

Fundamentos Matemáticos

Julio López

Instituto de Computação - UNICAMP

Abril, 2010

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Fundamentos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Fundamentos

Números inteiros

Aritmética modular

Grupos

Corpos finitos

Problema do logaritmo discreto

Exercícios:

Números inteiros

Fundamentos

- **Números inteiros**
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- \mathbb{Z} é o conjunto dos números inteiros.

Números inteiros

Fundamentos

- **Números inteiros**
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- \mathbb{Z} é o conjunto dos números inteiros.
- Sejam a e b números inteiros. Dizemos que a é *divisível por b* se existe inteiro q tal que $a = qb$. Nesse caso, b é divisor de a

$3|21$, mas $4 \nmid 15$.

Números inteiros

Fundamentos

- **Números inteiros**
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- \mathbb{Z} é o conjunto dos números inteiros.
- Sejam a e b números inteiros. Dizemos que a é *divisível por b* se existe inteiro q tal que $a = qb$. Nesse caso, b é divisor de a

$3|21$, mas $4 \nmid 15$.

- Um número inteiro $p \geq 2$ é *primo* se é divisível somente por 1 e por ele mesmo.

Números inteiros

Fundamentos

- **Números inteiros**
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- \mathbb{Z} é o conjunto dos números inteiros.
- Sejam a e b números inteiros. Dizemos que a é *divisível por b* se existe inteiro q tal que $a = qb$. Nesse caso, b é divisor de a

$$3|21, \text{ mas } 4 \nmid 15.$$

- Um número inteiro $p \geq 2$ é *primo* se é divisível somente por 1 e por ele mesmo.
- Todo inteiro $n \geq 2$ pode ser escrito como um produto de potências de números primos; a *fatoração* de n .

Números inteiros

Fundamentos

- **Números inteiros**
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- \mathbb{Z} é o conjunto dos números inteiros.
- Sejam a e b números inteiros. Dizemos que a é *divisível por b* se existe inteiro q tal que $a = qb$. Nesse caso, b é divisor de a

$$3|21, \text{ mas } 4 \nmid 15.$$

- Um número inteiro $p \geq 2$ é *primo* se é divisível somente por 1 e por ele mesmo.
- Todo inteiro $n \geq 2$ pode ser escrito como um produto de potências de números primos; a *fatoração* de n .

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Aritmética modular

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 1 *Sejam a, n números inteiros com $n > 0$. O resto ou resíduo da divisão de a por n é o único inteiro r , com $0 \leq r \leq n - 1$, tal que $a = qn + r$ para algum inteiro q , o quociente da divisão.*

Por essa definição o resto da divisão de 7 por 3 é 1 (com quociente 2), e o resto da divisão de -7 por 3 é 2 (com quociente -3).

Aritmética modular

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 3 *Sejam a, n números inteiros com $n > 0$. O resto ou resíduo da divisão de a por n é o único inteiro r , com $0 \leq r \leq n - 1$, tal que $a = qn + r$ para algum inteiro q , o quociente da divisão.*

Por essa definição o resto da divisão de 7 por 3 é 1 (com quociente 2), e o resto da divisão de -7 por 3 é 2 (com quociente -3).

Definição 4 *Para a, n números inteiros com $n > 0$, a expressão $a \bmod n$ é a redução de a módulo n , definida como o resto da divisão de a por n .*

Aritmética modular

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 5 *Sejam a, n números inteiros com $n > 0$. O resto ou resíduo da divisão de a por n é o único inteiro r , com $0 \leq r \leq n - 1$, tal que $a = qn + r$ para algum inteiro q , o quociente da divisão.*

Por essa definição o resto da divisão de 7 por 3 é 1 (com quociente 2), e o resto da divisão de -7 por 3 é 2 (com quociente -3).

Definição 6 *Para a, n números inteiros com $n > 0$, a expressão $a \bmod n$ é a redução de a módulo n , definida como o resto da divisão de a por n .*

Portanto, $0 \bmod 5 = 0$ e $(3 - 8) \bmod 4 = -1 \bmod 4 = 3$.

