|d$. Ou seja, $M \leq d$. Por outro lado, temos que $d \leq M$ pela definição de M. Logo, $M = d$. $\square$

Aula 14 - Relacionando com primos

Proposição
Se p é primo e $p \nmid a$ para $a \in \mathbb{Z}$, então $mdc(p, a) = 1$.

Aula 14 - Relacionando com primos

Proposição
Se p é primo e $p \nmid a$ para $a \in \mathbb{Z}$, então $mdc(p, a) = 1$.

Demonstração.
Seja $d \geq 0$ tal que $d|a$ e $d|p$.

Proposição
Se p é primo e $p \nmid a$ para $a \in \mathbb{Z}$, então $mdc(p, a) = 1$.

Demonstração.
Seja $d \geq 0$ tal que $d|a$ e $d|p$. Note que, como p é primo, temos que $d = p$ ou $d = 1$.

Proposição
Se p é primo e $p \nmid a$ para $a \in \mathbb{Z}$, então $mdc(p, a) = 1$.

Demonstração.
Seja $d \geq 0$ tal que $d|a$ e $d|p$. Note que, como p é primo, temos que $d = p$ ou $d = 1$. Como $p \nmid a$, temos que $d = 1$. □

Aula 14 - Primo dividindo produto

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \nmid a$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \not| a$. Então $mdc(a, p) = 1$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \not| a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \not| a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$. Assim, temos que $b = abx + pby$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \not| a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$. Assim, temos que $b = abx + pby$. Seja k tal que $pk = ab$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \not| a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$. Assim, temos que $b = abx + pby$. Seja k tal que $pk = ab$. Temos que $b = pkx + pby = p(kx + by)$.

Aula 14 - Primo dividindo produto

Proposição
Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.

Demonstração.
Suponha que $p \nmid a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$. Assim, temos que $b = abx + pby$. Seja k tal que $pk = ab$. Temos que $b = pkx + pby = p(kx + by)$. Logo, $p|b$. $\square$

Aula 14 - Generalizando

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n.

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente.

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$.

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$. Suponha $p|a_1 \cdots a_{n+1}$.

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$. Suponha $p|a_1 \cdots a_{n+1}$. Se $p|a_{n+1}$, terminamos.

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$. Suponha $p|a_1 \cdots a_{n+1}$. Se $p|a_{n+1}$, terminamos. Caso contrário, $p|a_1 \cdots a_n$ (pela proposição anterior).

Corolário
Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.

Demonstração.
Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$. Suponha $p|a_1 \cdots a_{n+1}$. Se $p|a_{n+1}$, terminamos. Caso contrário, $p|a_1 \cdots a_n$ (pela proposição anterior). Assim, por hipótese de indução, temos que $p|a_j$ para algum $j = 1, ..., n$. □

Aula 14 - Unicidade da decomposição

Aula 14 - Unicidade da decomposição

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Aula 14 - Unicidade da decomposição

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$.

Aula 14 - Unicidade da decomposição

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdots p_n = q_1 \cdots q_m$.

Aula 14 - Unicidade da decomposição

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdots p_n = q_1 \cdots q_m$. Vamos mostrar que $p_1 = q_1$.

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdots p_n = q_1 \cdots q_m$. Vamos mostrar que $p_1 = q_1$. Suponha que $p_1 \leq q_1$ (o outro caso é análogo).

Aula 14 - Unicidade da decomposição

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdots p_n = q_1 \cdots q_m$. Vamos mostrar que $p_1 = q_1$. Suponha que $p_1 \leq q_1$ (o outro caso é análogo). Note que $p_1 | a$, então $p_1 | q_1 \cdots q_m$.

Aula 14 - Unicidade da decomposição

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdots p_n = q_1 \cdots q_m$. Vamos mostrar que $p_1 = q_1$. Suponha que $p_1 \leq q_1$ (o outro caso é análogo). Note que $p_1 | a$, então $p_1 | q_1 \cdots q_m$. Assim, p_1 divide algum dos q_j's e, portanto, é igual a algum deles.

Teorema
A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdots p_n = q_1 \cdots q_m$. Vamos mostrar que $p_1 = q_1$. Suponha que $p_1 \leq q_1$ (o outro caso é análogo). Note que $p_1 | a$, então $p_1 | q_1 \cdots q_m$. Assim, p_1 divide algum dos q_j's e, portanto, é igual a algum deles. Como q_1 é o menor dos q_j's, temos que $q_1 \leq p_1$ - como a gente já tinha suposto $p_1 \leq q_1$, temos a igualdade.

Aula 14 - Provando

Agora, aplicando a lei do cancelamento, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Agora, aplicando a lei do cancelamento, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Com argumento análogo ao anterior, obtemos que $p_2 = q_2$.

Agora, aplicando a lei do cancelamento, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Com argumento análogo ao anterior, obtemos que $p_2 = q_2$. Repetimos o processo até "acabar" com os primos de um lado (sobrando 1 do outro lado).

Agora, aplicando a lei do cancelamento, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Com argumento análogo ao anterior, obtemos que $p_2 = q_2$. Repetimos o processo até "acabar" com os primos de um lado (sobrando 1 do outro lado). Note que teríamos um produto de primos resultando em 1 - ou seja, a única possibilidade é se os primos do outro lado também acabarem.

Agora, aplicando a lei do cancelamento, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Com argumento análogo ao anterior, obtemos que $p_2 = q_2$. Repetimos o processo até "acabar" com os primos de um lado (sobrando 1 do outro lado). Note que teríamos um produto de primos resultando em 1 - ou seja, a única possibilidade é se os primos do outro lado também acabarem. Em outras palavras, $n = m$. □

Aula 14 - Congruência

Definição
Seja $m \in \mathbb{N}$, com $m \neq 0$. Considere a seguinte relação sobre $\mathbb{Z}$: $a \equiv_m b$ se, e somente se, $m|a - b$ (para $a, b \in \mathbb{Z}$). A notação mais usual para isso é $a \equiv b \mod m$.

Aula 14 - É uma relação de equivalência

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$.

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$:

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$:

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$.

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

(c) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$:

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

(c) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$: Seja $p \in \mathbb{Z}$ tal que $pm = a - b$ e seja $q \in \mathbb{Z}$ tal que $qm = b - c$.

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

(c) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$: Seja $p \in \mathbb{Z}$ tal que $pm = a - b$ e seja $q \in \mathbb{Z}$ tal que $qm = b - c$. Temos que $pm + qm = a - b + b - c$, isto é, $(p + q)m = a - c$.

Aula 14 - É uma relação de equivalência

Proposição
A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração.
Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

(c) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$: Seja $p \in \mathbb{Z}$ tal que $pm = a - b$ e seja $q \in \mathbb{Z}$ tal que $qm = b - c$. Temos que $pm + qm = a - b + b - c$, isto é, $(p + q)m = a - c$. Logo, $m|a - c$ com queríamos.

□

Aula 14 - Propriedades básicas

Aula 14 - Propriedades básicas

Proposição
Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Proposição
Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Demonstração.

- Temos que $m|a - b$. Note que $m|b - a$.

Proposição
Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Demonstração.

- Temos que $m|a - b$. Note que $m|b - a$.
- Temos que $m|a - b$. Note que $(a + c) - (b + c) = a - b$.

Proposição
Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Demonstração.

- Temos que $m|a - b$. Note que $m|b - a$.
- Temos que $m|a - b$. Note que $(a + c) - (b + c) = a - b$. Logo, $m|(a + c) - (b + c)$;

Proposição
Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Demonstração.

- Temos que $m|a - b$. Note que $m|b - a$.
- Temos que $m|a - b$. Note que $(a + c) - (b + c) = a - b$. Logo, $m|(a + c) - (b + c)$;
- Temos que $m|a - b$.

Proposição
Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Demonstração.

- Temos que $m|a - b$. Note que $m|b - a$.
- Temos que $m|a - b$. Note que $(a + c) - (b + c) = a - b$. Logo, $m|(a + c) - (b + c)$;
- Temos que $m|a - b$. Note que $m|c(a - b)$.

Aula 14 - Provando

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$.

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$.

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo,
  $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo,
  $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$.
  Logo, $m|(a+c)-(b+d)$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$. Suponha que vale para $r = n$ e vamos mostrar para $r = n+1$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$. Suponha que vale para $r = n$ e vamos mostrar para $r = n+1$. Temos que $a \equiv_m b$, logo, pela hipótese de indução, temos que $a^n \equiv_m b^n$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$. Suponha que vale para $r = n$ e vamos mostrar para $r = n+1$. Temos que $a \equiv_m b$, logo, pela hipótese de indução, temos que $a^n \equiv_m b^n$. Assim, pelo item (e), temos que $a^n a \equiv_m b^n b$.

Aula 14 - Provando

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$. Suponha que vale para $r = n$ e vamos mostrar para $r = n+1$. Temos que $a \equiv_m b$, logo, pela hipótese de indução, temos que $a^n \equiv_m b^n$. Assim, pelo item (e), temos que $a^n a \equiv_m b^n b$. Isto é, $a^{n+1} \equiv_m b^{n+1}$.

□

Aula 14 - Unicidade do resto

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *com* $m \neq 0$. *Sejam* r_1, r_2 *dados pelo algoritmo da divisão de Euclides de* a *e* b *por* m, *isto é,* $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *com* $0 \leq r_1, r_2 < m$. *Então* $a \equiv_m b$ *se, e somente se,* $r_1 = r_2$.

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *com* $m \neq 0$. *Sejam* r_1, r_2 *dados pelo algoritmo da divisão de Euclides de* a *e* b *por* m, *isto é,* $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *com* $0 \leq r_1, r_2 < m$. *Então* $a \equiv_m b$ *se, e somente se,* $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$.

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *com* $m \neq 0$. *Sejam* r_1, r_2 *dados pelo algoritmo da divisão de Euclides de* a *e* b *por* m, *isto é,* $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *com* $0 \leq r_1, r_2 < m$. *Então* $a \equiv_m b$ *se, e somente se,* $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$.

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *com* $m \neq 0$. *Sejam* r_1, r_2 *dados pelo algoritmo da divisão de Euclides de* a *e* b *por* m, *isto é,* $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *com* $0 \leq r_1, r_2 < m$. *Então* $a \equiv_m b$ *se, e somente se,* $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$.

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *com* $m \neq 0$. *Sejam* r_1, r_2 *dados pelo algoritmo da divisão de Euclides de* a *e* b *por* m, *isto é,* $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *com* $0 \leq r_1, r_2 < m$. *Então* $a \equiv_m b$ *se, e somente se,* $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo).

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *com* $m \neq 0$. *Sejam* r_1, r_2 *dados pelo algoritmo da divisão de Euclides de* a *e* b *por* m, *isto é,* $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *com* $0 \leq r_1, r_2 < m$. *Então* $a \equiv_m b$ *se, e somente se,* $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo). Temos

$$r_1 - r_2 \quad = \quad (a - mq_1) - (b - mq_2)$$

Proposição

Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ com $m \neq 0$. Sejam r_1, r_2 dados pelo algoritmo da divisão de Euclides de a e b por m, isto é, $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1, r_2 < m$. Então $a \equiv_m b$ se, e somente se, $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo). Temos

$$\begin{aligned} r_1 - r_2 &= (a - mq_1) - (b - mq_2) \\ &= (a - b) + (mq_2 - mq_1) \end{aligned}$$

Proposição

Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ com $m \neq 0$. Sejam r_1, r_2 dados pelo algoritmo da divisão de Euclides de a e b por m, isto é, $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1, r_2 < m$. Então $a \equiv_m b$ se, e somente se, $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo). Temos

$$\begin{aligned} r_1 - r_2 &= (a - mq_1) - (b - mq_2) \\ &= (a - b) + (mq_2 - mq_1) \\ &= mn - m(q_2 - q_1) \end{aligned}$$

Aula 14 - Unicidade do resto

Proposição

Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ com $m \neq 0$. Sejam r_1, r_2 dados pelo algoritmo da divisão de Euclides de a e b por m, isto é, $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1, r_2 < m$. Então $a \equiv_m b$ se, e somente se, $r_1 = r_2$.

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo). Temos

$$\begin{aligned} r_1 - r_2 &= (a - mq_1) - (b - mq_2) \\ &= (a - b) + (mq_2 - mq_1) \\ &= mn - m(q_2 - q_1) \\ &= m(n - q_2 + q_1) \end{aligned}$$

Aula 14 - Provando

Logo, $m|r_1 - r_2$.

Logo, $m|r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$.

Logo, $m|r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$. Assim, a única possibilidade para que $m|r_1 - r_2$ é se $r_1 - r_2 = 0$, isto é, $r_1 = r_2$ como queríamos.

Logo, $m|r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$. Assim, a única possibilidade para que $m|r_1 - r_2$ é se $r_1 - r_2 = 0$, isto é, $r_1 = r_2$ como queríamos.

Agora suponha que $r_1 = r_2$.

Logo, $m|r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$. Assim, a única possibilidade para que $m|r_1 - r_2$ é se $r_1 - r_2 = 0$, isto é, $r_1 = r_2$ como queríamos.

Agora suponha que $r_1 = r_2$. Temos que
$a - b = mq_1 - r_1 - (mq_2 - r_2) = m(q_1 - q_2)$.

Logo, $m|r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$. Assim, a única possibilidade para que $m|r_1 - r_2$ é se $r_1 - r_2 = 0$, isto é, $r_1 = r_2$ como queríamos.

Agora suponha que $r_1 = r_2$. Temos que $a - b = mq_1 - r_1 - (mq_2 - r_2) = m(q_1 - q_2)$. Isto é, $m|a - b$. $\square$

Aula 14 - Exemplos

Aula 14 - Exemplos

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Aula 14 - Exemplos

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo.

Aula 14 - Exemplos

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo.

Aula 14 - Exemplos

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Isto é, sábado.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Isto é, sábado. Vamos calcular em que dia semana será uma data daqui a 90 dias.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Isto é, sábado. Vamos calcular em que dia semana será uma data daqui a 90 dias. No nosso exemplo, vamos supor que hoja é sexta.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Isto é, sábado. Vamos calcular em que dia semana será uma data daqui a 90 dias. No nosso exemplo, vamos supor que hoja é sexta. Logo, o dia associado é 5.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Isto é, sábado. Vamos calcular em que dia semana será uma data daqui a 90 dias. No nosso exemplo, vamos supor que hoja é sexta. Logo, o dia associado é 5.

Assim, daqui a 90 dias, será o resto de 95 dividido por 7.

Exemplo
Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Isto é, sábado. Vamos calcular em que dia semana será uma data daqui a 90 dias. No nosso exemplo, vamos supor que hoja é sexta. Logo, o dia associado é 5.

Assim, daqui a 90 dias, será o resto de 95 dividido por 7. Como $95 = 13 \cdot 7 + 4$, teremos que o dia da semana será o correspondente a 4, isto é, quinta.

Aula 14 - Exemplos

Aula 14 - Exemplos

Exemplo
Qual é o o último dígito de 27^{500}?

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$. Note também que $7^2 = 49$.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$. Note também que $7^2 = 49$. Logo $7^2 \equiv_{10} 49 \equiv_{10} 9 \equiv_{10} -1$.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$. Note também que $7^2 = 49$. Logo $7^2 \equiv_{10} 49 \equiv_{10} 9 \equiv_{10} -1$. Assim,
$7^{500} = (7^2)^{250} \equiv_{10} (-1)^{250} \equiv_{10} 1$.

