Teorema de Schur

Combinando

Abril 2020

Teoremas de Ramsey

Teorema de Ramsey - v. infinita

Dada uma coloração finita sobre $\binom{\mathbb{N}}{2}$, existe $H \subset \mathbb{N}$ infinito e homogêneo.

Teoremas de Ramsey

Teorema de Ramsey - v. infinita

Dada uma coloração finita sobre $\binom{\mathbb{N}}{2}$, existe $H \subset \mathbb{N}$ infinito e homogêneo.

Teorema de Ramsey - v. finita

Dados $t, k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\binom{\{1,2,\cdots,n\}}{2}$ existe H de tamanho t homogêneo.

Teorema de Schur

Último Teorema de Fermat

Dado $k \in \mathbb{N},\ k > 2$, não existem $a, b, c \in \mathbb{Z},\ a, b, c \neq 0$, tais que

$$a^k + b^k = c^k$$

Teorema de Schur

Último Teorema de Fermat

Dado $k \in \mathbb{N},\ k > 2$, não existem $a, b, c \in \mathbb{Z},\ a, b, c \neq 0$, tais que

$$a^k + b^k = c^k$$

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z},\ a, b, c \neq 0$, tais que

$$a^k + b^k \equiv c^k \pmod{p}$$

Teorema de Schur

Lema (Schur) - v. infinita

Para cada coloração finita de $\mathbb{N}$, existem naturais x, y e z da mesma cor tais que $x + y = z$. Em outras palavras, a equação $x + y = z$ possui uma solução monocromática.

Teorema de Schur

Lema (Schur) - v. infinita

Para cada coloração finita de $\mathbb{N}$, existem naturais x, y e z da mesma cor tais que $x + y = z$. Em outras palavras, a equação $x + y = z$ possui uma solução monocromática.

Demonstração: Seja c uma k-coloração sobre $\mathbb{N}$. Defina a k-coloração γ sobre $\binom{\mathbb{N}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$.

Teorema de Schur

Lema (Schur) - v. infinita

Para cada coloração finita de $\mathbb{N}$, existem naturais x, y e z da mesma cor tais que $x + y = z$. Em outras palavras, a equação $x + y = z$ possui uma solução monocromática.

Demonstração: Seja c uma k-coloração sobre $\mathbb{N}$. Defina a k-coloração γ sobre $\binom{\mathbb{N}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Pelo Teorema de Ramsey existe um conjunto infinito $H \subset \mathbb{N}$ homogêneo, i.e., tal que $\binom{H}{2}$ é monocromático por γ.

Teorema de Schur

Lema (Schur) - v. infinita

Para cada coloração finita de $\mathbb{N}$, existem naturais x, y e z da mesma cor tais que $x + y = z$. Em outras palavras, a equação $x + y = z$ possui uma solução monocromática.

Demonstração: Seja c uma k-coloração sobre $\mathbb{N}$. Defina a k-coloração γ sobre $\binom{\mathbb{N}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Pelo Teorema de Ramsey existe um conjunto infinito $H \subset \mathbb{N}$ homogêneo, i.e., tal que $\binom{H}{2}$ é monocromático por γ. Sejam $u, v, w \in H$ tais que $u < v < w$.

Teorema de Schur

Lema (Schur) - v. infinita

Para cada coloração finita de $\mathbb{N}$, existem naturais x, y e z da mesma cor tais que $x + y = z$. Em outras palavras, a equação $x + y = z$ possui uma solução monocromática.

Demonstração: Seja c uma k-coloração sobre $\mathbb{N}$. Defina a k-coloração γ sobre $\binom{\mathbb{N}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Pelo Teorema de Ramsey existe um conjunto infinito $H \subset \mathbb{N}$ homogêneo, i.e., tal que $\binom{H}{2}$ é monocromático por γ. Sejam $u, v, w \in H$ tais que $u < v < w$. Então

$$\gamma(w, v) = \gamma(v, u) = \gamma(w, u) \therefore c(w - v) = c(v - u) = c(w - u)$$

Teorema de Schur

Lema (Schur) - v. infinita

Para cada coloração finita de $\mathbb{N}$, existem naturais x, y e z da mesma cor tais que $x + y = z$. Em outras palavras, a equação $x + y = z$ possui uma solução monocromática.

