UNIVERSIDADE ESTADUAL DE MARINGÁ
DEPARTAMENTO DE MATEMÁTICA - CCE
SEMINÁRIOS DE INICIAÇÃO CIENTÍFICA

Orientadora: Prof^a Dr^a Ana Paula Peron
Acadêmica: Raquel Polizeli

Introdução à Teoria dos Números

Relatório final do projeto de iniciação científica.

Maringá - PR, Setembro de 2002.

Resumo

Atualmente a Teoria dos Números é ferramenta indispensável para o estudo de qualquer área da Matemática, sendo a base de cada uma delas. Além disso, é uma das áreas mais fascinantes tendo em vista a formulação simples de vários de seus problemas, porém de grande dificuldade na verificação. O objetivo deste projeto é estudar tópicos fundamentais da Teoria dos Números, tais como: indução matemática, divisibilidade, máximo divisor comum, algoritmo de Euclides, mínimo múltiplo comum, números primos e congruência.

Sumário

Introdução

O objetivo central da Teoria dos Números é o estudo das propriedades dos números inteiros positivos. Os principais ramos em que se divide a Teoria dos Números são três: Teoria Elementar, Teoria Analítica e Teoria Algébrica.

Estudamos vários tópicos da Teoria Elementar, os quais possuem resultados básicos e de extrema importância para o estudo das partes Analíticas e Algébricas, e também, mesmo que implicitamente, em diversos campos da Matemática.

Os tópicos estudados foram:

- Números Inteiros: propriedades, valor absoluto, fatorial, número binomial, números binomiais complementares e consecutivos;

- Indução Matemática: princípio da boa ordenação, princípio de indução finita, indução matemática;

- Divisibilidade: relação de divisibilidade nos inteiros, divisores comuns de dois inteiros, algoritmo da divisão;

- Máximo Divisor Comum: existência e unicidade do máximo divisor comum, inteiros primos entre si, caracterização do máximo divisor comum de dois inteiros, máximo divisor comum de vários inteiros;

- Algoritmo de Euclides e Mínimo Múltiplo Comum: algoritmo de Euclides, múltiplos comuns de dois inteiros, mínimo múltiplo comum de dois inteiros, relação entre o máximo divisor comum e o mínimo múltiplo comum, mínimo múltiplo comum de vários inteiros;

- Números Primos: números primos e compostos, teorema fundamental da aritmética, fórmulas que dão primos, crivo de Erastótenes, primos gêmeos, seqüências de inteiros consecutivos compostos, conjectura de Goldbach, método de fatoração de Fermat;

- Congruências: inteiros congruentes, caracterização de inteiros congruentes, propriedades das congruências, sistemas completos de restos.

A referência principal utilizada foi [1].

Neste relatório destacaremos alguns dos tópicos estudados, e será apresentado na seguinte forma.

Na Seção 1, daremos um breve histórico sobre os números inteiros.

Na Seção 2, as duas principais formas do Princípio de Indução Finita serão abordadas, sendo que uma delas será demonstrada e um exemplo de como aplicá-la será dado.

Na Seção 3, demonstraremos o Algoritmo da Divisão que é o mais importante resultado entre as propriedades de divisibilidade. Um exemplo será apresentado.

Na Seção 4, descreveremos o Algoritmo de Euclides, o qual nos possibilita encontrar o máximo divisor comum entre dois números inteiros. Um exemplo mostra a praticidade de tal método.

Na Seção 5, daremos uma prova da existência de infinitos números primos e apresentaremos um método para encontrarmos os números primos menores que um dado inteiro positivo, conhecido como Crivo de Erastótenes.

Finalmente na Seção 6, o conceito de congruência será introduzido e apresentaremos um exemplo importante sobre sistemas completos de restos.

1 Números Inteiros

Os números foram considerados durante milênios como entes intuitivos e algumas de suas propriedades, como por exemplo a comutatividade e a associatividade da adição e da multiplicação, eram consideradas inerentes à sua própria natureza, portanto não necessitando de demonstração. A criação do Cálculo Diferencial no século XVII colocou os matemáticos diante de novos problemas que, para serem melhor compreendidos e solucionados, requeriam uma fundamentação mais rigorosa do conceito de número. Esta tarefa foi iniciada pelos matemáticos do século XIX. Karl Weierstran foi o primeiro a idealizar um método para a construção dos números inteiros negativos, segundo vários matemáticos da época não seria possível construir tais números a partir dos números naturais.

