Brazilian ICPC Summer School

Teoria dos Números

Felipe Chen

Cronograma

Dia 1

- Números primos e Teorema Fundamental da Aritmética
- Testes de primalidade/Fatoração
- Máximo Divisor Comum (MMC) e Mínimo Múltiplo Comum (MDC)
- Função Aritmética
- Soma e quantidade de divisores de um número
- Algoritmo de Euclides
- Função Totiente de Euler
- Equações Diofantinas
- Crivo de Eratóstenes
- Soma Harmônica
- Aritmética Modular
- Exponenciação Rápida
- Teorema de Fermat/Euler
- Inverso modular
- Teorema Chinês do Resto (TCR)
- Teorema de Wilson e Teorema de Lucas

Cronograma

Dia 2

- Ordem Multiplicativa
- Raiz Primitiva
- Logaritmo Discreto
- Função de Mobius
- Inversão de Moebius
- Lema Harmônico

Números Primos e Teorema Fundamental da Aritmética

- **Números primos:** Números inteiros que possuem exatamente 2 divisores: 1 e ele mesmo.

Números Primos e Teorema Fundamental da Aritmética

- **Números primos:** Números inteiros que possuem exatamente 2 divisores: 1 e ele mesmo.
- **Teorema Fundamental da Aritmética:** Todo número inteiro positivo pode ser escrito como um produto único de fatores primos.

Números Primos e Teorema Fundamental da Aritmética

- **Números primos:** Números inteiros que possuem exatamente 2 divisores: 1 e ele mesmo.
- **Teorema Fundamental da Aritmética:** Todo número inteiro positivo pode ser escrito como um produto único de fatores primos.
- Todo inteiro positivo n pode ser escrito como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (fatoração de n) para algum $k \geq 0$ inteiro, p_i distintos, $\alpha_i > 0$.

Teste de primalidade/fatoração

- Divisão por tentativa - testar se n é divisível por algum dos números menores ou iguais a $\sqrt{n}$.

Teste de primalidade/fatoração

- Divisão por tentativa - testar se n é divisível por algum dos números menores ou iguais a $\sqrt{n}$.
- Pollard Rho Algorithm - probabilístico em $O(n^{\frac{1}{4}})$

Máximo Divisor Comum (MDC/GCD) e Mínimo Múltiplo Comum (MMC/LCM)

- **gcd(a, b):=** O maior inteiro positivo que divide a e b.

Máximo Divisor Comum (MDC/GCD) e Mínimo Múltiplo Comum (MMC/LCM)

- **gcd(a, b):=** O maior inteiro positivo que divide a e b.
- **lcm(a, b):=** O menor inteiro positivo que é divisível por a e b.

Máximo Divisor Comum (MDC/GCD) e Mínimo Múltiplo Comum (MMC/LCM)

- **gcd(a, b):=** O maior inteiro positivo que divide *a* e *b*.
- **lcm(a, b):=** O menor inteiro positivo que é divisível por *a* e *b*.
- Se $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$:

$$\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Máximo Divisor Comum (MDC/GCD) e Mínimo Múltiplo Comum (MMC/LCM)

- **gcd(a, b):=** O maior inteiro positivo que divide a e b.
- **lcm(a, b):=** O menor inteiro positivo que é divisível por a e b.
- Se $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$:

$$\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

- Dizemos que a e b são coprimos se $\gcd(a, b) = 1$.

Máximo Divisor Comum (MDC/GCD) e Mínimo Múltiplo Comum (MMC/LCM)

- **gcd(a, b):=** O maior inteiro positivo que divide a e b.
- **lcm(a, b):=** O menor inteiro positivo que é divisível por a e b.
- Se $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$:

$$\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

- Dizemos que a e b são coprimos se $\gcd(a, b) = 1$.
- Uma propriedade que temos é $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.