Exemplo
Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$. Note também que $7^2 = 49$. Logo $7^2 \equiv_{10} 49 \equiv_{10} 9 \equiv_{10} -1$. Assim, $7^{500} = (7^2)^{250} \equiv_{10} (-1)^{250} \equiv_{10} 1$. Logo, o último dígito de 27^{500} é 1.

Aula 14 - Exemplos

Exemplo
Maneira alternativa de resolver o problema anterior:

Exemplo
Maneira alternativa de resolver o problema anterior: Partimos do ponto em que temos que $27^{500} \equiv 7^{500}$.

Exemplo
Maneira alternativa de resolver o problema anterior: Partimos do ponto em que temos que $27^{500} \equiv 7^{500}$. Vejamos como se comportam as potências de 7 módulo 10.

Exemplo
Maneira alternativa de resolver o problema anterior: Partimos do ponto em que temos que $27^{500} \equiv 7^{500}$. Vejamos como se comportam as potências de 7 módulo 10. Temos $7^0 \equiv 1$, $7^1 \equiv_{10} 7$, $7^2 \equiv_{10} 9$, $7^3 \equiv_{10} 3$, $7^4 \equiv_{10} 1$, ou seja, elas formam um ciclo de comprimento 4.

Exemplo
Maneira alternativa de resolver o problema anterior: Partimos do ponto em que temos que $27^{500} \equiv 7^{500}$. Vejamos como se comportam as potências de 7 módulo 10. Temos $7^0 \equiv 1$, $7^1 \equiv_{10} 7$, $7^2 \equiv_{10} 9$, $7^3 \equiv_{10} 3$, $7^4 \equiv_{10} 1$, ou seja, elas formam um ciclo de comprimento 4. Assim, temos que $7^{500} \equiv_{10} 7^0 \equiv_{10} 1$, pois 500 tem resto 0 na divisão por 4.

Aula 15 - Inteiros mod n

Definição
Dado $n \in \mathbb{N}_{>1}$, vamos chamar de **inteiros mod n** o conjunto $\mathbb{Z}/\equiv_n$ com as operações usuais. Por comodidade, vamos denotar os elementos de tal conjunto por $0, ..., n-1$. Vamos denotar tal conjunto por MOD_n.

Aula 15 - Abusos

Aula 15 - Abusos

Vamos adotar o seguinte abuso: dados $a, b \in MOD_n$, podemos nos referir a eles como $a = b$ (pensando neles como as clases) ou $a \equiv_n b$ (pensando neles com representantes das classes).

Aula 15 - Abusos

Vamos adotar o seguinte abuso: dados $a, b \in MOD_n$, podemos nos referir a eles como $a = b$ (pensando neles como as clases) ou $a \equiv_n b$ (pensando neles com representantes das classes). Note que isso não dá problema pois existe um único representante entre $0, ..., n-1$.

Aula 15 - Propriedades básicas

Proposição
Seja p primo. Sejam $a, b \in MOD_p$. Se $ab \equiv_p 0$, então $a \equiv_p 0$ ou $b \equiv_p 0$.

Proposição
Seja p primo. Sejam $a, b \in MOD_p$. Se $ab \equiv_p 0$, então $a \equiv_p 0$ ou $b \equiv_p 0$.

Demonstração.
Note que se $ab \equiv_p 0$, então $p|ab$.

Proposição
Seja p primo. Sejam $a, b \in MOD_p$. Se $ab \equiv_p 0$, então $a \equiv_p 0$ ou $b \equiv_p 0$.

Demonstração.
Note que se $ab \equiv_p 0$, então $p|ab$. Como p é primo, temos que $p|a$ ou $p|b$.

Proposição
Seja p primo. Sejam $a, b \in MOD_p$. Se $ab \equiv_p 0$, então $a \equiv_p 0$ ou $b \equiv_p 0$.

Demonstração.
Note que se $ab \equiv_p 0$, então $p|ab$. Como p é primo, temos que $p|a$ ou $p|b$. O primeiro caso implica que $a \equiv_p 0$ e o segundo implica que $b \equiv_p 0$. □

Aula 15 - Propriedades básicas

Proposição

Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.

Proposição

Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.

Demonstração.
Como $ax \equiv_p ay$, temos que $ax - ay \equiv_p 0$.

Proposição

Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.

Demonstração.
Como $ax \equiv_p ay$, temos que $ax - ay \equiv_p 0$. Isto é,

$$a(x - y) \equiv_p 0$$

Proposição

Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.

Demonstração.
Como $ax \equiv_p ay$, temos que $ax - ay \equiv_p 0$. Isto é,

$$a(x - y) \equiv_p 0$$

Pelo resultado anterior, temos que $a \equiv_p 0$ ou $(x - y) \equiv_p 0$.

Proposição

Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.

Demonstração.
Como $ax \equiv_p ay$, temos que $ax - ay \equiv_p 0$. Isto é,

$$a(x - y) \equiv_p 0$$

Pelo resultado anterior, temos que $a \equiv_p 0$ ou $(x - y) \equiv_p 0$. Como $a \not\equiv_p 0$, temos que $x \equiv_p y$ como queríamos. □

Aula 15 - Propriedades básicas

Lema
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é injetora.

Lema
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é injetora.

Demonstração.
Suponha $x, y \in MOD_p$.

Lema
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é injetora.

Demonstração.
Suponha $x, y \in MOD_p$. Note que $\pi_a(x) = \pi_a(y)$ quer dizer $ax \equiv_p ay$.

Lema
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é injetora.

Demonstração.
Suponha $x, y \in MOD_p$. Note que $\pi_a(x) = \pi_a(y)$ quer dizer $ax \equiv_p ay$. Pelo resultado anterior, temos que $x = y$. □

Aula 15 - Propriedades básicas

Corolário
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é bijetora.

Corolário
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é bijetora.

Demonstração.
Note que, como a função é injetora, ela tem p elementos na imagem.

Corolário
Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é bijetora.

Demonstração.
Note que, como a função é injetora, ela tem p elementos na imagem. Como o contradomínio também tem p elementos, temos que a função é sobrejetora. □

Aula 15 - Propriedades básicas

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Demonstração.
Considere a função π_a acima.

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Demonstração.
Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$.

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Demonstração.
Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$. Isto é, $ab = 1$.

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Demonstração.
Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$. Isto é, $ab = 1$.

Vejamos agora que ele é único.

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Demonstração.
Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$. Isto é, $ab = 1$.

Vejamos agora que ele é único. Sejam $b, c \in MOD_p$ tais que $ab = 1$ e $ac = 1$.

Proposição

Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.

Demonstração.
Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$. Isto é, $ab = 1$.

Vejamos agora que ele é único. Sejam $b, c \in MOD_p$ tais que $ab = 1$ e $ac = 1$. Então, pela Proposição 15.3, temos de $ab = ac$ que $b = c$. □

Aula 15 - Corpo

Definição
Dizemos que $(F, \oplus, \odot)$ éum **corpo** se $\oplus$ e $\odot$ são associativas, comutativas e ainda valem, para todo $a, b, c \in F$:

(i) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$;

(ii) Existe $0 \in F$ tal que $0 \oplus x = x$ para todo $x \in F$;

(iii) Existe $1 \in F$ tal que $1 \odot x = x$ para todo $x \in F$;

(iv) Existe $x \in F$ tal que $a \oplus x = 0$;

(v) Se $a \neq 0$, existe $x \in F$ tal que $x \odot a = 1$.

Aula 15 - Exemplos

Aula 15 - Exemplos

Tanto os racionais como os reais satisfazem a definição de corpo com as operações usuais.

Aula 15 - MOD_p é corpo

Aula 15 - MOD_p é corpo

Proposição
Seja p primo. Então MOD_p é um corpo com as operações usuais.

Proposição
Seja p primo. Então MOD_p é um corpo com as operações usuais.

Demonstração.
Note que as operações serem associativas, comutativas e a regra de distributividade seguem diretamente das mesmas propriedades sobre $\mathbb{Z}$.

Proposição
Seja p primo. Então MOD_p é um corpo com as operações usuais.

Demonstração.
Note que as operações serem associativas, comutativas e a regra de distributividade seguem diretamente das mesmas propriedades sobre $\mathbb{Z}$. Note que 0 e 1 também fazem os papeis de elementos neutros em MOD_p.

Aula 15 - MOD_p é corpo

Proposição
Seja p primo. Então MOD_p é um corpo com as operações usuais.

Demonstração.
Note que as operações serem associativas, comutativas e a regra de distributividade seguem diretamente das mesmas propriedades sobre $\mathbb{Z}$. Note que 0 e 1 também fazem os papeis de elementos neutros em MOD_p. Dado $a \in MOD_p$, note que $a + (p - a) = p \equiv_p 0$.

Proposição
Seja p primo. Então MOD_p é um corpo com as operações usuais.

Demonstração.
Note que as operações serem associativas, comutativas e a regra de distributividade seguem diretamente das mesmas propriedades sobre $\mathbb{Z}$. Note que 0 e 1 também fazem os papeis de elementos neutros em MOD_p. Dado $a \in MOD_p$, note que $a + (p - a) = p \equiv_p 0$. Já a última propriedade é simplesmente a Proposição 15.6. □

Aula 15 - Propriedades de corpos

Aula 15 - Propriedades de corpos

Vamos ver algumas propriedades simples sobre corpos:

Aula 15 - Propriedades de corpos

Vamos ver algumas propriedades simples sobre corpos:

Lema
Seja F um corpo. Dado $x \in F$, temos que $0x = 0$.

Aula 15 - Propriedades de corpos

Vamos ver algumas propriedades simples sobre corpos:

Lema
Seja F um corpo. Dado $x \in F$, temos que $0x = 0$.

Demonstração.
Seja $y \in F$ tal que $0x + y = 0$.

Aula 15 - Propriedades de corpos

Vamos ver algumas propriedades simples sobre corpos:

Lema
Seja F um corpo. Dado $x \in F$, temos que $0x = 0$.

Demonstração.
Seja $y \in F$ tal que $0x + y = 0$. Temos

$$0x = (0 + 0)x = 0x + 0x$$

Vamos ver algumas propriedades simples sobre corpos:

Lema
Seja F um corpo. Dado $x \in F$, temos que $0x = 0$.

Demonstração.
Seja $y \in F$ tal que $0x + y = 0$. Temos

$$0x = (0 + 0)x = 0x + 0x$$

Somando y dos dois lados, obtemos

$$0 = 0x + y = 0x + 0x + y = 0x$$

como queríamos. □

Aula 15 - Propriedades de corpos

Proposição
Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.

Proposição
Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.

Demonstração.
Suponha que $a \neq 0$.

Proposição
Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.

Demonstração.
Suponha que $a \neq 0$. Vamos provar que $b = 0$ (note que isso é suficiente para o que queremos).

Proposição
Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.

Demonstração.
Suponha que $a \neq 0$. Vamos provar que $b = 0$ (note que isso é suficiente para o que queremos). Então existe $x \in F$ tal que $ax = 1$.

Proposição
Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.

Demonstração.
Suponha que $a \neq 0$. Vamos provar que $b = 0$ (note que isso é suficiente para o que queremos). Então existe $x \in F$ tal que $ax = 1$. Assim, de $0 = ab$, temos $0x = xab$.

Proposição
Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.

Demonstração.
Suponha que $a \neq 0$. Vamos provar que $b = 0$ (note que isso é suficiente para o que queremos). Então existe $x \in F$ tal que $ax = 1$. Assim, de $0 = ab$, temos $0x = xab$. Como $0x = 0$ pelo lema anterior, temos que $0 = b$. □

Aula 15 - Quando MOD_m não é corpo

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Demonstração.
Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Demonstração.
Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Demonstração.
Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$. Seja b tal que $ab = m$.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Demonstração.
Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$. Seja b tal que $ab = m$. Note que $b \neq 1$ e $b \neq m$.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Demonstração.
Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$. Seja b tal que $ab = m$. Note que $b \neq 1$ e $b \neq m$. Note também que $a, b \neq 0$.

Aula 15 - Quando MOD_m não é corpo

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição
Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.

Demonstração.
Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$. Seja b tal que $ab = m$. Note que $b \neq 1$ e $b \neq m$. Note também que $a, b \neq 0$. Mas temos

$$ab = m \equiv_m 0.$$

□

Aula 15 - Primos entre si

Aula 15 - Primos entre si

Definição
Dizemos que $a, b \in \mathbb{Z}_{>1}$ são **primos entre si** se $mdc(a, b) = 1$.

Aula 15 - Algumas propriedades básicas

Aula 15 - Algumas propriedades básicas

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$.

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$.

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$z = z(ax + by)$$

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$\begin{aligned} z &= z(ax + by) \\ &= zax + zby \end{aligned}$$

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$\begin{aligned} z &= z(ax + by) \\ &= zax + zby \\ &= bnax + amby \end{aligned}$$

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$\begin{aligned} z &= z(ax + by) \\ &= zax + zby \\ &= bnax + amby \\ &= ab(nx + my) \end{aligned}$$

Lema

Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.

Demonstração.
Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$\begin{aligned} z &= z(ax + by) \\ &= zax + zby \\ &= bnax + amby \\ &= ab(nx + my) \end{aligned}$$

Ou seja, $ab|z$. □

Aula 15 - Algumas propriedades básicas

Aula 15 - Algumas propriedades básicas

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Demonstração.
Seja x divisor comum entre ab e c.

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Demonstração.
Seja x divisor comum entre ab e c. Suponha que $x \neq 1$.

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Demonstração.
Seja x divisor comum entre ab e c. Suponha que $x \neq 1$. Então existe p primo tal que $p|x$.

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Demonstração.
Seja x divisor comum entre ab e c. Suponha que $x \neq 1$. Então existe p primo tal que $p|x$. Logo, $p|ab$ e $p|c$.

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Demonstração.
Seja x divisor comum entre ab e c. Suponha que $x \neq 1$. Então existe p primo tal que $p|x$. Logo, $p|ab$ e $p|c$. Como $p|ab$, temos que $p|a$ ou $p|b$.

Lema
Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.

Demonstração.
Seja x divisor comum entre ab e c. Suponha que $x \neq 1$. Então existe p primo tal que $p|x$. Logo, $p|ab$ e $p|c$. Como $p|ab$, temos que $p|a$ ou $p|b$. Logo, a e c não são primos entre si, ou b e c não são primos entre si. □

Aula 15 - Algumas propriedades básicas

Corolário

Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ *primos entre si. Então* $a_1 \cdots a_n$ *e* b *são primos entre si.*

Corolário

Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ *primos entre si. Então* $a_1 \cdots a_n$ *e* b *são primos entre si.*

Demonstração.
Por indução sobre n.

Corolário

Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ primos entre si. Então $a_1 \cdots a_n$ e b são primos entre si.

Demonstração.
Por indução sobre n. Se $n = 2$, é exatamente o lema anterior.

Corolário

Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ primos entre si. Então $a_1 \cdots a_n$ e b são primos entre si.

Demonstração.
Por indução sobre n. Se $n = 2$, é exatamente o lema anterior.

Note que, por hipótese de indução, temos que $a_1 \cdots a_n$, a_{n+1} e b são primos entre si.

Corolário

Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ primos entre si. Então $a_1 \cdots a_n$ e b são primos entre si.

