MATIN Cours du 30.11.2020

lundi, 30 novembre 2020 08:20

Exponentiation rapide

But : calculer $R = a^X \bmod N \quad a, X, N \in \mathbb{N}^*$

($a \in \mathbb{Z}$ possible et $N \in \mathbb{Z}$ possible
$X \notin \mathbb{Z}$! $X \in \mathbb{N}^*$)

Algorithme :

```
Si a = 0 =>   R = 0
Si x = 0 =>   R = 1
Sinon, pose r = 1, e = X et b = a mod N

  Tant que e > 0 :
    x_i = e mod 2
    si x_i == 1 alors:
        r = (r · b) mod N        } r = (r · b^{x_i}) mod N
    end
    b = (b^2) mod N
    e = e/2 (partie entière !!)
  Fin
  Réponse   a^x mod N = r
```

$X \,|\, 2$; $x_0 \,|\, q_0 \,|\, 2$; $x_1 \,|\, q_1 \,|\, 2$; $x_2 \,|\, q_2$

$X = x_0 \cdot 2^0 + x_1 \cdot 2^1 + \ldots$

$a^X \equiv_N a^{x_0 \cdot 2^0 + x_1 \cdot 2^1 + \ldots}$

$\equiv_N a^{x_0 \cdot 2^0} \cdot (a^{x_1 \cdot 2^1}) \cdot (a^{x_2 \cdot 2^2}) \ldots$) mod N

$\equiv_N \underbrace{a^{x_0}}_{} \cdot (a^2)^{x_1} \cdot (a^4)^{x_2} \ldots$

$x_0 = 1 \downarrow$ $\quad x_0 = 0 \downarrow$

$a \cdot \quad 1$

mod N

$a^x \equiv_N \underbrace{a^{x_0} \bmod N}_{1 \text{ si } x_0 = 0} \cdot \underbrace{(a^2)^{x_1} \bmod N}_{1 \text{ si } x_1 = 0} \cdot (a^4)^{x_2} \bmod N \ldots$

$(a \bmod N$ si $x_0 = 1)$ $\quad (\;)^2 \bmod N$ si $x_1 = 1$

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

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

$3^{108} = (3^1)^{\overset{x_0}{0}}$

Init :

$r = 1 \qquad e = 108 \qquad b = 3 \bmod 7 = 3$

x_0 : $e = 108 > 0$

$x_0 = 108 \bmod 2 = 0$

$r = (1 \cdot 3^0) \bmod N = 1$

$b = b^2 \bmod 7 = 3^2 \bmod 7 = 2$

$e = e/2 = 54$

x_1 : $e = 54 > 0$

$x_1 = 54 \bmod 2 = 0$

$r = (1 \cdot (3^2)^0) \bmod 7 = 1$

$b = (3^4) \bmod N = (3^2)^2 \bmod N = 4 \bmod 7 = 4$

$e = 54/2 = 27$

$108 \,|\, 2$; $0 \,|\, 54 \,|\, 2$; $0 \,|\, 27 \,|\, 2$; $1 \,|\, 13$

$3^{108} \equiv_N \underbrace{\underbrace{(3^1)^0 \bmod N}_{1} \cdot \underbrace{(3^2)^0 \bmod 7}_{1}}_{}$

$\underbrace{(1 \cdot 1 \bmod 7 = 1) \cdot \underbrace{3^4 \bmod 7}_{4}}_{4}$

$\underline{x_2 :}$ $e = 27 > 0$

$x_2 = 27 \bmod 2 = 1$

$r = 1 \cdot (3^4)^1 \bmod 7 = 1 \cdot 4 \bmod 7 = \underline{4}$

$b = 3^8 \bmod N = (3^4)^2 \bmod 7 = 4^2 \bmod 7 = 2$

$e = 27/2 = 13$

$\underline{x_3 :}$ $e = 13 > 0$

$x_3 = 13 \bmod 2 = 1$

$r = (\overset{r}{\underline{4}} \cdot 3^8) \bmod 7 = 4 \cdot 2 \bmod 7 = 1$

$b = 3^{16} \bmod N = (3^8)^2 \bmod 7 = 2^2 \bmod 7 = 4$

$e = 13/2 = 6$

En exercice à finir !

$$3^{108} \equiv_7 \underbrace{(3^1)^0}_{r_0 = 1} \cdot \underbrace{(3^2)^0}_{1} \cdot \underbrace{(3^4)^1}_{4} \cdot \underbrace{(3^8)^1}_{2} \cdot \underbrace{(3^{16})^0}_{1} \cdot \underbrace{(3^{32})^1}_{2} \cdot \underbrace{(3^{64})^1}_{4}$$