Demonstração: Seja c uma k-coloração sobre $\mathbb{N}$. Defina a k-coloração γ sobre $\binom{\mathbb{N}}{2}$ dada por

$$\gamma(\{i,j\}) = c(j-i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Pelo Teorema de Ramsey existe um conjunto infinito $H \subset \mathbb{N}$ homogêneo, i.e., tal que $\binom{H}{2}$ é monocromático por γ. Sejam $u, v, w \in H$ tais que $u < v < w$. Então

$$\gamma(w,v) = \gamma(v,u) = \gamma(w,u) \therefore c(w-v) = c(v-u) = c(w-u)$$

Dessa forma, temos nossa solução monocromática:

$$(w-v) + (v-u) = (w-u)$$

Lemas de Schur

Lema (Schur) - v. finita

Dado $k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$, a equação $x + y = z$ possui solução monocromática.

Lemas de Schur

Lema (Schur) - v. finita

Dado $k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$, a equação $x + y = z$ possui solução monocromática.

Demonstração: Pelo Teorema de Ramsey existe n tal que, para toda k-coloração sobre $\binom{\{1,2,\cdots,n\}}{2}$, existe um conjunto $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo.

Lema (Schur) - v. finita

Dado $k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$, a equação $x + y = z$ possui solução monocromática.

Demonstração: Pelo Teorema de Ramsey existe n tal que, para toda k-coloração sobre $\binom{\{1,2,\cdots,n\}}{2}$, existe um conjunto $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo. Seja c uma k-coloração sobre $\{1, 2, \cdots, n\}$. Defina a k-coloração γ sobre $\binom{\{1,2,\cdots,n\}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$.

Lema (Schur) - v. finita

Dado $k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$, a equação $x + y = z$ possui solução monocromática.

Demonstração: Pelo Teorema de Ramsey existe n tal que, para toda k-coloração sobre $\binom{\{1,2,\cdots,n\}}{2}$, existe um conjunto $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo. Seja c uma k-coloração sobre $\{1, 2, \cdots, n\}$. Defina a k-coloração γ sobre $\binom{\{1,2,\cdots,n\}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Seja $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo, e sejam $u, v, w \in H$ tais que $u < v < w$.

Lema (Schur) - v. finita

Dado $k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$, a equação $x + y = z$ possui solução monocromática.

Demonstração: Pelo Teorema de Ramsey existe n tal que, para toda k-coloração sobre $\binom{\{1,2,\cdots,n\}}{2}$, existe um conjunto $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo. Seja c uma k-coloração sobre $\{1, 2, \cdots, n\}$. Defina a k-coloração γ sobre $\binom{\{1,2,\cdots,n\}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Seja $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo, e sejam $u, v, w \in H$ tais que $u < v < w$. Então

$$\gamma(w, v) = \gamma(v, u) = \gamma(w, u) \therefore c(w - v) = c(v - u) = c(w - u)$$

Lema (Schur) - v. finita

Dado $k \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$, a equação $x + y = z$ possui solução monocromática.

Demonstração: Pelo Teorema de Ramsey existe n tal que, para toda k-coloração sobre $\binom{\{1,2,\cdots,n\}}{2}$, existe um conjunto $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo. Seja c uma k-coloração sobre $\{1, 2, \cdots, n\}$. Defina a k-coloração γ sobre $\binom{\{1,2,\cdots,n\}}{2}$ dada por

$$\gamma(\{i, j\}) = c(j - i)$$

para todo $i, j \in \mathbb{N},\ i \leq j$. Seja $H \subset \{1, 2, \cdots, n\}$ de tamanho 3 homogêneo, e sejam $u, v, w \in H$ tais que $u < v < w$. Então

$$\gamma(w, v) = \gamma(v, u) = \gamma(w, u) \therefore c(w - v) = c(v - u) = c(w - u)$$

Dessa forma, temos nossa solução monocromática:

$$(w - v) + (v - u) = (w - u)$$

Miscelânia sobre $\mathbb{Z}_p$

Seja n um número natural. Considere a relação de equivalência $\equiv_n$ sobre $\mathbb{Z}$ dada por

$$a \equiv_n b \iff n | a - b$$

para $a, b \in \mathbb{Z}$, e seja $\overline{a} := \{z \in \mathbb{Z} : z \equiv_n a\}$.

