# TEOREMA DOS RESTOS CHINÊS

→ sistemas de congruências:

$N \equiv 2 \pmod 3$ e $N \equiv 1 \pmod 4$

$N = 3 \cdot q + 2$ (I)

substituindo na segunda relação:

$3q + 2 \equiv 1 \pmod 4$

$3q \equiv -1 \pmod 4$

$3q \equiv 3 \pmod 4$

Como $mdc(3,4) = 1$, vale fazer:

$\cancel{3}q \equiv \cancel{3} \pmod 4$

$q \equiv 1 \pmod 4$

$q = 4b + 1$, $b \in \mathbb{N}$ (III)

substituindo III em I:

$N = 3q + 2 \rightarrow N = 3 \cdot (4b+1) + 2$

$N = 12b + 5 \rightarrow N \equiv (5 \pmod{12})$

$N = 5 \pmod{12}$ → infinitas soluções

Teorema: Sejam $m_1, m_2 \cdots m_n$ primos entre si, o sistema:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_n \pmod n$

possui uma única solução módulo m. E $m = m_1 \cdot m_2 \cdot \cdots m_n$. Ou seja, existe uma solução x com $0 \leq x < m$. E todas as outras são congruentes mod m com essa solução.

exemplo:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

→ $m = 3 \cdot 5 \cdot 7 = 105$

$x \equiv 50 \pmod{105}$

$M_1 = 35$, $M_2 = 21$, $M_3 = 15$

(→ multiplicar os números primos)

calcular os inversos:

$y_1 \cdot M_1 \equiv 1 \pmod 3$

$y_2 \cdot M_2 \equiv 1 \pmod 5$

$y_3 \cdot M_3 \equiv 1 \pmod 7$

E chegaremos a fórmula geral:

$x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{105}$

solução:

$m = 5 \cdot 7 \cdot 3 = 105$

$M_1 = 35$ ; $M_2 = 21$ ; $M_3 = 15$

1.a) $y_1 M_1 \equiv 1 \pmod 3$

$y_1 \cdot 35 \equiv 1 \pmod 3$, $35 \equiv 2 \pmod 3$

$y_1 \cdot 2 \equiv 1 \pmod 3$ ($y_1 = 2 \pmod 3$)

1.b) $y_2 M_2 \equiv 1 \pmod 5$

$y_2 \cdot 21 \equiv 1 \pmod 5$, $21 \equiv 1 \pmod 5$

$y_2 \cdot 1 \equiv 1 \pmod 5$ ($y_2 \equiv 1 \pmod 5$)

1.c) $y_3 M_3 \equiv 1 \pmod 7$

$y_3 \cdot 15 \equiv 1 \pmod 7$, $15 \equiv 1 \pmod 7$

$y_3 \cdot 1 \equiv 1 \pmod 7$ ($y_3 \equiv 1 \pmod 7$)

Fórmula geral:

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{105}$

$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$

$x \equiv 233 \pmod{105}$, fora do mod

$x \equiv 23 \pmod{105}$. Resp: 23 //

## PEQUENO TEOREMA DE FERMAT

**Teorema:** se p é primo e a é um inteiro não divisível por p, então:

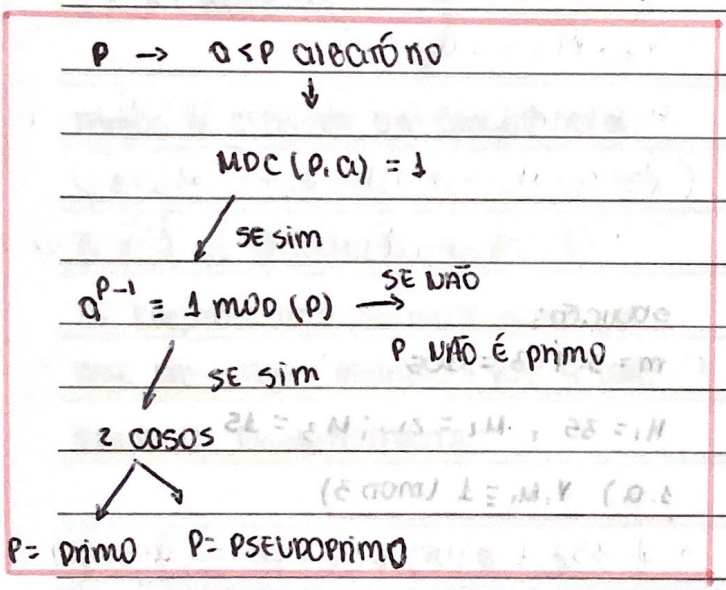
$$a^{p-1} \equiv 1 \pmod{p}$$

além disso, para todo inteiro a:

$$a^{p} \equiv a \pmod{p}$$

O primeiro formato ($a^{p-1} \equiv 1 \bmod p$) é para quando $mdc(a, p) = 1$.

Como seria um algoritmo de teste?




* pseudo primos são raros
* esse algoritmo é probabilístico (testa com vários valores de a)

**Exemplo:**

a) $3^{204}$ (mod 5)

pelo teorema: $a^{p-1} \equiv 1 \bmod p$, se p = primo.

e sabemos que $3^4 \equiv 1 \pmod 5$

$3^{204} \equiv (3^4)^{51} \equiv (1)^{51} \pmod 5 = 1$