Teorema 1.3.7: (Teorema Fundamental da Aritmética)

Todo o número inteiro maior do que um pode ser escrito como um produto de números primos (com um só factor, no caso do número ser primo). Além disso, uma tal decomposição em números primos é essencialmente única, i.e. duas decomposições apenas diferem na ordem pela qual os primos são escritos.

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \qquad p_1, p_2, \ldots, p_k \text{ são números primos}$$

Exemplo: Escrever n=51975 como o produto de números primos.

Decompor em factores primos

51975	3
17325	3
5775	5
1155	3
385	5
77	11
7	7
1	

51975 = 3x3x3x5x5x11x7

$= 3^3.5^2.11.7 = 5^2.3^3.\ 7.11$

$= 3^3.5^2.\ 7.11$

forma standard de n

(Base crescente)

Teorema 1.3.8:

Sejam

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \quad e \quad n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

($k \in \mathbb{N}$), em que $p_1 < p_2 < \cdots < p_k$ são números primos e s_i e t_i são números inteiros não negativos, para $i = 1, 2, \ldots, k$. Sejam

$$u_i = min\{s_i, t_i\} \quad e \quad v_i = max\{s_i, t_i\},$$

para qualquer $i = 1, 2, \ldots, k$. Então:

1. $mdc\{m, n\} = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$;
2. $mmc\{m, n\} = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$.

Exemplo:

$mmc\{32, 60\} =$

32	2
16	2
8	2
4	2
2	2
1	

$32 = 2^5$

$mdc\{32, 60\} =$

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \times 3 \times 5$

Teorema 1.3.8:

Sejam

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \quad e \quad n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

($k \in \mathbb{N}$), em que $p_1 < p_2 < \cdots < p_k$ são números primos e s_i e t_i são números inteiros não negativos, para $i = 1, 2, \ldots, k$. Sejam

$$u_i = min\{s_i, t_i\} \quad e \quad v_i = max\{s_i, t_i\},$$

para qualquer $i = 1, 2, \ldots, k$. Então:

1. $mdc\{m, n\} = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$;
2. $mmc\{m, n\} = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$.

Exemplo:

$mmc\{32, 60\} = 2^5 \times 3^1 \times 5^1$

$mdc\{32, 60\} = 2^2 \times 3^0 \times 5^0$

32	2
16	2
8	2
4	2
2	2
1	

$32 = 2^5 \times 3^0 \times 5^0$

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \times 3 \times 5$

Hoje em dia são conhecidos inúmeros resultados importantes sobre números primos que não permitem no entanto caracterizar todos estes números.

Teorema 1.3.9: Todo o número primo maior que 2 é da forma $4n \pm 1$, com n um natural.

Demonstração.

Seja p um número primo. Pelo algoritmo da divisão, existem inteiros m e r tais que

$$p = 4m + r, \quad 0 \leq r < 4.$$

Assim, $r = 0, 1, 2, 3$. É fácil concluir que se p é primo então $r \neq 0$ e $r \neq 2$. Se p é primo então é da forma

$$p = 4m + 1 \text{ com } m \in \mathbb{N}$$

ou

$$p = 4m + 3 = 4m + 3 - 4 + 4 = 4\underbrace{(m+1)}_{n \in \mathbb{N}} - 1. \square$$

Questão: O número 79 é primo?

Como 79=4x20-1 então o resultado anterior não permite decidir se é ou não primo.

Teorema 1.3.10:

Se $n \geq 2$ não é um número primo, então existe um número primo p tal que $p|n$ e $p^2 \leq n$.

Prova. Como $n \geq 2$ e n não é primo, então $n = pqa$, com p e q primos tais que $p \leq q$ e $a \in \mathbb{N}$. Donde $p^2 \leq pq \leq n$.

Questão: O número 79 é primo?

Se 79 não fosse primo, pela propriedade anterior, teria de existir um número primo p divisor de 79 tal que $p^2 \leq 79$. Como $11^2 = 121 > 79$, então $p \in \{2, 3, 5, 7\}$. Mas nenhum destes quatro primos é divisor de 79.

1.4 Congruências lineares

Sejam $n \in \mathbb{N}$ e R a relação de congruência módulo n (sobre $\mathbb{Z}$). X= $\mathbb{Z}$

aRb se e só se $(\exists k \in \mathbb{Z})\, a - b = kn.$

a- b é múltiplo n

$a \equiv b \pmod{n}$

a é congruente com b módulo n

É uma relação de equivalência

classe (de congruência) módulo n de $a \in \mathbb{Z}$ (classe de equivalência de a)

$$[a]_n = \{\ldots,\ a-2n,\ a-n,\ a,\ a+n,\ a+2n,\ldots\} = a + n\mathbb{Z}.$$

Exemplos: Para $n = 4$,

- $[0]_4 = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8,\ldots\} = 4\mathbb{Z}$;
- $[1]_4 = \{\ldots,\ -7,\ -3,\ 1,\ 5,\ 9,\ldots\} = 1 + 4\mathbb{Z}$;
- $[2]_4 = \{\ldots,\ -6,\ -2,\ 2,\ 6,\ 10,\ldots\} = 2 + 4\mathbb{Z}$;
- $[3]_4 = \{\ldots,\ -5,\ -1,\ 3,\ 7,\ 11,\ldots\} = 3 + 4\mathbb{Z}$.

O conjunto quociente $\mathbb{Z}/R$ com R a relação $\equiv (\mathrm{mod}\ n)$ designa-se por

$$\mathbb{Z}/R = \mathbb{Z}_n$$

diz-se o "Conjunto dos inteiros módulo n"

Ora,

$$\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\} = \{[0]_n, [1]_n, [2]_n, [3]_n, \ldots, [n-1]_n\}$$

Se $a \in \mathbb{Z}$ então, aplicando o algoritmo da divisão,

$$a = nq + r, \quad 0 \leq r < n.$$

$$\Updownarrow$$

$$a - r = nq \text{ (múltiplo de n)}$$

$$\Updownarrow$$

$$a \equiv r (\mathrm{mod}\ n)$$

$$\Updownarrow$$

$$[a]_n = [r]_n$$

Teorema 1.4.1: *Seja* $n \in \mathbb{N}$.

Então cada inteiro é congruente módulo n precisamente com um dos inteiros $0,\ 1,\ 2, \ldots,\ n-1$, *i.e.*

$$\mathbb{Z}_n = \{[0]_n,\ [1]_n, \ldots,\ [n-1]_n\}.$$

Exemplo: n=4.

Qual a classe de congruência de 25?

25=4x6+1 $\Rightarrow\ [25]_4 = [1]_4$ **"25 é congruente módulo 4 com 1"**

Qual a classe de congruência de -201?

$$\begin{aligned} 201 = 4\times 50+1 \Rightarrow\ -201 &= -4\times 50-1 \\ &= 4(-50)-1+4-4 \\ &= 4(-51)+3 \ \Rightarrow\ [-201]_4 = [3]_4 \end{aligned}$$

"-201 é congruente módulo 4 com 3"