Demonstração.
Por indução sobre n. Se $n = 2$, é exatamente o lema anterior.
Note que, por hipótese de indução, temos que $a_1 \cdots a_n$, a_{n+1} e b são primos entre si. Então, novamente pelo lema, temos que $a_1 \cdots a_{n+1}$ e b são primos entre si. □

Aula 15 - Algumas propriedades básicas

Proposição
Sejam a, b primos entre si. Sejam r e s inteiros. Então o sistema

$$\begin{cases} x \equiv_a r \\ x \equiv_b s \end{cases}$$

admite alguma solução c e é equivalente a

$$x \equiv_{ab} c$$

Proposição
Sejam a, b primos entre si. Sejam r e s inteiros. Então o sistema

$$\begin{cases} x \equiv_a r \\ x \equiv_b s \end{cases}$$

admite alguma solução c e é equivalente a

$$x \equiv_{ab} c$$

Demonstração. Como a e b são primos entre si, existem $\alpha, \beta \in \mathbb{Z}$ tais que

$$\alpha a + \beta b = 1.$$

Aula 15 - Provando

Considere

$$c = s\alpha a + r\beta b.$$

Considere

$$c = s\alpha a + r\beta b.$$

Vamos mostrar que tal c satisfaz as condições do enunciado.

Considere

$$c = s\alpha a + r\beta b.$$

Vamos mostrar que tal c satisfaz as condições do enunciado.
Suponha que x seja uma solução para $x \equiv_{ab} c$.

Considere

$$c = s\alpha a + r\beta b.$$

Vamos mostrar que tal c satisfaz as condições do enunciado. Suponha que x seja uma solução para $x \equiv_{ab} c$. Ou seja, existe $k \in \mathbb{Z}$ tal que

$$x = c + kab = s\alpha a + r\beta b + kab.$$

Considere

$$c = s\alpha a + r\beta b.$$

Vamos mostrar que tal c satisfaz as condições do enunciado. Suponha que x seja uma solução para $x \equiv_{ab} c$. Ou seja, existe $k \in \mathbb{Z}$ tal que

$$x = c + kab = s\alpha a + r\beta b + kab.$$

Vejamos que tal x é, de fato, uma solução para o sistema.

Aula 15 - Provando

Primeiramente, temos que

$$x - r = s\alpha a + r\beta b + kab - r$$

Primeiramente, temos que

$$\begin{aligned} x - r &= s\alpha a + r\beta b + kab - r \\ &= s\alpha a + r(\beta b - 1) + kab \end{aligned}$$

Primeiramente, temos que

$$\begin{aligned} x - r &= s\alpha a + r\beta b + kab - r \\ &= s\alpha a + r(\beta b - 1) + kab \\ &= s\alpha a - \alpha ar + kab \end{aligned}$$

Primeiramente, temos que

$$\begin{aligned} x - r &= s\alpha a + r\beta b + kab - r \\ &= s\alpha a + r(\beta b - 1) + kab \\ &= s\alpha a - \alpha ar + kab \\ &= a(s\alpha - r\alpha + kb) \end{aligned}$$

Primeiramente, temos que

$$\begin{aligned} x - r &= s\alpha a + r\beta b + kab - r \\ &= s\alpha a + r(\beta b - 1) + kab \\ &= s\alpha a - \alpha ar + kab \\ &= a(s\alpha - r\alpha + kb) \end{aligned}$$

Ou seja, temos que

$$x \equiv_a r.$$

Primeiramente, temos que

$$\begin{aligned} x - r &= s\alpha a + r\beta b + kab - r \\ &= s\alpha a + r(\beta b - 1) + kab \\ &= s\alpha a - \alpha ar + kab \\ &= a(s\alpha - r\alpha + kb) \end{aligned}$$

Ou seja, temos que

$$x \equiv_a r.$$

De forma análoga, podemos mostrar que $x \equiv_b s$.

Aula 15 - Provando

Aula 15 - Provando

Agora suponha x uma solução para o sistema.

Agora suponha x uma solução para o sistema. Note que, pelo que vimos acima, c é uma solução para o sistema.

Agora suponha x uma solução para o sistema. Note que, pelo que vimos acima, c é uma solução para o sistema. Logo:

$$x \equiv_a c$$

$$x \equiv_b c$$

Agora suponha x uma solução para o sistema. Note que, pelo que vimos acima, c é uma solução para o sistema. Logo:

$$x \equiv_a c$$

$$x \equiv_b c$$

Ou seja, $a|(x-c)$ e $b|(x-c)$.

Agora suponha x uma solução para o sistema. Note que, pelo que vimos acima, c é uma solução para o sistema. Logo:

$$x \equiv_a c$$

$$x \equiv_b c$$

Ou seja, $a|(x-c)$ e $b|(x-c)$. Como a, b são primos entre si, pelo Lema 15.13, temos que $ab|(x-c)$.

Agora suponha x uma solução para o sistema. Note que, pelo que vimos acima, c é uma solução para o sistema. Logo:

$$x \equiv_a c$$

$$x \equiv_b c$$

Ou seja, $a|(x-c)$ e $b|(x-c)$. Como a, b são primos entre si, pelo Lema 15.13, temos que $ab|(x-c)$. Ou seja, $x \equiv_{ab} c$. □

Aula 15 - Teorema chinês do resto

Corolário (Teorema chinês do resto)
Sejam $a_1, ..., a_n$ *primos entre si e sejam* $r_1, ..., r_n \in \mathbb{Z}$.

Corolário (Teorema chinês do resto)
Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Corolário (Teorema chinês do resto)
Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Demonstração. Vamos provar por indução sobre n.

Corolário (Teorema chinês do resto)
Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Demonstração. Vamos provar por indução sobre n. O caso 2 é o resultado anterior.

Corolário (Teorema chinês do resto)
Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Demonstração. Vamos provar por indução sobre n. O caso 2 é o resultado anterior. Suponha então que temos $n+1$ equações como no enuciado.

Corolário (Teorema chinês do resto)
Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Demonstração. Vamos provar por indução sobre n. O caso 2 é o resultado anterior. Suponha então que temos $n+1$ equações como no enuciado. Por hipótese de indução, existe b' tal que o sistema formado pelas primeiras n equações é equivalente a $x \equiv_{A'} b'$, onde $A' = a_1 \cdots a_n$.

Aula 15 - Provando

Pelo Corolário 15.15, temos que a_{n+1} e A' são primos entre si.

Pelo Corolário 15.15, temos que a_{n+1} e A' são primos entre si. Assim, novamente pelo resultado anterior, temos que existe b tal que o sistema

$$\begin{cases} x & \equiv_{A'} & b' \\ x & \equiv_{a_{n+1}} & r_{n+1} \end{cases}$$

é equivalente a

$$x \equiv_A b$$

onde $A = A' a_{n+1} = a_1 \cdots a_{n+1}$.

Pelo Corolário 15.15, temos que a_{n+1} e A' são primos entre si. Assim, novamente pelo resultado anterior, temos que existe b tal que o sistema

$$\begin{cases} x & \equiv_{A'} & b' \\ x & \equiv_{a_{n+1}} & r_{n+1} \end{cases}$$

é equivalente a

$$x \equiv_A b$$

onde $A = A'a_{n+1} = a_1 \cdots a_{n+1}$. Ou seja, a última equação é equivalente ao sistema do enunciado. □

Aula 15 - Exemplo

Aula 15 - Exemplo

Qual o menor natural k tal que k dividido por 3 tem resto 2, dividido por 5 tem resto 3 e dividido por 7 tem resto 2?

Aula 15 - Exemplo

Qual o menor natural k tal que k dividido por 3 tem resto 2, dividido por 5 tem resto 3 e dividido por 7 tem resto 2?

Primeiramente, note que a pergunta é equivalente a perguntar qual a menor solução positiva para

$$\begin{cases} x & \equiv_3 & 2 \\ x & \equiv_5 & 3 \\ x & \equiv_7 & 2 \end{cases}$$

Aula 15 - Provando

Aula 15 - Provando

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a.

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil.

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil. A terceira equação é equivalente a encontrar b tal que $x = 7b + 2$.

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil. A terceira equação é equivalente a encontrar b tal que $x = 7b + 2$. Substituindo na segunda equação, obtemos $7b + 2 \equiv_5 3$.

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil. A terceira equação é equivalente a encontrar b tal que $x = 7b + 2$. Substituindo na segunda equação, obtemos $7b + 2 \equiv_5 3$. Ou seja $2b \equiv_5 1$.

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil. A terceira equação é equivalente a encontrar b tal que $x = 7b + 2$. Substituindo na segunda equação, obtemos $7b + 2 \equiv_5 3$. Ou seja $2b \equiv_5 1$. Lembrando que 3 é o inverso de 2 em MOD_5, multiplicando ambos os lados por 3, temos

$$b \equiv_5 3.$$

Ou seja, existe c tal que $b = 5c + 3$.

Ou seja, existe c tal que $b = 5c + 3$. Substituindo o b, temos $x = 7b + 2 = 7(5c + 3) + 2 = 35c + 23$.

Ou seja, existe c tal que $b = 5c + 3$. Substituindo o b, temos $x = 7b + 2 = 7(5c + 3) + 2 = 35c + 23$. Substituindo na primeira equação $35c + 23 \equiv_3 2$

Ou seja, existe c tal que $b = 5c + 3$. Substituindo o b, temos $x = 7b + 2 = 7(5c + 3) + 2 = 35c + 23$. Substituindo na primeira equação $35c + 23 \equiv_3 2$ Ou seja

$$2c \equiv_3 0.$$

Ou seja, existe c tal que $b = 5c + 3$. Substituindo o b, temos $x = 7b + 2 = 7(5c + 3) + 2 = 35c + 23$. Substituindo na primeira equação $35c + 23 \equiv_3 2$ Ou seja

$$2c \equiv_3 0.$$

Assim,

$$c \equiv_3 0.$$

Logo, existe d tal que $c = 3d$.

Logo, existe d tal que $c = 3d$. Voltando na equação com x:

$$x = 35c + 21 = 35(3d) + 23 = 105d + 23.$$

Logo, existe d tal que $c = 3d$. Voltando na equação com x:

$$x = 35c + 21 = 35(3d) + 23 = 105d + 23.$$

Para termos o menor k possível, fazemos $d = 0$ e, portanto, $k = 23$.

Aula 16 - Racionais

Definição
Considere o conjunto$A = \{(a, b) \in \mathbb{Z} : b \neq 0\}$ e considere $\sim$ a seguinte relação sobre A: dados $(a, b), (x, y) \in A$, definimos $(a, b) \sim (x, y)$ se, e somente se, $ay = bx$.

Aula 16 - É relação de equivalência

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$. Temos

$$ay = bx$$

$$x\beta = y\alpha.$$

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$. Temos

$$ay = bx$$

$$x\beta = y\alpha.$$

Assim, multiplicando por β a primeira equação, temos $ay\beta = bx\beta$.

Aula 16 - É relação de equivalência

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$. Temos

$$ay = bx$$

$$x\beta = y\alpha.$$

Assim, multiplicando por β a primeira equação, temos $ay\beta = bx\beta$. Logo, $ay\beta = by\alpha$.

Proposição
A relação $\sim$ definida acima é uma relação de equivalência sobre A.

Demonstração.
Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$. Temos

$$ay = bx$$

$$x\beta = y\alpha.$$

Assim, multiplicando por β a primeira equação, temos $ay\beta = bx\beta$. Logo, $ay\beta = by\alpha$. Como $y \neq 0$, temos $a\beta = b\alpha$ como queríamos. □

Aula 16 - Definição formal

Aula 16 - Definição formal

Definição
Denotamos por $\mathbb{Q}$ o conjunto $A/\sim$. Chamamos tal conjunto de conjunto dos **números racionais**.

Aula 16 - A soma

Definição
Definimos a operação de **soma** sobre os racionais da seguinte maneira: dados $[(a, b)], [(x, y)] \in \mathbb{Q}$, definimos
$[(a, b)] + [(x, y)] = [(ay + xb, by)]$.

Aula 16 - Está bem definida

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0).

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes.

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$.

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$.

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$.

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$. Logo

$$(ad + cb)yz \quad = \quad adyz + cbyz$$

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$. Logo

$$\begin{aligned} (ad + cb)yz &= adyz + cbyz \\ &= aydz + czby \end{aligned}$$

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$. Logo

$$\begin{aligned} (ad + cb)yz &= adyz + cbyz \\ &= aydz + czby \\ &= bxdz + dwby \end{aligned}$$

Aula 16 - Está bem definida

Proposição

A operação de soma está bem definida.

Demonstração.
Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$. Logo

$$\begin{aligned}(ad + cb)yz &= adyz + cbyz \\ &= aydz + czby \\ &= bxdz + dwby \\ &= (xz + wy)db\end{aligned}$$

□

Aula 16 - O produto

Definição
Definimos a operação de **produto** sobre os racionais da seguinte maneira: dados $[(a, b)], [(x, y)] \in \mathbb{Q}$, definimos $[(a, b)] \cdot [(x, y)] = [(ax, by)]$.

Aula 16 - Está bem definida

Aula 16 - Está bem definida

Proposição
A operação de produto está bem definida.

Aula 16 - Está bem definida

Proposição
A operação de produto está bem definida.

Demonstração.
Veja o Exercício **??**. □

Aula 16 - Forma canônica

Definição
Dizemos que um elemento $[(a, b)] \in \mathbb{Q}$ está na **forma canônica** se $b > 0$.

Aula 16 - Forma canônica

Proposição
Todo número $q \in \mathbb{Q}$ admite uma representação na forma canônica.

Proposição
Todo número $q \in \mathbb{Q}$ admite uma representação na forma canônica.

Demonstração.
Seja $[(a, b)] = q$.

Proposição
Todo número $q \in \mathbb{Q}$ admite uma representação na forma canônica.

Demonstração.
Seja $[(a, b)] = q$. Se $b > 0$, nada temos a fazer.

Proposição
Todo número $q \in \mathbb{Q}$ admite uma representação na forma canônica.

Demonstração.
Seja $[(a, b)] = q$. Se $b > 0$, nada temos a fazer. Se $b < 0$, observe que $[(-a, -b)] = [(a, b)]$ (pois $-ab = -ba$) e $[(-a, -b)]$ está na forma canônica. □

Aula 16 - Ordem

Definição
Sejam $q, r \in \mathbb{Q}$. Dizemos que $q \leq r$ se $ay \leq xb$ se $q = [(a, b)]$, $r = [(x, y)]$ e $[(a, b)]$ e $[(x, y)]$ estão na forma canônica.

Aula 16 - Bem definida

Aula 16 - Bem definida

Proposição
A relação $\leq$ definida acima está bem definida.

Proposição
A relação $\leq$ definida acima está bem definida.

Demonstração. Precisamos mostrar que se valem

$$[(a_1, b_1)] = [(a_2, b_2)]$$

$$[(x_1, y_1)] = [(x_2, y_2)]$$

$$[(a_1, b_1)] \leq [(x_1, y_1)]$$

Proposição
A relação $\leq$ definida acima está bem definida.

Demonstração. Precisamos mostrar que se valem

$$[(a_1, b_1)] = [(a_2, b_2)]$$

$$[(x_1, y_1)] = [(x_2, y_2)]$$

$$[(a_1, b_1)] \leq [(x_1, y_1)]$$

então vale $[(a_2, b_2)] \leq [(x_2, y_2)]$.

Aula 16 - Provando

Aula 16 - Provando

Note que as duas primeiras equações se traduzem para $a_1 b_2 = b_1 a_2$ e $x_1 y_2 = y_1 x_2$.