Em 1888 Dedekind publicou um trabalho onde, a partir de noções básicas da teoria dos conjuntos, ele constrói um modelo para os números naturais, definindo as operações de adição e multiplicação e demonstrando suas propriedades básicas, na época a construção de Dedekind não teve muita difusão por ser bastante complicada, assim a axiomática dada por Giuseppe Peano em 1889 ficou mais popular.

E através do estudo da Teoria Elementar dos Números, sabemos que o conjunto $\mathbb{Z}$ dos números inteiros é constituido por inteiros positivos e inteiros negativos, e é munido de duas operações, a adição $(+)$ e a multiplicação $(\cdot)$, além de uma relação de ordem $(\leq)$.

2 Indução Matemática

A Indução Matemática é um poderoso instrumento para demonstrar teoremas que envolvem os números inteiros não negativos e vem sendo utilizada de uma forma implícita desde a antiguidade. Foi explicitamente enunciada pela primeira vez por Francesco Maurolycus em 1575 e por ele usada, por exemplo, para provar a fórmula apresentada no Exemplo 1 que daremos a seguir. O método tornou-se popular após a publicação em 1665 do artigo “Traité du Triangle Arithmétique” por Blaise Pascal, onde era utilizado.

Existem basicamente duas formas de usarmos o método de indução matemática, as quais apresentaremos a seguir. Demonstraremos apenas a primeira forma, pois a prova da segunda é similar à dada. Para isso utilizaremos o Princípio da Boa Ordenação.

Princípio da Boa Ordenação: *Todo conjunto não-vazio de inteiros não negativos contém o elemento mínimo.*

Denotaremos o conjunto dos números inteiros positivos por $\mathbb{N}$. O resultado abaixo é conhecido como Primeira Forma do Princípio da Indução Finita.

Teorema 2.1. *Seja A um subconjunto de $\mathbb{N}$ satisfazendo as seguintes condições*
(1) $1 \in A$;
(2) Para todo $k \in \mathbb{N}$, se $k \in A$ então $k+1 \in A$.
Então, A contém todos os inteiros positivos, ou seja, $A = \mathbb{N}$.

Demonstração:

Suponhamos que A satisfaça as condições (1) e (2) e não contenha todos os inteiros positivos. Seja R o conjunto dos inteiros positivos não contidos em A. Como $R \neq \emptyset$, pelo Princípio da Boa Ordenação, R possui o elemento mínimo r_0. Pela condição (1) concluímos que $r_0 > 1$ e portanto, $r_0 - 1 \in A$. Como A satisfaz (2), segue que $r_0 \in A$, o que é uma contradição. Logo, A contém todos os inteiros positivos. ■

Usualmente a condição (1) do Teorema 2.1 é chamada de base de indução e a condição (2) de hipótese de indução.

Exemplo 1: Demonstrar que

$$1 + 3 + 5 + \cdots + (2n-1) = n^2, \quad n \in \mathbb{N}. \tag{2.1}$$

Solução:

Consideremos o subconjunto A de $\mathbb{N}$ definido por

$$A := \{k \in \mathbb{N} :\ 1 + 3 + \cdots + (2k-1) = k^2\}.$$

Claro que $1 \in A$, visto que $1 = 1^2$. Agora, suponhamos que $k \in A$, ou seja,

$$1 + 3 + \cdots + (2k-1) = k^2.$$

Adicionando $2k+1$ a ambos membros desta igualdade, e utilizando a hipótese de indução, obtemos:

$$1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = k^2 + (2k+1) = (k+1)^2,$$

o que implica que $k+1 \in A$. Assim, pelo Teorema 2.1, $A = \mathbb{N}$. Isto mostra que (2.1) é verdadeira.

Para finalizar esta seção enunciamos a Segunda Forma do Princípio de Indução Finita.

Teorema 2.2. *Seja A um subconjunto de $\mathbb{N}$ satisfazendo as seguintes condições*
(1) $1 \in A$;
(2) Para todo inteiro positivo k, se $1, 2, \ldots, k \in A$, então $k+1 \in A$.
Então, A contém todos os inteiros positivos, ou seja, $A = \mathbb{N}$.