Aritmética modular

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 7 *Dado um inteiro $n \geq 1$, denotamos por \mathbb{Z}_n ao conjunto $\{0, 1, \dots, n - 1\}$ de resíduos módulo n , isto é dos restos possíveis de divisões de números inteiros por n .*

Como todo número inteiro produz um resto ao ser dividido por n , \mathbb{Z}_n tem em si um representante para cada número inteiro. A próxima definição captura essa idéia.

Aritmética modular

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 9 *Dado um inteiro $n \geq 1$, denotamos por \mathbb{Z}_n ao conjunto $\{0, 1, \dots, n - 1\}$ de resíduos módulo n , isto é dos restos possíveis de divisões de números inteiros por n .*

Como todo número inteiro produz um resto ao ser dividido por n , \mathbb{Z}_n tem em si um representante para cada número inteiro. A próxima definição captura essa idéia.

Definição 10 *Para a, b, n números inteiros com $n > 0$, escrevemos $a \equiv b \pmod{n}$, quando $a \bmod n = b \bmod n$. Dizemos que a e b são congruentes módulo n .*

Assim, $0 \equiv 3 \pmod{3}$ e $43 \equiv 1 \pmod{2}$.

O máximo divisor comum (m.d.c)

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Considere a, b dois números inteiros, não ambos nulos.

O máximo divisor comum (m.d.c)

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Considere a, b dois números inteiros, não ambos nulos.
- O *máximo divisor comum* de a e b , $\text{mdc}(a, b)$, é o maior inteiro d que divide ambos a e b .

O máximo divisor comum (m.d.c)

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Considere a, b dois números inteiros, não ambos nulos.
- O *máximo divisor comum* de a e b , $\text{mdc}(a, b)$, é o maior inteiro d que divide ambos a e b .

$$\text{mdc}(20, 8) = 4$$

O máximo divisor comum (m.d.c)

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Considere a, b dois números inteiros, não ambos nulos.
- O *máximo divisor comum* de a e b , $\text{mdc}(a, b)$, é o maior inteiro d que divide ambos a e b .

$$\text{mdc}(20, 8) = 4$$

$$\text{mdc}(20, 0) = 20$$

O máximo divisor comum (m.d.c)

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Considere a, b dois números inteiros, não ambos nulos.
- O *máximo divisor comum* de a e b , $\text{mdc}(a, b)$, é o maior inteiro d que divide ambos a e b .

$$\text{mdc}(20, 8) = 4$$

$$\text{mdc}(20, 0) = 20$$

$$\text{mdc}(20, 7) = 1$$

O máximo divisor comum (m.d.c)

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Considere a, b dois números inteiros, não ambos nulos.
- O *máximo divisor comum* de a e b , $\text{mdc}(a, b)$, é o maior inteiro d que divide ambos a e b .

$$\text{mdc}(20, 8) = 4$$

$$\text{mdc}(20, 0) = 20$$

$$\text{mdc}(20, 7) = 1$$

- Quando $\text{mdc}(a, b) = 1$, dizemos que a e b são *primos entre si* ou *coprimos*.

O Algoritmo de Euclides, é o método mais popular para o cálculo do mdc.

O Algoritmo de Euclides

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Entrada: inteiros a, b , com $a > 0, b \geq 0$.

Saída: inteiro d , onde $d = \text{mdc}(a, b)$.

$$\text{mdc}(a, b) = \text{mdc}(b, a \bmod b);$$

$$\text{mdc}(a, 0) = a.$$

$$\begin{aligned} \text{mdc}(18, 4) &= \text{mdc}(4, 18 \bmod 4) \\ &= \text{mdc}(4, 2) \\ &= \text{mdc}(2, 4 \bmod 2) \\ &= \text{mdc}(2, 0) \\ &= 2. \end{aligned}$$

O Algoritmo de Euclides

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Entrada: inteiros a, b , com $a > 0, b \geq 0$.

Saída: inteiro d , onde $d = \text{mdc}(a, b)$.

