Algébra 01

Sumário

1 Princípios Básicos **3**
1.1 Propriedades . . . 3
1.2 Definições . . . 3
1.3 Números Reais . . . 3
1.4 Múltiplos e Divisores . . . 4
1.5 Princípio da Boa Ordenação e Indução . . . 4
1.6 Exemplos . . . 5
2 Fórmula Binomial **7**
3 Divisão Euclidiana e Máximo Divisor Comum **9**
3.1 Divisão Euclidiana . . . 9
3.2 Máximo Divisor Comum . . . 11
4 Números Primos e Coprimos **11**
4.1 Números Coprimos . . . 11
4.2 Números Primos . . . 13
5 Equações Diofantinas **15**
5.1 Exemplos . . . 16
6 Inteiros Gaussianos **19**
6.1 Divisibilidade e Associados . . . 21
6.2 Primos Gaussianos . . . 21
6.3 $x^2 + y^2 = p$ . . . 23
7 Provas **25**
7.1 Prova 1 . . . 25
7.2 Prova 2 . . . 25
7.3 Prova 3 . . . 26

1 Princípios Básicos

- Assumimos os conceitos de **conjuntos** e **subconjuntos**.
  ↪ $\in$: "é elemento de"
  ↪ $\mathbb{N}$: Naturais
  ↪ $\mathbb{Z}$: Inteiros
  ↪ $\mathbb{Q}$: Racionais
  ↪ $\mathbb{R}$: Reais
  ↪ $\mathbb{C}$: Complexos

1.1 Propriedades

- Assumindo que esses conjuntos númericos tenham essas propriedades :

A1. $(x + y) + z = x + (y + z)$
A2. $0 + x = x$
A3. A equação $a+x = b$ possui uma única solução em $\mathbb{Z}$, se $a, b \in \mathbb{Z}$ (respectivamente, $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$).
A4. $x + y = y + x$

M1. $(xy)z = x(yz)$
M2. $1 \cdot x = x$
M3. A equação $ax = b$ possui uma única solução em $\mathbb{Q}$, se $a, b \in \mathbb{Q}$ (respectivamente, $\mathbb{R}$ e $\mathbb{C}$).
M4. $xy = yx$

MA. $x \cdot (y + z) = xy + xz$ e $(x + y) \cdot z = xy + xz$ (**Lei Distributiva**).

Para $a \neq 0$. As soluções para **A3** e **M3** são respectivamente: $b - a$ e $\frac{b}{a}$.

1.2 Definições

- **Anel:** Possui as propriedades **A1**, **A2**, **A3**, **A4** e **MA**.
- **Corpo:** Possui todas as **noves** propriedades.

1.3 Números Reais

- Aqui estão algumas inferências sobre os números reais ($\mathbb{R}$).

1. É positivo ($0 \geq$) ou negativo ($0 \leq$).
2. 0 é positivo e negativo.
3. $b \geq a$ (ou $a \leq b$) $\rightarrow a - b \geq 0$.
4. $b > a$ (ou $a < b$) $\rightarrow b \geq a$ e $b \neq a$.

1.4 Múltiplos e Divisores

- Se a, b e c são inteiros e $\boxed{b = a \cdot c}$
  $\hookrightarrow b$: É múltiplo de a
  $\hookrightarrow a$ divide b ou a é divisor de b.
  $\hookrightarrow$ **Notação** : $a|b$.

Definição : Par

b é um inteiro **par** se $2|b$, caso contrário, b é **ímpar**

Exemplo : Soma dos Divisores

$6 \Rightarrow 1 + 2 + 3 + 6 = 12$
$15 \Rightarrow 24$
$945 \Rightarrow 1920$

Questão (Números Perfeitos)

Existe um número ímpar n tal que a soma dos seus divisores positivos seja igual a $2n$?

1.5 Princípio da Boa Ordenação e Indução

Definição : Princípio da Boa Ordenação (PBO)

Cada conjunto não vazio de interios positivos contém um menor elemento.

Exemplo : Prove que não existe um número inteiro x tal que $0 < x < 1$.

De fato, se o conjunto de todos os inteiros x tais que $0 < x < 1$ fosse não vazio, o Princípio da Boa Ordenação é garantido que existiria um menor inteiro m tal que, $0 < m < 1$.
Então, teriamos que $0 < m^2 < m < 1$; uma contradição

Uma formulação equivalente do **Princípio da Boa Ordenação** é o **Princípio da Indução Matemática**.

Definição : Princípio da Indução Matemática (PIM)

Se uma senteça sobre um inteiro positivo n é verdadeira para $n = 0$, e se sua veracidade para cada n com $0 \leq n \leq N$ implica sua veracidade para $n = N$,então ela é verdadeira para todo $n \geq 0$.

1.6 Exemplos

Exemplo : Soma dos primeiros números naturais

Mostre que a igualdade $1 + 2 + \cdots + n = \frac{n \cdot (n+1)}{2}$ vale para cada $n \geq 1$.

De fato, para $n = 1$ temos :

$$1 = \frac{1(1+1)}{2}$$

Suponhamos que a igualdade seja válida para cada n com $1 \leq n < N$.

Daí,

$$\begin{aligned} 1 + 2 + \ldots + (N-1) + N &= (1 + 2 + \ldots + N - 1) + N \\ &= \frac{(N-1) \cdot ((N-1)+1)}{2} + N \\ &= \frac{N^2 - N + 2N}{2} \\ &= \frac{N \cdot (N+1)}{2} \end{aligned}$$

Logo, pelo Princípio da Indução Matemática a igualdade é válida para todo $n \geq 1$.

Exemplo

Demostre a validade de $2^n > 18(n+1)$ para cada $n \geq 8$.

De fato, para $n = 8$ temos :

$$2^8 = 256 > 162 = 18 \cdot (9)$$

Suponhamos que essa afirmação é válida para cada n com $8 \leq n < N$.

Daí,

$$\begin{aligned} 2^N = 2^{N-1} \cdot 2 &> 18 \cdot (N - 1 + 1) \cdot 2 \\ &> (18N) \cdot 2 = 18N + 18N \\ &> 18N + 18 = 18 \cdot (N+1) \end{aligned}$$

Logo, pelo Princípio da Indução Matemática a afirmação é válida para cada $n \geq 8$.

