Teoria dos Números

Divisão Inteira

Como calcular o quociente e o resto de uma divisão inteira? Por exemplo, calcular o quociente e o resto da divisão inteira de 1025 por 34.

1. $1025 : 34 = 30,14705882 \Leftarrow$ quociente$= 30$.
2. resto$= 1025 - 30 \times 34$.

Algoritmo de Euclides

O Algoritmo de Euclides serve para determinar o máximo divisor comum de dois números inteiros.

Exemplo. Determinar o máximo divisor comum de 17154 e 357, mdc(17154,357).

dividendo	divisor	resto	quociente
17154	357	18	48
357	18	15	19
18	15	**3**	1
15	**3**	0	5

O máximo divisor comum é o último resto diferente de zero.

Números Primos

Definição. Um número inteiro $p > 1$ é primo se só é divisível por 1 e por ele próprio.

Teorema. Todo o número natural (diferente de 1) escreve-se de forma única como um produto de números primos.

Este Teorema é conhecido por Teorema Fundamental da Aritmética.

Exemplos: $108 = 2^2 \times 3$; $225 = 3^2 \times 5^2$; $3260 = 2^2 \times 163$.

Definição. Dois números naturais a e b são primos entre si se mdc(a, b)=1.

Quaisquer dois números primos são primos entre si, mas o recíproco não é verdadeiro.

Congruências

<u>Definição.</u> Seja m um número natural. Dois números a e b são *congruentes módulo* m se $a - b$ é divisível por m. Escreve-se $a \equiv b \pmod{m}$.

Proposição. $a \equiv b \pmod{m}$ se e só se a e b têm o mesmo resto na divisão por m.

Exemplos: $13 \equiv 1751 \pmod{2}$; $352 \equiv 1272 \pmod{10}$; $5 \equiv 19 \pmod{7}$.

Somas, produtos e potências módulo m.

- $a \underset{m}{\oplus} b = r$ se r é o resto da divisão de $a + b$ por m. (Lê-se a mais b módulo m.)

- $a \underset{m}{\otimes} b = s$ se s é o resto da divisão de $a \times b$ por m. (Lê-se a vezes b módulo m.)

- $a \overset{b}{\underset{m}{\otimes}} = t$ se t é o resto da divisão de a^b por m. (Lê-se a elevado a b módulo m.)

Exemplos:

$$3 \underset{8}{\oplus} 7 = 2; \qquad 59 \underset{100}{\oplus} 73 = 32;$$

$$59 \underset{60}{\otimes} 7 = 53; \qquad 7 \underset{13}{\otimes} 11 = 2;$$

$$2 \overset{9}{\underset{7}{\otimes}} = 1; \qquad 63 \overset{3}{\underset{17}{\otimes}} = 11.$$