Álgebra e Teoria dos Números

Diego F. Aranha

Institute of Computing
UNICAMP

Primos e divisibilidade

Divisibilidade

Para $a, b \in \mathbb{Z}$, dizemos que a *divide* b (denotado por $a \mid b$) ou que a é *divisor* de b se existe $c \in \mathbb{Z}$ tal que $ac = b$. Se $a \notin \{1, b\}$, dizemos que a é *fator* ou divisor *não-trivial* de b.

Primalidade

Um número inteiro $p > 1$ é *primo* se não possui fatores, ou seja, só possui divisores triviais. Um número que não é primo é dito *composto*.

Teorema Fundamental da Aritmética

Qualquer número inteiro $N > 1$ pode ser expressado *unicamente* (a menos de permutação) como um produto de fatores primos $N = \prod_i p_i^{e_i}$, com p_i distintos e $e_i \geq 1$ para todo i.

Divisibilidade

Divisão

Seja $a \in Z$ e b inteiro positivo. Existem inteiros únicos q, r tais que $a = bq + r$, com $0 \leq r < b$.

Máximo Divisor Comum

Sejam a, b inteiros positivos. Existem inteiros x, y tais que $ax + by = mdc(a, b)$ e $mdc(a, b)$ é o menor inteiro que pode ser escrito dessa forma.

Propriedades

- Se $c \mid ab$ e $mdc(a, c) = 1$, então $c \mid b$. Em particular, se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.
- Se $p \mid N, q \mid N$ e $mdc(p, q) = 1$, então $pq \mid N$.

Algoritmo de Euclides

Algorithm 1 Cálculo de $mdc(a, b)$.

1: $r_0 \leftarrow a, r_1 \leftarrow b, m \leftarrow 1$
2: **while** $r_m \neq 0$ **do**
3: $\quad q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor$
4: $\quad r_{m+1} \leftarrow r_{m-1} - q_m r_m$
5: $\quad m \leftarrow m + 1$
6: **end while**
7: $m \leftarrow m - 1$
8: **return** $(q_1, \ldots, q_m; r_m = mdc(a, b))$

Invariantes

- Para $0 \leq i \leq r_{m-2} : r_i = q_{i+1} r_{i+1} + r_{i+2}$, com $0 < r_{i+2} < r_{i+1}$;
- Temos que $r_{m-1} = q_m r_m$;
- $mdc(r_0, r_1) = mdc(r_1, r_2) = \cdots = mdc(r_{m-1}, r_m) = r_m$

Algoritmo de Euclides

Sejam as duas seqüências:

$$t_j = \begin{cases} 0 & \text{se } j = 0 \\ 1 & \text{se } j = 1 \\ t_{j-2} - q_{j-1} t_{j-1} & \text{se } j \geq 2 \end{cases}$$

$$s_j = \begin{cases} 1 & \text{se } j = 0 \\ 0 & \text{se } j = 1 \\ s_{j-2} - q_{j-1} s_{j-1} & \text{se } j \geq 2 \end{cases}$$

Teorema

Para $0 \leq j \leq m$, temos que $r_j = s_j r_0 + t_j r_1$.

Prova: Por indução forte!

Algoritmo Estendido de Euclides

Algorithm 2 Cálculo de $r = mdc(a, b) = sa + tb$, com $r, s, t \in \mathbb{Z}$.

1: $a_0 \leftarrow a, b_0 \leftarrow b$
2: $t_0 \leftarrow 0, t \leftarrow 1, s_0 \leftarrow 1, s \leftarrow 0$
3: $q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor, r \leftarrow a_0 - q b_0$
4: **while** $r > 0$ **do**
5: $\quad T \leftarrow t_0 - qt, t_0 \leftarrow t, t \leftarrow T$
6: $\quad T \leftarrow s_0 - qs, s_0 \leftarrow s, s \leftarrow T$
7: $\quad a_0 \leftarrow b_0, b_0 \leftarrow r, q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor, r \leftarrow a_0 - q b_0$
8: **end while**
9: $r \leftarrow b_0$
10: **return** (r, s, t)

Aritmética Modular

Definições

Sejam $a, b, N \in \mathbb{Z}$, com $N > 1$. A *redução modular* de a *módulo* N (a mod N) denota o resto da divisão inteira de a por N. Dizemos que a, b são *congruentes* módulo N ($a \equiv b \pmod{N}$) se $a \bmod N = b \bmod N$ ou ainda se $N \mid (a - b)$. A relação de congruência é *reflexiva*, *simétrica* e *transitiva*.