Exemplo : Sequências

$$a_n = \begin{cases} 1, & \text{se } n = 1, \\ a_{n-1} + 3, & \text{se } n \geq 2, \end{cases} \qquad b_n = a_1 + \ldots + a_n \; = \; \sum_{k=1}^{n} a_k.$$

Para cada $n \geq 1$ mostre que :

i. $a_n = 1 + 3 \cdot (n-1)$

ii. $b_n = \frac{3n^2 - n}{2}$

De fato, para $n = 1$ temos :

$$a_n = 1 + 3 \cdot (1-1) = 1$$

Suponhamos que a afirmação seja válida para cada n com $1 \leq n < N$.

Daí,

$$\begin{aligned} a_N &= a_{N-1} + 3 \\ &= 1 + 3 \cdot ((N-1) - 1) + 3 \\ &= 1 + 3 \cdot ((N-1) - 1 + 1) = 1 + 3 \cdot (N-1) \end{aligned}$$

Logo, pelo Princípio da Indução Matemática a afirmação é válida para todo $n \geq 1$.

Por outro lado, para $n = 1$ temos :

$$b_N = 1 = \frac{3(1)^2 - (1)}{2}$$

Suponhamos que a afirmação seja válida para cada n com $1 \leq n < N$.

Daí,

$$\begin{aligned} b_N &= a_1 + \ldots + a_{N-1} + a_N \\ &= \frac{3(N-1)^2 - (N-1)}{2} + 1 + 3 \cdot (N-1) \\ &= \frac{3N^2 - 6N + 3 - N + 1 + 2 + 6N + 3}{2} \\ &= \frac{3N^2 - N}{2} \end{aligned}$$

Logo, pelo Princípio da Indução Matemática a afirmação é válida para cada $n \geq 1$.

2 Fórmula Binomial

Definição : Fórmula Binomial

- Seja $n, k \in \mathbb{Z} \geq 0$. Definimos :

$$\binom{n}{k} = \begin{cases} \dfrac{n \cdot (n-1) \cdot \ldots \cdot (n-k-1)}{k!}, & \text{se } n \geq k, \\ 0, & \text{se } n < k, \end{cases}$$

em que $k!$ denota o **produto** dos inteiros ≥ 1 e $\leq k$.

- Dessa definição decorre que :

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}, \text{ sempre que } 1 \leq k \leq n.$$

(∗) Afirmação : Dado um inteiro $n \geq 1$ para cada inteiro k com $0 \leq k \leq n$, vale que o máximo $\binom{n}{k}$ é um inteiro.

Demonstração :

De fato, para $n = 1$ temos :

$$\binom{1}{0} = 1 = \binom{1}{1}$$

Suponhamos que essa afirmação seja válida para cada n com $0 \leq n \leq N+1$, sempre que $0 \leq k \leq n$.

Daí, $\binom{N+1}{0} = 1 = \binom{N+1}{N+1}$, e se $1 \leq k < N$ sabemos que $\binom{N+1}{N+1}$ é a soma de dois inteiros.

Logo, pelo Princípio da Indução Matemática a afirmação é válida.

(∗) Proposição : Dado dos números reais (ou complexos) a e b e um inteiro $n \geq 1$ vale a seguinte afirmação :

$$\begin{aligned} (a+b)^n &= a^n + \ldots + \binom{n}{k} a^{n-k} \cdot b^k + \ldots b^n \\ &= \sum_{0 \leq k \leq n} \binom{n}{k} a^{n-k} \cdot b^k \end{aligned}$$

Demonstração :

Para $n = 1$, temos :

$$(a+b)^1 = \binom{1}{0}a + \binom{1}{1}b$$

Suponhamos que a fórmula binomial seja verdadeira para cada n com $1 \leq n \leq N+1$

Daí,

$$\begin{aligned}(a+b)^{N+1} &= (a+b)^N \cdot (a+b) \\ &= a^{N+1} + \binom{N}{1}a^N b + \binom{N}{2}a^{N-1}b^2 + \ldots + \binom{N}{N}ab^N \\ &+ \binom{N}{0}a^N b + \binom{N}{1}a^{N-1}b^2 + \ldots + b^{N+1} \\ &= a^{N+1} + \binom{N+1}{1}a^N b + \binom{N+2}{2}a^{N-1}b^2 + \ldots + b^{N+1}\end{aligned}$$

Logo, pelo Princípio da Indução Matemática a fórmula binomial está demostrada para cada $n \geq 1$.

Exemplo

Mostre que para cada inteiro $n \geq 0$ vale que $n^5 - n$ é um múltiplo de 5.

De fato, para $n = 0$ temos

$$0^5 - 0 = 5 \cdot (0)$$

Suponhamos que $n^5 - n$ é um multíplo de 5 para cada n com $0 \leq n < N+1$

Daí,

$$\begin{aligned}(N+1)^5 - (N+1) &= N^5 - N + 5N^4 + 10N^3 + 10N^2 + 5N + 1 - 1 \\ &= N^5 - N + 5 \cdot (N^4 + 2N^3 + 2N^2 + N)\end{aligned}$$

que é um multíplo de 5

Logo, pelo Princípio da Indução Matemática $n^5 - n$ é um multíplo de 5 para $n \geq 0$.

3 Divisão Euclidiana e Máximo Divisor Comum

- Vamos começar com um exemplo para calcular o mdc entre dois **números inteiros**.

Exemplo : $mdc(2014, 1486) = 106$

$$2014 = 1 \cdot 1484 + 530$$
$$1484 = 2 \cdot 530 + 424$$
$$530 = 1 \cdot 424 + 106$$
$$424 = 4 \cdot 106 + 0.$$

- Analisando de baixo para cima, 106 divide 1484 (106|1484) e 106 divide 2014 (106|2014), e de cima para baixo, se um **inteiro** d divide 2014 e 1484, então d divide 106 (d|106).
- Assim, podemos reescrever a equações de cima para baixo do seguinte modo :

$$530 = 2014 + (-1) \cdot 1484$$
$$424 = 1484 + (-2) \cdot 530 = (-2) \cdot 2014 + 3 \cdot 1484$$
$$106 = 530 + (-1) \cdot 424 = 3 \cdot 2014 + (-4) \cdot 1484.$$

3.1 Divisão Euclidiana

(∗) Lema 4.1. : **Divisão Euclidiana**

Se a e d são **inteiros** com $d > 0$, então existe um único maior múltiplo qd de d que é menor do que ou igual a a; ele pode ser caracterizado por $qd \leq a < (q+1)d$, ou por :

$$a = qd + r, \text{ com } 0 \leq r < d$$

r : **Resto** da divisão de a.
d : **Divisor**.
q : **Quociente**.

Demonstração :

O conjunto dos inteiros positivos da forma $a - zd$, com $z \in \mathbb{Z}$ é não-vazio, pois podemos tomar $z = -N$ em que N é um inteiro não-negativo suficientemente grande.