Miscelânia sobre $\mathbb{Z}_p$

Seja n um número natural. Considere a relação de equivalência $\equiv_n$ sobre $\mathbb{Z}$ dada por

$$a \equiv_n b \iff n | a - b$$

para $a, b \in \mathbb{Z}$, e seja $\overline{a} := \{z \in \mathbb{Z} : z \equiv_n a\}$. Chamamos de $\mathbb{Z}_n$ o conjunto $\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ munido das operações

- soma $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ dada por

$$\overline{a} + \overline{b} := \overline{a + b}$$

- produto $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ dada por

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

Miscelânia sobre $\mathbb{Z}_p$

Podemos reescrever o teorema de Schur da forma

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Dado p primo, $\mathbb{Z}_p$ é um corpo, i.e., $\forall x, y, z \in \mathbb{Z}_p$

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + \overline{0} = x$
- $\exists - x \in \mathbb{Z}_p : \ x + (-x) = \overline{0}$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $x \cdot \overline{1} = x$
- $\exists x^{-1} \in \mathbb{Z}_p : \ x \cdot x^{-1} = \overline{1}, \ x \neq \overline{0}$
- $x \cdot (y + z) = x \cdot y + x \cdot z$

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Dado p primo, $\mathbb{Z}_p$ é um corpo, i.e., $\forall x, y, z \in \mathbb{Z}_p$

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + \overline{0} = x$
- $\exists - x \in \mathbb{Z}_p : \ x + (-x) = \overline{0}$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $x \cdot \overline{1} = x$
- $\exists x^{-1} \in \mathbb{Z}_p : \ x \cdot x^{-1} = \overline{1}, \ x \neq \overline{0}$
- $x \cdot (y + z) = x \cdot y + x \cdot z$

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.
- Caso $n \Rightarrow n + 1$: Seja

$$P(x) = \sum_{k=0}^{n+1} a_k x^k, \ a_k \in \mathbb{K}$$

um polinômio de grau $n + 1$.

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.
- Caso $n \Rightarrow n + 1$: Seja

$$P(x) = \sum_{k=0}^{n+1} a_k x^k, \ a_k \in \mathbb{K}$$

um polinômio de grau $n + 1$. Se P não possui raízes, acabou.

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.
- Caso $n \Rightarrow n + 1$: Seja

$$P(x) = \sum_{k=0}^{n+1} a_k x^k, \ a_k \in \mathbb{K}$$

um polinômio de grau $n + 1$. Se P não possui raízes, acabou. Caso contrário, seja α raíz de P. Então $P(\alpha) = 0$

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.
- Caso $n \Rightarrow n + 1$: Seja

$$P(x) = \sum_{k=0}^{n+1} a_k x^k, \ a_k \in \mathbb{K}$$

um polinômio de grau $n + 1$. Se P não possui raízes, acabou. Caso contrário, seja α raíz de P. Então $P(\alpha) = 0 \therefore$

$$P(x) = P(x) - P(\alpha)$$

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.
- Caso $n \Rightarrow n + 1$: Seja

$$P(x) = \sum_{k=0}^{n+1} a_k x^k, \ a_k \in \mathbb{K}$$

um polinômio de grau $n + 1$. Se P não possui raízes, acabou. Caso contrário, seja α raíz de P. Então $P(\alpha) = 0 \therefore$

$$P(x) = P(x) - P(\alpha) = \sum_{k=0}^{n+1} a_k x^k - \sum_{k=0}^{n+1} a_k \alpha^k$$

O que sabemos sobre $\mathbb{Z}_p$?

Teorema

Um polinômio P de grau n sobre um corpo $\mathbb{K}$ possui no máximo n raízes.

Demonstração: Prova por indução.

- Caso $n = 0$: Se P tem grau 0, então P é constante não nulo, logo, possui 0 raízes.
- Caso $n \Rightarrow n + 1$: Seja

$$P(x) = \sum_{k=0}^{n+1} a_k x^k, \ a_k \in \mathbb{K}$$

um polinômio de grau $n + 1$. Se P não possui raízes, acabou. Caso contrário, seja α raíz de P. Então $P(\alpha) = 0 \therefore$

$$P(x) = P(x) - P(\alpha) = \sum_{k=0}^{n+1} a_k x^k - \sum_{k=0}^{n+1} a_k \alpha^k = \sum_{k=0}^{n+1} a_k (x^k - \alpha^k)$$

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k)$$

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

$$= (x-\alpha)\underbrace{\sum_{k=0}^{n+1} a_k(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})}_{Q(x)}$$

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

$$= (x-\alpha)\underbrace{\sum_{k=0}^{n+1} a_k(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})}_{Q(x)} = (x-\alpha)Q(x)$$

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

$$= (x-\alpha)\underbrace{\sum_{k=0}^{n+1} a_k(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})}_{Q(x)} = (x-\alpha)Q(x)$$

Note que Q é um polinômio de grau n, logo, pela hipótese de indução, possui no máximo n raízes.