Observamos que o Princípio da Boa Ordenação, a Primeira e a Segunda Formas da Indução Finita são equivalentes. Uma prova dessa equivalência pode ser encontrada em [3].

3 Algoritmo da Divisão

O algoritmo da divisão, apresentado no Teorema 3.2 abaixo, é um resultado de extrema importância que nos garante a existência e a unicidade do quociente e do resto na divisão de inteiros.

Definição 3.1. *Sejam a e b inteiros com $a \neq 0$, dizemos que a* divide *b, e denotamos por $a|b$, se existe um inteiro c tal que $b = ac$.*

Teorema 3.2. *Dados a e b inteiros, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r, \quad 0 \leq r < b.$$

O número q é chamado de quociente *e r de* resto *da divisão de a por b.*

Demonstração:

Seja S o conjunto de todos os inteiros não negativos da forma

$$a - bx, \quad x \in \mathbb{Z}.$$

Tomando-se $x = -|a|$, como $b \geq 1$, temos

$$a - bx = a + b|a| \geq a + |a| \geq 0.$$

Portanto $S \neq \emptyset$. Assim, pelo Princípio da Boa Ordenação, existe o elemento mínimo r de S. Pela definição de S, segue que, $r \geq 0$ e existe $q \in \mathbb{Z}$ tal que $r = a - bq$. Além disso, $r < b$ pois, caso contrário, teríamos

$$0 \leq r - b = a - bq - b = a - b(q + 1),$$

ou seja, $r - b \in S$ e $r - b < r$, contrariando o fato de r ser o elemento mínimo de S. Portanto, existem inteiros q e r tais que

$$a = bq + r, \quad 0 \leq r < b.$$

Para demonstrar a unicidade de q e r, suponhamos que existam inteiros q_1 e r_1 tais que

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

Então, $bq_1 + r_1 = bq + r$, ou seja,

$$r_1 - r = (q - q_1)b. \tag{3.1}$$

Logo,

$$b|(r_1 - r).$$

Por outro lado, como $-b < -r \leq 0$ e $0 \leq r_1 < b$, segue que $-b < (r_1 - r) < b$, isto é,

$$|r_1 - r| < b.$$

Como $b|(r_1 - r)$, concluímos que $r_1 - r = 0$. Finalmente, como $b \neq 0$, segue de (3.1) que $q - q_1 = 0$. Portanto, $r_1 = r$ e $q_1 = q$. ■

Observamos que $b|a$ se, e somente se, $r = 0$.

Exemplo 2: Achar o quociente q e o resto r na divisão de $a = -79$ por $b = 11$ que satisfazem as condições do algoritmo da divisão.

Solução:

Pelo processo da divisão usual dos valores absolutos de a e b, obtemos $79 = 11.7+2$, o que implica

$$-79 = 11(-7) - 2.$$

Como $r = -2 < 0$ não satisfaz a condição $0 \leq r < 11$, somando e subtraindo o valor 11 de b ao segundo membro da igualdade anterior, obtemos

$$-79 = 11(-7) - 11 + 11 - 2 = 11(-8) + 9, \quad 0 \leq 9 \leq 11.$$

Portanto, obtemos o quociente $q = -8$ e o resto $r = 9$ satisfazendo as condições do algoritmo da divisão.

4 Algoritmo de Euclides

O Algoritmo de Euclides ou processo das divisões sucessivas é um método de cálculo recursivo utilizado para encontrar o máximo divisor comum de dois inteiros, sendo um dos mais eficientes do ponto de vista computacional.

A questão da eficiência ou "custo" de um determinado algoritmo é central em computação científica, pois o seu sucesso é em função da rapidez com a qual uma máquina pode efetuar os cálculos.

Definição 4.1. *O* máximo divisor comum *de dois inteiros a e b (a ou b não nulos), denotado por (a, b), é o maior inteiro positivo que divide a e b.*

Para determinarmos o máximo divisor comum basta analisarmos o caso em que a e b são inteiros positivos distintos tais que b não divide a. Sem perda de generalidade, podemos assumir $a > b$. Nessas condições, a aplicação repetida do algoritmo da divisão nos fornece as seguintes igualdades

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b \\ b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\ r_2 &= r_3 q_4 + r_4, \quad 0 < r_4 < r_3 \end{aligned}$$

....