Assim, pelo **Princípio da Boa Ordenação**, digamos que seja r o menor elemento daquele conjunto, e escrevamos $r = a - qd$. Então, $r \geq 0$ e, $r < d$ pois caso contrário $a - (q+1)d$ pertenceria ao conjunto e seria $< r$.

Exemplo

Os **números ímpares** são da forma $2n+1$, com $n \in \mathbb{Z}$.
A diferença entre quaisquer dois **números ímpares** é um **número par**.

(∗) **Proposição 4.2.** : Seja M um conjunto não-vazio de inteiros. Se M é **fechado** com respeito à subtração, então existe um único $m \geq 0$ tal que M é o conjunto de **todos** os múltiplos de m :

$$M = \{mz : z \in \mathbb{Z}\} = m\mathbb{Z}$$

Demonstração :

Começemos com algumas observações. Se $x \in M$, então pela hipótese $0 = x - x \in M$, e $-x = 0 - x \in M$. Se, além disso, $y \in M$, então $y + x = y - (-x) \in M$, logo M é fechado com respeito à adição. Se $x \in M$ e $nx \in M$ em que n é um inteiro não-negativo qualquer, então $(n+1)x \in M$. Portanto, pelo **Princípio da Indução Matemática**, $nx \in M$ para cada $n \geq 0$, e logo para cada $n \in \mathbb{Z}$. Finalmente, todas as combinações lineares de elementos de M com coeficientes inteiros ainda pertencem a M. Como essa propriedade resulta em M ser fechado com respeito à adição e à subtração, ela é equivalente à hipótese sobre M.

Se $M = \{0\}$, a proposição é verdadeira tomando-se $m = 0$. Caso contrário, o conjunto dos elementos > 0 em M é não-vazio. Tomemos m como o menor desses elementos. Todos os múltiplos de m pertencem a M. Para cada $x \in M$, aplicamos o Lema 4.1 (Divisão Euclidiana) e escrevemos $x = my + r$ com $0 \leq r < m$; então, $r = x - my \in M$. Pela definição de m, isto implica $r = 0$, ou seja, $x = my$. Portanto, $M = m\mathbb{Z}$. Finalmente, como m é o menor elemento > 0 em $m\mathbb{Z}$, ele é unicamente determinado quando M é dado.

(∗) **Corolário 4.3.** : Se $a, b, \ldots, c$ são inteiros em qualquer quantidade finita, então existe um único inteiro $d \geq 0$ tal que o conjunto de todas as combinações lineares $ax + by + \cdots + cz$ de $a, b, \ldots, c$ com coeficientes inteiros $x, y, \ldots, z$ consiste em todos os múltiplos de d.

$$\{ax + by + \ldots + cz : x, y, \ldots, z \in \mathbb{Z}\} = d\mathbb{Z}$$

Demonstração :

Aplique a Proposição ao conjunto das tais combinações lineares.

(∗) **Corolário 4.4.** : Sob as notações e hipóteses do Corolário 4.3, vale que d é um divisor de cada um dos inteiros $a, b, \ldots, c$ e cada divisor comum desses inteiros é um divisor de d.

Demonstração :

Cada um dos inteiros $a, b, \ldots, c$ pertence ao conjunto das suas combinações lineares; e cada divisor comum de $a, b, \ldots, c$ é um divisor de cada uma das suas combinações lineares, e em particular, de d.

3.2 Máximo Divisor Comum

Definição 4.5 : Máximo Divisor Comum

- O inteiro d definido nos corolários da Proposição é chamado de o **máximo divisor comum** (ou abreviadamente $m.d.c.$) de $a, b, \ldots, c$; ele é denotado por $(a, b, \ldots, c)$.
- Como o $m.d.c.$ $(a, b, \ldots, c)$ pertence ao conjunto das combinações lineares, ele pode ser escrito da forma:

$$(a, b, \ldots, c) = ax_0 + by_0 + \ldots + cz_0,$$

em que $x_0, y_0, \ldots, z_0$ são inteiros.

Exemplo

1. Temos $(6, 10, 15) = 1$, $(6, 10) = 2$, $(6, 15) = 3$, e $(10, 15) = 5$.
2. Para $a \geq 0$, temos $(a, b) = a$ se, e somente se, $a \mid b$.
3. Se $a = qb + c$, então $(a, b) = (b, c)$.

4 Números Primos e Coprimos

4.1 Números Coprimos

Definição 5.1. :

Dizemos que inteiros $a, b, \ldots, c$ são **mutuamente relativamente primos** (ou **coprimos**) se o m.d.c. deles for 1.

- Em outras palavras, eles são **mutuamente relativamente primos** se **não** possuem um divisor comum positivo diferente de 1.
- Se a e b são **mutuamente relativamente primos**, dizemos que a é primo a b e que b é primo a a.
- Quando isso ocorre, observamos que **cada divisor** de a é primo a b, e que **cada divisor** de b é primo a a.

Exemplo

1. Os números $6, 10$ e 15 são mutuamente relativamente primos, pois $(6, 10, 15) = 1$ (o que segue diretamente de $6 + 10 - 15 = 1$).
2. A fração $\dfrac{14n+3}{21n+4}$ é irredutível para cada inteiro $n \geq 0$, pois $(-2)(21n + 4) + (3)(14n + 3) = 1$.
3. Para qualquer m, $(1, m) = 1$; e $(k, m) = 1$ se, e somente se, $(m - k, m) = 1$ (de fato, $kx + my = 1$ equivale a $(m - k)x' + my' = 1$ para $x' = -x$ e $y' = x + y$).

(∗) Proposição 5.2. : Os inteiros $a, b, \ldots, c$ são mutuamente relativamente primos se, e somente se, a equação $ax + by + \cdots + cz = 1$ possui uma solução em inteiros $x, y, \ldots, z$.

Demonstração :

Se a equação possui uma solução, então cada divisor comum $d \geq 0$ de $a, b, \ldots, c$ deve dividir 1, logo, deve ser 1.

Reciprocamente, se $(a, b, \ldots, c) = 1$, então a Proposição 4.2 garante que a equação possui uma solução.

(∗) Corolário 5.3. : Se $d > 0$ é o $m.d.c.$ dos inteiros $a, b, \ldots, c$, então $\frac{a}{d}, \frac{b}{d}, \ldots, \frac{c}{d}$ são mutuamente relativamente primos.

Demonstração :

Isto segue-se de escrever $d = ax_0 + by_0 + \cdots + cz_0$.

(∗) Proposição 5.4. : Se a, b, c são inteiros tais que a é primo a b e a divide bc, então a divide c.