Função Aritmética

- Uma função aritmética f é
  Aditiva se $f(mn) = f(n) + f(m)$ para todos números inteiros n e m coprimos.
  Multiplicativa se $f(mn) = f(n)f(m)$ para todos números inteiros n e m coprimos.
- São funções aritméticas multiplicativas: Quantidade de divisores, Soma dos divisores, Função Totiente de Euler, Função de Moebius.

Soma e quantidade de divisores de n

- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e d divide n (escrevemos $d|n$) temos $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, com $0 \leq \beta_i \leq \alpha_i$.

Soma e quantidade de divisores de n

- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e d divide n (escrevemos $d|n$) temos $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, com $0 \leq \beta_i \leq \alpha_i$.
- **Quantidade de divisores de n:**

$$d(n) = (\alpha_1 + 1) * (\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Soma e quantidade de divisores de n

- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e d divide n (escrevemos $d|n$) temos $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, com $0 \leq \beta_i \leq \alpha_i$.
- **Quantidade de divisores de n:**

$$d(n) = (\alpha_1 + 1) * (\alpha_2 + 1) \cdots (\alpha_k + 1)$$

- **Soma dos divisores de n:**

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

Função Totiente de Euler

- $\phi(n) :=$ Quantidade de números inteiros entre 1 e n que são coprimos com n.

Função Totiente de Euler

- $\phi(n) :=$ Quantidade de números inteiros entre 1 e n que são coprimos com n.
- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$:

$$\phi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$$

Função Totiente de Euler

- $\phi(n) :=$ Quantidade de números inteiros entre 1 e n que são coprimos com n.
- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$:

$$\phi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$$

- Outra forma de calcular $\phi(n)$ é

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

Algoritmo de Euclides

- Sejam a e b inteiros positivos com $a > b$. Os divisores comuns de a e b são os mesmos divisores comuns de $a - b$ e b.

Algoritmo de Euclides

- Sejam a e b inteiros positivos com $a > b$. Os divisores comuns de a e b são os mesmos divisores comuns de $a - b$ e b.
- Em particular, $\text{gcd}(a, b) = \text{gcd}(a - b, b)$. Daí obtemos

$$gcd(a, b) = gcd(a\%b, b) = gcd(b, a\%b)$$

Equações Diofantinas/Lema de Bézout

- Sejam a e b inteiros com $\gcd(a, b) = d$. Então, existem inteiros x e y tais que $ax + by = d$.

Equações Diofantinas/Lema de Bézout

- Sejam a e b inteiros com $\gcd(a, b) = d$. Então, existem inteiros x e y tais que $ax + by = d$.
- Mais precisamente, dada uma solução inicial x_0 e y_0 com $ax_0 + by_0 = d$, todas as outras soluções são da forma $x = x_0 + \frac{b}{d}k$ e $y = y_0 - \frac{a}{d}k$, k inteiro qualquer.

Equações Diofantinas/Lema de Bézout

- Sejam a e b inteiros com $\gcd(a, b) = d$. Então, existem inteiros x e y tais que $ax + by = d$.
- Mais precisamente, dada uma solução inicial x_0 e y_0 com $ax_0 + by_0 = d$, todas as outras soluções são da forma $x = x_0 + \frac{b}{d}k$ e $y = y_0 - \frac{a}{d}k$, k inteiro qualquer.
- Podemos encontrar uma solução inicial pelo Algoritmo de Euclides estendido.

Crivo de Eratóstenes

- É um algoritmo para achar todos os primos entre 1 e n.

Crivo de Eratóstenes

- É um algoritmo para achar todos os primos entre 1 e n.
- Também utilizado para calcular funções aritméticas.

Crivo de Eratóstenes

- É um algoritmo para achar todos os primos entre 1 e n.
- Também utilizado para calcular funções aritméticas.
- $\sum_{i=1}^{n} \frac{n}{i} \approx n \log n$

Alguns resultados sobre primos

- A quantidade de primos menores ou iguais a n é approximadamente $n \log n$.
- O k-ésimo primo é approximadamente igual a $k \log k$.
- Para todo inteiro n, existe um primo entre n e $2n$.
- **Teorema de Dirichlet:** Para quaisquer inteiros a e b coprimos, existem infinitos primos da forma $ax + b$.