Como os restos r_i são todos inteiros positivos tais que

$$b > r_1 > r_2 > r_3 > r_4 > \ldots$$

e existem apenas $b - 1$ inteiros menores que b, necessariamente se chega a uma divisão onde o resto $r_{n+1} = 0$, isto é, teremos

$$\begin{aligned} r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0 \end{aligned}$$

O último resto não nulo ($r_n \neq 0$) da seqüência de divisores citada acima é o máximo divisor comum de a e b. Este processo para calcular o máximo divisor comum é conhecido como Algoritmo de Euclides.

Este algoritmo também pode ser usado para expressar $(a, b) = r_n$ como combinação linear de a e b. Para isto basta eliminarmos sucessivamente os restos $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ entre as n primeiras igualdades anteriores.

Uma forma prática de utilizar tal método é dada da seguinte maneira

	q_1	q_2	...	q_n	q_{n+1}
a	b	r_1	...	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	...	0	

Exemplo 3: Usando o Algoritmo de Euclides

(i) Calcular (7469, 2387);

(ii) Encontrar os inteiros x e y que verifiquem $(7469, 2387) = 7469x + 2387y$.

Solução:

(i) Pelo Algoritmo de Euclides temos:

	3	7	1	3
7469	2387	308	231	77
308	231	77	0	

Logo, (7489, 2387) = 77.

(ii) Pelo item anterior podemos escrever

$$\begin{aligned} 7469 &= 2387(3) + 308 \\ 2387 &= 308(7) + 231 \\ 308 &= 231(1) + 77 \\ 231 &= 77(3) + 0. \end{aligned}$$

Agora, eliminando os restos 231 e 308 das três primeiras igualdades anteriores obtemos

$$\begin{aligned} 77 &= 308 - 231(1) = \\ &= 308 - [2387 - (7)308](1) = 308(8) - 2387 = \\ &= [7469 - 2387(3)](8) - 2387 = \\ &= 7469(8) + 2387(-25). \end{aligned}$$

Assim, $x = 8$ e $y = -25$.

5 Números Primos e Compostos

Estão relacionados com números primos alguns dos problemas mais famosos da Matemática. Alguns desses problemas ainda não foram resolvidos, enquanto outros só foram resolvidos com a utilização de técnicas matemáticas sofisticadas de áreas como Álgebra, Análise Real e Análise Complexa.

Definição 5.1. *Um número inteiro n ($n > 1$) possuindo somente dois divisores positivos n e 1 é chamado* primo. *Se $n > 1$ não é primo, dizemos que n é* composto.

Existem vários pares de primos que diferem de duas unidades, por exemplo,

3 e 5; 5 e 7; 11 e 13; 41 e 43; 107 e 109; 239 e 241,

entre outros. Pares de primos como estes são chamados de *primos gêmeos*. Até o presente momento ainda não se sabe se os primos gêmeos são em número finito ou infinito. Entretanto, o problema análogo para ternas, ou seja, três primos ímpares consecutivos, é de fácil resolução, pois como $3|n(n+2)(n+4)$, concluímos que 3, 5 e 7 é a única terna satisfazendo a propriedade requerida.

Os números primos são, do ponto de vista da divisibilidade, os mais simples, pois são irredutíveis. Um resultado importante envolvendo os números primos é o Teorema Fundamental da Aritmética, apresentado no Teorema 5.2 abaixo. Omitiremos sua prova a qual envolve um procedimento simples de repetições sucessivas e indução matemática.

Teorema 5.2. (Teorema Fundamental da Aritmética) *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Uma pergunta que surge é : Quantos são os primos ? A resposta de Euclides é a seguinte.

Teorema 5.3. (Euclides) *A seqüência dos números primos é infinita.*

Demonstração:

Vamos supor que a seqüência de primos seja finita. Seja $p_1, p_2, \ldots, p_n$ a lista de todos os primos. Consideremos o número $R = p_1.p_2 \ldots p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas, pelo Teorema 5.2, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence a nossa lista. Portanto a seqüência dos números primos não pode ser finita. ■

O próximo resultado justifica o Crivo de Erastóstenes, o qual fornece uma maneira prática de encontrar todos os números primos menores que um dado inteiro positivo.