Note que as duas primeiras equações se traduzem para $a_1 b_2 = b_1 a_2$ e $x_1 y_2 = y_1 x_2$. Assim, de $a_1 y_1 \leq b_1 x_1$, multiplicando ambos os lados por $b_2 y_2$ (que é maior que 0), temos

$$a_1 y_1 b_2 y_2 \leq b_1 x_1 b_2 y_2.$$

Note que as duas primeiras equações se traduzem para $a_1 b_2 = b_1 a_2$ e $x_1 y_2 = y_1 x_2$. Assim, de $a_1 y_1 \leq b_1 x_1$, multiplicando ambos os lados por $b_2 y_2$ (que é maior que 0), temos

$$a_1 y_1 b_2 y_2 \leq b_1 x_1 b_2 y_2.$$

Substituindo $a_1 b_2$ por $b_1 a_2$ do lado esquerdo e $x_1 y_2$ por $x_2 y_1$ do lado direito, obtemos:

$$b_1 a_2 y_1 y_2 \leq b_2 y_1 x_2 b_1.$$

Note que as duas primeiras equações se traduzem para $a_1 b_2 = b_1 a_2$ e $x_1 y_2 = y_1 x_2$. Assim, de $a_1 y_1 \leq b_1 x_1$, multiplicando ambos os lados por $b_2 y_2$ (que é maior que 0), temos

$$a_1 y_1 b_2 y_2 \leq b_1 x_1 b_2 y_2.$$

Substituindo $a_1 b_2$ por $b_1 a_2$ do lado esquerdo e $x_1 y_2$ por $x_2 y_1$ do lado direito, obtemos:

$$b_1 a_2 y_1 y_2 \leq b_2 y_1 x_2 b_1.$$

Cancelando $b_1 y_1$ (que é diferente de 0), temos $a_2 y_2 \leq b_2 x_2$, isto é, $[(a_2, b_2)] \leq [(x_2, y_2)]$ como queríamos. □

Aula 16 - É total

Aula 16 - É total

Proposição
A relação $\leq$ definida acima é uma ordem total sobre $\mathbb{Q}$.

Aula 16 - É total

Proposição
A relação $\leq$ definida acima é uma ordem total sobre $\mathbb{Q}$.

Demonstração.
Ver o exercício **??** □

Aula 16 - Notação

Definição
Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Aula 16 - Notação

Definição
Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Note que tal notação fica coerente com o que tínhamos antes.

Definição
Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Note que tal notação fica coerente com o que tínhamos antes. Isto é, $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = a + b$, onde a última soma é entre inteiros.

Definição
Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Note que tal notação fica coerente com o que tínhamos antes. Isto é, $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = a + b$, onde a última soma é entre inteiros. Note que temos a mesma coisa para o produto.

Definição
Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Note que tal notação fica coerente com o que tínhamos antes. Isto é, $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = a + b$, onde a última soma é entre inteiros. Note que temos a mesma coisa para o produto.

Assim, como fizemos antes no caso de $\mathbb{N}$ para $\mathbb{Z}$, vamos considerar que $\mathbb{Z} \subset \mathbb{Q}$ como usualmente.

Aula 16 - É corpo

Veja nos exercícios que, com as operações aqui apresentadas, $\mathbb{Q}$ é corpo.

Aula 17 - Números reais

Aula 17 - Números reais

Começamos estendendo a noção de intervalo apresentada anteriormente.

Aula 17 - Números reais

Começamos estendendo a noção de intervalo apresentada anteriormente. Antes, definimos intervalo apenas para $\mathbb{R}$.

Começamos estendendo a noção de intervalo apresentada anteriormente. Antes, definimos intervalo apenas para $\mathbb{R}$. Mas podemos fazer o mesmo para qualquer conjunto totalmente ordenado:

Começamos estendendo a noção de intervalo apresentada anteriormente. Antes, definimos intervalo apenas para $\mathbb{R}$. Mas podemos fazer o mesmo para qualquer conjunto totalmente ordenado:

Definição
Seja X um conjunto totalmente ordenado. Um subconjunto $A \subset X$ é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in X$ é tal que $a < c < b$, então $c \in A$.

Aula 17 - Exemplos

Note que, nesse contexto, algo ser um intervalo ou não depende de "onde" ele é subconjunto.

Aula 17 - Exemplos

Note que, nesse contexto, algo ser um intervalo ou não depende de "onde" ele é subconjunto.

O conjunto $\{n \in \mathbb{N} : 3 < n \text{ e } n < 20\}$ é um intervalo nos naturais.

Aula 17 - Exemplos

Note que, nesse contexto, algo ser um intervalo ou não depende de "onde" ele é subconjunto.

O conjunto $\{n \in \mathbb{N} : 3 < n \text{ e } n < 20\}$ é um intervalo nos naturais.
O conjunto $\{q \in \mathbb{Q} : 3 < q \text{ e } q < 20\}$ também é um intervalo em $\mathbb{Q}$.

Aula 17 - Exemplos

Note que, nesse contexto, algo ser um intervalo ou não depende de "onde" ele é subconjunto.

O conjunto $\{n \in \mathbb{N} : 3 < n \text{ e } n < 20\}$ é um intervalo nos naturais. O conjunto $\{q \in \mathbb{Q} : 3 < q \text{ e } q < 20\}$ também é um intervalo em $\mathbb{Q}$. Mas o conjunto $\{n \in \mathbb{Q} : 3 < n, n < 20 \text{ e } n \in \mathbb{N}\}$ não é um intervalo em $\mathbb{Q}$.

Aula 17 - Corte de Dedekind

Definição
Chamamos de um **corte de Dedekind** um par (I, J) onde $I, J \subset \mathbb{Q}$ são intervalos não vazios tais que

- $I \cup J = \mathbb{Q}$;
- se $i \in I$, existe $k \in I$ tal que $i < k$;
- dados $i \in I$ e $j \in J$ temos que $i < j$.

Aula 17 - Exemplo

Aula 17 - Exemplo

Exemplo
(I, J) é um corte de Dedekind, onde $I = \{q \in \mathbb{Q} : q < 0\}$ e $J = \{q \in \mathbb{Q} : q \geq 0\}$ (exercício).

Aula 17 - Qual é o truque

Aula 17 - Qual é o truque

O truque com os cortes para se construir os reais é mais ou menos o seguinte: cada corte vai representar um real e a ideia desse real é ser o elemento que fica entre I e J.

Aula 17 - Qual é o truque

O truque com os cortes para se construir os reais é mais ou menos o seguinte: cada corte vai representar um real e a ideia desse real é ser o elemento que fica entre I e J. No exemplo acima, o real representado é o 0.

Aula 17 - Qual é o truque

O truque com os cortes para se construir os reais é mais ou menos o seguinte: cada corte vai representar um real e a ideia desse real é ser o elemento que fica entre I e J. No exemplo acima, o real representado é o 0. Note que ele é o mínimo de J (isso acontece com qualquer outro racional).

Aula 17 - Qual é o truque

O truque com os cortes para se construir os reais é mais ou menos o seguinte: cada corte vai representar um real e a ideia desse real é ser o elemento que fica entre I e J. No exemplo acima, o real representado é o 0. Note que ele é o mínimo de J (isso acontece com qualquer outro racional). A situação fica mais interessante quando o corte representa um irracional, como vamos ver no próximo exemplo (não vamos usar isso no exemplo, mas tenha em mente que o corte representa o número $\sqrt{2}$).

Aula 17 - Exemplo

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício).

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$. Se $q < 0$, $q \in I$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$. Se $q < 0$, $q \in I$. Se $q \geq 0$, temos dois casos.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$. Se $q < 0$, $q \in I$. Se $q \geq 0$, temos dois casos. Se $qq < 2$, então $q \in I$.

Aula 17 - Exemplo

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$. Se $q < 0$, $q \in I$. Se $q \geq 0$, temos dois casos. Se $qq < 2$, então $q \in I$. Se $qq > 2$, temos que $qq \in J$.

Aula 17 - Fazendo as contas

Aula 17 - Fazendo as contas

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$.

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$.

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}.$$

Aula 17 - Fazendo as contas

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}.$$

Primeiramente, note que $k > i$ pois

$$i \quad = \quad \frac{i(i+2)}{i+2}$$

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}.$$

Primeiramente, note que $k > i$ pois

$$\begin{aligned} i &= \frac{i(i+2)}{i+2} \\ &= \frac{ii+2i}{i+2} \end{aligned}$$

Aula 17 - Fazendo as contas

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}.$$

Primeiramente, note que $k > i$ pois

$$\begin{aligned} i &= \frac{i(i+2)}{i+2} \\ &= \frac{ii+2i}{i+2} \\ &< \frac{2+2i}{i+2} \end{aligned}$$

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}.$$

Primeiramente, note que $k > i$ pois

$$\begin{aligned} i &= \frac{i(i+2)}{i+2} \\ &= \frac{ii+2i}{i+2} \\ &< \frac{2+2i}{i+2} \\ &= k \end{aligned}$$

Aula 17 - Fazendo as contas

Note também que $kk < 2$, pois

$$2 - kk \quad = \quad 2 - \frac{2i+2}{i+2}\frac{2i+2}{i+2}$$

Note também que $kk < 2$, pois

$$\begin{aligned} 2 - kk &= 2 - \frac{2i+2}{i+2}\frac{2i+2}{i+2} \\ &= 2 - \frac{4i^2+8i+4}{i^2+4i+4} \end{aligned}$$

Note também que $kk < 2$, pois

$$\begin{aligned} 2 - kk &= 2 - \frac{2i+2}{i+2}\frac{2i+2}{i+2} \\ &= 2 - \frac{4i^2+8i+4}{i^2+4i+4} \\ &= \frac{2i^2+8i+8-(4i^2+8i+4)}{i^2+4i+4} \end{aligned}$$

Aula 17 - Fazendo as contas

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador.

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador. Assim

$$2i^2 + 8i + 8 - 4i^2 - 8i - 4 \quad = \quad 4 - 2i^2$$

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador. Assim

$$\begin{aligned} 2i^2 + 8i + 8 - 4i^2 - 8i - 4 &= 4 - 2i^2 \\ &> 4 - 2 \cdot 2 \end{aligned}$$

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador. Assim

$$\begin{aligned} 2i^2 + 8i + 8 - 4i^2 - 8i - 4 &= 4 - 2i^2 \\ &> 4 - 2 \cdot 2 \\ &= 0 \end{aligned}$$

Ou seja, tal diferença é positiva, como queríamos.

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador. Assim

$$\begin{aligned} 2i^2 + 8i + 8 - 4i^2 - 8i - 4 &= 4 - 2i^2 \\ &> 4 - 2 \cdot 2 \\ &= 0 \end{aligned}$$

Ou seja, tal diferença é positiva, como queríamos.

Finalmente, só precisamos mostrar que, dados $i \in I$ e $j \in J$, temos que $i < j$ - vamos deixar isso como exercício.

Aula 17 - Resultados básicos

Aula 17 - Resultados básicos

Vamos agora provar alguns resultados básicos sobre os cortes.

Lema

Seja (I, J) *um corte de Dedekind. Se* $a \in I$ *e* $b < a$, *então* $b \in I$.

Vamos agora provar alguns resultados básicos sobre os cortes.

Lema

Seja (I, J) *um corte de Dedekind. Se* $a \in I$ *e* $b < a$*, então* $b \in I$*.*

Demonstração.
Suponha que não.

Vamos agora provar alguns resultados básicos sobre os cortes.

Lema

Seja (I, J) *um corte de Dedekind. Se* $a \in I$ *e* $b < a$, *então* $b \in I$.

Demonstração.
Suponha que não. Então $b \in J$.

Vamos agora provar alguns resultados básicos sobre os cortes.

Lema

Seja (I, J) *um corte de Dedekind. Se* $a \in I$ *e* $b < a$*, então* $b \in I$*.*

Demonstração.
Suponha que não. Então $b \in J$. Mas isso contraria a última propriedade da definição de corte. □

Aula 17 - Resultados básicos

Note que se tomarmos $q \in \mathbb{Q}$, existe um corte natural associado a ele:

$$I_q = \{r \in \mathbb{Q} : r < q\}$$

$$J_q = \{r \in \mathbb{Q} : r \geq q\}$$

Note que se tomarmos $q \in \mathbb{Q}$, existe um corte natural associado a ele:

$$I_q = \{r \in \mathbb{Q} : r < q\}$$

$$J_q = \{r \in \mathbb{Q} : r \geq q\}$$

Repare que é o análogo com o que fizemos com o 0 no primeiro exemplo.

Note que se tomarmos $q \in \mathbb{Q}$, existe um corte natural associado a ele:

$$I_q = \{r \in \mathbb{Q} : r < q\}$$

$$J_q = \{r \in \mathbb{Q} : r \geq q\}$$

Repare que é o análogo com o que fizemos com o 0 no primeiro exemplo. Por outro lado, note que não podemos fazer o análogo com $J = \{r \in \mathbb{Q} : r > q\}$, pois neste caso $q \in I$ e, portanto, I teria máximo, o que contraria a definição de corte.

Aula 17 - Resultados básicos

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$. Note que $a \in Y$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$. Note que $a \in Y$. Assim, para todo $z \in X$, temos que $z < a$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$. Note que $a \in Y$. Assim, para todo $z \in X$, temos que $z < a$. Em particular, temos $x < a$.

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição
Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.

Demonstração.
Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$. Note que $a \in Y$. Assim, para todo $z \in X$, temos que $z < a$. Em particular, temos $x < a$. Assim, $x \in A$ pelo lema. □

Aula 17 - Relacionando as ordens

Aula 17 - Relacionando as ordens

A ordem aqui apresentada é compatível com a que vem de $\mathbb{Q}$:

A ordem aqui apresentada é compatível com a que vem de $\mathbb{Q}$:

Proposição
Sejam $q, r \in \mathbb{Q}$. Então $q < r$ se, e somente se, $(I_q, J_q) < (I_r, J_r)$.

A ordem aqui apresentada é compatível com a que vem de $\mathbb{Q}$:

Proposição
Sejam $q, r \in \mathbb{Q}$. Então $q < r$ se, e somente se, $(I_q, J_q) < (I_r, J_r)$.

Demonstração.
Basta notar que, pela definição de I_q, $I_q \subset I_r$ se, e somente se, $q \leq r$. □

Aula 17 - Majorantes

Aula 17 - Majorantes

Definição
Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ um conjunto não vazio. Dizemos $m \in X$ é um **majorante** para A se $a \leq m$ para todo $a \in A$. Dizemos que $A \subset X$ é **limitado superiormente** se A admite um majorante.

Aula 17 - Exemplo

Aula 17 - Exemplo

1 e 3 são majorantes para o conjunto $[0, 1]$ em $\mathbb{Q}$.

Aula 17 - Supremo

Definição
Seja $(X, \leq)$ um conjunto totalmente ordenado. Seja $A \subset X$ um conjunto limitado superiormente. Dizemos que $a \in X$ é um **supremo** de A (notação $\sup A$), se $a = \min\{m : m \text{ é majorante de } A\}$.

Aula 17 - Um caso simples

Proposição
Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.

Proposição
Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.

Demonstração.
Seja $m \in X$ majorante para A.

Proposição
Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.

Demonstração.
Seja $m \in X$ majorante para A. Em particular, $m \geq a$.

Proposição
Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.

Demonstração.
Seja $m \in X$ majorante para A. Em particular, $m \geq a$. Assim, $\sup A \geq a$.

Proposição
Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.

Demonstração.
Seja $m \in X$ majorante para A. Em particular, $m \geq a$. Assim, $\sup A \geq a$. Por outro lado, note que o próprio a é um majorante para A.