1. **se** $b = 0$ **então** retorne (a) ;
2. **enquanto** $b > 0$ **faça**
 - 2.1 $q \leftarrow a \text{ div } b; r \leftarrow a - q * b;$
 - 2.2 $a \leftarrow b; b \leftarrow r;$
3. $d \leftarrow a;$
4. retorne (d) ;

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 11 *Para a, n números inteiros com $n > 0$, o inverso aditivo de a módulo n é o inteiro $b = -a \pmod{n}$; ou seja $a + b \equiv 0 \pmod{n}$.*

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 12 Para a, n números inteiros com $n > 0$, o inverso aditivo de a módulo n é o inteiro $b = -a \pmod{n}$; ou seja $a + b \equiv 0 \pmod{n}$.

O inverso multiplicativo de a módulo n , se existir, é o único inteiro b , $1 \leq b \leq n - 1$, tal que $ab \equiv 1 \pmod{n}$.

Denotamos o inverso multiplicativo de a módulo n por $a^{-1} \pmod{n}$.

- O inverso aditivo de 4 módulo 7 é 3.

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 13 Para a, n números inteiros com $n > 0$, o inverso aditivo de a módulo n é o inteiro $b = -a \pmod{n}$; ou seja $a + b \equiv 0 \pmod{n}$.

O inverso multiplicativo de a módulo n , se existir, é o único inteiro b , $1 \leq b \leq n - 1$, tal que $ab \equiv 1 \pmod{n}$.

Denotamos o inverso multiplicativo de a módulo n por $a^{-1} \pmod{n}$.

- O inverso aditivo de 4 módulo 7 é 3.
- O inverso multiplicativo de 2 módulo 5 é 3.

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 14 Para a, n números inteiros com $n > 0$, o inverso aditivo de a módulo n é o inteiro $b = -a \pmod{n}$; ou seja $a + b \equiv 0 \pmod{n}$.

O inverso multiplicativo de a módulo n , se existir, é o único inteiro b , $1 \leq b \leq n - 1$, tal que $ab \equiv 1 \pmod{n}$.

Denotamos o inverso multiplicativo de a módulo n por $a^{-1} \pmod{n}$.

- O inverso aditivo de 4 módulo 7 é 3.
- O inverso multiplicativo de 2 módulo 5 é 3.
- O inverso multiplicativo de 2 módulo 6 não existe.

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 15 Para a, n números inteiros com $n > 0$, o inverso aditivo de a módulo n é o inteiro $b = -a \pmod{n}$; ou seja $a + b \equiv 0 \pmod{n}$.

O inverso multiplicativo de a módulo n , se existir, é o único inteiro b , $1 \leq b \leq n - 1$, tal que $ab \equiv 1 \pmod{n}$.

Denotamos o inverso multiplicativo de a módulo n por $a^{-1} \pmod{n}$.

- O inverso aditivo de 4 módulo 7 é 3.
- O inverso multiplicativo de 2 módulo 5 é 3.
- O inverso multiplicativo de 2 módulo 6 não existe.

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Teorema 1 *Para a, n números inteiros com $n > 0$, o inverso multiplicativo de a módulo n existe se e somente se $\text{mdc}(a, n) = 1$.*

Se $\text{mdc}(a, n) = 1$, como calcular $a^{-1} \pmod n$?

Inversos

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Teorema 2 *Para a, n números inteiros com $n > 0$, o inverso multiplicativo de a módulo n existe se e somente se $\text{mdc}(a, n) = 1$.*

Se $\text{mdc}(a, n) = 1$, como calcular $a^{-1} \pmod n$?

Extensão do Algoritmo de Euclides:

$$1 = \text{mdc}(a, n) = sa + nt$$

$$1 = sa \pmod n$$

$$a^{-1} = s \pmod n.$$

Extensão do Algoritmo de Euclides

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Dados a, n , a extensão do Algoritmo de Euclides, retorna inteiros (d, s, t) onde $d = \text{mdc}(a, n)$ e $d = sa + tn$. Isto é, $sa \equiv d \pmod{n}$. Assim, quando $\text{mdc}(a, n) = 1$, o inteiro s é $a^{-1} \pmod{n}$.

