UDESC

Teoria dos números

uber.renan@gmail.com

Departamento de Ciência da Computação
Centro de Ciências e Tecnológias
Universidade do Estado de Santa Catarina

4 de Novembro de 2016

Teoria dos Números

- Antigamente era chamada de Aritmética;
- Iniciou com Euclides em 300 B.C;
- Estuda os números inteiros;
- Atualmente possui aplicações diretas em criptografia;
    - Diffie-Hellman;
    - RSA;
    - Cusvas Ellipticas;

Números Primos

- Um número natural $n > 1$ é dito primo se ele é divisível apenas por 1 e n;
- Pode-se dizer ainda que se p é primo, para $p = a * b, a$ e $b \in \mathbb{N}, a < b$, segue que $a = 1$ e $b = p$;
- 1 não é primo;
- 0 não é primo;
- Existem infinitos números primos;
- Teorema fundamental da aritimética;

Testando números primos

Três abordagens:

- Teste de força bruta (ver código);
- Miller-Rabin;
- Crivo (ver outro código);

Divisibilidade

- a divide b, denotado por $a|b$, se $\exists b \in \mathbb{N}$ tal que $a = kb$;
- Segue que qualquer número possui 1 como seu menor divisor;
- Baseado na fatoração prima de pode-se construir a lista de todos os divisores de um número;
- Todo número $n \in \mathbb{N}$ pode ser escrito de forma única como $n = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * \ldots * p_m^{a_m}$, onde p_i é o i-ésimo primo;
- O total de fatores de um número é dado por $\prod_{i=1}^{m}(a_i + 1)$;
- Exemplo;

Maior divisor comum, MDC ou GCD

- O GDC de x e y é o maior natural k tal que $x = k * a$ e $y = k * b$, para algum $a, b \in \mathbb{N}$;
- Denotado por $gdc(x, y)$;
- Se $gdc(x, y) = 1$, então x e y são primos relativos;
- Se $x|y$, $gdc(x, y) = x$;
- Se $a = bt + r$ para $t, r \in \mathbb{N}$, então $gcd(a, b) = gcd(b, r)$;
- Com base nas observações acima, Eclides apresentou o que é aceito por muitos como o primeiro algoritmo da história: O algoritmo de euclides;
- Código;

Mínimo multiplo comum, MMC ou LCM

- Útil para detectar periodicidade simultanena de dois eventos periodiocos;
- Denotado por $lcm(x, y)$;
- Segue que $lcm(x, y) \geq max(x, y)$;
- Sabe-se que $x * y$ é um múltiplo de x e y, logo $lcm(x, y) \leq x * y$;
- Tem-se que $lcm(x, y) = \frac{x*y}{gcd(x,y)}$;
- Dijkstra tem um algoritmo que não utiliza multiplicação, evitando assim um possível *overflow*;

Aritmética modular

- $(x + y) \mod n = ((x \mod n) + (y \mod n) \mod n)$;
- $(x - y) \mod n = ((x \mod n) - (y \mod n) \mod n)$;
- $(x * y) \mod n = ((x \mod n) * (y \mod n) \mod n)$;
- Divisão é treta;
- $x^y \mod n = (x \mod n)^y \mod n$;
- Pode ser usado para determinar os ultimos digitos de um número;
- RSA e Diffie-Hellman;

Congruencias

- É uma forma de representar a aritmética modular;
- Por definição $a \equiv b \pmod{n}$ se $n | (a - b)$;
- Se $a \mod n = b$ então $a \equiv b \pmod{n}$;
- Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então $(a + c) \equiv (b + d) \pmod{n}$;
- Adição é uma adição com números negativos;
- Se $a \equiv b \pmod{n}$ então $a * d \equiv b * d \pmod{n}$
- Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então $(a * c) \equiv (b * d) \pmod{n}$;
- Quando que $2 * x \equiv 3 \pmod{9}$? E $2 * x \equiv 3 \pmod{4}$?

Equações Diofantinas

- São equações com o dominio limitado aos inteiros;
- $a^n + b^n = c^n$;
- Divisão é um problema;
- Décimo problema de Hilbert;
- Algumas possuem solução polinomial:
  - $ax - ny = b$;
  - $x^2 - ny^2 = \pm 1$;

Problemas do URI

URI

- 1381;
- 1807;
- 1221;
- 1760;
- 1308;

Project Euler

- 66;
- 108;
- 110;
- 142;
- 97;