Proposição
Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.

Demonstração.
Seja $m \in X$ majorante para A. Em particular, $m \geq a$. Assim, $\sup A \geq a$. Por outro lado, note que o próprio a é um majorante para A. Então $\sup A \leq a$. □

Aula 17 - Exemplo

Aula 17 - Exemplo

Um supremo pode não existir:

Aula 17 - Exemplo

Um supremo pode não existir:

Exemplo
Em $\mathbb{Q}$, não existe $\sup A$, onde $A = \{q \in \mathbb{Q} : q > 0 \wedge q^2 < 2\}$.

Aula 17 - Unicidade

Aula 17 - Unicidade

Mas, se o supremo existe, ele é único:

Mas, se o supremo existe, ele é único:

Proposição
Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ conjunto limitado superiormente. Sejam a, b supremos de A. Então $a = b$.

Mas, se o supremo existe, ele é único:

Proposição
Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ conjunto limitado superiormente. Sejam a, b supremos de A. Então $a = b$.

Demonstração.
Como a é o menor dos majorantes de A e como b é um majorante de A, temos que $a \leq b$.

Mas, se o supremo existe, ele é único:

Proposição
Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ conjunto limitado superiormente. Sejam a, b supremos de A. Então $a = b$.

Demonstração.
Como a é o menor dos majorantes de A e como b é um majorante de A, temos que $a \leq b$. A outra desigualdade é análoga. $\square$

Aula 17 - Completude

Definição
Seja $(X, \leq)$ conjunto totalmente ordenado. Dizemos que $\leq$ é uma **ordem completa** se, para todo $A \subset X$ limitado, existe $a = \sup A$.

Aula 17 - É completa

Aula 17 - É completa

Proposição
A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.

Aula 17 - É completa

Proposição
A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.

Demonstração. Seja $\mathcal{A}$ um conjunto de cortes que seja limitado.

Proposição
A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.

Demonstração. Seja $\mathcal{A}$ um conjunto de cortes que seja limitado. Isto é, existe (I, J) tal que, para todo $(A, B) \in \mathcal{A}$, temos que $A \subset I$.

Proposição
A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.

Demonstração. Seja $\mathcal{A}$ um conjunto de cortes que seja limitado. Isto é, existe (I, J) tal que, para todo $(A, B) \in \mathcal{A}$, temos que $A \subset I$. Vamos provar que existe um supremo para $\mathcal{A}$.

Proposição
A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.

Demonstração. Seja $\mathcal{A}$ um conjunto de cortes que seja limitado. Isto é, existe (I, J) tal que, para todo $(A, B) \in \mathcal{A}$, temos que $A \subset I$. Vamos provar que existe um supremo para $\mathcal{A}$. Considere (X, Y) onde

$$X = \bigcup_{(A,B)\in\mathcal{A}} A$$

$$Y = \mathbb{Q} \setminus X$$

Aula 17 - Provando

Aula 17 - Provando

Vamos provar que $(X, Y) = \sup \mathcal{A}$.

Aula 17 - Provando

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$.

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$.

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que X é um intervalo.

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que X é um intervalo. De fato, sejam $a, b \in X$ e $c \in \mathbb{Q}$ tais que $a < c < b$.

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que X é um intervalo. De fato, sejam $a, b \in X$ e $c \in \mathbb{Q}$ tais que $a < c < b$. Seja A tal que $(A, B) \in \mathcal{A}$ e tal que $b \in A$ (existe pela definição de X).

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que X é um intervalo. De fato, sejam $a, b \in X$ e $c \in \mathbb{Q}$ tais que $a < c < b$. Seja A tal que $(A, B) \in \mathcal{A}$ e tal que $b \in A$ (existe pela definição de X). Pelo Lema 17.4, temos que $c \in A$ e, portanto, $c \in X$ como queríamos.

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que X é um intervalo. De fato, sejam $a, b \in X$ e $c \in \mathbb{Q}$ tais que $a < c < b$. Seja A tal que $(A, B) \in \mathcal{A}$ e tal que $b \in A$ (existe pela definição de X). Pelo Lema 17.4, temos que $c \in A$ e, portanto, $c \in X$ como queríamos. Vamos deixar o restante da prova de que (X, Y) é um corte como exercício.

Aula 17 - Provando

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor. Para isso, basta mostrar que $X \subset I$.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor. Para isso, basta mostrar que $X \subset I$. De fato, dado $x \in X$, temos que $x \in A$ para algum $(A, B) \in \mathcal{A}$.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor. Para isso, basta mostrar que $X \subset I$. De fato, dado $x \in X$, temos que $x \in A$ para algum $(A, B) \in \mathcal{A}$. Como (I, J) é majorante, temos que $A \subset I$.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor. Para isso, basta mostrar que $X \subset I$. De fato, dado $x \in X$, temos que $x \in A$ para algum $(A, B) \in \mathcal{A}$. Como (I, J) é majorante, temos que $A \subset I$. Logo, $x \in I$ como queríamos. $\square$

Aula 17 - Os reais

Finalmente, conseguimos nossa primeira definição do conjunto $\mathbb{R}$:

Definição
Chamamos de $\mathbb{R}$ o conjunto de todos os cortes de Dedekind com a ordem apresentada acima.

Aula 17 - Operações

Aula 17 - Operações

As operações sobre $\mathbb{R}$ podem ser definidas de maneira natural a partir das operações definidas sobre $\mathbb{Q}$.

As operações sobre $\mathbb{R}$ podem ser definidas de maneira natural a partir das operações definidas sobre $\mathbb{Q}$. Por exemplo, $(A, B) + (X, Y) = (A \oplus X, B \oplus Y)$, onde $I \oplus J = \{i + j : i \in I, j \in j\}$.

Aula 18 - Sequência convergente

Aula 18 - Sequência convergente

Nesta seção vamos apresentar uma segunda maneira de definir números reais.

Aula 18 - Sequência convergente

Nesta seção vamos apresentar uma segunda maneira de definir números reais.

Começamos com a ideia do que é uma sequência ser convergente para um ponto:

Aula 18 - Sequência convergente

Nesta seção vamos apresentar uma segunda maneira de definir números reais.

Começamos com a ideia do que é uma sequência ser convergente para um ponto:

Definição
Seja $(q_n)_{n\in\mathbb{N}}$ uma sequência de racionais. Dizemos que tal sequência **converge para** q se, para todo $\varepsilon \in \mathbb{Q}_{>0}$, existe $n_0 \in \mathbb{N}$ tal que, para todo $m \geq n_0$, temos que $|q_m - q| < \varepsilon$.

Aula 18 - Exemplos

Aula 18 - Exemplos

Exemplo
Considere $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = q$ para todo $n \in \mathbb{N}$.

Exemplo
Considere $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = q$ para todo $n \in \mathbb{N}$. Vamos provar que $(q_n)_{n\in\mathbb{N}}$ converge para q.

Exemplo
Considere $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = q$ para todo $n \in \mathbb{N}$. Vamos provar que $(q_n)_{n\in\mathbb{N}}$ converge para q. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, temos

$$|q_n - q| = 0 < \varepsilon.$$

Exemplo
Considere $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = q$ para todo $n \in \mathbb{N}$. Vamos provar que $(q_n)_{n\in\mathbb{N}}$ converge para q. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, temos

$$|q_n - q| = 0 < \varepsilon.$$

Ou seja, podemos tomar $n_0 = 0$.

Aula 18 - Exemplos

Exemplo
A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0.

Exemplo
A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, note que $\varepsilon = \frac{a}{b}$ com $a, b > 0$.

Exemplo
A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, note que $\varepsilon = \frac{a}{b}$ com $a, b > 0$. Seja $n_0 = b$.

Exemplo
A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, note que $\varepsilon = \frac{a}{b}$ com $a, b > 0$. Seja $n_0 = b$. Note que

$$\frac{1}{b} < \frac{a}{b}$$

Exemplo
A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, note que $\varepsilon = \frac{a}{b}$ com $a, b > 0$. Seja $n_0 = b$. Note que

$$\frac{1}{b} < \frac{a}{b}$$

Assim, dado $m \geq n_0$, temos

$$|\frac{1}{m+1} - 0| = \frac{1}{m+1} < \frac{1}{m} \leq \frac{1}{n_0} = \frac{1}{b} < \frac{a}{b} = \varepsilon$$

Aula 18 - Sequência de Cauchy

Aula 18 - Sequência de Cauchy

Intuitivamente, uma sequência convergente tem seus pontos ficando arbitrariamente próximos de um ponto fixado (para onde a sequência converge).

Aula 18 - Sequência de Cauchy

Intuitivamente, uma sequência convergente tem seus pontos ficando arbitrariamente próximos de um ponto fixado (para onde a sequência converge). Podemos mudar um pouco o conceito e pedir que os pontos da sequência fiquem próximos uns dos outros - mas não necessariamente próximos de um ponto fixado:

Aula 18 - Sequência de Cauchy

Intuitivamente, uma sequência convergente tem seus pontos ficando arbitrariamente próximos de um ponto fixado (para onde a sequência converge). Podemos mudar um pouco o conceito e pedir que os pontos da sequência fiquem próximos uns dos outros - mas não necessariamente próximos de um ponto fixado:

Definição
Seja $(q_n)_{n\in\mathbb{N}}$ uma sequência de racionais. Dizemos que $(q_n)_{n\in\mathbb{N}}$ é uma **sequência de Cauchy** se, para todo $\varepsilon \in \mathbb{Q}_{>0}$, existe $n_0 \in \mathbb{N}$ tal que, para todo $m, n \geq n_0$ temos $|q_n - q_m| < \varepsilon$.

Aula 18 - Relacionando

Se os pontos da sequência ficam próximos de um ponto fixado, eles ficam próximos entre si:

Proposição
Se $(q_n)_{n\in\mathbb{N}}$ é uma sequência convergente, então $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.

Se os pontos da sequência ficam próximos de um ponto fixado, eles ficam próximos entre si:

Proposição
Se $(q_n)_{n\in\mathbb{N}}$ é uma sequência convergente, então $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.

Demonstração. Seja q tal que $(q_n)_{n\in\mathbb{N}}$ converge para q.

Se os pontos da sequência ficam próximos de um ponto fixado, eles ficam próximos entre si:

Proposição
Se $(q_n)_{n\in\mathbb{N}}$ é uma sequência convergente, então $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.

Demonstração. Seja q tal que $(q_n)_{n\in\mathbb{N}}$ converge para q. Seja $\varepsilon \in \mathbb{Q}_{>0}$.

Se os pontos da sequência ficam próximos de um ponto fixado, eles ficam próximos entre si:

Proposição
Se $(q_n)_{n\in\mathbb{N}}$ é uma sequência convergente, então $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.

Demonstração. Seja q tal que $(q_n)_{n\in\mathbb{N}}$ converge para q. Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(q_n)_{n\in\mathbb{N}}$ converge para q, existe n_0 tal que, para todo $k \geq n_0$, temos

$$|q_k - q| < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Sejam $n, m \geq n_0$.

Sejam $n, m \geq n_0$. Temos

$$|q_n - q_m| \quad = \quad |q_n - q + q - q_m|$$

Sejam $n, m \geq n_0$. Temos

$$\begin{aligned} |q_n - q_m| &= |q_n - q + q - q_m| \\ &\leq |q_n - q| + |q - q_m| \end{aligned}$$

Sejam $n, m \geq n_0$. Temos

$$\begin{aligned} |q_n - q_m| &= |q_n - q + q - q_m| \\ &\leq |q_n - q| + |q - q_m| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \end{aligned}$$

Sejam $n, m \geq n_0$. Temos

$$\begin{aligned} |q_n - q_m| &= |q_n - q + q - q_m| \\ &\leq |q_n - q| + |q - q_m| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

□

Aula 18 - Problemas e soluções

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$.

Aula 18 - Problemas e soluções

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$. A ideia aqui será representar cada real por uma sequência de Cauchy - lembrando que as sequências de Cauchy neste contexto são formadas por números racionais.

Aula 18 - Problemas e soluções

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$. A ideia aqui será representar cada real por uma sequência de Cauchy - lembrando que as sequências de Cauchy neste contexto são formadas por números racionais. Um problema que aparece aqui é a falta de unicidade.

Aula 18 - Problemas e soluções

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$. A ideia aqui será representar cada real por uma sequência de Cauchy - lembrando que as sequências de Cauchy neste contexto são formadas por números racionais. Um problema que aparece aqui é a falta de unicidade. Para cada real existem diversas sequências de Cauchy que convergem para ele.

Aula 18 - Problemas e soluções

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$. A ideia aqui será representar cada real por uma sequência de Cauchy - lembrando que as sequências de Cauchy neste contexto são formadas por números racionais. Um problema que aparece aqui é a falta de unicidade. Para cada real existem diversas sequências de Cauchy que convergem para ele. Por isso, teremos que trabalhar com classes de equivalências e considerar como iguais as sequências que convergem para o mesmo lugar.

Aula 18 - Problemas e soluções

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$. A ideia aqui será representar cada real por uma sequência de Cauchy - lembrando que as sequências de Cauchy neste contexto são formadas por números racionais. Um problema que aparece aqui é a falta de unicidade. Para cada real existem diversas sequências de Cauchy que convergem para ele. Por isso, teremos que trabalhar com classes de equivalências e considerar como iguais as sequências que convergem para o mesmo lugar. Mas como ainda não temos para onde essas sequências convergem (afinal, ainda estamos definindo os reais), precisamos usar um truque parecido com a definição de sequência de Cauchy.

Aula 18 - Uma relação de equivalência

Aula 18 - Uma relação de equivalência

Definição
Sejam $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ sequências de Cauchy.

Aula 18 - Uma relação de equivalência

Definição
Sejam $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ sequências de Cauchy. Dizemos que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ se $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0.

Aula 18 - É uma relação de equivalência

Aula 18 - É uma relação de equivalência

Proposição
A relação $\cong$ definida acima é uma relação de equivalência.

Aula 18 - É uma relação de equivalência

Proposição
A relação $\cong$ definida acima é uma relação de equivalência.

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Aula 18 - É uma relação de equivalência

Proposição
A relação $\cong$ definida acima é uma relação de equivalência.

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$.

Aula 18 - É uma relação de equivalência

Proposição
A relação $\cong$ definida acima é uma relação de equivalência.

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, então a sequência $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0.

Aula 18 - É uma relação de equivalência

Proposição
A relação $\cong$ definida acima é uma relação de equivalência.

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, então a sequência $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0. Ou seja, dado $\varepsilon \in \mathbb{Q}_{>0}$, existe n_0 tal que, para todo $k \geq n_0$, temos que $|x_k - y_k| < \varepsilon$.

Aula 18 - É uma relação de equivalência

Proposição
A relação $\cong$ definida acima é uma relação de equivalência.

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, então a sequência $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0. Ou seja, dado $\varepsilon \in \mathbb{Q}_{>0}$, existe n_0 tal que, para todo $k \geq n_0$, temos que $|x_k - y_k| < \varepsilon$. Como $|x_k - y_k| = |y_k - x_k|$, temos o resultado.

Aula 18 - Provando

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$.

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Assim, considere $n_0 = \max\{n_1, n_2\}$.