Lembrete: $ad \equiv cd \pmod{N}$ nem sempre implica $a \equiv c \pmod{N}$.

Inverso

Sejam $a, N \in Z$, com $N > 1$. Então a é *inversível* módulo N sse $mdc(a, N) = 1$. O *inverso único* de a é denotado por a^{-1} e pode ser calculado pelo Algoritmo Estendido de Euclides.

Exemplo: 14 é o inverso de 11 módulo 17.

Grupos

Definição

Um *grupo* $\mathbb{G}$ é um conjunto equipado com uma *operação binária* $\circ$ que possui as seguintes propriedades:

- *Fechamento:* Se $g, h \in \mathbb{G}$, então $g \circ h \in \mathbb{G}$;
- *Elemento Neutro:* $\exists e \in \mathbb{G}$ tal que $\forall g \in \mathbb{G}, g \circ e = e \circ g = g$.
- *Inverso:* $\forall g \in \mathbb{G}, \exists h \in \mathbb{G}$ tal que $g \circ h = e = g \circ e$.
- *Associatividade:* $\forall g_1, g_2, g_3 \in \mathbb{G}$, $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$.

Quando $\mathbb{G}$ é um grupo finito, denotamos o número de elementos (*ordem*) de $\mathbb{G}$ por $|\mathbb{G}|$. Um grupo é dito *abeliano* se $\circ$ é uma relação *comutativa*, ou seja, $\forall g_1, g_2 \in \mathbb{G}, g_1 \circ g_2 = g_2 \circ g_1$.

Exemplos: $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{R}^*, \times), (\mathbb{Z}_N = \{0, 1, \ldots, N-1\}, +)$.

Subgrupo

Se $\mathbb{G}$ é um grupo, um conjunto $\mathbb{H} \subseteq \mathbb{G}$ é *subgrupo* se $\mathbb{H}$ for um grupo sob a mesma operação de $\mathbb{G}$.

Grupos

Notação

A operação de grupo pode utilizar notação *aditiva* ou *multiplicativa*. Quando a operação de grupo é aplicada $(m-1)$ vezes a um elemento g, utilizamos a notação aditiva $m \cdot g$ ou multiplicativa g^m. Inversos e elementros neutros são denotados por $(-g, 0)$ e $(g^{-1}, 1)$, respectivamente.

Importante: Não confundir com adição ou multiplicação inteira.

Teorema

Seja $\mathbb{G}$ um grupo finito de ordem m. Para todo $g \in G$ e $i \in Z$, temos que $g^m = 1$ e se $m > 1, g^i = g^{i \bmod m}$.

Corolário

Seja $d, e \in \mathbb{Z}$ e $\mathbb{G}$ um grupo finito de ordem $m > 1$. A função $f_e : \mathbb{G} \to \mathbb{G}$ tal que $f_e(g) = g^e$ é uma permutação quando $mdc(e, m) = 1$ e f_d é função inversa de f_e se $d = e^{-1} \bmod m$.

O grupo $\mathbb{Z}_N^*$

Teorema

Sejam um inteiro $N > 1$ com fatoração $N = \prod_i p_i^{e_i}$ e $\mathbb{Z}_N^* = \{a \in \{1, \ldots, N-1\} \mid mdc(a, N) = 1\}$. Então $\mathbb{Z}_N^*$ é um grupo abeliano sob a multiplicação módulo N. A ordem do grupo é dada pela função totiente de Euler $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$.

Corolário

Seja $N > 1$ inteiro e $a \in \mathbb{Z}_N^*$. Então $a^{\phi(N)} = 1 \bmod N$. Se N é primo e $a \in \mathbb{Z}_p$, temos que $a^{p-1} = 1 \bmod p$.

Teorema Chinês do Resto

Isomorfismo

Sejam $\mathbb{G}, \mathbb{H}$ grupos com operações $\circ_{\mathbb{G}}, \circ_{\mathbb{H}}$, respectivamente. A função $f : \mathbb{G} \to \mathbb{H}$ é um *isomorfismo* se f é uma bijeção e $\forall g_1, g_2 \in \mathbb{G}, f(g_1 \circ_{\mathbb{G}} g_2) = f(g_1) \circ_{\mathbb{H}} f(g_2)$.

Teorema

Seja $N = pq$, com p, q relativamente primos. A função $f(x) = (x \bmod p, x \bmod q)$ é um isomorfismo de $\mathbb{Z}_N$ para $\mathbb{Z}_p \times \mathbb{Z}_q$ e de $\mathbb{Z}_N^*$ para $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

Importante: A mudança de representação afeta o custo computacional de operações em grupo.