Teorema 5.4. *Se um inteiro positivo $n > 1$ não é primo , então n possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.*

Demonstração:

Seja $n > 1$ um inteiro composto. Então,

$$n = n_1 n_2, \quad 1 < n_1 < n, \quad 1 < n_2 < n.$$

Sem perda de generalidade vamos supor $n_1 \leq n_2$. Logo, $n_1 \leq \sqrt{n}$ pois, caso contrário, teríamos

$$n = n_1 n_2 \geq n_1 n_1 > \sqrt{n}\sqrt{n} = n,$$

o que é um absurdo. Assim, pelo Teorema 5.2, n_1 possui algum fator primo $p \leq \sqrt{n}$. Portanto, p é também um fator primo de n. ■

Como os números primos aparecem com muita irregularidade na seqüência dos inteiros positivos, muitas fórmulas que geram números primos foram construídas. Por exemplo, a fórmula de Euler

$$F_n = n^2 + n + 41$$

fornece primos para $n = 0, 1, 2, \ldots, 39$, mas para $n = 40$ e $n = 41$, obtém-se inteiros compostos. Há outras fórmulas para a obtenção de primos tais como:

$$F_n = 2n^2 + 29, \quad 0 \leq n \leq 28,$$

$$F_n = n^2 - 79n + 1601, \quad 0 \leq n \leq 79.$$

Exemplo 4 : Construir a tabela de todos os primos menores que 100.

Solução:

O processo que utilizaremos é conhecido como Crivo de Erastótenes. Os primos p tais que $p \leq \sqrt{100} = 10$ são 2, 3, 5 e 7. Escrevemos na ordem natural todos os inteiros desde 2 até 100 e, em seguida, eliminamos todos os inteiros compostos que são múltiplos de $2, 3, 5$ e 7.

	2	3	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	23	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	29	$\cancel{30}$
31	$\cancel{32}$	$\cancel{33}$	$\cancel{34}$	$\cancel{35}$	$\cancel{36}$	37	$\cancel{38}$	$\cancel{39}$	$\cancel{40}$
41	$\cancel{42}$	$\cancel{43}$	$\cancel{44}$	$\cancel{45}$	$\cancel{46}$	47	$\cancel{48}$	$\cancel{49}$	$\cancel{50}$
$\cancel{51}$	$\cancel{52}$	53	$\cancel{54}$	$\cancel{55}$	$\cancel{56}$	$\cancel{57}$	$\cancel{58}$	59	$\cancel{60}$
61	$\cancel{62}$	$\cancel{63}$	$\cancel{64}$	$\cancel{65}$	$\cancel{66}$	67	$\cancel{68}$	$\cancel{69}$	$\cancel{70}$
71	$\cancel{72}$	73	$\cancel{74}$	$\cancel{75}$	$\cancel{76}$	$\cancel{77}$	$\cancel{78}$	79	$\cancel{80}$
$\cancel{81}$	$\cancel{82}$	83	$\cancel{84}$	$\cancel{85}$	$\cancel{86}$	$\cancel{87}$	$\cancel{88}$	89	$\cancel{90}$
$\cancel{91}$	$\cancel{92}$	$\cancel{93}$	$\cancel{94}$	$\cancel{95}$	$\cancel{96}$	97	$\cancel{98}$	$\cancel{99}$	$\cancel{100}$

Os inteiros positivos não eliminados são

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Suponhamos que algum desses números seja composto, denotemos por a. Pelo Teorema 5.4, a possui um fator primo $p \leq \sqrt{a} \leq \sqrt{100}$. Mas, estes números já foram todos eliminados. Portanto, os números listados acima são todos os primos menores que 100.

6 Congruência

Grande parte dos resultados sobre congruência foi introduzido por Gauss (1777-1855) em um trabalho publicado em 1801 *(Disquisitiones Arithmeticae)* quando tinha 24 anos. Estudamos resultados de grande importância, os quais serviram de base para o desenvolvimento da Teoria dos Números. Até mesmo a notação introduzida no trabalho de Gauss é a que utilizamos hoje:

$$a \equiv b \mod m,$$

indicando que a é congruente a b módulo m.

Definimos congruência do seguinte modo.

Definição 6.1. *Sejam a e b números inteiros e m um inteiro positivo. Dizemos que a é* congruente a b módulo m *se $m|(a-b)$. Se m não divide $(a-b)$, dizemos que a é* incongruente a b módulo m *e denotamos por $a \not\equiv b \mod m$.*

A relação R de "congruência módulo m" em $\mathbb{Z}$ dada por

$$aRb \Longleftrightarrow a \equiv b \mod m$$

é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência em $\mathbb{Z}$.