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Assim, considere $n_0 = \max\{n_1, n_2\}$. Dado $k \geq n_0$, temos:

$$|x_k - z_k| \quad = \quad |x_k - y_k + y_k - z_k|$$

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Assim, considere $n_0 = \max\{n_1, n_2\}$. Dado $k \geq n_0$, temos:

$$\begin{aligned} |x_k - z_k| &= |x_k - y_k + y_k - z_k| \\ &\leq |x_k - y_k| + |y_k - z_k| \end{aligned}$$

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Assim, considere $n_0 = \max\{n_1, n_2\}$. Dado $k \geq n_0$, temos:

$$\begin{aligned} |x_k - z_k| &= |x_k - y_k + y_k - z_k| \\ &\leq |x_k - y_k| + |y_k - z_k| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \end{aligned}$$

Aula 18 - Provando

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Assim, considere $n_0 = \max\{n_1, n_2\}$. Dado $k \geq n_0$, temos:

$$\begin{aligned} |x_k - z_k| &= |x_k - y_k + y_k - z_k| \\ &\leq |x_k - y_k| + |y_k - z_k| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$.

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$.

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$. Então $\varepsilon = |x - y| > 0$.

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$. Então $\varepsilon = |x - y| > 0$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$,

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$. Então $\varepsilon = |x - y| > 0$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$,

$$|x_k - y_k| < \frac{\varepsilon}{3}.$$

Aula 18 - Se convergem para o mesmo ponto, são equivalentes

Proposição
Se $(x_n)_{n\in\mathbb{N}}$ *e* $(y_n)_{n\in\mathbb{N}}$ *convergem para* x *e* y *respectivamente, então* $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ *se, e somente se,* $x = y$.

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$. Então $\varepsilon = |x - y| > 0$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$,

$$|x_k - y_k| < \frac{\varepsilon}{3}.$$

Como $(x_n)_{n\in\mathbb{N}}$ converge para x, existe n_2 tal que, para todo $k \geq n_2$,

$$|x - x_k| < \frac{\varepsilon}{3}.$$

Aula 18 - Provando

Analogamente, existe n_3 tal que, para todo $k \geq n_3$,

$$|y - y_k| < \frac{\varepsilon}{3}.$$

Assim, seja $k = \max\{n_1, n_2, n_3\}$. Temos

$$|x - y| \quad = \quad |x - x_k + x_k - y_k + y_k - y|$$

Analogamente, existe n_3 tal que, para todo $k \geq n_3$,

$$|y - y_k| < \frac{\varepsilon}{3}.$$

Assim, seja $k = \max\{n_1, n_2, n_3\}$. Temos

$$\begin{aligned} |x - y| &= |x - x_k + x_k - y_k + y_k - y| \\ &\leq |x - x_k| + |x_k - y_k| + |y_k - y| \end{aligned}$$

Analogamente, existe n_3 tal que, para todo $k \geq n_3$,

$$|y - y_k| < \frac{\varepsilon}{3}.$$

Assim, seja $k = \max\{n_1, n_2, n_3\}$. Temos

$$\begin{aligned} |x - y| &= |x - x_k + x_k - y_k + y_k - y| \\ &\leq |x - x_k| + |x_k - y_k| + |y_k - y| \\ &< \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} \end{aligned}$$

Analogamente, existe n_3 tal que, para todo $k \geq n_3$,

$$|y - y_k| < \frac{\varepsilon}{3}.$$

Assim, seja $k = \max\{n_1, n_2, n_3\}$. Temos

$$\begin{aligned} |x - y| &= |x - x_k + x_k - y_k + y_k - y| \\ &\leq |x - x_k| + |x_k - y_k| + |y_k - y| \\ &< \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} \\ &= \varepsilon \end{aligned}$$

contrariando a definição de ε.

Aula 18 - Provando

Aula 18 - Provando

Agora suponha $x = y$.

Aula 18 - Provando

Agora suponha $x = y$. Seja $\varepsilon > 0$.

Aula 18 - Provando

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Considere $n_0 = \max\{n_1, n_2\}$. Assim, dado $k \geq n_0$, temos

$$|x_k - y_k| \quad = \quad |x_k - x + x - y_k|$$

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Considere $n_0 = \max\{n_1, n_2\}$. Assim, dado $k \geq n_0$, temos

$$\begin{aligned} |x_k - y_k| &= |x_k - x + x - y_k| \\ &\leq |x_k - x| + |x - y_k| \end{aligned}$$

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Considere $n_0 = \max\{n_1, n_2\}$. Assim, dado $k \geq n_0$, temos

$$\begin{aligned} |x_k - y_k| &= |x_k - x + x - y_k| \\ &\leq |x_k - x| + |x - y_k| \\ &= |x_k - x| + |y - y_k| \end{aligned}$$

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Considere $n_0 = \max\{n_1, n_2\}$. Assim, dado $k \geq n_0$, temos

$$\begin{aligned} |x_k - y_k| &= |x_k - x + x - y_k| \\ &\leq |x_k - x| + |x - y_k| \\ &= |x_k - x| + |y - y_k| \\ &< \varepsilon \end{aligned}$$

□

Aula 18 - Definindo $\mathbb{R}$

Definição
Podemos definir $\mathbb{R}$ como sendo o conjunto de todas as classes de equivalência de sequências de Cauchy de racionais pela relação acima.

Aula 18 - Soma

Como exemplo, vamos fazer a soma.

Aula 18 - Soma

Como exemplo, vamos fazer a soma. Dadas duas sequências $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$, definimos $[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}]$ como $[(x_n + y_n)_{n\in\mathbb{N}}]$.

Aula 18 - Soma

Como exemplo, vamos fazer a soma. Dadas duas sequências $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$, definimos $[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}]$ como $[(x_n + y_n)_{n\in\mathbb{N}}]$.

Vejamos que isso está bem definido.

Aula 18 - Soma

Como exemplo, vamos fazer a soma. Dadas duas sequências $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$, definimos $[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}]$ como $[(x_n + y_n)_{n\in\mathbb{N}}]$.

Vejamos que isso está bem definido. Vamos começar provando que $x_n + y_n$ é de Cauchy.

Como exemplo, vamos fazer a soma. Dadas duas sequências $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$, definimos $[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}]$ como $[(x_n + y_n)_{n\in\mathbb{N}}]$.

Vejamos que isso está bem definido. Vamos começar provando que $x_n + y_n$ é de Cauchy. Seja $\varepsilon > 0$. Sejam n_x, n_y tais que, se $n, m > n_x$,

$$|x_n - x_m| < \frac{\varepsilon}{2}$$

e que, se $n, m > n_y$,

$$|y_n - y_m| < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Aula 18 - Provando

Seja $n_0 > n_x, n_y$.

Seja $n_0 > n_x, n_y$. Temos então que, dados $n, m > n_0$,

$$|(x_n + y_n) - (x_m - y_m)| \quad \leq \quad |x_n - x_m| + |y_n - y_m|$$

Seja $n_0 > n_x, n_y$. Temos então que, dados $n, m > n_0$,

$$\begin{aligned} |(x_n + y_n) - (x_m - y_m)| &\leq |x_n - x_m| + |y_n - y_m| \\ &< \frac{e}{2} + \frac{e}{2} \end{aligned}$$

Seja $n_0 > n_x, n_y$. Temos então que, dados $n, m > n_0$,

$$\begin{aligned} |(x_n + y_n) - (x_m - y_m)| &\leq |x_n - x_m| + |y_n - y_m| \\ &< \tfrac{e}{2} + \tfrac{e}{2} \\ &= \varepsilon \end{aligned}$$

Para terminar que está bem definida, resta mostrar que, se $(x_n)_{n\in\mathbb{N}} \cong (a_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (b_n)_{n\in\mathbb{N}}$, então $(x_n + y_n)_{n\in\mathbb{N}} \cong (a_n + b_n)_{n\in\mathbb{N}}$.

Para terminar que está bem definida, resta mostrar que, se $(x_n)_{n\in\mathbb{N}} \cong (a_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (b_n)_{n\in\mathbb{N}}$, então $(x_n + y_n)_{n\in\mathbb{N}} \cong (a_n + b_n)_{n\in\mathbb{N}}$. De fato, fixe $\varepsilon > 0$.

Para terminar que está bem definida, resta mostrar que, se $(x_n)_{n\in\mathbb{N}} \cong (a_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (b_n)_{n\in\mathbb{N}}$, então $(x_n + y_n)_{n\in\mathbb{N}} \cong (a_n + b_n)_{n\in\mathbb{N}}$. De fato, fixe $\varepsilon > 0$. Sejam n_x, n_y tais que, se $n > n_x$,

$$|x_n - a_n| < \frac{\varepsilon}{2}$$

e, se $n > n_y$,

$$y_n - b_n < \frac{\varepsilon}{2}.$$

Aula 18 - Provando

Aula 18 - Provando

Fixe $n_0 > n_x, n_y$.

Fixe $n_0 > n_x, n_y$. Assim, dado $n > n_0$, temos

$$|(x_n + y_n) - (a_n - b_n) \quad \leq \quad |x_n - a_n| + |y_n - b_n|$$

Fixe $n_0 > n_x, n_y$. Assim, dado $n > n_0$, temos

$$\begin{aligned} |(x_n + y_n) - (a_n - b_n) &\leq |x_n - a_n| + |y_n - b_n| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \end{aligned}$$

Fixe $n_0 > n_x, n_y$. Assim, dado $n > n_0$, temos

$$\begin{aligned} |(x_n + y_n) - (a_n - b_n) &\leq |x_n - a_n| + |y_n - b_n| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

Aula 19 - Cardinalidade

Definição
Sejam A e B dois conjuntos. Dizemos que A e B tem a mesma **cardinalidade** se existe $f : A \to B$ bijetora. Notação: $|A| = |B|$.

Aula 19 - Exemplos

Aula 19 - Exemplos

Proposição
$|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$

Proposição
$|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$

Demonstração.
Basta considerar $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ dada por $f(n) = n + 1$. □

Aula 19 - Exemplos

Aula 19 - Exemplos

Proposição
Considere $P = \{n \in \mathbb{N} : n \text{ é par}\}$. *Então* $|P| = |\mathbb{N}|$.

Proposição
Considere $P = \{n \in \mathbb{N} : n \text{ é par}\}$. *Então* $|P| = |\mathbb{N}|$.

Demonstração.
Basta notar que a função $f : \mathbb{N} \to P$ dada por $f(n) = 2n$ é uma bijeção (exercício). □

Aula 19 - Transitividade

Proposição
Sejam A, B, C conjuntos. Se $|A| = |B|$ e $|B| = |C|$, então $|A| = |C|$.

Proposição
Sejam A, B, C conjuntos. Se $|A| = |B|$ e $|B| = |C|$, então $|A| = |C|$.

Demonstração.
Sejam $f : A \to B$ e $g : B \to C$ funções bijetoras.

Proposição
Sejam A, B, C conjuntos. Se $|A| = |B|$ e $|B| = |C|$, então $|A| = |C|$.

Demonstração.
Sejam $f : A \to B$ e $g : B \to C$ funções bijetoras. Note que $g \circ f : A \to C$ é bijetora (exercício). □

Aula 19 - Mais exemplos

Aula 19 - Mais exemplos

Proposição
Considere $I = \{n \in \mathbb{N} : n \text{ é ímpar}\}$. *Então* $|I| = |\mathbb{N}|$.

Proposição
Considere $I = \{n \in \mathbb{N} : n \text{ é ímpar}\}$. *Então* $|I| = |\mathbb{N}|$.

Demonstração.
Basta notar que $f : \mathbb{N} \to I$ dada por $f(n) = 2n + 1$ é bijetora (exercício). □

Aula 19 - Mais exemplos

Corolário
$|P| = |I|$.

Aula 19 - Mais exemplos

Aula 19 - Mais exemplos

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Aula 19 - Mais exemplos

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício).

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora.

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora. Seja $z \in \mathbb{Z}$. Se $z \geq 0$, tome $n = 2z$.

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora. Seja $z \in \mathbb{Z}$. Se $z \geq 0$, tome $n = 2z$. Note que $f(n) = \frac{2z}{2} = z$.

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora. Seja $z \in \mathbb{Z}$. Se $z \geq 0$, tome $n = 2z$. Note que $f(n) = \frac{2z}{2} = z$. Se $z < 0$, tome $n = -2z - 1$.

Proposição
$|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração.

Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora. Seja $z \in \mathbb{Z}$. Se $z \geq 0$, tome $n = 2z$. Note que $f(n) = \frac{2z}{2} = z$. Se $z < 0$, tome $n = -2z - 1$. Note que $f(n) = -\frac{-2z-1+1}{2} = z$. □

Aula 19 - Dificuldades

Aula 19 - Dificuldades

Nem sempre é fácil verificar a existência de funções injetoras.

Aula 19 - Dificuldades

Nem sempre é fácil verificar a existência de funções injetoras. Por exemplo, pode-se provar que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Nem sempre é fácil verificar a existência de funções injetoras. Por exemplo, pode-se provar que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Uma maneira é você perceber que a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por

Nem sempre é fácil verificar a existência de funções injetoras. Por exemplo, pode-se provar que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Uma maneira é você perceber que a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por

$$f(a, b) = \frac{1}{2}(a + b)(a + b + 1) + b$$

é bijetora.

Nem sempre é fácil verificar a existência de funções injetoras. Por exemplo, pode-se provar que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Uma maneira é você perceber que a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por

$$f(a, b) = \frac{1}{2}(a + b)(a + b + 1) + b$$

é bijetora.

Não é tarefa simples encontrar uma função como acima, nem mostrar que ela de fato é bijetora (vale tentar um pouco).

Aula 19 - Cantor-Bernstein-Schroeder

Para contornar esse tipo de problema, o seguinte resultado ajuda bastante:

Teorema (Cantor-Bernstein-Schroeder)

Sejam A, B conjuntos e sejam $f : A \to B$ e $g : B \to A$ funções injetoras. Então $|A| = |B|$.

Para contornar esse tipo de problema, o seguinte resultado ajuda bastante:

Teorema (Cantor-Bernstein-Schroeder)

Sejam A, B conjuntos e sejam $f : A \to B$ e $g : B \to A$ funções injetoras. Então $|A| = |B|$.

Ver desenho na lousa, depois leia nas notas de aula.

Aula 19 - Aplicando

Aula 19 - Aplicando

Assim, fica mais fácil mostrar o resultado que comentamos:

Assim, fica mais fácil mostrar o resultado que comentamos:

Proposição
$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Assim, fica mais fácil mostrar o resultado que comentamos:

Proposição
$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Demonstração.
Considere $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $f(n) = (n, n)$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $g(a, b) = 2^a 3^b$.

Assim, fica mais fácil mostrar o resultado que comentamos:

Proposição
$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Demonstração.
Considere $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $f(n) = (n, n)$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $g(a, b) = 2^a 3^b$. Note que as duas funções são injetoras facilmente. □

Aula 19 - Aplicando

Também podemos provar o seguinte:

Proposição
$|\mathbb{Q}| = |\mathbb{N}|$.

Também podemos provar o seguinte:

Proposição
$|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração.
Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora.

Também podemos provar o seguinte:

Proposição
$|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração.
Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora.

Por outro lado, podemos tomar a função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(\frac{a}{b}) = (a, b)$, onde $\frac{a}{b}$ está na forma simplificada.

Também podemos provar o seguinte:

Proposição
$|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração.
Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora.

Por outro lado, podemos tomar a função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(\frac{a}{b}) = (a, b)$, onde $\frac{a}{b}$ está na forma simplificada. Note que tal função é injetora.

