Exemple (Exponentiation rapide) $3^{108} \bmod 7$

$108 \mid 2$ → 54, $x_0 = 0$
$54 \mid 2$ → 27, $x_1 = 0$
$27 \mid 2$ → 13, $x_2 = 1$
$13 \mid 2$ → 6, 1
$6 \mid 2$ → 3, 0
$3 \mid 2$ → 1, 1
$1 \mid 2$ → 0, 1

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 3^2 \bmod 7 = 2$
$3^4 \bmod 7 = 2^2 \bmod 7 = \boxed{4}$
$3^8 \bmod 7 = 4^2 \bmod 7 = 2$
$3^{16} \bmod 7 = 4$
$3^{32} \bmod 7 = 2$
$3^{64} \bmod 7 = 4$

b

$(108)_{10} = (x_0 x_1 \ldots x_5)_2 = (1101100)_2$

$$3^{108} = 3^{x_0\cdot 2^0 + x_1 \cdot 2^1 + x_2 \cdot 2^2 + \ldots} = \underbrace{3^{x_0\cdot 2^0}}_{1} \cdot 3^{x_1\cdot 2^1} \cdot \ldots \equiv_7 (3^1)^0 \cdot (3^2)^0 \cdot (3^{2^2})^1 \cdot (3^8)^1 \cdot (3^{16})^0 \cdot (3^{32})^1 \cdot (3^{64})^1$$

$3^{0\cdot 2^1} = 3^0 = 1$

$r =$ 1, 1, $\boxed{4}$, 2, 1, 2, 4

$r = r \cdot 1 = 1$

$r = 1 \cdot 4 \equiv_7 4$

$r = 4 \cdot 2 \equiv_7 1$

$r = 1 \cdot 1 \equiv_7 1$

$r = 1 \cdot 2 \equiv_7 2$

$r = 2 \cdot 4 \equiv_7 1$

Algorithme d'exponentiation rapide

Objectif : calculer $R = a^X \bmod N$ $\quad a, N \in \mathbb{Z}\ (\mathbb{N})$, $X \in \mathbb{N}$ Donnés

Pré-test

Si $a = 0 \Rightarrow R = 0$ STOP

$X = 0 \Rightarrow R = 1$ STOP

$N = 0$ ou $1 \Rightarrow$ STOP (pas de sens)

Initialisation

$r = 1$
$e = X$

$b = a \bmod N$
$i = 0$

Tant que e > 0 :

$X_i = e \bmod 2$

$e = e/2$ (DIVISION ENTIERE)

$r = (r \cdot b^{X_i}) \bmod N$

$b = b^2 \bmod N$

$i = i+1$

Fin

Résultat : $R = a^X \bmod N = \underline{\underline{r}}$

Exemple : $3^{108} \bmod 7$

$a = 3$
$X = 108$
$N = 7$

Init:
$i = 0$
$e = 108$
$b = 3 \bmod 7 = 3$
$r = 1$

i=0:
$X_0 = 108 \bmod 2 = \boxed{0}$
$e = 108 / 2 = 54$
$r = r \cdot b^{X_0} \bmod 7 = (1 \cdot 3^{\boxed{0}}) \bmod 7 = 1$
$b = b^2 \bmod 7 \equiv_7 3^2 \equiv_7 \underline{2}$ $\quad b = 3^{2^0} \bmod 7 = 3 \bmod 7$
$i = 0+1$

i=1:
$X_1 = 54 \bmod 2 = 0$
$e = 54 / 2 = 27$
$r = r \cdot b^{X_1} \bmod 7 = (1 \cdot 2^0) \bmod 7 = 1$
$b = b^2 \bmod 7 = 2^2 \bmod 7 = \underline{4}$ $\quad b = 3^{2^1} \bmod 7 = 3^2 \bmod 7$
$i = 1+1$

i=2:
$X_2 = 27 \bmod 2 = \boxed{1}$
$e = 27/2 = 13$
$r = r \cdot b^{X_2} \bmod 7 = 1 \cdot 4^{\boxed{1}} \bmod 7 = \underline{4}$
$b = b^2 \bmod 7 = 4^2 \bmod 7 = 2$ $\quad b = 3^{2^2} \bmod 7 = 3^4 \bmod 7$

$b = b^2 \bmod 7 = 4^2 \bmod 7 = \underline{2}$ $\quad b = 3^{2^2} \bmod 7 = 3^4 \bmod 7$

