Capítulo 6

Introdução a Teoria dos Números

Plano de Curso

- Números Primos e Relativamente Primos
- Aritmética Modular
- Teorema de Euler e Fermat
- Teste da Primalidade
- Algoritmo de Euclides - gcd
- Teorema Chinês do Resto
- Logaritmos Discretos

Divisores

Diz-se que **b ≠ 0** divide **a** se **a = mb**, onde **a**,**b** e **m** são inteiros

a	**b**
0	**m**

Relações que se mantém:

- Se **a|1**, então **a = ±1**
- Se **a|b** e **b|a**, então **a = ±b**
- Qualquer **b≠0** divide **0**
- Se **b|g** e **b|h**, então **b|(mg+nh)** para arbitrários **m** e **n**

Exemplo:

b=7; **g=14**; **h=63**; **m=3**; **n=2**
7|14 e 7|63 => 7|(3x14+2x63)
Tem-se que (3x14+2x63) = 7(3x2+2x9)
Então 7|7(3x2+2x9)

Números Primos

Qualquer inteiro **p>1** é um número primo <u>se e somente se</u> seus únicos divisores são **±1** e **±p**

Qualquer inteiro **a > 1** pode ser fatorado, de forma única, como:

$$\mathrm{a} = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$$

Onde: $p_1 > p_2 > \ldots p_t$ são números primos

$$\alpha_i > 0$$

$$\mathrm{a} = \prod_{\mathrm{P}} p^{a_p}, \quad a_p \geq 0$$

Conjunto dos Números Primos

91=7x13; 11011=7x11^2x13

24200=$2^3 3^0 5^2 7^0 11^2$

Representação dos Números Primos

$12 = \{a_2=2, a_3=1\}$
$18 = \{a_2=1, a_3=2\}$

Multiplicação = Soma dos correspondentes expoentes

$$k = mn \rightarrow k_p = m_p + n_p \quad \text{para todo } p$$

$k = 12x18 = 216$
$k_2 = 2+1=3;\ k_3 = 1+2 = 3$
$216 = 2^3x3^3$

$$a|b \rightarrow a_p \leq b_p \quad \text{para todo } p$$

$a = 12;\ b = 36;\ 12|36;\ 12 = 2^2 \times 3;\ 36 = 2^2 \times 3^2$
$a_2 = 2 = b_2$
$a_3 = 1 \leq 2 = b_3$

Números Relativamente Primos

c = mdc(a,b) = Maior Divisor Comum de **a** e **b**

c é um divisor de **a** e de **b**
Qualquer divisor de **a** e **b** é um divisor de **c**

mdc(a,b)=max[**k**, tal que **k**|**a** e **k**|**b**

mdc(a,b) = mdc(a,-b) = mdc(-a,b) = mdc(-a,-b)

mdc(60,24) = mdc(60,-24) = 12
mdc(a,0) = |a|

$300 = 2^2 \times 3^1 \times 5^2$
$18 = 2^1 \times 3^2$
$\gcd(18,300) = 2^1 \times 3^1 \times 5^0 = 6$

$\mathbf{k} = \mathbf{mdc(a,b)} \rightarrow \mathbf{k_p} = \min(\boldsymbol{a_p},\boldsymbol{b_p})$ para todo $\boldsymbol{p}$

mdc(a,b) = 1

8 e 15 são relativamente primos
8 = 1 x 2 x 4
15 = 1 x 3 x 5

Aritmética Modular

Dois inteiros **a** e **b** são congruentes módulo **n** se

(a mod n) = (b mod n)

ou

$a \equiv b \bmod n$

Exemplo:

$73 \equiv 4 \bmod 23$; $21 \equiv -9 \bmod 10$

Propriedades

- $a \equiv b \bmod n$ se $n \mid (a-b)$
- $(a \bmod n) = (b \bmod n)$ implica $a \equiv b \bmod n$
- $a \equiv b \bmod n$ implica $b \equiv a \bmod n$
- $a \equiv b \bmod n$ e $b \equiv c \bmod n$ implica $a \equiv c \bmod n$

$23 \equiv 8 \bmod 5$ porque $23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \bmod 8$ porque $-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 \bmod 27$ porque $81 - 0 = 81 = 27 \times 3$

Exponenciação

$11^7 \bmod 13$

$11^2 = 121 \equiv 4 \bmod 13$

$11^4 = 4^2 \equiv 3 \bmod 13$

$11^7 = 11 \text{ x } 4 \text{ x } 3 \equiv 2 \bmod 13$

Propriedades da Aritmética Modular

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Exercício:
11 mod 8 = 3;   15 mod 8 = 7

Propriedades da Aritmética Modular

- Comutativa
  - $(w + x) \bmod n = (x + w) \bmod n$
  - $(w \times x) \bmod n = (x \times w) \bmod n$
- Associativa
  - $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
  - $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
- Distributiva
  - $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
- Identidades
  - $(0 + w) \bmod n = w \bmod n$
  - $(1 \times w) \bmod n = w \bmod n$
- Aditiva Inversa
  - $w \in Z_n$, existe z tal que $w + z \equiv 0 \bmod n$

$Z_n = \{0,1, \ldots (n-1)\}$

Peculiaridades

- Se $(a+b) \equiv (a+c) \bmod n$ então $b \equiv c \bmod n$
  - $(5 + 23) \equiv (5 + 7) \bmod 8$; $23 \equiv 7 \bmod 8$
- Se $(a \times b) \equiv (a \times c) \bmod n$ então $b \equiv c \bmod n$
  - se **a** é relativamente primo a **n**
  - $6 \times 3 = 18 \equiv 2 \bmod 8$ e $6 \times 7 = 42 \equiv 2 \bmod 8$ mas

    $3 \not\equiv 7 \bmod 8$

Multiplicativa Inversa: Para cada $w \in Z_p$, existe z tal que $w \times z \equiv 1 \bmod p$

Teorema de Fermat

Se p é primo e a inteiro positivo não divisível por p

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

$a = 7, p = 19$
$7^2 = 49 \equiv 11 \bmod 19$
$7^4 \equiv 121 \equiv 7 \bmod 19$
$7^8 \equiv 49 \equiv 11 \bmod 19$
$7^{16} \equiv 121 \equiv 7 \bmod 19$
$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \bmod 19$

Se **p** é primo e **a** um inteiro positivo

$$\boxed{a^p \equiv a \bmod p}$$

$p = 5, a = 3, 3^5 = 243 \equiv 3 \bmod 5$
$p = 5, a = 10, 10^5 = 100000 \bmod 5 \equiv 0 \bmod 5$

Função Totiente de Euler

ϕ(n) é
Número de Inteiros positivos menores que **n** e relativamente primos a **n**

Se p e q são primos então **$\phi(p) = p-1$ e $\phi(q) = q-1$**

$\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$

$\phi(21) = 12 = \phi(3)\phi(7) = 2 \times 6 = (3-1)(7-1)$
onde os 12 inteiros são {1,2,4,5,8,10,11,13,16,17,19,20}

Teorema de Euler

$a^{\phi(n)} \equiv 1 \bmod n$

Com **a** e **n** relativamente primos

$a = 3; n = 10; \phi(10) = 4; 3^4 = 81 \equiv 1 \bmod 10$
$a = 2; n = 11; \phi(11) = 10; 2^{10} = 1024 \equiv 1 \bmod 11$

Forma alternativa para o TeoremaEuler

$a^{\phi(n)+1} \equiv a \bmod n$