Também podemos provar o seguinte:

Proposição
$|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração.
Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora. Por outro lado, podemos tomar a função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(\frac{a}{b}) = (a, b)$, onde $\frac{a}{b}$ está na forma simplificada. Note que tal função é injetora. Como $|\mathbb{N}| = |\mathbb{Z}|$, temos que $|\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$ (veja os alongamentos) e como $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, temos que $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$.

Também podemos provar o seguinte:

Proposição
$|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração.
Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora. Por outro lado, podemos tomar a função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(\frac{a}{b}) = (a, b)$, onde $\frac{a}{b}$ está na forma simplificada. Note que tal função é injetora. Como $|\mathbb{N}| = |\mathbb{Z}|$, temos que $|\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$ (veja os alongamentos) e como $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, temos que $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$. Assim, existe $h : \mathbb{Q} \to \mathbb{N}$ injetora. □

Aula 19 - Partes aumenta de cardinalidade

Aula 19 - Partes aumenta de cardinalidade

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração.
Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção.

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração.
Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$.

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração.
Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$. Como f é uma bijeção e $A \in \wp(\mathbb{N})$, temos que existe $b \in \mathbb{N}$ tal que $f(b) = A$.

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração.
Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$. Como f é uma bijeção e $A \in \wp(\mathbb{N})$, temos que existe $b \in \mathbb{N}$ tal que $f(b) = A$. Vamos ver que isso dá uma contradição.

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração.
Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$. Como f é uma bijeção e $A \in \wp(\mathbb{N})$, temos que existe $b \in \mathbb{N}$ tal que $f(b) = A$. Vamos ver que isso dá uma contradição. Note que se $b \in A$, então $b \in f(b)$ e, portanto, $b \notin A$.

Proposição

$|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração.
Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$. Como f é uma bijeção e $A \in \wp(\mathbb{N})$, temos que existe $b \in \mathbb{N}$ tal que $f(b) = A$. Vamos ver que isso dá uma contradição. Note que se $b \in A$, então $b \in f(b)$ e, portanto, $b \notin A$. Por outro lado, se $b \notin A$, então $b \notin f(b)$ e, portanto, $b \in A$. □

Aula 19 - $\mathbb{R}$ e $\wp(\mathbb{N})$

Proposição

Existe uma função injetora de $\mathbb{R}$ *em* $\wp(\mathbb{N})$.

Proposição

Existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{N})$.

Demonstração. Note que basta provarmos que existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{Q})$.

Proposição

Existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{N})$.

Demonstração. Note que basta provarmos que existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{Q})$. Para cada $r \in \mathbb{R}$, existe $(q_n^r)_{n\in\mathbb{N}}$ sequência de racionais que converge para r.

Proposição

Existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{N})$.

Demonstração. Note que basta provarmos que existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{Q})$. Para cada $r \in \mathbb{R}$, existe $(q_n^r)_{n\in\mathbb{N}}$ sequência de racionais que converge para r. Podemos tomar tal sequência de forma que $x_n^r \neq x_m^r$ se $n \neq m$ (pense um pouco para se convencer disso).

Proposição

Existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{N})$.

Demonstração. Note que basta provarmos que existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{Q})$. Para cada $r \in \mathbb{R}$, existe $(q_n^r)_{n\in\mathbb{N}}$ sequência de racionais que converge para r. Podemos tomar tal sequência de forma que $x_n^r \neq x_m^r$ se $n \neq m$ (pense um pouco para se convencer disso). Vamos provar que a função $f : \mathbb{R} \to \wp(\mathbb{Q})$ dada por

$$f(r) = \{x_n^r : n \in \mathbb{N}\}$$

é injetora.

Aula 19 - Provando

Aula 19 - Provando

Sejam $r \neq s \in \mathbb{R}$.

Aula 19 - Provando

Sejam $r \neq s \in \mathbb{R}$. Considere $\varepsilon = |r - s|$.

Sejam $r \neq s \in \mathbb{R}$. Considere $\varepsilon = |r - s|$. Como $(x_n^r)_{n\in\mathbb{N}}$ converge para r, existe n_r tal que, se $n \geq n_r$, temos

$$|x_n^r - r| < \frac{\varepsilon}{2}.$$

Sejam $r \neq s \in \mathbb{R}$. Considere $\varepsilon = |r - s|$. Como $(x_n^r)_{n\in\mathbb{N}}$ converge para r, existe n_r tal que, se $n \geq n_r$, temos

$$|x_n^r - r| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_s tal que, se $n \geq n_s$, temos

$$|x_n^s - s| < \frac{\varepsilon}{2}.$$

Sejam $r \neq s \in \mathbb{R}$. Considere $\varepsilon = |r - s|$. Como $(x_n^r)_{n\in\mathbb{N}}$ converge para r, existe n_r tal que, se $n \geq n_r$, temos

$$|x_n^r - r| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_s tal que, se $n \geq n_s$, temos

$$|x_n^s - s| < \frac{\varepsilon}{2}.$$

Vamos mostrar que $f(x_r) \cap f(x_s)$ é finito - note que isso prova que $f(x_r) \neq f(x_s)$ já que eles são infinitos.

Aula 19 - Provando

Suponha que não, então existe $a \in f(x_r) \cap f(x_s)$ tal que $a = x_n^r$ e $a = x_k^s$ com $n > n_r$ e $k > n_s$.

Suponha que não, então existe $a \in f(x_r) \cap f(x_s)$ tal que $a = x_n^r$ e $a = x_k^s$ com $n > n_r$ e $k > n_s$. Assim,

$$|r - s| \quad = \quad |r - a + a - s|$$

Suponha que não, então existe $a \in f(x_r) \cap f(x_s)$ tal que $a = x_n^r$ e $a = x_k^s$ com $n > n_r$ e $k > n_s$. Assim,

$$\begin{aligned} |r - s| &= |r - a + a - s| \\ &\leq |r - a| + |a - s| \end{aligned}$$

Suponha que não, então existe $a \in f(x_r) \cap f(x_s)$ tal que $a = x_n^r$ e $a = x_k^s$ com $n > n_r$ e $k > n_s$. Assim,

$$\begin{aligned} |r - s| &= |r - a + a - s| \\ &\leq |r - a| + |a - s| \\ &= |r - x_n^r| + |x_k^s - s| \end{aligned}$$

Suponha que não, então existe $a \in f(x_r) \cap f(x_s)$ tal que $a = x_n^r$ e $a = x_k^s$ com $n > n_r$ e $k > n_s$. Assim,

$$\begin{aligned} |r-s| &= |r-a+a-s| \\ &\leq |r-a|+|a-s| \\ &= |r-x_n^r|+|x_k^s-s| \\ &< \varepsilon \end{aligned}$$

contradição. □

Aula 19 - Função característica

Definição

Dados conjuntos $A \subset B$, denotamos por $\chi_A^B : B \to \{0,1\}$ a função dada por

$$\chi_A^B(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

Chamamos tal função de **função característica** de A em B.

Normalmente, quando B está claro no contexto, o omitimos.

Aula 19 - Mesma cardinalidade

Aula 19 - Mesma cardinalidade

Proposição
$|\mathcal{F}| = |\wp(\mathbb{N})|$ *onde* $\mathcal{F} = \{\chi_A^{\mathbb{N}} : A \subset \mathbb{N}\}$.

Proposição
$|\mathcal{F}| = |\wp(\mathbb{N})|$ *onde* $\mathcal{F} = \{\chi_A^{\mathbb{N}} : A \subset \mathbb{N}\}$.

Demonstração.
Basta notar que a função $\varphi : \mathcal{F} \to \wp(\mathbb{N})$ dada por $\varphi(\chi_A) = A$ é bijetora. □

Aula 19 - Existe uma injetora

Aula 19 - Existe uma injetora

Proposição
Existe uma função injetora de $\wp(\mathbb{N})$ *em* $\mathbb{R}$.

Aula 19 - Existe uma injetora

Proposição
Existe uma função injetora de $\wp(\mathbb{N})$ em $\mathbb{R}$.

Demonstração.
Note que é suficiente mostrarmos que existe uma função injetora de $\mathcal{F}$ em $\mathbb{R}$.

Aula 19 - Existe uma injetora

Proposição
Existe uma função injetora de $\wp(\mathbb{N})$ em $\mathbb{R}$.

Demonstração.
Note que é suficiente mostrarmos que existe uma função injetora de $\mathcal{F}$ em $\mathbb{R}$. Considere $\varphi : \mathcal{F} \to \mathbb{R}$ dada por

$$\varphi(\chi_A) = 0, \chi_A(0)\chi_A(1)\cdots\chi_A(n)\cdots$$

□

Aula 19 - Juntando tudo

Corolário
$|\mathbb{R}| = |\wp(\mathbb{N})|$

Corolário
$|\mathbb{R}| = |\wp(\mathbb{N})|$

Demonstração.
Note que temos o seguinte diagrama (cada "flecha" indica uma função injetora):

Corolário
$|\mathbb{R}| = |\wp(\mathbb{N})|$

Demonstração.
Note que temos o seguinte diagrama (cada "flecha" indica uma função injetora):

$$\wp(\mathbb{N}) \leftrightarrow \mathcal{F} \to \mathbb{R}$$

Corolário
$|\mathbb{R}| = |\wp(\mathbb{N})|$

Demonstração.
Note que temos o seguinte diagrama (cada "flecha" indica uma função injetora):

$$\wp(\mathbb{N}) \leftrightarrow \mathcal{F} \rightarrow \mathbb{R}$$

$$\wp(\mathbb{N}) \leftrightarrow \wp(\mathbb{Q}) \leftarrow \mathbb{R}$$

□

Aula 19 - Consequência

Corolário
Não existe $f : \mathbb{R} \to \mathbb{N}$ *injetora.*

Aula 21 - Axiomas para conjuntos

Aula 21 - Axiomas para conjuntos

Qual a ideia intuitiva que temos de conjuntos?

Aula 21 - Axiomas para conjuntos

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisas.

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisas. Seguindo esse raciocínio, poderíamos fazer:

$$T = \{X : X \text{ é um conjunto}\}.$$

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisas. Seguindo esse raciocínio, poderíamos fazer:

$$T = \{X : X \text{ é um conjunto}\}.$$

Este seria o conjunto de todos os conjuntos.

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisas. Seguindo esse raciocínio, poderíamos fazer:

$$T = \{X : X \text{ é um conjunto}\}.$$

Este seria o conjunto de todos os conjuntos. Como o próprio T é um conjunto, temos que $T \in T$.

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisas. Seguindo esse raciocínio, poderíamos fazer:

$$T = \{X : X \text{ é um conjunto}\}.$$

Este seria o conjunto de todos os conjuntos. Como o próprio T é um conjunto, temos que $T \in T$. Isso é estranho, mas ainda assim não parece ser uma contradição.

Aula 21 - Paradoxo

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$.

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$.

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R?

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R:

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$.

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$. Por outro lado, se $R \notin R$, novamente pela definição de R, temos que $R \in R$.

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$. Por outro lado, se $R \notin R$, novamente pela definição de R, temos que $R \in R$. Ou seja, a existência de R implica numa contradição.

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$. Por outro lado, se $R \notin R$, novamente pela definição de R, temos que $R \in R$. Ou seja, a existência de R implica numa contradição. Este é conhecido como o **paradoxo de Russel**.

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$. Por outro lado, se $R \notin R$, novamente pela definição de R, temos que $R \in R$. Ou seja, a existência de R implica numa contradição. Este é conhecido como o **paradoxo de Russel**. Quem quiser saber mais sobre a história deste problema, recomendamos [**?**].

Aula 21 - Axiomas para conjuntos

Aula 21 - Axiomas para conjuntos

Para evitar problemas como o Paradoxo de Russel, apresentamos uma lista do que podemos fazer com conjuntos.

Aula 21 - Axiomas para conjuntos

Para evitar problemas como o Paradoxo de Russel, apresentamos uma lista do que podemos fazer com conjuntos. Esta lista é conhecida como ZFC (Zermelo, Fraenkel e Axioma da Escolha).

Aula 21 - Axiomas para conjuntos

Para evitar problemas como o Paradoxo de Russel, apresentamos uma lista do que podemos fazer com conjuntos. Esta lista é conhecida como ZFC (Zermelo, Fraenkel e Axioma da Escolha). Vamos apresentar a lista aqui, com alguns comentários.

Aula 21 - Axiomas para conjuntos

Para evitar problemas como o Paradoxo de Russel, apresentamos uma lista do que podemos fazer com conjuntos. Esta lista é conhecida como ZFC (Zermelo, Fraenkel e Axioma da Escolha). Vamos apresentar a lista aqui, com alguns comentários.

Quem quiser saber mais sobre o assunto, recomendamos [**?**].

Aula 21 - Existência

Aula 21 - Existência

Existe um conjunto que não possui elementos.

Aula 21 - Existência

Existe um conjunto que não possui elementos. Em símbolos, $\exists x \, \forall y \; y \notin x$.

Aula 21 - Existência

Existe um conjunto que não possui elementos. Em símbolos, $\exists x \, \forall y \; y \notin x$. Denotamos tal conjunto por $\emptyset$.

Aula 21 - Extensão

Aula 21 - Extensão

Dois conjuntos são iguais se possuem os mesmos elementos.

Aula 21 - Extensão

Dois conjuntos são iguais se possuem os mesmos elementos. Em símbolos:
$\forall x\ \forall y(\forall z\ (z \in x \to z \in y) \wedge (z \in y \to z \in x)) \to x = y$.

Aula 21 - Observação

Aula 21 - Observação

Quando ocorre $\forall z\ z \in y \rightarrow z \in x$, usamos a seguinte notação: $y \subset x$.

Aula 21 - Observação

Quando ocorre $\forall z\ z \in y \rightarrow z \in x$, usamos a seguinte notação: $y \subset x$. Desta forma, podemos denotar o último axioma como $\forall x\ \forall y(x \subset y \wedge y \subset x) \rightarrow x = y$.

Aula 21 - Separação

Aula 21 - Separação

Se P é uma propriedade e x é um conjunto, existe o subconjunto y que contém exatamente os elementos de x que satisfazem a propriedade P.

Aula 21 - Separação

Se P é uma propriedade e x é um conjunto, existe o subconjunto y que contém exatamente os elementos de x que satisfazem a propriedade P. Em símbolos
$\forall x\ \exists y((\forall z \in x\ P(z) \rightarrow z \in y) \wedge (\forall z \in y \rightarrow (z \in x \wedge P(z)))).$

Aula 21 - Separação

Se P é uma propriedade e x é um conjunto, existe o subconjunto y que contém exatamente os elementos de x que satisfazem a propriedade P. Em símbolos
$\forall x\ \exists y((\forall z \in x\ P(z) \to z \in y) \wedge (\forall z \in y \to (z \in x \wedge P(z))))$. A notação usual para isso é $y = \{z \in x : P(z)\}$.

Aula 21 - Par

Aula 21 - Par

Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos.

Aula 21 - Par

Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos. Em símbolos: $\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$.

Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos. Em símbolos: $\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$. Note que tal axioma não garante que os únicos elementos de z sejam x e y mas, para isso, podemos usar o axioma da Separação.

Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos. Em símbolos: $\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$. Note que tal axioma não garante que os únicos elementos de z sejam x e y mas, para isso, podemos usar o axioma da Separação. No caso em que os únicos elementos de z sejam x e y a notação fica $z = \{x, y\}$.

Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos. Em símbolos: $\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$. Note que tal axioma não garante que os únicos elementos de z sejam x e y mas, para isso, podemos usar o axioma da Separação. No caso em que os únicos elementos de z sejam x e y a notação fica $z = \{x, y\}$. Se, além disso, se $x = y$, usamos a notação $z = \{x\}$.

Aula 21 - União

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x.

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos:
$\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \rightarrow a \in y$.

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos:
$\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \rightarrow a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação.

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos:
$\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \rightarrow a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação. No caso em que o conjunto y contém exatamente tais elementos, a notação usual é $y = \bigcup_{z \in x} z$.

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos:
$\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \rightarrow a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação. No caso em que o conjunto y contém exatamente tais elementos, a notação usual é $y = \bigcup_{z \in x} z$. Agora podemos provar que dados conjuntos A e B, existe o conjunto $A \cup B$.

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos:
$\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \rightarrow a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação. No caso em que o conjunto y contém exatamente tais elementos, a notação usual é $y = \bigcup_{z \in x} z$. Agora podemos provar que dados conjuntos A e B, existe o conjunto $A \cup B$. Primeiramente mostramos que existe o conjunto $\{A, B\}$ (exercício).

Aula 21 - União

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos:
$\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \rightarrow a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação. No caso em que o conjunto y contém exatamente tais elementos, a notação usual é $y = \bigcup_{z \in x} z$. Agora podemos provar que dados conjuntos A e B, existe o conjunto $A \cup B$. Primeiramente mostramos que existe o conjunto $\{A, B\}$ (exercício). Depois, mostramos que existe $y = \bigcup_{z \in \{A,B\}} z$ (note que este é o conjunto desejado).

Aula 21 - Partes

Aula 21 - Partes

Dado x um conjunto, existe um conjunto y que contém todos os subconjuntos de x.

Aula 21 - Partes

Dado x um conjunto, existe um conjunto y que contém todos os subconjuntos de x. Em símbolos: $\forall x\ \exists y\ \forall z\ z \subset x \to z \in y$.

Aula 21 - Partes

Dado x um conjunto, existe um conjunto y que contém todos os subconjuntos de x. Em símbolos: $\forall x\ \exists y\ \forall z\ z \subset x \to z \in y$. Novamente, não temos garantido que os únicos elementos de y sejam os subconjuntos de x, mas podemos contornar isso com o axioma da separação.

Aula 21 - Partes

Dado x um conjunto, existe um conjunto y que contém todos os subconjuntos de x. Em símbolos: $\forall x\ \exists y\ \forall z\ z \subset x \to z \in y$. Novamente, não temos garantido que os únicos elementos de y sejam os subconjuntos de x, mas podemos contornar isso com o axioma da separação. Se for o caso em que os elementos de y forem os subconjuntos de x, usamos a notação $y = \wp(x)$.

Aula 21 - Infinito

Dado um conjunto x, denotamos por $S(x)$ o conjunto $x \cup \{x\}$ (podemos fazer isso pelo axioma do par (veja o Exercício **??** e da união).

Dado um conjunto x, denotamos por $S(x)$ o conjunto $x \cup \{x\}$ (podemos fazer isso pelo axioma do par (veja o Exercício **??** e da união). O axioma do infinito diz que existe um conjunto A tal que $\emptyset \in A$ e tal que para todo $x \in A$, $S(x) \in A$.

Aula 21 - Infinito

Dado um conjunto x, denotamos por $S(x)$ o conjunto $x \cup \{x\}$ (podemos fazer isso pelo axioma do par (veja o Exercício **??** e da união). O axioma do infinito diz que existe um conjunto A tal que $\emptyset \in A$ e tal que para todo $x \in A$, $S(x) \in A$. Em símbolos: $\exists A\ \emptyset \in A \wedge (\forall x \in A\ S(x) \in A)$.

Aula 21 - Uma outra interpretação

Aula 21 - Uma outra interpretação

Há mais alguns axiomas, mas os faremos após uma pequena digressão.

Aula 21 - Uma outra interpretação

Há mais alguns axiomas, mas os faremos após uma pequena digressão.

Uma característica do método axiomático é que podemos ter diferentes interpretações para o que os axiomas descrevem.

Aula 21 - Uma outra interpretação

Há mais alguns axiomas, mas os faremos após uma pequena digressão.

Uma característica do método axiomático é que podemos ter diferentes interpretações para o que os axiomas descrevem. Isso ocorre também com os axiomas aqui apresentados.

Aula 21 - Uma outra interpretação

Há mais alguns axiomas, mas os faremos após uma pequena digressão.

Uma característica do método axiomático é que podemos ter diferentes interpretações para o que os axiomas descrevem. Isso ocorre também com os axiomas aqui apresentados. Por exemplo, considere a relação $\ll$ definida sobre $\mathbb{N}$ da seguinte forma:

$a \ll b$ se, e somente se, o a-ésimo termo da expansão binária de b é 1

Aula 21 - Exemplo

Aula 21 - Exemplo

Por exemplo, $b = 25$ em binário dá 11001_2 então $0 \ll 25$, $1 \not\ll 25$, $4 \ll 25$.

Aula 21 - Exemplo

Por exemplo, $b = 25$ em binário dá 11001_2 então $0 \ll 25$, $1 \not\ll 25$, $4 \ll 25$.

Essa relação satisfaz todos os axiomas apresentados acima, com exceção ao do infinito (interpretando $\ll$ como $\in$).

Aula 21 - Exemplo

Por exemplo, $b = 25$ em binário dá 11001_2 então $0 \ll 25$, $1 \not\ll 25$, $4 \ll 25$.

Essa relação satisfaz todos os axiomas apresentados acima, com exceção ao do infinito (interpretando $\ll$ como $\in$). Por exemplo, o número 0 faz papel de $\emptyset$ uma vez que não existe a tal que $a \ll 0$.

Aula 21 - Exemplo

Por exemplo, $b = 25$ em binário dá 11001_2 então $0 \ll 25$, $1 \not\ll 25$, $4 \ll 25$.

Essa relação satisfaz todos os axiomas apresentados acima, com exceção ao do infinito (interpretando $\ll$ como $\in$). Por exemplo, o número 0 faz papel de $\emptyset$ uma vez que não existe a tal que $a \ll 0$. Se a e b são números distintos, o número $k = 2^a + 2^b$ é tal que $a \ll k$ e $b \ll k$.

Aula 21 - Fórmulas tipo função

Aula 21 - Fórmulas tipo função

Começamos com a ideia principal de uma função: associar a cada elemento de um lado, um único elemento do outro.

Aula 21 - Fórmulas tipo função

Começamos com a ideia principal de uma função: associar a cada elemento de um lado, um único elemento do outro. Com isso em mente, podemos definir uma fórmula do "tipo função".

Aula 21 - Fórmulas tipo função

Começamos com a ideia principal de uma função: associar a cada elemento de um lado, um único elemento do outro. Com isso em mente, podemos definir uma fórmula do "tipo função".
Basicamente é uma fórmula P, que a cada $a_1, ..., a_n$ conjuntos, associa um único conjunto b tal que $P(b, a_1, ..., a_n)$ seja satisfeita.

Aula 21 - Fórmulas tipo função

Começamos com a ideia principal de uma função: associar a cada elemento de um lado, um único elemento do outro. Com isso em mente, podemos definir uma fórmula do "tipo função".
Basicamente é uma fórmula P, que a cada $a_1, ..., a_n$ conjuntos, associa um único conjunto b tal que $P(b, a_1, ..., a_n)$ seja satisfeita.
Muitas vezes usamos uma notação mais parecida com função $b = f(a_1, ..., a_n)$.

Aula 21 - Exemplos

Aula 21 - Exemplos

Exemplo
Considere $P(x, y)$ sendo $y \in x \wedge (\forall z \in x \; z = y)$.

Exemplo
Considere $P(x, y)$ sendo $y \in x \wedge (\forall z \in x\ z = y)$. Note que a cada a que tomarmos, só existe um conjunto b satisfazendo $P(b, a)$ (a saber, $b = \{a\}$).

Aula 21 - Exemplos

Exemplo
Se omitirmos a parte "$\forall z \in x\ z = y$" na propriedade P anterior, não temos mais que P é do tipo função.

Exemplo
Se omitirmos a parte "$\forall z \in x\ z = y$" na propriedade P anterior, não temos mais que P é do tipo função. Pois tanto $b_1 = \{a, \emptyset\}$ como $b_2 = \{a\}$ (suponha $a \neq \emptyset$) são distintos e $P(b_1, a)$ e $P(b_2, a)$ são satisfeitas.

Aula 21 - Par ordenado

Aula 21 - Par ordenado

Podemos formalizar a ideia do que é uma função usando o que já temos até aqui.

Aula 21 - Par ordenado

Podemos formalizar a ideia do que é uma função usando o que já temos até aqui. Comecemos com a ideia do par ordenado:

Aula 21 - Par ordenado

Podemos formalizar a ideia do que é uma função usando o que já temos até aqui. Comecemos com a ideia do par ordenado:

Definição
Sejam x, y dois conjuntos. Definimos o **par ordenado** como o conjunto $\{\{x\}, \{x, y\}\}$. Notação (x, y). Neste caso, dizemos que x é a primeira coordenada do par e que y é a segunda.

Aula 21 - Algumas propriedades

- Existe uma fórmula P tal que $P(x)$ é verdadeira se, e somente se, x é um par ordenado;

Aula 21 - Algumas propriedades

- Existe uma fórmula P tal que $P(x)$ é verdadeira se, e somente se, x é um par ordenado;
- Existe uma fórmula P_1 tal que $P_1(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a primeira coordenada de x;

Aula 21 - Algumas propriedades

- Existe uma fórmula P tal que $P(x)$ é verdadeira se, e somente se, x é um par ordenado;
- Existe uma fórmula P_1 tal que $P_1(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a primeira coordenada de x;
- Existe uma fórmula P_2 tal que $P_2(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a segunda coordenada de x;

Aula 21 - Algumas propriedades

Proposição
Sejam (x, y) *e* (a, b) *dois pares ordenados. Então* $(x, y) = (a, b)$ *se, e somente se,* $x = a$ *e* $y = b$.

Aula 21 - Conjunto dos pares ordenados

Aula 21 - Conjunto dos pares ordenados

Definição
Se X e Y são conjuntos, denotamos por $X \times Y$ o conjunto de todos os pares ordenados (x, y) tais que $x \in X$ e $y \in Y$.

Aula 21 - Observação

Aula 21 - Observação

Na verdade, é necessário provar que se X e Y são conjuntos, então $X \times Y$ é de fato um conjunto.

Aula 21 - Observação

Na verdade, é necessário provar que se X e Y são conjuntos, então $X \times Y$ é de fato um conjunto. Isso é possível usando o fato que $X \cup Y$ é um conjunto e, portanto, $\wp(\wp(X \cup Y))$ é conjunto.

Aula 21 - Observação

Na verdade, é necessário provar que se X e Y são conjuntos, então $X \times Y$ é de fato um conjunto. Isso é possível usando o fato que $X \cup Y$ é um conjunto e, portanto, $\wp(\wp(X \cup Y))$ é conjunto. Finalmente, usamos o axioma da separação para tomarmos apenas os pares ordenados desejados.

Aula 21 - Função

Definição
Chamamos de uma função f de X em Y um subconjunto de $X \times Y$ tal que, para todo $x \in X$, existe $y \in Y$ tal que $(x, y) \in f$ e que se $(x, y_1), (x, y_2) \in f$, então $y_1 = y_2$. Neste caso, denotamos $(x, y) \in f$ como $f(x) = y$.

Aula 21 - Substituição

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função.

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x.

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x. Em símbolos:
$\forall x \ \ (\forall a_1, ..., a_n \in x \exists! z \ P(z, a_1, ..., a_n)) \rightarrow (\exists y \forall z \ \forall a_1, ..., a_n \in xP(z, a_1, ..., a_n) \rightarrow z \in y)$.

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x. Em símbolos:
$\forall x \ \ (\forall a_1, ..., a_n \in x \exists! z \ P(z, a_1, ..., a_n)) \rightarrow (\exists y \forall z \ \forall a_1, ..., a_n \in xP(z, a_1, ..., a_n) \rightarrow z \in y)$.

O $\exists! z$ quer dizer "existe um único z satisfazendo o que vem a seguir".

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x. Em símbolos:
$\forall x \ \ (\forall a_1, ..., a_n \in x \exists! z \ P(z, a_1, ..., a_n)) \rightarrow (\exists y \forall z \ \forall a_1, ..., a_n \in xP(z, a_1, ..., a_n) \rightarrow z \in y)$.

O $\exists! z$ quer dizer "existe um único z satisfazendo o que vem a seguir". No caso em que y contém exatamente tais elementos, denotamos $y = \{z : P(z, a_1, ..., a_n), a_1, ..., a_n \in x\}$.

Aula 21 - Substituição

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x. Em símbolos:
$\forall x \ \ (\forall a_1, ..., a_n \in x \exists! z \ P(z, a_1, ..., a_n)) \rightarrow (\exists y \forall z \ \forall a_1, ..., a_n \in xP(z, a_1, ..., a_n) \rightarrow z \in y)$.

O $\exists! z$ quer dizer "existe um único z satisfazendo o que vem a seguir". No caso em que y contém exatamente tais elementos, denotamos $y = \{z : P(z, a_1, ..., a_n), a_1, ..., a_n \in x\}$. Ou, usando a notação de função, $y = \{f(a_1, ..., a_n) : a_1, ..., a_n\}$.

Aula 21 - Fundação

Todo conjunto x não vazio possui um elemento que é disjunto de x.

Aula 21 - Fundação

Todo conjunto x não vazio possui um elemento que é disjunto de x. Em símbolos $\forall x\ x \neq \emptyset \rightarrow (\exists y \in x\ y \cap x = \emptyset)$.

Aula 21 - Fundação

Todo conjunto x não vazio possui um elemento que é disjunto de x. Em símbolos $\forall x\ x \neq \emptyset \rightarrow (\exists y \in x\ y \cap x = \emptyset)$. Este é o axioma de ZFC que é menos usado em matemática em geral.

Aula 21 - Fundação

Todo conjunto x não vazio possui um elemento que é disjunto de x. Em símbolos $\forall x\ x \neq \emptyset \rightarrow (\exists y \in x\ y \cap x = \emptyset)$. Este é o axioma de ZFC que é menos usado em matemática em geral. Apesar disso, serve, por exemplo, para impedir que existam conjuntos x tais que $x \in x$ (veja o Exercício **??**).

Aula 21 - Fundação

Todo conjunto x não vazio possui um elemento que é disjunto de x. Em símbolos $\forall x\ x \neq \emptyset \rightarrow (\exists y \in x\ y \cap x = \emptyset)$. Este é o axioma de ZFC que é menos usado em matemática em geral. Apesar disso, serve, por exemplo, para impedir que existam conjuntos x tais que $x \in x$ (veja o Exercício **??**). Também o usaremos para mostrar a propriedade fundamental do par ordenado.

Aula 21 - Escolha

Se x é um conjunto de conjuntos não vazios, então existe uma função $f : x \to \bigcup_{a \in x} a$ tal que $f(y) \in y$ para todo $y \in x$.

Aula 21 - Escolha

Se x é um conjunto de conjuntos não vazios, então existe uma função $f : x \to \bigcup_{a \in x} a$ tal que $f(y) \in y$ para todo $y \in x$. Ou seja, se temos uma família de conjuntos não vazios, podemos "escolher" um elemento de cada conjunto.