Entrada: inteiros a, b .

Saída: inteiros d, s, t , onde $d = \text{mdc}(a, b) = sa + tb$.

1. **se** $b = 0$ **então** retorne $(a, 1, 0)$;
2. $x_2 \leftarrow 1$; $x_1 \leftarrow 0$; $y_2 \leftarrow 0$; $y_1 \leftarrow 1$;
3. **enquanto** $b > 0$ **faça**
 - 3.1 $q \leftarrow a \text{ div } b$; $r \leftarrow a - q * b$;
 - 3.2 $s \leftarrow x_2 - q * x_1$; $t \leftarrow y_2 - q * y_1$;
 - 3.3 $a \leftarrow b$; $b \leftarrow r$; $x_2 \leftarrow x_1$; $x_1 \leftarrow s$;
 - 3.4 $y_2 \leftarrow y_1$; $y_1 \leftarrow t$;
4. $d \leftarrow a$; $s \leftarrow x_2$; $t \leftarrow y_2$;
5. retorne (d, s, t) ;

Aritmética modular em \mathbb{Z}_n^*

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 16 *Dado um inteiro $n \geq 2$, denotamos por \mathbb{Z}_n^* ao conjunto $\{a \mid \text{mdc}(a, n) = 1, 1 \leq a \leq n - 1\}$. O tamanho de \mathbb{Z}_n^* é representado por $\phi(n)$, a função de Euler.*

Aritmética modular em \mathbb{Z}_n^*

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 17 *Dado um inteiro $n \geq 2$, denotamos por \mathbb{Z}_n^* ao conjunto $\{a \mid \text{mdc}(a, n) = 1, 1 \leq a \leq n - 1\}$. O tamanho de \mathbb{Z}_n^* é representado por $\phi(n)$, a função de Euler.*

Assim, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ e $\phi(10) = 4$. Também, $\phi(n) = n - 1$ sempre que n for primo.

Aritmética modular em \mathbb{Z}_n^*

Fundamentos

- Números inteiros
- **Aritmética modular**
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Definição 18 *Dado um inteiro $n \geq 2$, denotamos por \mathbb{Z}_n^* ao conjunto $\{a \mid \text{mdc}(a, n) = 1, 1 \leq a \leq n - 1\}$. O tamanho de \mathbb{Z}_n^* é representado por $\phi(n)$, a função de Euler.*

Assim, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ e $\phi(10) = 4$. Também, $\phi(n) = n - 1$ sempre que n for primo.

- É fácil verificar que as operações de soma, subtração e multiplicação modular são as mesmas da aritmética usual mas com o resultado reduzido módulo n . A divisão é a única exceção: $(a/b) \bmod n$ é sempre escrita e interpretada como $ab^{-1} \bmod n$.

Grupos

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Um *grupo* é formado por um conjunto \mathbb{G} e uma operação $+$, com as seguintes propriedades, para todos $a, b, c \in \mathbb{G}$:

1. (fechamento) $a + b \in \mathbb{G}$;
2. (associatividade) $(a + b) + c = a + (b + c)$;
3. (existência de elemento neutro ou *identidade*) existe um elemento em \mathbb{G} , denotado 0 , tal que $a + 0 = a$;
4. (existência de inversos) para todo $a \in \mathbb{G}$, existe em \mathbb{G} um elemento denotado $-a$, tal que $a + (-a) = 0$.

Um grupo é *abeliano* se $a + b = b + a$ para todos $a, b \in \mathbb{G}$.

Grupos (cont.)

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Exemplos de grupos são:

- números inteiros, racionais e reais com a soma usual;

Grupos (cont.)

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Exemplos de grupos são:

- números inteiros, racionais e reais com a soma usual;
- os elementos de $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$, $n > 0$, com a operação de soma módulo n ;

Grupos (cont.)

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Exemplos de grupos são:

- números inteiros, racionais e reais com a soma usual;
- os elementos de $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$, $n > 0$, com a operação de soma módulo n ;
- os elementos de $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$, $p > 1$, primo, com a operação de multiplicação módulo p .