Demonstração :

Escrevemos $1 = ax_0 + by_0$ e obtemos $c = cax_0 + cby_0$. Como a divide ambos os termos do lado direito desta igualdade, a divide c.

(∗) Corolário 5.5. : Se a, b, c são inteiros e a é primo a ambos b e c, então a é primo a bc.

Demonstração :

Se $d \geq 0$ e d divide a e bc, então d é primo a b (pois d é divisor de a), logo, d divide c, pela Proposição 5.4.

Como $(a, c) = 1$, d deve ser 1.

(∗) Corolário 5.6. : Se um inteiro é primo a cada um dos inteiros $a, b, \ldots, c$, então ele é primo ao produto $ab \cdots c$.

Demonstração :

Isto decorre do Corolário 5.5 por indução sobre o número de fatores no produto.

4.2 Números Primos

Definição 5.7. : Números Primos

Dizemos que um inteiro $p > 1$ é primo se ele **não** possui outros divisores positivos além de **si mesmo** e 1; caso contrário, ele é dito composto.

- Em outros termos, ele é **primo** se possui exatamente **dois divisores** positivos.
- Cada inteiro > 1 possui **pelo menos** um divisor **primo**, a saber, seu menor divisor > 1.
- Se a é um inteiro qualquer e p é um primo, então ou $p \mid a$ ou p é primo a a.

Exemplo

1. Os primos ≤ 50 estão circulados na seguinte tabela:

1	②	③	4	⑤	6	⑦	8
⑨	10	⑪	12	⑬	14	15	16
⑰	18	⑲	20	21	22	㉓	24
25	26	㉗	28	㉙	30	㉛	32
33	34	35	36	㉗	38	㉙	40
㊶	42	㊸	44	45	46	㊼	48
49	50						

(Crivo de Eratóstenes – números primos circulados).

2. O maior primo conhecido pode ser visto em `www.mersenne.org` (Great Internet Mersenne Prime Search).
3. Temos $2014 = 2 \cdot 1007 = 2 \cdot 19 \cdot 53$, $1484 = 2 \cdot 742 = 2^2 \cdot 371 = 2^2 \cdot 7 \cdot 53$, e $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59509$.

(∗) Proposição 5.8. : Se um primo divide um produto de certos inteiros, então ele divide pelo menos um dos fatores.

Demonstração :

Isto decorre da Proposição 5.4 por indução sobre o número de fatores no produto.

Teorema 5.9. : Teorema Fundamental da Aritmética

Cada inteiro > 1 pode ser escrito como um produto de primos, e pode ser assim escrito de modo único, exceto pela ordem dos fatores.

Demonstração :

Seja $a > 1$ e seja p um divisor primo de a. Se $a = p$, o teorema vale para a. Senão, $\frac{a}{p}$ é > 1 e $< a$.

Se a primeira afirmação do teorema vale para $\frac{a}{p}$, então ela vale para a. Portanto, a primeira afirmação segue-se por **indução** sobre a.

A segunda afirmação do teorema também pode ser provada por **indução**.

De fato, suponhamos que a seja escrito de duas maneiras como produto de primos:

$$a = pq \cdots r \quad \text{e} \quad a = p'q' \cdots s'.$$

Como p divide a, a Proposição 3.8 garante que p deve dividir um dos primos $p', q', \ldots, s'$, digamos p'. Assim, $p = p'$.

Aplicando a segunda parte do teorema para $\frac{a}{p}$, segue-se que $q' \cdots s'$ deve ser o mesmo que $q \cdot \ldots \cdot r$, a menos da ordem. Por **indução**, a segunda parte está provada.

Demonstração da **Unicidade**:

Escreva a como um produto de primos, $a = pq \cdots r$.

Seja P um primo qualquer, e seja n o número de vezes que P aparece dentre os fatores $p, q, \ldots, r$.

1. Por um lado, a é múltiplo de P^n.
2. Por outro, a **não** é múltiplo de P^{n+1} (pois pela Proposição 3.8, $a \cdot P^{-n}$ **não** é múltiplo de P).

Assim, n é unicamente determinado como o maior inteiro tal que P^n divide a, e podemos escrever $n = v_P(a)$.

Logo, em quaisquer duas maneiras de escrever a como um produto de primos, os mesmos primos devem aparecem, devem ocorrer o mesmo número de vezes me **ambos** os produtos.

Exemplo

A **fatoração única** pode ser usada para determinar o **máximo divisor comum** ($m.d.c.$) de inteiros > 0. De fato, se

$$a = \prod_{p \text{ primo}} p^{v_p(a)} \quad \text{e} \quad b = \prod_{p \text{ primo}} p^{v_p(b)},$$

(em que quase todos os expoentes são $= 0$), então

$$(a, b) = \prod_{p \text{ primo}} p^{\min\{v_p(a), v_p(b)\}}.$$

$(2014, 1484) = 2 \cdot 53 = 106$.

Teorema 5.10. :

Existe uma quantidade infinita de primos.

Demonstração :

(**Argumento de Euclides**). Se $p, q, \ldots, r$ são primos, então cada divisor primo de $p \cdot q \cdots r + 1$ deve ser diferente de $p, q, \ldots, r$.

5 Equações Diofantinas

- Sejam $a, b,$ e $c \in \mathbb{Z}$. A equação : $aX + bY = c$

i. Possui uma solução **inteira** se, e somente se, d divide c, neste caso, temos infinitas tais soluções

ii. Além disso, se $ax_0 + by_0 = c$ com $x_0, y_0 \in \mathbb{Z}$, então todas as soluções são dadas por :

$$x = x_0 + \frac{b}{d} \cdot t, \text{com } t \in \mathbb{Z}$$

$$y = y_0 - \frac{a}{d} \cdot t, \text{com } t \in \mathbb{Z}$$

Demonstração :

Se $ax_0 + by_0 = c$, então $d \mid c$.

Reciprocamente, se $c \mid d$, então $c = d \cdot e$.