Aritmética Modular

- Dado um inteiro $m > 0$ (chamado módulo), dois inteiros a e b são ditos congruentes se existe k inteiro tal que $a - b = km$. É denotado por $a \equiv b$.
- Congruência módulo m é uma relação de equivalência que é compatível com as operações de adição, subtração e multiplicação.

Propriedades da Congruência Modular

- **Reflexividade:** $a \equiv a \pmod{n}$
- **Simetria:** Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$, para todos os inteiros a, b e n.
- **Transitividade:** Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$.
- Se $a_1 \equiv b_1 \pmod{n}$ e $a_2 \equiv b_2 \pmod{n}$, ou se $a \equiv b \pmod{n}$, então:
- **Translação:** $a + k \equiv b + k \pmod{n}$, para qualquer inteiro k.
- **Escalar:** $ka \equiv kb \pmod{n}$, para qualquer inteiro k.
- **Adição:** $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.
- **Subtração:** $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$.
- **Multiplicação:** $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.
- **Exponenciação:** $a^k \equiv b^k \pmod{n}$, para qualquer inteiro não negativo k.
- **Polinômio:** $p(a) \equiv p(b) \pmod{n}$, para qualquer polinômio $p(x)$ com coeficientes inteiros.

Teorema de Euler/Fermat

- Se a e n são coprimos:
- **Teorema de Euler:** $a^{\phi(n)} \equiv 1 \pmod{n}$.
- Em particular, se $n = p$, p primo:
- **Teorema de Fermat:** $a^{p-1} \equiv 1 \pmod{p}$.

Exponenciação Rápida

- Podemos calcular $a^x \mod m$ em $O(\log x)$
- Se $x = 2^{k_1} + 2^{k_2} + \cdots 2^{k_c}$, $a^x = a^{2^{k_1}} a^{2^{k_2}} \cdots a^{2^{k_c}}$.

Inverso Modular

- Se a e n são coprimos, então existe b tal que $ab \equiv 1 \pmod{n}$.
- Denotamos b por a^{-1}.
- Temos que $a^{-1} \equiv a^{\phi(n)}a^{-1} \equiv a^{\phi(n)-1}aa^{-1} \equiv a^{\phi(n)-1} \pmod{n}$

Teorema do Chinês do Resto (TCR)

- Sejam $m_1, m_2, \cdots m_k > 1$ inteiros, coprimos dois a dois. Seja $M = m_1 m_2 \cdots m_k$.
  Para quaisquer inteiros $a_1, a_2, \cdots, a_k$ existe um único inteiro $0 \leq x < M$ tal que:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\cdots$$

$$x \equiv a_k \pmod{m_k}$$

Teorema de Wilson e Teorema de Lucas

- **Teorema de Wilson:** $(p-1)! \equiv -1 \pmod{p}$, se p é primo.

Teorema de Wilson e Teorema de Lucas

- **Teorema de Wilson:** $(p-1)! \equiv -1 \pmod p$, se p é primo.
- **Teorema de Lucas:** Sejam m e n números inteiros não negativos, p um número primo e sejam

$$m = m_0 + m_1 p + \cdots m_{k-1} p^{k-1} + m_k p^k$$

$$n = n_0 + n_1 p + \cdots n_{k-1} p^{k-1} + n_k p^k$$

as expansões de m e n na base p. Então

$$\binom{m}{n} \equiv \prod_{i=1}^{k} \binom{m_i}{n_i} \mod p$$

Ordem Multiplicativa

- A ordem multiplicativa de a módulo n é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{n}$. Denotamos por $\mathrm{ord}_n(a)$.

Ordem Multiplicativa

- A ordem multiplicativa de a módulo n é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{n}$. Denotamos por $\text{ord}_n(a)$.
- Seja k inteiro tal que $a^k \equiv 1 \pmod{n}$. Então $d|k$.