Grupos (cont.)

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

Exemplos de grupos são:

- números inteiros, racionais e reais com a soma usual;
- os elementos de $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$, $n > 0$, com a operação de soma módulo n ;
- os elementos de $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$, $p > 1$, primo, com a operação de multiplicação módulo p .

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Denotaremos o grupo definido acima por $(\mathbb{G}, +)$, ou simplesmente \mathbb{G} , quando a operação $+$ estiver subentendida no texto.

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Denotaremos o grupo definido acima por $(\mathbb{G}, +)$, ou simplesmente \mathbb{G} , quando a operação $+$ estiver subentendida no texto.
- Essa definição usa a notação aditiva, isto é, $a + a + a + a$ é denotado por $4a$, 0 é a identidade, e $0 \cdot a = 0$.

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Denotaremos o grupo definido acima por $(\mathbb{G}, +)$, ou simplesmente \mathbb{G} , quando a operação $+$ estiver subentendida no texto.
- Essa definição usa a notação aditiva, isto é, $a + a + a + a$ é denotado por $4a$, 0 é a identidade, e $0 \cdot a = 0$.
- Poderíamos ter usado uma notação multiplicativa, onde a operação do grupo seria denotada ' \cdot '. Assim, $a \cdot a \cdot a$ (ou aaa) seria denotado por a^3 , o elemento identidade seria 1 , e $a^0 = 1$.

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Denotaremos o grupo definido acima por $(\mathbb{G}, +)$, ou simplesmente \mathbb{G} , quando a operação $+$ estiver subentendida no texto.
- Essa definição usa a notação aditiva, isto é, $a + a + a + a$ é denotado por $4a$, 0 é a identidade, e $0 \cdot a = 0$.
- Poderíamos ter usado uma notação multiplicativa, onde a operação do grupo seria denotada ' \cdot '. Assim, $a \cdot a \cdot a$ (ou aaa) seria denotado por a^3 , o elemento identidade seria 1 , e $a^0 = 1$.

Como já ficou claro, essas não são necessariamente as operações usuais de soma e multiplicação.

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- O número de elementos de \mathbb{G} é a sua *ordem*. Se a ordem é finita, então \mathbb{G} é um *grupo finito*.

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- **Grupos**
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- O número de elementos de \mathbb{G} é a sua *ordem*. Se a ordem é finita, então \mathbb{G} é um *grupo finito*.
- A *ordem de um elemento* $a \in \mathbb{G}$ é o menor inteiro positivo t tal que $ta = 0$. É um fato bem conhecido que a ordem de um elemento divide a ordem do grupo.

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- O número de elementos de \mathbb{G} é a sua *ordem*. Se a ordem é finita, então \mathbb{G} é um *grupo finito*.
- A *ordem de um elemento* $a \in \mathbb{G}$ é o menor inteiro positivo t tal que $ta = 0$. É um fato bem conhecido que a ordem de um elemento divide a ordem do grupo.
- Quando, para um grupo finito \mathbb{G} de ordem n , existe um elemento α de ordem n , dizemos que \mathbb{G} é *cíclico* e que α é um *gerador* de \mathbb{G} .

Grupos aditivos e multiplicativos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- O número de elementos de \mathbb{G} é a sua *ordem*. Se a ordem é finita, então \mathbb{G} é um *grupo finito*.
- A *ordem de um elemento* $a \in \mathbb{G}$ é o menor inteiro positivo t tal que $ta = 0$. É um fato bem conhecido que a ordem de um elemento divide a ordem do grupo.
- Quando, para um grupo finito \mathbb{G} de ordem n , existe um elemento α de ordem n , dizemos que \mathbb{G} é *cíclico* e que α é um *gerador* de \mathbb{G} .