Teorema Chinês do Resto

Sejam $m_1, \ldots, m_r$ inteiros co-primos entre si dois a dois e suponha $a_1, \ldots, a_r$ inteiros.

Considere o sistema de equações:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

O Teorema Chinês do Resto fornece uma solução única para esse sistema módulo $M = \prod_{i=1}^{r} m_i$:

Teorema

A solução para o sistema de equações é $x = \sum_{i=1}^{r} a_i M_i y_i \bmod M$, onde $M_i = M/m_i$ e $y_i = M_i^{-1} \bmod m_i$, para $1 \leq i \leq r$.

Geração de números primos

Precisamos da geração de números primos grandes, ou ainda, a geração de números grandes e teste de sua primalidade.

Alternativas:

- Teste determinístico polinomial: [AKS 2002], $O(n^6)$;
- Teste probabilístico: mais rápido, chance de erro.

Teorema dos números primos

Seja $\pi(N)$ a quantidade de números primos menores ou iguais a N. Podemos aproximar $\pi(N) \approx N/\ln(N)$.

Exemplo: Para n com 1024 *bits*, precisamos gerar p, q com 512 *bits*. Um número aleatório com 512 *bits* tem probabilidade $2/355$ de ser primo ímpar.

Algoritmo probabilístico

Definição

Um algoritmo probabilístico é qualquer algoritmo que utiliza números aleatórios. Quando há chance de erro, o algoritmo é dito de Monte Carlo. Quando a resposta é sempre correta, mas com chance de falha, o algoritmo é dito Las Vegas. Classificação para solução de problemas de decisão:

1. **Monte Carlo com viés positivo:** uma resposta SIM é sempre correta, mas uma resposta $\mathrm{N\tilde{A}O}$ pode estar incorreta;
2. **Monte Carlo com viés negativo:** uma resposta $\mathrm{N\tilde{A}O}$ é sempre correta, mas uma resposta SIM pode estar incorreta.

A probabilidade de erro é limitada superiormente por ϵ.

Importante: como transformar Monte Carlo em Las Vegas?

Problema de decisão

Composto(n), $n \geq 2$

O conjunto $D(n)$ de divisores distintos de n possui mais do que dois elementos?

Alternativas para resolver o problema:

1. Solovay-Strassen: Monte Carlo com viés positivo, $\epsilon = 1/2$;
2. Miller-Rabin: Monte Carlo com viés positivo, $\epsilon = 1/4$.

Problema de decisão

Definição

Seja p um primo ímpar e a inteiro. Dizemos que a é *resíduo quadrático* módulo p se $a \neq 0 \pmod{p}$ e $y^2 \equiv a \pmod{p}$ possui duas soluções $(y, -y)$ módulo p. Caso contrário, a é *resíduo não-quadrático*.

Exemplo: Em $\mathbb{Z}_{11}$, os resíduos quadráticos são 1, 3, 4, 5 e 9. Os resíduos não-quadráticos são 2, 6, 7, 8 e 10.

Lema

Se p é um primo ímpar, então as únicas raízes quadradas de 1 módulo p são 1 e -1 mod p.

Símbolos de Jacobi e Legendre

Teorema (Critério de Euler)

Seja p primo ímpar. Então a é resíduo quadrático módulo p sse $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Prova: Suponha que $a \equiv y^2 \pmod{p}$. Se p é primo, então $a^{p-1} \equiv 1 \pmod{p}, \forall a \not\equiv 0 \pmod{p}$. Logo:

$$a^{(p-1)/2} \equiv (y^2)^{(p-1)/2} \equiv 1 \pmod{p}.$$

Símbolos de Jacobi e Legendre

Teorema (Critério de Euler)

Seja p primo ímpar. Então a é resíduo quadrático módulo p sse $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Prova: Suponha que $a \equiv y^2 \pmod{p}$. Se p é primo, então $a^{p-1} \equiv 1 \pmod{p}, \forall a \not\equiv 0 \pmod{p}$. Logo:

$$a^{(p-1)/2} \equiv (y^2)^{(p-1)/2} \equiv 1 \pmod{p}.$$

Agora, suponha que $a^{(p-1)/2} \equiv 1 \pmod{p}$. Seja b um elemento primitivo módulo p. Então $a \equiv b^i \pmod{p}$ para $i \in \mathbb{Z}$. Logo:

$$a^{(p-1)/2} \equiv (b^i)^{(p-1)/2} \pmod{p}.$$

Como b tem ordem $p-1$, então $(p-1)|i(p-1)/2$. Então i é par e as raízes quadradas de a são $\pm b^{i/2}$ mod p.