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

$$= (x-\alpha)\underbrace{\sum_{k=0}^{n+1} a_k(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})}_{Q(x)} = (x-\alpha)Q(x)$$

Note que Q é um polinômio de grau n, logo, pela hipótese de indução, possui no máximo n raízes. Além disso, $\beta \neq \alpha$ é raíz de P se, e só se, $P(\beta) = (\beta - \alpha)Q(\beta) = 0$

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

$$= (x-\alpha)\underbrace{\sum_{k=0}^{n+1} a_k(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})}_{Q(x)} = (x-\alpha)Q(x)$$

Note que Q é um polinômio de grau n, logo, pela hipótese de indução, possui no máximo n raízes. Além disso, $\beta \neq \alpha$ é raíz de P se, e só se, $P(\beta) = (\beta - \alpha)Q(\beta) = 0 \therefore Q(\beta) = 0$ i.e., β é raíz de Q.

O que sabemos sobre $\mathbb{Z}_p$?

$$\sum_{k=0}^{n+1} a_k(x^k - \alpha^k) = \sum_{k=0}^{n+1} a_k(x-\alpha)(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})$$

$$= (x-\alpha)\underbrace{\sum_{k=0}^{n+1} a_k(x^{k-1} + x^{k-2}\alpha + \cdots + x\alpha^{k-2} + \alpha^{k-1})}_{Q(x)} = (x-\alpha)Q(x)$$

Note que Q é um polinômio de grau n, logo, pela hipótese de indução, possui no máximo n raízes. Além disso, $\beta \neq \alpha$ é raíz de P se, e só se, $P(\beta) = (\beta - \alpha)Q(\beta) = 0 \therefore Q(\beta) = 0$ i.e., β é raíz de Q. Logo, P possui no máximo $n+1$ raízes.

Miscelânia sobre $\mathbb{Z}_p$

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, definimos a **ordem** de g como sendo o menor inteiro positivo θ tal que $g^\theta = \overline{1}$, e denotamos por $ord(g)$.

Miscelânia sobre $\mathbb{Z}_p$

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, definimos a **ordem** de g como sendo o menor inteiro positivo θ tal que $g^\theta = \overline{1}$, e denotamos por $ord(g)$.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

Miscelânia sobre $\mathbb{Z}_p$

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, definimos a **ordem** de g como sendo o menor inteiro positivo θ tal que $g^\theta = \overline{1}$, e denotamos por $ord(g)$.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

Lema

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, então $g^t = \overline{1}$ com t inteiro positivo se, e somente se, $ord(g)|t$.

Miscelânia sobre $\mathbb{Z}_p$

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, definimos a **ordem** de g como sendo o menor inteiro positivo θ tal que $g^\theta = \overline{1}$, e denotamos por $ord(g)$.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

Lema

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, então $g^t = \overline{1}$ com t inteiro positivo se, e somente se, $ord(g)|t$.

Demonstração: Sejam $q, r \in \mathbb{Z}_+$, $r < ord(g)$, tais que $t = ord(g) \cdot q + r$.

Miscelânia sobre $\mathbb{Z}_p$

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, definimos a **ordem** de g como sendo o menor inteiro positivo θ tal que $g^\theta = \overline{1}$, e denotamos por $ord(g)$.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

Lema

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, então $g^t = \overline{1}$ com t inteiro positivo se, e somente se, $ord(g)|t$.