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Definição 19 *Um corpo é formado por um conjunto \mathbb{F} e duas operações, ‘+’ e ‘·’, satisfazendo as seguintes propriedades:*

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Definição 20 *Um corpo é formado por um conjunto \mathbb{F} e duas operações, ‘+’ e ‘·’, satisfazendo as seguintes propriedades:*

- $(\mathbb{F}, +)$ é um grupo abeliano com identidade 0;
- $(\mathbb{F} \setminus \{0\}, \cdot)$ é um grupo abeliano com identidade 1; e
- a operação \cdot é distributiva sobre a operação $+$, isto é, $a \cdot (b + c) = a \cdot b + a \cdot c$, para todos $a, b, c \in \mathbb{F}$.

Números racionais, reais e complexos são exemplos de corpos infinitos.

A *ordem* de um corpo finito é o número de elementos em \mathbb{F} . Quando a ordem é finita dizemos que o corpo é *finito*.

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Sejam a, b dois elementos de um corpo, finito ou não. Então

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Sejam a, b dois elementos de um corpo, finito ou não. Então

- $a - b$ é equivalente a $a + (-b)$, onde $-b$ é o (único) inverso aditivo de b ;

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Sejam a, b dois elementos de um corpo, finito ou não. Então

- $a - b$ é equivalente a $a + (-b)$, onde $-b$ é o (único) inverso aditivo de b ;
- a/b é equivalente a $a \cdot (b^{-1})$, onde b^{-1} é o (único) inverso multiplicativo de b ;
- ka denota a adição de k parcelas iguais a a ;

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Sejam a, b dois elementos de um corpo, finito ou não. Então

- $a - b$ é equivalente a $a + (-b)$, onde $-b$ é o (único) inverso aditivo de b ;
- a/b é equivalente a $a \cdot (b^{-1})$, onde b^{-1} é o (único) inverso multiplicativo de b ;
- ka denota a adição de k parcelas iguais a a ;
- a^k denota a multiplicação de k parcelas iguais a a , onde $a^0 = 1$.

Corpos finitos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

Sejam a, b dois elementos de um corpo, finito ou não. Então

- $a - b$ é equivalente a $a + (-b)$, onde $-b$ é o (único) inverso aditivo de b ;
- a/b é equivalente a $a \cdot (b^{-1})$, onde b^{-1} é o (único) inverso multiplicativo de b ;
- ka denota a adição de k parcelas iguais a a ;
- a^k denota a multiplicação de k parcelas iguais a a , onde $a^0 = 1$.

Corpos finitos - existência

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Existe um corpo finito de ordem q , se e somente se $q = p^m$ para algum primo p e inteiro $m > 0$.

Corpos finitos - existência

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Existe um corpo finito de ordem q , se e somente se $q = p^m$ para algum primo p e inteiro $m > 0$.
- O primo p é a *característica* de \mathbb{F} .

Corpos finitos - existência

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Existe um corpo finito de ordem q , se e somente se $q = p^m$ para algum primo p e inteiro $m > 0$.
- O primo p é a *característica* de \mathbb{F} .
- Quando q é primo, i.e. $m = 1$, dizemos que o corpo é *primo*. Quando $m > 1$, o corpo é *de extensão*.

Corpos finitos - existência

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Existe um corpo finito de ordem q , se e somente se $q = p^m$ para algum primo p e inteiro $m > 0$.
- O primo p é a *característica* de \mathbb{F} .
- Quando q é primo, i.e. $m = 1$, dizemos que o corpo é *primo*. Quando $m > 1$, o corpo é *de extensão*.
- Denotamos o corpo finito de ordem q por \mathbb{F}_q .

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- O conjunto \mathbb{Z}_p , p primo, com as operações de soma e multiplicação *módulo* p formam o corpo primo \mathbb{F}_p de ordem p .

