- Critério de divisibilidade por 6

$$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 + a_0$$

$$a_0 \equiv a_0 \pmod 6$$

$$10 \equiv 4 \pmod 6$$
$$10^2 \equiv 16 \pmod 6 \Rightarrow 10^2 \equiv 4 \pmod 6$$
$$10^3 \equiv 40 \pmod 6 \Rightarrow 10^3 \equiv 4 \pmod 6$$

É facil concluir que $10^i \equiv 4 \pmod 6$ $i \in \mathbb{N}$

Então

$$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv 4(a_n + a_{n-1} + \cdots + a_2 + a_1) + a_0 \pmod 6$$

- Critério de divisibilidade por 8

$$10 \equiv 2 \pmod 8$$
$$10^2 \equiv 4 \pmod 8$$
$$10^3 \equiv 40 \pmod 8 \Rightarrow 10^3 \equiv 0 \pmod 8$$
$$\Rightarrow 10^i \equiv 0 \pmod 8, \quad \forall i \in \mathbb{N} \text{ com } i \geq 3$$

$$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} = a_0 + 2a_1 + 4 \times a_2 \pmod 8$$

- Critério de divisibilidade por 7

$$1 \equiv 1 \pmod 7$$
$$10 \equiv 3 \pmod 7$$
$$10^2 \equiv 2 \pmod 7$$
$$10^3 \equiv 20 \pmod 7 \Rightarrow 10^3 \equiv -1 \pmod 7$$
$$10^4 \equiv -10 \pmod 7 \Rightarrow 10^4 \equiv -3 \pmod 7$$
$$10^5 \equiv -30 \pmod 7 \Rightarrow 10^5 \equiv -2 \pmod 7$$
$$10^6 \equiv -20 \pmod 7 \Rightarrow 10^6 \equiv 1 \pmod 7$$
$$10^7 \equiv 10 \pmod 7 \Rightarrow 10^7 \equiv 3 \pmod 7 \quad \cdots$$

Então:

$$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} = (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5)$$
$$+ (a_6 + 3a_7 + 2a_8) - (a_9 + 3a_{10} + 2a_{11}) + \cdots$$
$$\pmod 7$$

Exemplo:

$$157 \equiv 7+3\times 5+2\times 1 \pmod 7$$
$$\equiv 24 \pmod 7 \equiv 4+3\times 2 \pmod 7 \equiv 10 \pmod 7$$
$$\equiv 0+3\times 1 \pmod 7 \equiv 3 \pmod 7$$

$$791 \equiv 1+3\times 9+2\times 7 \pmod 7 \equiv 42 \pmod 7 \equiv 0 \pmod 7$$

$$3739 \equiv 9+3\times 3+2\times 7-3 \pmod 7 \equiv 29 \pmod 7$$
$$\equiv 9+3\times 2 \pmod 7 \equiv 15 \pmod 7 \equiv 1 \pmod 7$$

Se apenas pretendemos saber se $7 \mid a$ ou $7 \nmid a$ temos um critério "mais simples"

Suponhamos $a = 10x+y$

$$10x+y \equiv 0 \pmod 7 \iff 10x+y-21y \equiv 0 \pmod 7$$
$$\iff 10x-20y \equiv 0 \pmod 7$$
$$\iff 10(x-2y) \equiv 0 \pmod 7$$
$$\iff x-2y \equiv 0 \pmod 7$$

Conclusão: $10x + y$ é divisível por 7 sse $x - 2y$ é divisível por 7

Atenção: apenas válido quando o resto na divisão por 7 é 0!

Exemplo: Resto da divisão de 48 por 7

$48 = 7 \times 6 + 6 \implies 48 \equiv 6 \pmod 7$

$48 = 4 \times 10 + 8 \longrightarrow 4 - 2 \times 8 \longrightarrow -12$

mas $-12 \equiv \underline{\underline{2}} \pmod 7$

Exemplo: $154 \longrightarrow 4 + 15 \times 10 \longrightarrow 15 - 2 \times 4 = 7$

Logo $7 \mid 154$

Exemplo: $3738 = 8 + 10 \times 373 \longrightarrow 373 - 2 \times 8 = 357$

$\longrightarrow -2 \times 7 + 35 \longrightarrow 21$

Logo como $7 \mid 21$ então $7 \mid 3738$

Função de Euler

Def: Para cada $n \geq 1$, seja $\phi(n)$ o número de naturais k com $k \leq n$ tais que $m.d.c(k, n) = 1$.

À função $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ chamamos função de Euler.

Exemplo:

$\phi(1) = 1$ $\quad$ $\phi(3) = 2$ $\quad$ $\phi(5) = 4$

$\phi(2) = 1$ $\quad$ $\phi(4) = 2$ $\quad$ $\phi(6) = 2$

NOTAS: É claro que $\phi(n) \leq n-1$

Se n é primo $\phi(n) = n-1$

Se n não é primo $\phi(n) \leq n-2$.

Lema: $p \in \mathbb{N}$, p é primo sse $\phi(p) = p-1$

Lema: $p \in \mathbb{N}$, p primo, $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

Lema: Sejam $m, n \in \mathbb{N}$ com $m.d.c(m, n) = 1$ então $\phi(mn) = \phi(m)\phi(n)$

Exemplo $\phi(60) = \phi(4 \times 3 \times 5) = \phi(4 \times 3)\,\phi(5) = \phi(4)\,\phi(3)\,\phi(5)$
$= 2 \times 2 \times 4 = 16$

Teorema Seja $n \in \mathbb{N}$ e $n = p_1^{k_1}\, p_2^{k_2} \cdots p_r^{k_r}$ a decomposição de n em fatores primos

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Teorema de Euler: $a^{\phi(n)} \equiv 1 \pmod{n}$

NOTA: generaliza o PTF

Exemplo: $a^2 \equiv 1 \pmod{6}$ $\qquad \phi(6) = 2$

Teorema de Wilson Se p é primo então $(p-1)! \equiv -1 \pmod{p}$

Teorema de Lagrange: Se n é tal que $(n-1)! \equiv -1 \pmod{n}$ então n é primo.

Exemplo: Resto da divisão de $12!$ por 13 é 12.

Pelo teorema de Wilson $12! \equiv -1 \pmod{13}$

logo $12! \equiv 12 \pmod{13}$

ou aplicando a técnica do inverso modular

$\underline{2} - \underline{3} - \underline{4} - \underline{5} - 6 - \underline{7} - \underline{8} - \underline{9} - \underline{10} - 11$

$$\left.\begin{aligned} 2\times 7 &\equiv 1 \pmod{13} \\ 3\times 9 &\equiv 1 \pmod{13} \\ 4\times 10 &\equiv 1 \pmod{13} \\ 5\times 8 &\equiv 1 \pmod{13} \\ 6\times 11 &\equiv 1 \pmod{13} \end{aligned}\right\} \Rightarrow 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10\times 11$$

$$\equiv 1 \pmod{13}$$

$$\Rightarrow 11! \equiv 1 \pmod{13}$$

$$\Rightarrow 12! \equiv 12 \pmod{13}$$