Como existem inteiros v e s tais que $av + bs = d$, temos:

$$a \cdot \left(x_0 + \frac{b}{d} \cdot t\right) + b \cdot \left(y_0 - \frac{a}{d} \cdot t\right) = ax_0 + by_0 = c, \quad \forall t \in \mathbb{Z}.$$

Além disso, se $ax + by = c$, então

$$a \cdot \left(x_0 + \tfrac{b}{d} \cdot t\right) = b \cdot \left(y_0 - \tfrac{a}{d} \cdot t\right) \tag{1}$$

Daí,

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0).$$

Como $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, existe $t \in \mathbb{Z}$ tal que

$$\boxed{x = x_0 + \tfrac{b}{d}t} \tag{2}$$

Substituindo (2) em (1), obtemos:

$$\boxed{y = y_0 - \frac{a}{d}t}.$$

5.1 Exemplos

1. 9X + 12Y = 1
   Nota-se que $(9, 12) = 3$ que **não** divide 1, logo a equação não possui solução em $\mathbb{Z}$.
2. 28X + 90Y = 22
   Note que,

$$\begin{aligned} 90 &= (3)\cdot 28 + 6 & \qquad 2 &= 6 + (-1)\cdot 4 \\ 28 &= (4)\cdot 6 + 4 & \qquad 2 &= (-1)\cdot 28 + (5)\cdot 6 \\ 6 &= (1)\cdot 4 + 2 & \qquad 2 &= (-16)\cdot 28 + (5)\cdot 90 \\ 4 &= (2)\cdot 2 + 0 \end{aligned}$$

   Dando

$$(28, 90) = 2 = (-16)\cdot 28 + (5)\cdot 90$$

   Assim,

$$(-16\cdot 11)\cdot 28 + (5\cdot 11)\cdot 90 = 22$$

   Portanto, todas as soluções da equação são:

$$x = -176 + 45t, \quad y = 55 - 14t, \quad t \in \mathbb{Z}.$$

3. 12X + 25Y = 1
   Pela divisão euclidiana temos :
   $25 = (2)12 + +1$,Ou Seja
   $1 = 25(1) + (-2)12$
   Assim, as soluções da equação são :

$$x = -2 + 25t, \quad y = 1 - 12t, \quad t \in \mathbb{Z}.$$

Polinômios

- Recordemos agora algumas propriedades elementares de **polinômios** sobre um corpo arbitrário.
- Estas são independentes da natureza do corpo, e análogas às propriedades dos inteiros descritas anteriormente.
- Seja K um corpo qualquer. Um polinômio P sobre K (isto é, com **coeficientes** em K), em uma indeterminada X, é dado por uma expressão :

$$P = a_0 + a_1X + \cdots + a_nX^n, \text{ com } a_0, a_1, \ldots, a_n \in K.$$

- Se $a_n \neq 0$, dizemos que P possui **grau** n e escrevemos $grau(P) = n$.
- Cada polinômio exceto 0 (o polinômio com todos os **coeficientes nulos**) possui um grau.
- A adição e a multiplicação, definidas de maneira usual, fazem com que os polinômios sobre K formem um **anel**, usualmente denotado por $K[X]$.
- Se P e Q são polinômios não nulos, então

$$\boxed{grau(PQ) = grau(P) + grau(Q)}.$$

(∗) Lema 6.1. : **Divisão Euclidiana**

Se A e B são polinômios sobre um corpo K com $B \neq 0$, então existe um único polinômio Q tal que

$$\boxed{A - BQ = 0} \quad \text{ou} \quad \boxed{grau(A - BQ) < grau(B)}.$$

Demonstração :

Se $A = 0$ ou grau$(A) <$ grau(B), tomamos $Q = 0$. Caso contrário, procedemos por **indução** sobre $n = grau(A)$.

Sejam bX^m o termo de *grau* m em B e aX^n o termo de *grau* n em A.

Definimos,

$$A' = A - B \cdot \frac{a}{b} X^{n-m},$$

que é de $grau < n$.

Pela **hipótese de indução**, podemos escrever

$$A' = BQ' + R, \text{ com } R = 0 \text{ ou } grau(R) < m.$$

Então,

$$A = BQ + R, \quad \text{com } Q = Q' + \frac{a}{b} X^{n-m}.$$

Quanto à Unicidade de Q :

Se $A - BQ$ e $A - BQ_1$ são **nulos** ou de $grau < m$, então o mesmo vale para $B(Q - Q_1)$. Como este possui $grau\ m + grau(Q - Q_1)$, a menos que $Q - Q_1 = 0$, chegamos a uma **contradição**. Portanto, $Q = Q_1$.

- Se $R = A - BQ = 0$, então $A = BQ$, neste caso :
  $\hookrightarrow$ A é um **múltiplo** de B
  $\hookrightarrow$ B é um **divisor** de A.
- Em particular, se $B = X - a$, então R deve ser 0 ou de $grau$ 0, isto é, uma constante $r \in K$, de modo que podemos escrever:

$$A = (X - a)Q + r, \text{ com } r \in K.$$

Substituindo $X = a$, obtemos $\boxed{A(a) = r}$.

- Se $r = 0$, dizemos que a é uma **raiz** de A.
- Assim, A é um **múltiplo** de $X - a$ se, e somente se, a é uma **raiz** de A.

Assim como a Proposição 5.2 foi derivada do Lema 4.1, teremos um análogo para polinômios.

$(*)$ Proposição 6.2. : Seja M um conjunto não-vazio de polinômios sobre um corpo. Se M é fechado com respeito à **subtração** e satisfaz a condição "se $A \in M$, então todos os **múltiplos** de A pertencem a M", então M consiste em todos os **múltiplos** de algum **polinômio** D, unicamente determinado a menos de multiplicação por uma constante não-nula.

Demonstração :

Se $M = \{0\}$, tomamos $D = 0$. Caso contrário, tomamos um polinômio D de menor grau d em M. Se $A \in M$, aplicamos o Lema 4.1 para A e D e escrevemos :

$$A = DQ + R, \text{ onde } R \text{ é } 0 \text{ ou possui } grau < d.$$

Então $A + D(-Q) \in M$, donde é 0 pela definição de D, e $A = DQ$.

- Se D_1 possui a mesma propriedade de D, então ele é um **múltiplo** de D e D é um **múltiplo** de D_1, de modo que ambos possuem o mesmo grau; escrevendo $D_1 = DE$, vemos que E possui $grau$ 0, e ele é uma constante não nula.
- Se aX^d é o termo de $grau$ d em D, dentre os polinômios diferindo de D por um fator constante não-nulo, existe um e exatamente um com **coeficiente** de mais alto $grau$ igual a 1, a saber $a^{-1}D$. Chamamos tal polinômio de **normalizado**.
- Podemos aplicar a **Proposição 6.2** ao conjunto M de todas as **combinações lineares** $AP + BQ + \ldots + CR$ de qualquer número de dados polinômios $A, B, \ldots, C$, aqui $P, Q, \ldots, R$ denotam **polinômios arbitrários**.

Daí, se M consiste nos **múltiplos** de D, onde D é 0 ou um **polinômio normalizado**, dizemos que D é o **máximo divisor comum** de $A, B, \ldots, C$ e o denotamos por :

$$(A, B, \ldots, C).$$

D : **Divisor** de A

$B, \ldots, C$ e cada divisor comum de $A, B, \ldots, C$ **divide** D.

