Teoria dos números

André Gustavo dos Santos

Departamento de Informática
Universidade Federal de Viçosa

INF 333 - 2024/1

Introdução

Teoria dos números

- Talvez a área mais interessante da matemática
- A prova de Euclides da existência de infinitos primos permanece clara e elegante até hoje, mesmo depois de mais de 2.000 anos
- Questões aparentemente inocentes como se $a^n + b^n = c^n$ tem solução inteiras para a, b, c quando $n > 2$ se mostraram não tão inocentes... esse é o chamado teorema de Fermat que ficou anos sem resposta!

Introdução

Teoria dos números

- O estudo de inteiros é interessante porque representam quantidades concretas, e descobrir novas propriedades de inteiros abrem portas para outras descobertas
- Computadores são muito usados em pesquisa de teoria dos números. Cálculos com inteiros grandes requer eficiência. Vejamos alguns algoritmos eficientes.

Números primos

Número primo

Números naturais com apenas dois divisores, o 1 e ele mesmo.

Lista dos 25 primeiros primos

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 ...

1 não é primo pois só tem 1 divisor

2 é o único número par primo

Números primos

Teste de primalidade

Um número n é primo se não é divisível por nenhum dos valores de 2 a $n - 1$

Teste de primalidade (rápido)

Um número n é primo se não é divisível por nenhum dos valores de 2 a $\sqrt{n}$

Prova

- Suponha que n não seja primo, mas não tenha nenhum divisor $\leq \sqrt{n}$.
- Se n não é primo, ele tem algum divisor x.
- E como x é divisor, então $n = xy$ para algum y.
- Se n não tem nenhum divisor $\leq \sqrt{n}$ então $x > \sqrt{n}$ e $y > \sqrt{n}$.
- Mas aí $xy > \sqrt{n}\sqrt{n} > n$, uma contradição, pois $xy = n$
- Logo, ou n é primo ou tem algum divisor $\leq \sqrt{n}$. $\square$

Números primos - fatoração

Teorema fundamental da aritmética

Todo número inteiro pode ser expresso de uma única forma como produto de primos

Exemplos

- $105 = 3 \times 5 \times 7$
- $32 = 2 \times 2 \times 2 \times 2 \times 2$

*Esta lista de primos multiplicados é chamada **fatoração***

Note que a ordem não importa, mas multiplicidade sim

Números primos - fatoração

```
void prime_factorization(long x)
{
  long i; /* counter */
  long c; /* remaining product to factor */

  c = x;
  while ((c % 2) == 0) {
    cout << 2 << endl;
    c = c / 2;
  }

  i = 3;
  while (i <= (sqrt(c)+0.01)) {   /* +0.01 para evitar erro de precisao */
    if ((c % i) == 0) {
      cout << i << endl;
      c = c / i;
    }
    else
      i = i + 2;
  }

  if (c > 1) cout << c << endl;
}
```

Máximo Divisor Comum (MDC)

Definição

O MDC de dois números naturais é o maior de seus divisores.

Exemplos

- $mdc(24, 30) = 6$
- $mdc(75, 30) = 15$
- $mdc(50, 21) = 1$
- $mdc(12, 0) = 12$

Note que $mdc(n, 0) = n$ *para todo natural* $n > 0$

Máximo Divisor Comum (MDC)

Algoritmo de Euclides

```
long mdc(long a, long b)
{
  if (b==0)
    return a;
  else
    return mdc(b, a%b);
}
```

Exemplo: mdc(60,100) = mdc(100,60) = mdc(60,40)= mdc(40,20) = mdc(20,0) = 20

Mínimo Múltiplo Comum

Relação entre MDC e MMC

- $mmc(a, b) \times mdc(a, b) = a \times b$

Portanto, $mmc(a, b) = a(b/mdc(a, b))$

Note a divisão primeiro, para evitar overflow em ab

MDC, MMC e Fatoração

Propriedades

- $mmc(a, b)$ é a "união" dos fatores primos comuns
- $mdc(a, b)$ é a "interseção" dos fatores primos comuns

Exemplo

- $100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$
- $120 = 2 \times 2 \times 2 \times 3 \times 5 = 2^3 \times 3 \times 5$
- $mmc(100, 120) = 2 \times 2 \times 2 \times 3 \times 5 \times 5 = 2^3 \times 3 \times 5^2 = 600$
- $mdc(100, 120) = 2 \times 2 \times 5 = 2^2 \times 5 = 20$

Máximo Divisor Comum (euclides estendido)

Algoritmo de Euclides estendido

Além de fornecer o MDC entre a e b, fornece também coeficientes x e y que satisfazem $ax + by = mdc(a, b)$

Exemplo

- $25x + 18y = 1$
- O algoritmo fornece a solução $x = -5, y = 7$

Máximo Divisor Comum (euclides estendido)

```
long mdc(long p, long q, long *x, long *y)
{
 long x1,y1;     /* coeficientes anteriores */
 long m;         /* valor do mdc(p,q) */

 if (q > p) return mdc(q,p,y,x);

 if (q == 0) {
    *x = 1;
    *y = 0;
    return p;
 }

 m = mdc(q, p%q, &x1, &y1);
 *x = y1;
 *y = (x1 - floor(p/q)*y1);
 return m;
}
```

Além de retornar o mdc de p e q, encontra x e y tal que $px + qy = mdc(p, q)$

Máximo Divisor Comum (euclides estendido)

Equação Diofantina

Equação em que as incógnitas só podem assumir valores inteiros

Equação Diofantina Linear (de 2 variáveis)

- $ax + by = c$
- Tem solução se e somente se $mdc(a, b)$ é divisor de c

Exemplo

Uma compra contendo maçãs e laranjas deu um total de R$8,39. Sabe-se que uma maçã custa 25 centavos e uma laranja 18. Quantas de cada fruta havia na compra?