Demonstração: Sejam $q, r \in \mathbb{Z}_+$, $r < ord(g)$, tais que $t = ord(g) \cdot q + r$. Então $g^t = g^{ord(g)\cdot q + r} = (g^{ord(g)})^q g^r = \overline{1} \cdot g^r = g^r$

Miscelânia sobre $\mathbb{Z}_p$

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, definimos a **ordem** de g como sendo o menor inteiro positivo θ tal que $g^\theta = \overline{1}$, e denotamos por $ord(g)$.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

Lema

Dado $g \in \mathbb{Z}_p$, $g \neq \overline{0}$, então $g^t = \overline{1}$ com t inteiro positivo se, e somente se, $ord(g)|t$.

Demonstração: Sejam $q, r \in \mathbb{Z}_+$, $r < ord(g)$, tais que $t = ord(g) \cdot q + r$. Então $g^t = g^{ord(g)\cdot q + r} = (g^{ord(g)})^q g^r = \overline{1} \cdot g^r = g^r$, logo $g^t = \overline{1} \iff g^r = \overline{1}$ o que ocorre se, e somente se, $r = 0$, i.e., $ord(g)|t$.

Miscelânia sobre $\mathbb{Z}_p$

Se $ord(g) = p - 1$, dizemos que g é **raíz primitiva** de $\mathbb{Z}_p$.

Miscelânia sobre $\mathbb{Z}_p$

Se $ord(g) = p - 1$, dizemos que g é **raíz primitiva** de $\mathbb{Z}_p$.

Lema

Se g é raíz primitiva de $\mathbb{Z}_p$, então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$.

Miscelânia sobre $\mathbb{Z}_p$

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Miscelânia sobre $\mathbb{Z}_p$

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Demonstração: Seja $d \in \mathbb{Z}_+$ tal que $d|p-1$. Defina

$$N_d := |\{g \in \mathbb{Z}_p : ord(g) = d\}|$$

Miscelânia sobre $\mathbb{Z}_p$

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Demonstração: Seja $d \in \mathbb{Z}_+$ tal que $d|p-1$. Defina

$$N_d := |\{g \in \mathbb{Z}_p : ord(g) = d\}|$$

Se $N_d \neq 0$, então $\exists h \in \mathbb{Z}_p$ tal que $ord(h) = d \therefore h, h^2, \cdots, h^d$ são todos distintos.

Miscelânia sobre $\mathbb{Z}_p$

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Demonstração: Seja $d \in \mathbb{Z}_+$ tal que $d|p-1$. Defina

$$N_d := |\{g \in \mathbb{Z}_p : ord(g) = d\}|$$

Se $N_d \neq 0$, então $\exists h \in \mathbb{Z}_p$ tal que $ord(h) = d \therefore h, h^2, \cdots, h^d$ são todos distintos. Além disso, $h, h^2, \cdots, h^d$ são raízes do polinômio sobre $\mathbb{Z}_p$, $x^d - \overline{1}$, portanto, as *únicas* raízes.

Miscelânia sobre $\mathbb{Z}_p$

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Demonstração: Seja $d \in \mathbb{Z}_+$ tal que $d|p-1$. Defina

$$N_d := |\{g \in \mathbb{Z}_p : ord(g) = d\}|$$

Se $N_d \neq 0$, então $\exists h \in \mathbb{Z}_p$ tal que $ord(h) = d \therefore h, h^2, \cdots, h^d$ são todos distintos. Além disso, $h, h^2, \cdots, h^d$ são raízes do polinômio sobre $\mathbb{Z}_p$, $x^d - \overline{1}$, portanto, as *únicas* raízes. Como $h^t = \overline{1} \iff d|t$, t inteiro positivo, temos que $ord(h^i)$ deve ser o menor inteiro tal que $d|i \cdot ord(h^i)$, $i \in \{1, 2, ..., d\}$.

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Demonstração: Seja $d \in \mathbb{Z}_+$ tal que $d|p-1$. Defina

$$N_d := |\{g \in \mathbb{Z}_p : ord(g) = d\}|$$

Se $N_d \neq 0$, então $\exists h \in \mathbb{Z}_p$ tal que $ord(h) = d \therefore h, h^2, \cdots, h^d$ são todos distintos. Além disso, $h, h^2, \cdots, h^d$ são raízes do polinômio sobre $\mathbb{Z}_p$, $x^d - \overline{1}$, portanto, as *únicas* raízes. Como $h^t = \overline{1} \iff d|t$, t inteiro positivo, temos que $ord(h^i)$ deve ser o menor inteiro tal que $d|i \cdot ord(h^i)$, $i \in \{1, 2, ..., d\}$. Dessa forma, é fácil ver que $ord(h^i) = d$ se, e somente se, $mdc(i, d) = 1$.