- Se $D = 1$, então $A, B, \ldots, C$ são ditos **mutuamente relativamente primos**. Isto ocorre se, e somente se, existem polinômios $P, Q, \ldots, R$ tais que :

$$\boxed{AP + BQ + \cdots + CR = 1}.$$

- Se $(A, B) = 1$, dizemos que A é primo a B, e que B é primo a A.
- Um polinômio de grau $n > 0$ é **irredutível** se ele **não** possui divisor de $grau > 0$ e $< n$.

- Cada polinômio de *grau* 1 é irredutível.

Exemplo : Polinômios Redutiveis

Notemos que a propriedade de um polinômio ser irredutível não precisa ser **preservada** quando mudamos o corpo dos coeficientes :
↪ $X^2 + 1$ é **irredutível** sobre $\mathbb{Q}$, e também sobre $\mathbb{R}$
↪ Mas **não** sobre $\mathbb{C}$ pois $X^2 + 1 = (X + i)(X - i)$.

Poderíamos mostrar que cada polinômio de $grau > 0$ pode ser escrito de modo essencialmente **único** como um produto de **polinômios irredutíveis**. Contudo, apenas faremos uso do seguinte resultado mais fraco:

(∗) Proposição 6.3. : Se A é um polinômio de grau $n > 0$ sobre um corpo K, então ele pode ser escrito, unicamente a menos da ordem dos fatores, na forma :

$$A = (X - a_1)(X - a_2) \cdots (X - a_m)Q,$$

em que $0 \leq m \leq n$, $a_1, a_2, \ldots, a_m \in K$, e Q não possui raiz alguma em K.

Demonstração:

Se A **não** possui raiz, isto é claro; caso contrário, procedemos por **indução** sobre n. Se A possui uma raiz a, escrevemos : $A = (X - a)A'$.

Como A' possui $grau\ n - 1$, podemos aplicar o teorema a ele. Escrevendo A' na forma prescrita, obtemos um produto similar para A.

Se A pode ser escrito como acima e também como

$$A = (X - b_1)(X - b_2) \cdots (X - b_r)R,$$

em que R **não** possui raiz em K, então a **raiz** a de A deve ocorrer dentre os a_i e também dentre os b_j. Dividindo por $(X - a)$, obtemos para A' dois produtos os quais, por **indução**, devem coincidir.

(∗) Corolário 4.4. : Um polinômio de grau $n > 0$ sobre um corpo possui no máximo n raízes distintas.

6 Inteiros Gaussianos

- Recordemos o conceito de um **número complexo** : ↪ $a = x + iy$, onde x e y são números reais ↪ i satisfaz $i^2 = -1$.
- As regras para a adição e a multiplicação são as usuais:

$$(x + iy) + (x' + iy') = (x + x') + i(y + y'),$$

$$(x+iy)(x'+iy') = (xx'-yy') + i(yx'+xy').$$

- Provido de tais operações, o conjunto $\mathbb{C}$ dos **números complexos** torna-se um **anel** associativo, comutativo e unitário, com $1 = 1 + i \cdot 0$.
- Se $a = x + iy$, escrevemos $\boxed{\overline{a} = x - iy}$ e chamamos $\overline{a}$ de **conjugado complexo** de a; o conjugado de $\overline{a}$ é a.
- A aplicação $a \mapsto \overline{a}$ é uma bijeção de $\mathbb{C}$ sobre **si mesma** que preserva as operações de adição e multiplicação; logo, ela é um *automorfismo* de $\mathbb{C}$, isto é, um *isomorfismo* de $\mathbb{C}$ em $\mathbb{C}$.

Escrevemos $N(a) = a \cdot \overline{a}$ e chamamos $N(a)$ de *norma* de a. Pela regra da multiplicação, se $a = x + iy$ então :

$$N(a) = x^2 + y^2,$$

e, pela **comutatividade** da multiplicação, temos

$$N(ab) = N(a)N(b).$$

A norma de a é 0 se, e somente se, $a = 0$; caso contrário, ela é um número real > 0. Consequentemente, para cada $a = x + iy \neq 0$, consideramos

$$a' = N(a)^{-1}\,\overline{a} = \frac{x}{N(a)} - i\frac{y}{N(a)}.$$

- Então $aa' = 1$, e, para cada $b \in \mathbb{C}$, vale $a(a'b) = b$. Reciprocamente, se $az = b$, então $a'(az) = a'b$, donde, pela associatividade, obtemos $z = a'b$. Isso mostra que $\mathbb{C}$ é um **corpo**.

De maneira usual, fazemos corresponder o número complexo $a = x + iy$ ao ponto (x, y) no plano euclidiano; sua distância da origem 0 é

$$|a| = \sqrt{x^2 + y^2} = \sqrt{N(a)}.$$

- Esse valor é também chamado de *valor absoluto* de a.

Para nossos propósitos, vamos considerar, em vez de $\mathbb{C}$, o subconjunto

$$\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$$

consistindo nos números complexos cujas partes real e imaginária são inteiras.

Pode ser imediatamente verificado que $\mathbb{Z}[i]$ é um **anel** associativo, comutativo e unitário, com $1 = 1 + i \cdot 0$. Ele é chamado **anel Gaussiano**, e seus elementos são chamados **inteiros Gaussianos**.

A bijeção $a \mapsto \overline{a}$ preserva as operações desse anel. Se a é um inteiro Gaussiano qualquer, então :

$$N(a) = a \cdot \overline{a}$$

é um inteiro ≥ 0.

- Ocasionalmente também consideramos os números $x + iy$ com $x, y \in \mathbb{Q}$; como anteriormente, eles formam um **corpo** (o **corpo Gaussiano**).

6.1 Divisibilidade e Associados

- Se $a, b, c \in \mathbb{Z}[i]$ e $b = ac$, então :
  $\hookrightarrow$ b é um múltiplo de a,
  $\hookrightarrow$ a divide b (ou que a é um divisor de b).
- Quando isso ocorre, $N(a)$ divide $N(b)$.
- Cada inteiro Gaussiano divide a sua **norma**.
  - Um divisor de 1 é chamado **invertível**.
  - Se $a = x + iy$ é **invertível**, então $N(a) = 1$. Como $x, y \in \mathbb{Z}$, isso implica que $a \in \{\pm 1, \pm i\}$.
  - Dois inteiros Gaussianos não nulos a e b dividem um ao outro se, e somente se, diferem por um fator invertível, isto é, $a = ub$ com $u \in \{\pm 1, \pm i\}$. Nesse caso, chamamos a e b de **associados**.