Dentre o conteúdo estudado destacamos o sistema completo de restos onde, um conjunto $A = \{r_1, r_2, \ldots, r_m\}$, de m inteiros, é dito ser um *sistema completo de restos módulo* m se todo inteiro a é congruente módulo m a um único elemento de A.

O próximo resultado nos fornece um exemplo importante de sistema completo de restos denominado sistema de restos mínimos módulo m.

Teorema 6.2. *Seja m um inteiro positivo. O conjunto $S = \{0, 1, \ldots, m-1\}$ é um sistema completo de restos módulo m.*

Demonstração:

Seja a um inteiro qualquer. Pelo Teorema 3.2, existe um único par de inteiros q e r tais que

$$a = mq + r, \quad 0 \leq r < m.$$

Então, pela Definição 6.1, temos:

$$a \equiv r \mod m.$$

Como r só pode assumir os valores $0, 1, 2, \ldots, m-1$, segue que o inteiro a é congruente módulo m a um único elemento do conjunto S. Portanto, S é um sistema completo de restos módulo m. ∎

Exemplo 5: Seja m um inteiro maior ou igual a 2. Mostrar que o conjunto

$$\{1^2, 2^2, 3^2, \ldots, m^2\}$$

não é um sistema completo de restos módulo m.

Solução:

Basta tomarmos dois inteiros positivos n e k, $n > k$, tais que $n + k = m$. Assim

$$n^2 - k^2 = (n+k)(n-k) = m(n-k) \equiv 0 \mod m.$$

Logo,

$$n^2 \equiv k^2 \mod m.$$

Como $n, k < m$ e $n^2 \equiv n^2 \mod m$, segue que o inteiro n é congruente a mais de um elemento do conjunto $\{1^2, 2^2, \ldots, m^2\}$. Portanto, este conjunto não é um sistema completo de restos módulo m.

Comentário Final

Neste projeto, foi estudado parte da *Teoria Elementar dos Números* nos fornecendo um ponto de partida para a aprendizagem da Teoria dos Números e de vários ramos da Matemática. Além de nos proporcionar um primeiro contato com a pesquisa, os seminários semanais, a orientação dos professores, a ajuda dos colegas e a resolução dos exercícios, bem como, a preparação das exposições, fez com que nós acadêmicos, desenvolvessemos ainda mais as técnicas e o raciocínio matemático, fundamentais para o bom desempenho profissional.

Referências

[1] Alencar Filho, E. *Teoria Elementar dos Números*. São Paulo: Nobel, 1992, 336p.

[2] Hefez, A. *Curso de Álgebra*, Volume 1. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1993, 226pp, (Coleção Matemática Universitária).

[3] Santos, J. P. O. *Introdução à Teoria dos Números*. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 2000, 199pp, (Coleção Matemática Universitária).

Raquel Polizeli
(Acadêmica)

Prof^a Dr^a Ana Paula Peron
(Orientadora)

Avaliação da orientadora sobre o Projeto "Seminários de Iniciação Científica"

Tendo em vista que este projeto esteve em andamento conjunto com mais oito professores e oito acadêmicos, considero que foi alcançado o objetivo de integração entre os alunos e professores durante os seminários. Porém, de um modo geral, houve pouco contato direto entre orientador e orientado impossibilitando sanar de uma forma mais específica alguma possível falha, seja no conteúdo matemático ou na forma de expressar-se escrita ou oralmente para uma apresentação.

Por outro lado, é uma grande oportunidade para os alunos do primeiro ano terem um contato inicial com um projeto de pesquisa, não necessariamente vinculado ao do orientador, uma vez que estando ainda no primeiro ano do curso de Matemática os acadêmicos não têm base teórica para um projeto mais elaborado.

PROF^a DR^a ANA PAULA PERON

Avaliação da orientadora sobre o desempenho da acadêmica no projeto

Apesar do conteúdo deste projeto não constar do programa do curso de Matemática, a acadêmica Raquel Polizeli teve um bom desempenho durante sua realização. Os tópicos estudados, relativamente simples, serviram para incentivar o raciocínio lógico e o rigor matemático que a acadêmica, do primeiro ano do curso de Matemática, deverá fortalecer no decorrer de sua graduação.

Prof^a Dr^a Ana Paula Peron