Teorema

$\mathbb{Z}_p$ possui uma raiz primitiva.

Demonstração: Seja $d \in \mathbb{Z}_+$ tal que $d|p-1$. Defina

$$N_d := |\{g \in \mathbb{Z}_p : ord(g) = d\}|$$

Se $N_d \neq 0$, então $\exists h \in \mathbb{Z}_p$ tal que $ord(h) = d \therefore h, h^2, \cdots, h^d$ são todos distintos. Além disso, $h, h^2, \cdots, h^d$ são raízes do polinômio sobre $\mathbb{Z}_p$, $x^d - \overline{1}$, portanto, as *únicas* raízes. Como $h^t = \overline{1} \iff d|t$, t inteiro positivo, temos que $ord(h^i)$ deve ser o menor inteiro tal que $d|i \cdot ord(h^i)$, $i \in \{1, 2, ..., d\}$. Dessa forma, é fácil ver que $ord(h^i) = d$ se, e somente se, $mdc(i, d) = 1$. Então $N_d = \varphi(d)$, onde $\varphi(d)$ denota o número de elementos em $\{1, 2, \cdots, d\}$ primos com d.

Miscelânia sobre $\mathbb{Z}_p$

Provamos, então, que $N_d = 0$ ou $N_d = \varphi(d)$.

Miscelânia sobre $\mathbb{Z}_p$

Provamos, então, que $N_d = 0$ ou $N_d = \varphi(d)$.

Lema

$$\sum_{d|n} \varphi(d) = n$$

Provamos, então, que $N_d = 0$ ou $N_d = \varphi(d)$.

Lema

$$\sum_{d|n} \varphi(d) = n$$

Demonstração do lema: Considere os n números

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n}{n}$$

Provamos, então, que $N_d = 0$ ou $N_d = \varphi(d)$.

Lema

$$\sum_{d|n} \varphi(d) = n$$

Demonstração do lema: Considere os n números

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n}{n}$$

Realizadas as devidas simplificações, obtemos para cada d divisor de n todas as $\varphi(d)$ frações da forma $\frac{q}{d}$, onde $q \in \{1, 2, \cdots, d\}$ e $mdc(d, q) = 1$.

Provamos, então, que $N_d = 0$ ou $N_d = \varphi(d)$.

Lema

$$\sum_{d|n} \varphi(d) = n$$

Demonstração do lema: Considere os n números

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n}{n}$$

Realizadas as devidas simplificações, obtemos para cada d divisor de n todas as $\varphi(d)$ frações da forma $\frac{q}{d}$, onde $q \in \{1, 2, \cdots, d\}$ e $mdc(d, q) = 1$. Como temos n frações, segue que

$$\sum_{d|n} \varphi(d) = n$$

Como $N_d = 0$ ou $N_d = \varphi(d)$, temos

$$p - 1 = \sum_{d|p-1} N_d \leq \sum_{d|p-1} \varphi(d) = p - 1$$

Como $N_d = 0$ ou $N_d = \varphi(d)$, temos

$$p - 1 = \sum_{d|p-1} N_d \leq \sum_{d|p-1} \varphi(d) = p - 1$$

Disso, segue que $N_d = \varphi(d)$.

Miscelânia sobre $\mathbb{Z}_p$

Como $N_d = 0$ ou $N_d = \varphi(d)$, temos

$$p - 1 = \sum_{d|p-1} N_d \leq \sum_{d|p-1} \varphi(d) = p - 1$$

Disso, segue que $N_d = \varphi(d)$. Em particular, $N_{p-1} = \varphi(p-1) \geq 1$, i.e., $\mathbb{Z}_p$ possui uma raiz primitiva.

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Teorema de Schur

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Demonstração: Seja g raíz primitiva de $\mathbb{Z}_p$. Então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$.

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Demonstração: Seja g raíz primitiva de $\mathbb{Z}_p$. Então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Note que, para cada $a \in \mathbb{Z}_p$ existe um único $t \in \{1, 2, \cdots, p-1\}$ tal que $a = g^t$

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Demonstração: Seja g raíz primitiva de $\mathbb{Z}_p$. Então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Note que, para cada $a \in \mathbb{Z}_p$ existe um único $t \in \{1, 2, \cdots, p-1\}$ tal que $a = g^t$, de modo que podemos definir a k-coloração sobre $\mathbb{Z}_p$ dada por $c(a) = t \pmod{k}$.