$r_1 = 1 \cdot 1$

$r_2 = 1 \cdot 4$

$r_3 = 2 \cdot 4 \bmod 7 = 1$

$3^{108} \bmod 7 = 1$

Propriétés en Modulo
Existence de l'inverse modulaire

Dans les $\mathbb{R}$: l'inverse est unique et si $x \neq 0$, alors

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

Inverse modulaire :

- L'inverse n'existe pas toujours !
- Il n'est pas forcément unique !
- Il est UNIQUE modulo N si $N \in \mathbb{Z} \setminus \{0, 1, -1\}$

1. Existence de l'inverse mod N $(N \in \mathbb{Z} \setminus \{0, 1, -1\})$

a admet un inverse mod N, on l'écrit a^{-1}

$\underline{\underline{\text{Si}}}$ $\text{PGCD}(a, N) = 1 \underset{\substack{\uparrow \\ \text{Bachet-Bézout}}}{=} a \cdot a^{-1} + \underbrace{N \cdot y}_{0} \equiv_N a \cdot \underset{\substack{\uparrow \\ \text{il existe bien !}}}{a^{-1}}$

2. Unicité : s'il y a 1 inverse, il y en a en fait une infinité ! (par l'infinité des paires de coefficients de Bézout).

3. Si a^{-1} est inverse de a, alors $(a^{-1} \bmod N)$ est unique.

Exemple: Quels sont les inverses de 2 mod 5 ?

$$\left.\begin{array}{ll} 2 \cdot 3 \equiv_5 1 & \Rightarrow 3 \text{ est inverse de } 2 \\ 2 \cdot 8 = 16 \equiv_5 1 & \Rightarrow 8 \text{ est inverse de } 2 \\ 2 \cdot (-2) = -4 \equiv_5 1 & \Rightarrow -2 \text{ est inverse de } 2 \end{array}\right\} \; 3 + k \cdot 5 \text{ est inverse de } 2 \text{ mod } 5 \; (k \in \mathbb{Z})$$

$$3 + k \cdot 5 \equiv_5 \underset{\underset{\text{UNIQUE}}{4}}{\overset{3}{=}}$$

a^{-1} ne peut <u>pas</u> être congruent à autre chose que 3

$$a^{-1} \bmod N \neq \{0, 1, 2, 4\}$$

L'inverse modulaire, s'il existe, est unique "à multiples de N près".

Un nombre peut être son propre inverse modulaire, par exemple 2 est son propre inverse modulo 3

$$2 \cdot 2 \bmod 3 = 4 \bmod 3 = 1$$

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

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

1. $a^p \bmod p = a \bmod p \quad , \quad a^p \equiv_p a$
2. $a^{p-1} \bmod p = 1 \qquad a^{p-1} \equiv_p 1$
3. Il existe un entier $k \in \mathbb{N}^*$ tel que a^k mod p = 1
   De plus, le plus petit de ces k vérifiant cette égalité divise p-1.

Exemple : a = 7 et p = 5

$$a^p = 7^5 \equiv_5 \underbrace{7}_{2} \cdot \underbrace{7^4}_{1} \equiv_5 2 \equiv_5 7$$

$7 \bmod 5 = 2$

$7^2 \bmod 5 = 4$

$7^4 \bmod 5 = 1 \quad // \quad \boxed{4 = p-1}$

$$a^p = 7^5 \equiv_5 \underbrace{7}_{2} \cdot \underbrace{7^4}_{1} \equiv_5 2 \equiv_5 7$$

$// \boxed{4 = p-1}$

$$7^4 \equiv_5 1$$

$$7^k \equiv_5 1$$

$7^1 \equiv_5 2 \neq 1$

$7^2 \equiv_5 4 \neq 1$

$7^3 \equiv_5 2 \cdot 4 \equiv_5 3 \neq 1$

$7^4 \equiv_5 1$ ✓ 4 diviser $p-1 = 5-1$

4 divise 4 ? OUI

Contre exemple : p = 2 a = 4

$a^p = 4^2 = 16 \equiv_2 0$ pas 1 ! FONCTIONNE PAS

car $PGCD(a, p) = 2 \neq 1$

Nombre d'Euler : $\varphi(n)$ = nombre de facteurs premiers compris entre 1 et n (inclus)

Exemple : $n = 7$ $\varphi(n) = 6$

1 est premier avec 7 $(PGCD(7,1) = 1)$
2 est premier
3 "
4 "
5 "
6 "

7 ne l'est pas $(PGCD(7,7) = 7 \neq 1)$

$n = 8$ $\varphi(n) = 4$

1 ✓
~~2~~
3 ✓
~~4~~
5 ✓
~~6~~
7 ✓
~~8~~

Extension au Théorème de Fermat

$$a^{\varphi(n)} \equiv_n 1 \quad \text{si} \quad PGCD(a, n) = 1$$