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- O conjunto \mathbb{Z}_p , p primo, com as operações de soma e multiplicação *módulo* p formam o corpo primo \mathbb{F}_p de ordem p .
- Exemplos de primos: (NIST)
 - $p = 2^{192} - 2^{64} - 1$
 - $p = 2^{521} - 1$

Corpos binários

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

O corpo *binário* \mathbb{F}_{2^m} é formado pelos polinômios em uma variável z de grau máximo $m - 1$, cujos coeficientes são 0 ou 1. As duas operações associadas são as de soma e multiplicação de polinômios, com as seguintes restrições:

- os coeficientes do polinômio resultante são reduzidos módulo 2;

Corpos binários

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

O corpo *binário* \mathbb{F}_{2^m} é formado pelos polinômios em uma variável z de grau máximo $m - 1$, cujos coeficientes são 0 ou 1. As duas operações associadas são as de soma e multiplicação de polinômios, com as seguintes restrições:

- os coeficientes do polinômio resultante são reduzidos módulo 2;
- o resultado da multiplicação de dois polinômios deve ser tomado módulo um polinômio *irredutível* $f(z)$ de grau m . Isto é, $f(z)$ não é o produto de dois polinômios binários de grau menor que m .

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Corpo Finito:

$$\mathbb{F}_{2^m} = \left\{ \sum_{i=0}^{m-1} a_i x^i \mid a_i \in \mathbb{Z}_2 \right\},$$

$f(x) = x^m + r(x)$ polinômio irredutível

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- **Corpo Finito:**

$$\mathbb{F}_{2^m} = \left\{ \sum_{i=0}^{m-1} a_i x^i \mid a_i \in \mathbb{Z}_2 \right\},$$

$f(x) = x^m + r(x)$ polinômio irredutível

- **Exemplo:** $m = 3$, \mathbb{F}_{2^3} , $f(x) = x^3 + x + 1$
 $\mathbb{F}_{2^3} = \{a_2 x^2 + a_1 x + a_0 \mid a_i \in \{0, 1\}\}$
 $= \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$
 $= \{000, 001, 010, 011, 100, 101, 110, 111\}$

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Os elementos não nulos de um corpo finito \mathbb{F}_q , juntamente com a multiplicação do corpo, formam um grupo cíclico, denotado por \mathbb{F}_q^* .

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Os elementos não nulos de um corpo finito \mathbb{F}_q , juntamente com a multiplicação do corpo, formam um grupo cíclico, denotado por \mathbb{F}_q^* .
- Portanto, existe para esse grupo pelo menos um gerador α , isto é,

$$\mathbb{F}_q^* = \{\alpha^i : 0 \leq i \leq q - 2\}.$$

Corpos finitos - exemplos

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- **Corpos finitos**
- Problema do logaritmo discreto
- Exercícios:

- Os elementos não nulos de um corpo finito \mathbb{F}_q , juntamente com a multiplicação do corpo, formam um grupo cíclico, denotado por \mathbb{F}_q^* .
- Portanto, existe para esse grupo pelo menos um gerador α , isto é,

$$\mathbb{F}_q^* = \{\alpha^i : 0 \leq i \leq q - 2\}.$$

Problema do logaritmo discreto

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- **Problema do logaritmo discreto**
- Exercícios:

Definição 21 (*Problema do logaritmo discreto*) *Dados elementos a, b de um grupo (G, \cdot) , tais que $b = a^l$, o problema do logaritmo discreto é o de encontrar l conhecendo a e b apenas.*

- Em \mathbb{Z}_p^* : $y = \alpha^x \pmod{p_{2048}}$, calcular x onde p_{2048} é um primo de 2048 bits.
- Os métodos conhecidos para o cálculo do logaritmo discreto em \mathbb{F}_{q^*} são todos muito ineficientes quando q é muito grande, da ordem de centenas de dígitos. Para outros grupos o cálculo é muito fácil, por exemplo, em $(\mathbb{Z}_n, +)$.

Exercícios:

Fundamentos

- Números inteiros
- Aritmética modular
- Grupos
- Corpos finitos
- Problema do logaritmo discreto
- Exercícios:

- Calcule $1093987656544568 \times 9996543298765401 \pmod{100}$.
- Calcule em \mathbb{Z}_{11} o número $8 \times 7 - 10$.
- Calcule $3^{22} \pmod{23}$.
- Determine números d , s e t tais que $d = \text{mdc}(234, 26) = 234 \times s + 26 \times t$.
- Calcule o inverso multiplicativo de 17 em \mathbb{Z}_{23}^* .
- Implemente em C a extensão do algoritmo de Euclides.