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Demonstração: Seja g raíz primitiva de $\mathbb{Z}_p$. Então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Note que, para cada $a \in \mathbb{Z}_p$ existe um único $t \in \{1, 2, \cdots, p-1\}$ tal que $a = g^t$, de modo que podemos definir a k-coloração sobre $\mathbb{Z}_p$ dada por $c(a) = t \pmod{k}$. Pelo lema de Schur, existe n tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$ existe uma solução monocromática para a equação $x + y = z$.

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Demonstração: Seja g raíz primitiva de $\mathbb{Z}_p$. Então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Note que, para cada $a \in \mathbb{Z}_p$ existe um único $t \in \{1, 2, \cdots, p-1\}$ tal que $a = g^t$, de modo que podemos definir a k-coloração sobre $\mathbb{Z}_p$ dada por $c(a) = t \pmod{k}$. Pelo lema de Schur, existe n tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$ existe uma solução monocromática para a equação $x + y = z$. Em particular, se p é um primo maior que n, havera uma solução monocromática para a equação $x + y = z$ com relação à coloração descrita

Teorema de Schur

Dado $k \in \mathbb{N}$, para todo primo p suficientemente grande, existem $a, b, c \in \mathbb{Z}_p$, $a, b, c \neq \overline{0}$, tais que

$$a^k + b^k = c^k$$

Demonstração: Seja g raíz primitiva de $\mathbb{Z}_p$. Então $\{g, g^2, \cdots, g^{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Note que, para cada $a \in \mathbb{Z}_p$ existe um único $t \in \{1, 2, \cdots, p-1\}$ tal que $a = g^t$, de modo que podemos definir a k-coloração sobre $\mathbb{Z}_p$ dada por $c(a) = t \pmod{k}$. Pelo lema de Schur, existe n tal que para toda k-coloração sobre $\{1, 2, \cdots, n\}$ existe uma solução monocromática para a equação $x + y = z$. Em particular, se p é um primo maior que n, havera uma solução monocromática para a equação $x + y = z$ com relação à coloração descrita, i.e., existem $x, y, z \in \mathbb{Z}_p$ com $c(x) = c(y) = c(z) = r$ tais que

$$x + y = z$$

Teorema de Schur

Note que

$$c(x) = c(y) = c(z) = r \Rightarrow x = g^{k \cdot q_1 + r},\ y = g^{k \cdot q_2 + r},\ z = g^{k \cdot q_3 + r}$$

Teorema de Schur

Note que

$$c(x) = c(y) = c(z) = r \Rightarrow x = g^{k \cdot q_1 + r},\ y = g^{k \cdot q_2 + r},\ z = g^{k \cdot q_3 + r}$$

Dessa forma, temos

$$x + y = z \Rightarrow g^{k \cdot q_1 + r} + g^{k \cdot q_2 + r} = g^{k \cdot q_3 + r}$$

Teorema de Schur

Note que

$$c(x) = c(y) = c(z) = r \Rightarrow x = g^{k \cdot q_1 + r},\ y = g^{k \cdot q_2 + r},\ z = g^{k \cdot q_3 + r}$$

Dessa forma, temos

$$x + y = z \Rightarrow g^{k \cdot q_1 + r} + g^{k \cdot q_2 + r} = g^{k \cdot q_3 + r}$$

Multiplicando a equação por g^{-r}, obtém-se

$$(g^{q_1})^k + (g^{q_2})^k = (g^{q_3})^k$$

Teorema de Schur

Note que

$$c(x) = c(y) = c(z) = r \Rightarrow x = g^{k \cdot q_1 + r},\ y = g^{k \cdot q_2 + r},\ z = g^{k \cdot q_3 + r}$$

Dessa forma, temos

$$x + y = z \Rightarrow g^{k \cdot q_1 + r} + g^{k \cdot q_2 + r} = g^{k \cdot q_3 + r}$$

Multiplicando a equação por g^{-r}, obtém-se

$$(g^{q_1})^k + (g^{q_2})^k = (g^{q_3})^k$$

Como queríamos.

Dúvidas?

Referências