Dentre os **quatro associados** de um dado inteiro Gaussiano b, existe um único, digamos $a = x + iy$, satisfazendo $x > 0$ e $y \geq 0$. Este será chamado de **normalizado**.

Exemplo

Dentre os associados $\pm 1 \pm i$ de $1 + i$, apenas $\boxed{1 + i}$ é normalizado.

- Geometricamente, os pontos no plano correspondentes aos associados de b são obtidos a partir de b por uma rotação em torno de 0 por um ângulo $n\pi/2$, com $n = 0, 1, 2, 3$.
- O normalizado é aquele no **primeiro quadrante** (ou sobre o semieixo real positivo).

6.2 Primos Gaussianos

- Um inteiro Gaussiano de norma > 1 é chamado **primo Gaussiano** se seus divisores são exatamente os seus associados e os invertíveis.
- Isso equivale a dizer que q é um primo Gaussiano se :
  $\hookrightarrow$ $q \neq 0$;
  $\hookrightarrow$ q **não** é invertível;
  $\hookrightarrow$ q q **não possui divisor** com norma > 1 e $< N(q)$.
- **Inteiros Ordinários** : São primos no sentido usual serão chamados primos racionais.
  $\hookrightarrow$ Se $q \in \mathbb{Z}[i]$ e $N(q)$ é um primo racional, então q é um primo Gaussiano.

↪ A recíproca, porém, não é verdadeira. Exemplo, $N(3) = 9$, e 3 é primo Gaussiano.
↪ Os **associados** de um primo Gaussiano também são primos Gaussianos, e existe apenas um normalizado.
↪ Se q é um primo Gaussiano, então $\overline{q}$ também o é.

- Se $a \in \mathbb{Z}[i]$, $a \neq 0$ e não invertível, então todo divisor de a com norma mínima > 1 deve ser um **primo Gaussiano**.

(∗) Lema 7.1. : **Divisão Euclidiana**

Se $a, b \in \mathbb{Z}[i]$ com $b \neq 0$, então existe $q \in \mathbb{Z}[i]$ tal que

$$N(a - bq) \leq \tfrac{1}{2}N(b).$$

Demonstração :

Para cada número real t, existe um maior inteiro $m \leq t$ tal que $m \leq t < m+1$. Chamamos m' de inteiro mais próximo de t, isto é, m ou $m+1$, de acordo com se $t - m \leq m + 1 - t$ ou não. Assim, $|t - m'| \leq \frac{1}{2}$.

Seja $z = x + iy \in \mathbb{C}$. Tomando m e n inteiros mais próximos de x e y, respectivamente, e definindo $q = m + in$, obtemos

$$N(z - q) = (x - m)^2 + (y - n)^2 \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}.$$

Aplicando isso para $z = \frac{a}{b}$, com $a, b \in \mathbb{Z}[i]$, segue que q satisfaz a propriedade desejada.

Exemplo

1. Para $a = 11 + 10i$ e $b = 4 + i$:

$$\frac{a}{b} = \frac{(11 + 10i)(4 - i)}{N(4 + i)} = \frac{54 + 29i}{17} \approx 3{,}17 + 1{,}71i.$$

   Tomando $q = 3 + 2i$, obtemos $a - bq = 1 - i$, e

$$N(a - bq) \leq \tfrac{1}{2}N(b).$$

2. Para $a = 3i$ e $b = 1 + i$, no lema, há 4 possíveis escolhas de q, e verifica-se que a desigualdade não pode ser melhorada em geral.

Questão (Fossas Gaussianas).

Existe uma sequência infinita de primos Gaussianos distintos tal que haja uma limitação para as diferenças entre os números consecutivos da sequência?

6.3 $x^2 + y^2 = p$

(∗) Proposição 8.1. : Seja M um conjunto não-vazio de inteiros Gaussianos. Se M é fechado com respeito à subtração e satisfaz a condição :

- "Se $a \in M$, então todos os seus **múltiplos** pertencem a M", então M consiste em todos os **múltiplos** de algum **inteiro Gaussiano** d, unicamente determinado a menos de um fator invertível.

Demonstração :

Se $M = \{0\}$, a proposição é verdadeira com $d = 0$. Senão, tomemos em M um elemento d de menor norma > 0. Se $a \in M$, pela divisão euclidiana em $\mathbb{Z}[i]$ (Lema 5.1), escrevemos $a = dq + r$ com $N(r) \leq \frac{1}{2}N(d)$.

Como $r = a - dq \in M$, temos $r = 0$, logo a é múltiplo de d.

Para a unicidade: se d' possui a mesma propriedade, então d e d' dividem um ao outro, portanto são associados.

- Podemos aplicar a **Proposição 8.1** anterior ao conjunto de todas as **combinações lineares** $ax + by + \ldots + cz$ com $a, b, \ldots, c \in \mathbb{Z}[i]$.

$$ax + by + \ldots + cz : a, b, \ldots, z \in \mathbb{Z}[i] = d\mathbb{Z}[i]$$

- Isso nos permite definir o $m.d.c.$ $(a, b, \ldots, c)$ em $\mathbb{Z}[i]$. Ele será unicamente determinado se prescrevermos que ele seja **normalizado**.
- Se $m.d.c.(a, b, \ldots, c) = 1$, então $a, b, \ldots, c$ são **mutuamente relativamente primos**.

(∗) Proposição 8.2. : Todo inteiro Gaussiano não-nulo pode ser escrito de modo *essencialmente único* como produto de um **invertível** e de **primos Gaussianos**.

- Aqui, as palavras *"essencialmente único"* têm o seguinte sentido. Sejam :

$$a = uq_1 \ldots q_r = u'q'_1 \ldots q'_s$$

  dois produtos do tipo desejado para algum $a \neq 0$, em que u e u' são **invertíveis** e q_j e q'_k são **primos Gaussianos**.
- Então, o teorema deve ser entendido por dizer que $r = s$ e que os q'_k podem ser ordenados de modo que q'_j seja um associado de q_j para $1 \leq j \leq r$; se a for **invertível**, então $r = 0$. Se prescrevermos que os fatores primos de a sejam "normalizados", então o produto é unicamente determinado a menos da ordem dos fatores.
- **Inteiros ordinários** também são **inteiros Gaussianos**; para obtermos a decomposição deles em **primos Gaussianos**, basta fazermos isso para os **primos "ordinários"**.

(∗) Proposição 8.3. : Se p é um primo racional ímpar, então ele é um **primo Gaussiano** ou é a norma de um primo Gaussiano q.