Ordem Multiplicativa

- A ordem multiplicativa de a módulo n é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{n}$. Denotamos por $\text{ord}_n(a)$.
- Seja k inteiro tal que $a^k \equiv 1 \pmod{n}$. Então $d|k$.
- $a^0, a^1, a^2, \cdots, a^{d-1}$ são todos distintos módulo n

Ordem Multiplicativa

- A ordem multiplicativa de a módulo n é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{n}$. Denotamos por $\text{ord}_n(a)$.
- Seja k inteiro tal que $a^k \equiv 1 \pmod{n}$. Então $d|k$.
- $a^0, a^1, a^2, \cdots, a^{d-1}$ são todos distintos módulo n
- $\text{ord}_n(a)|\phi(n)$

Ordem Multiplicativa

- A ordem multiplicativa de a módulo n é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{n}$. Denotamos por $\text{ord}_n(a)$.
- Seja k inteiro tal que $a^k \equiv 1 \pmod{n}$. Então $d|k$.
- $a^0, a^1, a^2, \cdots, a^{d-1}$ são todos distintos módulo n
- $\text{ord}_n(a)|\phi(n)$
- Se p é primo e $d|p-1$, então existem $\phi(d)$ números $0 < x < p$ tais que $\text{ord}_p(x) = d$.

Raiz Primitiva

- Dizemos que g é uma raiz primitiva módulo n se $\text{ord}_n(g) = \phi(n)$.

Raiz Primitiva

- Dizemos que g é uma raiz primitiva módulo n se $\text{ord}_n(g) = \phi(n)$.
- $g^0, g^1, g^2, \cdots, g^{\phi(n)-1}$ módulo n são todos os números coprimos com n.

Raiz Primitiva

- Dizemos que g é uma raiz primitiva módulo n se $\text{ord}_n(g) = \phi(n)$.
- $g^0, g^1, g^2, \cdots, g^{\phi(n)-1}$ módulo n são todos os números coprimos com n.
- Os únicos números que possuem alguma raiz primitiva são $2, 4, p^k, 2p^k$.

Logaritmo Discreto

- Consiste em achar o menor inteiro x tal que $a^x \equiv v \pmod{n}$. Nem sempre possui solução.
- Um dos algoritmos utilizados é o baby-step giant-step.

Função de Mobius

- A função de Mobius é definido como

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ (-1)^k & \text{se } n \text{ é o produto de } k \text{ primos distintos}, \\ 0 & \text{se} n \text{ divisível por algum quadrado} > 1. \end{cases}$$

- A função de Moebius satisfaz

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

- Essa igualdade leva a Fórmula de Inversão de Moebius.

Inversão de Moebius

- Se f e g são funções aritméticas satisfazendo

$$g(n) = \sum_{d|n} f(d) \text{para todo inteiro } n \geq 1$$

  então

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) \text{para todo inteiro } n \geq 1$$

- É, de certa forma, uma inclusão-exclusão nos divisores.

Lema Harmônico

- Considere o seguinte problema: Calcule $\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor$

Lema Harmônico

- Considere o seguinte problema: Calcule $\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor$
- Existem no máximo $2\sqrt{n}$ valores distintos de $\lfloor \frac{n}{i} \rfloor$.

Lema Harmônico

- Considere o seguinte problema: Calcule $\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor$
- Existem no máximo $2\sqrt{n}$ valores distintos de $\lfloor \frac{n}{i} \rfloor$.
- Podemos iterar pelos valores únicos de $\lfloor \frac{n}{i} \rfloor$.

Lema Harmônico

- Considere o seguinte problema: Calcule $\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor$
- Existem no máximo $2\sqrt{n}$ valores distintos de $\lfloor \frac{n}{i} \rfloor$.
- Podemos iterar pelos valores únicos de $\lfloor \frac{n}{i} \rfloor$.
- O maior y tal que $\lfloor \frac{n}{x} \rfloor = \lfloor \frac{n}{y} \rfloor$ para x inteiro é $y = \lfloor \frac{n}{\lfloor \frac{n}{x} \rfloor} \rfloor$.