Potências em Aritmética Modular: Teorema de Fermat

Teorema de Fermat: Se p é primo e a é primo com p,

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

Teorema de Fermat: Se p é primo,

$$\forall a,\ a^p \equiv a \mod p$$

$$8^{143} = 8^{14\times 10+3} = \left(8^{10}\right) 14 \times 8^3 \equiv 8^3 \mod 11$$

Potências em Aritmética Modular: Teorema de Fermat

Teorema de Fermat: Se p é primo e a é primo com p,

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

Teorema de Fermat: Se p é primo,

$$\forall a,\ a^p \equiv a \mod p$$

$$8^{143} = 8^{14\times 10+3} = \left(8^{10}\right) 14 \times 8^3 \equiv 8^3 \mod 11$$

$$8^3 = 64 \times 8 \equiv -2 \times 8 \equiv 6 \mod 11$$

Potências em Aritmética Modular: Teorema de Euler

$\mathbb{Z}_m^\times$ designa o conjunto das classes de congruência módulo m primas com m.

A função ϕ de Euler é definida como

$$\phi : \mathbb{N} \to \mathbb{N}, \qquad \phi(m) = \left|\mathbb{Z}_m^\times\right|$$

ou seja $\phi(m)$ é o número de classes de congruência módulo m primas com m.

Teorema de Euler: Se a é primo com m então

$$a^{\phi(m)} \equiv 1 \mod m$$

A Função ϕ de Euler

Se $m = p_1^{k_1} \cdots p_r^{k_r}$ for a factorização de m em factores primos,

$$\phi(m) = \phi\left(p_1^{k_1}\right) \cdots \phi\left(p_r^{k_r}\right).$$

$$\phi(p^k) = p^k - p^{k-1}$$

Portanto

$$\phi(m) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdots \left(p_r^{k_r} - p_r^{k_r-1}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Cálculo de potências

Calcular $3^{21} \mod 37$:

j	c	x	
21	3	1	$3^{21} =$
20	3	3	$= 3 \times 3^{20}$
10	9	3	$= 3 \times (3^2)^{10}$
5	7	3	$= 3 \times (3^4)^5$
4	7	21	$= (3 \cdot 3^4) \times (3^4)^4$
2	12	21	$= (3 \cdot 3^4) \times (3^8)^2$
1	33	21	$= (3 \cdot 3^4) \times 3^{16}$
0	33	27	$= 3 \cdot 3^4 \cdot 3^{16}$

Raízes mod m

$$x^k \equiv b \mod m$$

Se b é primo com m, e k é primo com $\phi(m)$, a equação tem solução única b^u onde u é um inteiro satisfazendo

$$ku \equiv 1 \mod \phi(m)$$

Exemplo: resolver $x^{43} \equiv 2 \mod 101$.

$mdc(2, 101) = 1$ e $mdc(43, \phi(101)) =$ (101 é primo!)
$= mdc(43, 100) = 1$, logo a equação tem solução única.

Pelo algoritmo de Euclides, $1 = -3 \times 100 + 7 \times 43$; logo a solução é

$$2^7 \equiv 27 \mod 101$$