Símbolos de Jacobi e Legendre

Definição

Para $a \in \mathbb{Z}$, p primo ímpar, o *símbolo de Legendre* $\left(\frac{a}{p}\right)$ é:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } a \equiv 0 \pmod{p} \\ 1 & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1 & \text{se } a \text{ é resíduo não-quadrático módulo } p. \end{cases}$$

Temos que $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Símbolos de Jacobi e Legendre

Definição

Para $a \in \mathbb{Z}$, p primo ímpar, o *símbolo de Legendre* $\left(\frac{a}{p}\right)$ é:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } a \equiv 0 \pmod{p} \\ 1 & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1 & \text{se } a \text{ é resíduo não-quadrático módulo } p. \end{cases}$$

Temos que $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Definição

Suponha $n \in \mathbb{Z}$ ímpar positivo com fatoração $n = \prod_{i=1}^{k} {p_i}^{e_i}$.
Seja $a \in \mathbb{Z}$. O *símbolo de Jacobi* $\left(\frac{a}{n}\right)$ é definido como:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

Algoritmo Solovay-Strassen

Para o símbolo de Jacobi, temos que $\left(\frac{a}{n}\right) = 0$ sse $mdc(a, n) \neq 1$.
Temos ainda que para n composto, a igualdade $\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod{n}$ é verdadeira para metade dos inteiros $a \in \mathbb{Z}_n^*$.

Algoritmo Solovay-Strassen

Para o símbolo de Jacobi, temos que $\left(\frac{a}{n}\right) = 0$ sse $mdc(a, n) \neq 1$.
Temos ainda que para n composto, a igualdade $\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod{n}$ é verdadeira para metade dos inteiros $a \in \mathbb{Z}_n^*$.

Algoritmo

1. Escolher inteiro aleatório a tal que $1 \leq a \leq n-1$
2. $x \leftarrow \left(\frac{a}{n}\right)$
3. Se $x = 0$, retorne $\mathrm{COMPOSTO}$
4. $y \leftarrow a^{(n-1)/2} \pmod{n}$
5. Se $x \equiv y \pmod{n}$, retorne PRIMO. Caso contrário, retorne $\mathrm{COMPOSTO}$.

Importante: Por que o algoritmo tem viés positivo com $\epsilon = 1/2$?

Algoritmo Solovay-Strassen

Propriedades do símbolo de Jacobi:

- Se $n > 0$ ímpar e $m_1 \equiv m_2 \pmod{n}$, então:

$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right).$$

- Se $n > 0$ ímpar, então:

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{se } n \equiv \pm 1 \pmod 8 \\ -1 & \text{se } n \equiv \pm 3 \pmod 8. \end{cases}$$

- Se $n > 0$ ímpar, então:

$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right), \text{ ou } \left(\frac{m = 2^k t}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right)$$

- Se $m, n > 0$ ímpares, então:

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{se } m \equiv n \equiv 3 \pmod 4 \\ \left(\frac{n}{m}\right) & \text{caso contrário.} \end{cases}$$

Algoritmo Miller-Rabin

Intuição: Não há raízes não-triviais de 1 módulo p primo. Extrair raízes quadradas de a^{n-1} mod n e verificar se todas são ± 1 mod n.

Algoritmo

1. Escrever $n - 1 = 2^k m$, com m ímpar
2. Escolher inteiro aleatório a tal que $1 \leq a \leq n - 1$
3. $b \leftarrow a^m \bmod n$
4. Se $b \equiv 1 \pmod n$, retorne PRIMO
5. Para $i \leftarrow 0$ até $k - 1$, faça:
   - Se $b \equiv -1 \pmod n$, retorne PRIMO
   - $b \leftarrow b^2 \bmod n$
6. Retorne $\mathrm{COMPOSTO}$

Importante: Por que o algoritmo tem viés positivo com $\epsilon = 1/4$?

RSA (Rivest, Shamir, Adleman, 1977)

Geração de chaves:

1. Gerar primos p e q com $k/2$ bits;
2. Calcular $N = pq$ e $\phi(N) = (p-1)(q-1)$;
3. Selecionar e tal que $mdc(e, \phi(N)) = 1$; (primo pequeno?)
4. Calcular d tal que $d = e^{-1} \bmod \phi(N)$;
5. $\mathcal{M} = \mathcal{C} = \mathbb{Z}_N$;
6. $K = (N, p, q, d, e)$.
7. Chave pública é (e, N), chave privada é (d, N, p, q).

Cifração: Calcular $Enc_K(x) = x^e \bmod N$;

Decifração: Calcular $Dec_K(y) = y^d \bmod N$.