- A resposta é solução da equação diofantina $25x + 18y = 839$

Máximo Divisor Comum (euclides estendido)

Solução

- Achar uma solução inteira para $25x + 18y = 839$
- Resultado do algoritmo euclides estendido:
  - $mdc(25, 18) = 1, x = -5, y = 7$
- Como 1 é divisor de 839, então há solução:
  - Pelo resultado do algoritmo de euclides estendido temos que...
  - $25 \times -5 + 18 \times 7 = 1$
  - Multiplicando por $839/mdc(25, 18)$ temos que
  - $25 \times -4195 + 18 \times 5873 = 839$
  - Então $x = -4195$ e $y = 5873$ é uma solução

Máximo Divisor Comum (euclides estendido)

Outras soluções

- Soluções alternativas podem ser encontradas com
  - $x' = x + b/mdc(a, b) \times n$
  - $y' = y - a/mdc(a, b) \times n$
  - sendo n um inteiro qualquer
- Para $n = 0$ temos a solução anterior
  - $(x', y') = (-4195, 5873)$
- Para $n = 1, 2, 3$ temos respectivamente
  - $(x', y') = (-4177, 5848), (-4159, 5823), (-4141, 5798)$
- Particularmente, $n = 234$ dá a única solução não negativa
  - $(x', y') = (17, 23)$
  - Então a compra tinha 17 maçãs e 23 laranjas

Números primos entre si

Definição

Dois números inteiros a e b são primos entre si se $mdc(a, b) = 1$

ou seja, se o único divisor comum é 1

Exemplos

- 10 e 21 são primos entre si
- 10 e 20 não são primos entre si

Função totiente de Euler

Definição

A função totiente, representada por $\varphi(n)$, conta o número de inteiros $< n$ relativamente primos com n

Exemplo

- $\varphi(36) = 12$ $\quad (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35)$

Produto de Euler para cálculo de $\varphi(n)$

$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ *Obs.: $p|n$ significa p é divisor de n*

Exemplo

- $36 = 2^2 \times 3^2$
- $\varphi(36) = 36 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 12$

Aritmética modular

Adição

$$(a+b)\%n = ((a\%n) + (b\%n))\%n$$

Subtração

$$(a-b)\%n = ((a\%n) - (b\%n))\%n$$

Se der negativo somar n até ficar positivo

Multiplicação

$$(ab)\%n = ((a\%n)(b\%n))\%n$$

Divisão

— *não é tão simples quanto as demais*

Exponenciação

$$(a^b)\%n = ((a\%n)^b)\%n$$

Aritmética modular

Dica

- Se a questão pede um resultado $\%n$, use aritmética modular para evitar overflow nos valores intermediários.
- Mesmo que o resultado final caiba na variável, certifique-se que os valores intermediários também caberão, usando $\%n$ em toda adição, subtração e multiplicação

Aritmética modular

Exemplo

Recebi $\$123,45$ de uma pessoa e $\$94,67$ de outra. Quantos centavos no total?

São $(12345 + 9467)\%100 = (12345\%100 + 9467\%100)\%100 = (45 + 67)\%100 = 12$

Exemplo

De $\$123,45$ gastei $\$81,53$. Quantos centavos no valor que resta?

São $(12345 - 8153)\%100 = (12345\%100 - 8153\%100)\%100 = (45 - 53)\%100 = 92$

Como daria negativo, somar 100 ao -8 e achará 92

Exemplo

Recebo $\$17,28$ por hora, e trabalhei 2.143 horas. Quantos centavos no total?

São $(1728 \times 2143)\%100 = (1728\%100 \times 2143\%100)\%100 = (28 \times 43)\%100 = 4$

Aritmética modular

Exemplo

Qual o último dígito de 2^{100} ?

Isso é o mesmo que $2^{100}\%10$

$2^4\%10 = 16\%10 = 6$
$2^8\%10 = ((2^4)^2)\%10 = ((2^4\%10)^2)\%10 = (6^2)\%10 = 36\%10 = 6$
$2^{16}\%10 = ((2^8)^2)\%10 = (6^2)\%10 = 6$ $2^{32}\%10 = ((2^{16})^2)\%10 = (6^2)\%10 = 6$
$2^{64}\%10 = ((2^{32})^2)\%10 = (6^2)\%10 = 6$

$2^{100}\%10 = (2^{64}2^{32}2^4)\%10 = (6 \times 6 \times 6)\%10 = (36 \times 6)\%10 = (6 \times 6)\%10 = 6$