$i = 2+1$

i=3: $x_3 = 13 \bmod 2 = 1$

$e = 13/2 = 6$

$r = r \cdot b^{x_3} \bmod 7 = \underline{4} \cdot \underline{2}^1 \bmod 7 = 1$

$b = b^2 \bmod 7 = 2^2 \bmod 7 = 4$ $\quad b = 3^{2^3} \bmod 7 = 3^8 \bmod 7$

Inverse dans $\mathbb{R}$

Si $x \neq 0$ Alors x admet un inverse unique $x^{-1} = \frac{1}{x}$

$$x \cdot x^{-1} = 1$$

Inverse Modulaire Modulo N

$(N \in \mathbb{Z} \setminus \{0, 1, -1\})$ ⚠

Si a admet un inverse modulaire modulo N, alors

$$a \cdot a^{-1} \equiv_N 1$$

1. L'inverse de a existe toujours si $a \neq 0$ et si $PGCD(a, N) = 1$

$$PGCD(a,N) = 1 = a \cdot \underbrace{x}_{a^{-1}} + N \cdot y$$

$$1 \equiv_N (ax) \bmod N + \overbrace{(N \cdot y) \bmod N}^{0}$$

$$\equiv_N a \cdot x \quad \Rightarrow x \text{ est } \underline{\text{inverse}} \text{ de } a \,!$$

2. S'il existe un inverse de a mod N, alors il en existe une infinité !

$a \cdot x \equiv_N 1 \qquad a \cdot x + k \cdot N \equiv_N 1$

$x + k \cdot N$ est donc aussi inverse de a
$k \in \mathbb{Z}$

Exemple : Inverse de 2 modulo 3 ?

$2 \cdot x \equiv_3 1$

$2 \cdot 5 = 10 \equiv_3 1$
$2 \cdot 8 = 16 \equiv_3 1$
$2 \cdot (-1) = -2 \equiv_3 1$
$2 \cdot 2 \equiv_3 1$

2 est son propre inverse modulo 3.

3. Si l'inverse de a modulo N existe, il est UNIQUE dans 0,…,N-1

Donc, tous les inverses modulaires sont congruent au même inverse dans 0,…,N-1 !!!!

<u>Petit Théorème de Fermat (1601-1655)</u>

Si *p* est un nombre premier ($\mathbb{N}^* \setminus \{1\}$) alors pour tout nombre $a \in \mathbb{Z}$ non divisible par *p*, on a

1. $(a^p) \bmod p \equiv_p a \bmod p \qquad (a^p \equiv_p a)$
2. $(a^{p-1}) \bmod p \equiv_p 1$
3. Il existe un entier *k* tel que $a^k \bmod p = 1 \qquad$ ($k=p-1$ est l'un des candidats)

En plus, le plus petit de ces k non nul vérifiant l'égalité est un diviseur de *p-1*.

Exemples : p = 5 et a=8

p est premier ✓

p ne divise pas a ✓

$$a^p = \underbrace{8^5}_{32768} \equiv_5 \underbrace{8 \bmod 5}_{3}$$

$32768 \equiv_5 3 = 3$

$8^5 \equiv_5 8$ ✓

$8^{5-1} = 4096 \equiv_5 1$ ✓

$8^4 \equiv_5 1$ → c'est le plus petit et 4 divise $5-1=4$!

$8^1 \equiv_5 3$

$8^2 \equiv_5 4$

$8^3 \equiv_5 3 \cdot 4 \bmod 5 \equiv_5 2$

Indice d'Euler : $\varphi(n)$ par $n \in \mathbb{N}^*$

Correspond au nombre de facteurs entre 1 et N-1 qui sont premiers avec n.

Alors (découle du petit Th. De Fermat) si PGCD(a,n) = 1, alors

$$\boxed{a^{\varphi(n)} \equiv_n 1}$$

Exemple : a = 8, p=n=5

$\varphi(n)$ = nombre de facteurs premiers

PGCD(1,5) = 1 ✓

PGCD(2,5) = 1 ✓

(3,5) = 1 ✓

(4,5) = 1 ✓

$\varphi(5) = 4$

$(4,5) = 1$ ✓

$(5,5) = 5$ ✗

$\varphi(n)$ = nombre de facteurs premiers entre 8 et 5

compris entre 1 et 5

$$8^4 = 4096 \equiv_5 1 \quad !$$

Si n est un nombre premier, alors $\varphi(n) = n-1$ (seul n divise n !)

tous les autres vérifient $PGCD(x,n) = 1$!