Neste último caso, $p = q\bar{\cdot}q$, q e $\bar{q}$ **não** são associados, e os únicos divisores de p são $q, \bar{q}$ e seus associados.

Demonstração :

Escrevamos $p = uq_1 \cdots q_r$ como na Proposição anterior. Tomando a norma:

$$p^2 = N(q_1)\, N(q_2) \cdots N(q_r).$$

Se algum $N(q_j) = p^2$, então $r = 1$, $p = uq_j$ e p seria um primo Gaussiano. Caso contrário, cada $N(q_j) = p$, e podemos escrever $p = q\bar{q}$ com q primo Gaussiano.

Escreva $q = x + iy$. Se $\bar{q}$ fosse associado a q, teríamos $\bar{q} = \pm q$ ou $\pm iq$. Isso implicaria $y = 0$ ($p = x^2$), ou $x = 0$ ($p = y^2$), ou $y = \pm x$ ($p = 2x^2$). Nenhum desses casos é possível, pois p é primo ímpar.

- Para $p = 2$, temos a decomposição:

$$2 = N(1 + i) = (1 + i)(1 - i) = i^3(1 + i)^2,$$

  ou seja, 2 possui um único fator primo normalizado $1 + i$.

(∗) Proposição 8.4. : Se p é um primo racional ímpar, então p é um primo Gaussiano ou a **norma** de um primo Gaussiano quando ele deixa resto 3 ou 1 na divisão por 4.

Demonstração :

Se $p = x^2 + y^2$, então um de x, y é par e o outro ímpar. Logo, um dos quadrados deixa resto 1 e o outro resto 0 módulo 4, logo $p \equiv 1 \pmod 4$.

Reciprocamente, se $p \equiv 1 \pmod 4$, então existe x tal que $x^2 \equiv -1 \pmod p$. Assim $p \mid (x + i)(x - i)$ em $\mathbb{Z}[i]$, logo p não pode ser primo Gaussiano, mas sim $p = (x + i)(x - i)$.

(∗) Corolário 8.5. : Cada primo Gaussiano $\pm 1 \pm i$, ou um associado de um primo racional que deixa **resto** 3 na divisão por 4 ou ainda sua norma é um primo racional que deixa **resto** 1 na divisão por 4.

Demonstração :

Cada primo Gaussiano q deve dividir algum **fator primo racional** p de sua norma $q\bar{q}$; aplicando a **Proposição 8.4** se p for ímpar, e as observações anteriores se $p = 2$, obtemos o desejado.

(∗) Corolário 8.6. : Um primo racional p pode ser escrito como soma de dois quadrados se, e somente se ele é igual à 2 ou deixa resto 1 na divisão por 4.

Demonstração :

Se $p = x^2 + y^2$, então p não é primo Gaussiano, pois divide $(x + iy)(x - iy)$. A recíproca vem da proposição anterior.

7 Provas

7.1 Prova 1

7.2 Prova 2

Questão 1

Sejam G e G' grupos e seja $f : G \to G'$ uma função bijetiva tal que $f(xy) = f(x)f(y)$ para todos $x, y \in G$.

a) Considere o conjunto $S = \{x \in G \mid f(x) = e'\}$, onde e' é a identidade de G'. Verifique se S é um subgrupo de G.

b) Seja H um subconjunto de G definido por alguma propriedade envolvendo multiplicação. Analise as condições para que H seja um subgrupo de G.

Questão 2

Seja G um grupo comutativo (abeliano). Verifique que:

(i) Se n é um inteiro qualquer, então $H = \{x^n \mid x \in G\}$ é um subgrupo de G.

(ii) Se H e K são subgrupos de G, então $S = \{hk \mid h \in H,\, k \in K\}$ é um subgrupo de G.

Questão 3

Considere os conjuntos $(\mathbb{Z}/32\mathbb{Z})^\times$ e $(\mathbb{Z}/34\mathbb{Z})^\times$, isto é, os grupos multiplicativos dos elementos invertíveis em $\mathbb{Z}/32\mathbb{Z}$ e $\mathbb{Z}/34\mathbb{Z}$, respectivamente.

a) Existe um isomorfismo de grupos entre $(\mathbb{Z}/32\mathbb{Z})^\times$ e $(\mathbb{Z}/34\mathbb{Z})^\times$? Justifique sua resposta.

b) Os anéis $\mathbb{Z}/32\mathbb{Z}$ e $\mathbb{Z}/34\mathbb{Z}$ são isomorfos? Existe um isomorfismo entre eles? Justifique sua resposta.

Questão 4

a) Para um inteiro $m > 1$, determine se $\mathbb{Z}/m\mathbb{Z}$ é um corpo. E determine se o grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^\times$ é um grupo cíclico.

b) Para p primo, determine se $\mathbb{Z}/p\mathbb{Z}$ é um corpo. E determine se o grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^\times$ é cíclico.

Questão 5

a) Seja $A = \{\, x + y\sqrt{2} \mid x, y \in \mathbb{Z} \,\}$. Prove que A é um anel, com as operações usuais.

b) Seja $K = \{\, x + y\sqrt{2} \mid x, y \in \mathbb{Q} \,\}$. Prove que K é um corpo, com as operações usuais.

Questão 6

Considere o conjunto $X = \{1, 2, 3, 4, 5\}$ e as funções (permutações) σ e τ dadas por:

$$\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 4,\ \sigma(4) = 5,\ \sigma(5) = 1$$

$$\tau(1) = 1,\ \tau(2) = 5,\ \tau(3) = 4,\ \tau(4) = 3,\ \tau(5) = 2$$

a) Analise a bijetividade das funções σ e τ e, se possível, descreva a ordem de σ por composições sucessivas (σ^k).

b) Verifique se $\sigma^4 \circ \tau = \sigma \circ \tau$. Justifique detalhadamente.

Além dos itens já listados, as perguntas sobre permutações podem incluir as seguintes hipóteses frequentes:

- Determinar explicitamente o mapeamento composto: calcular e escrever $\sigma \circ \tau(x)$ para cada $x \in X$.
- Reescrever $\sigma \circ \tau$ em notação de ciclo ou como produto de ciclos.
- Identificar a ordem da permutação $\sigma \circ \tau$, isto é, o menor n tal que $(\sigma \circ \tau)^n$ seja a identidade.
- Verificar se $\sigma \circ \tau$ é igual a $\tau \circ \sigma$ (comutatividade da composição).
- Encontrar a inversa explícita de $\sigma \circ \tau$ (se solicitado).

7.3 Prova 3