Cours du 30.11.2020

lundi, 30 novembre 2020 18:31

RSA - Pierre angulaire 1: Bachet-Bézout 17e s.

$$PGCD(a,b) = a \cdot x + b \cdot y$$

où $a, b, x, y \in \mathbb{Z}$

Pierre angulaire 2 : Exponentiation rapide $\Rightarrow a^x \bmod N \quad (a, x, N \in \mathbb{N}^*)$

début 18e s.

Pierre angulaire 3 : Petit Théorème de Fermat (indice d'Euler)

17e s.

Arithmétique Modulaire

$$(a+b) \bmod N = [(a \bmod N) + (b \bmod N)] \bmod N$$

$$a+b \equiv_N a \bmod N + b \bmod N$$ ← Distributivité du modulo par rapport à + en congruence !

$\underbrace{7+8}_{15} \equiv_{13} 2$ | $7 \bmod 13 + 8 \bmod 13 = 15 \neq 2$

$15 \equiv_{13} 2$

La distributivité du modulo fonctionne pour l'addition, la soustraction, la multiplication (la division entière aussi).

Exponentiation Rapide : $3^{108} \bmod 7$

$$3^{108} = \underbrace{3\cdot 3\cdot 3\cdot \ldots \cdot 3}_{108} = \underbrace{3^2\cdot 3^2\cdot 3^2 \cdots 3^2}_{54} = \underbrace{3^4\cdot 3^4 \cdots 3^4}_{27}$$

$$= 3^4 \cdot \underbrace{3^8\cdot 3^8 \cdots 3^8}_{13} = 3^4\cdot 3^8\cdot \underbrace{3^{16}\cdots 3^{16}}_{6} = 3^4\cdot 3^8\cdot \underbrace{3^{32}\cdots 3^{32}}_{3} = 3^4\cdot 3^8\cdot 3^{32}\cdot 3^{64}$$

$$\underbrace{(3^{2^0})^{x_0}}_{1}$$

$$= 3^{0\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2 + 1\cdot 2^3 + 0\cdot 2^4 + 1\cdot 2^5 + 1\cdot 2^6}$$

$$= 3^{(108)_{10}} = 3^{(x_6 x_5 \cdots x_0)_2}$$

① $(X)_{10} \longmapsto (\ )_2$

$$\begin{array}{l|l}
108 & 2 \\
x_0 = 0 & 54 \mid 2 \\
x_1 = 0 & 27 \mid 2 \\
x_2 = 1 & 13 \mid 2 \\
1 & 6 \mid 2 \\
0 & 3 \mid 2 \\
1 & 1 \mid 2 \\
1 & 0
\end{array}$$

$108_{10} = (1101100)_2$

②

$X_0 : \quad 3^{2^0} = 3^1 \equiv_7 3$

$X_1 : \quad 3^{2^1} = 3^2 \equiv_7 2$

$X_2 : \quad 3^{2^2} = 3^4 \equiv_7 \left[(3^2 \bmod 7)\cdot(3^2 \bmod 7)\right] \bmod 7 \equiv_7 (2\cdot 2) \bmod 7 \equiv_7 4$

$X_3 : \quad 3^{2^3} = 3^8 \equiv_7 3^4\cdot 3^4 \equiv_7 4\cdot 4 \equiv_7 2$

$X_4 : \quad 3^{2^4} = 3^{16} \equiv_7 3^8 \cdot 3^8 \equiv_7 2\cdot 2 \equiv_7 4$

$X_5 : \quad 3^{2^5} = 3^{32} \equiv_7 4\cdot 4 \equiv_7 2$

$X_6 : \quad 3^{2^6} = 3^{64} \equiv_7 4$

$$3^{108} = \underbrace{3^4}_{4}\cdot \underbrace{3^8}_{2}\cdot \underbrace{3^{32}}_{2}\cdot \underbrace{3^{64}}_{4} = \underbrace{(3^{2^0})^{x_0}}_{r_0 = 1}\cdot \underbrace{(3^{2^1})^{x_1}}_{1}\cdot \underbrace{(3^{2^2})^{x_2}}_{4} \cdots$$

$r = 8 \bmod 7$

$r = 1$

$1\cdot 2 = 2$

$r_1 = 1\cdot 1$

$r_2 = 1\cdot 4$

$$r = 2\cdot 4 \equiv_7 1 = 3^{108} \bmod 7$$

Algorithme d'exponentiation Rapide

Algorithme d'exponentiation Rapide

Objectif: $a^X \bmod N = R \qquad (N \in \mathbb{N} \setminus \{0, 1\})$

Pré-tests:

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

Si $X = 0 \Rightarrow R = 1$ STOP (0 si $N = 1$)

Initialisation:

$i = 0$

$R = 1$

$e = X$

$b = a \bmod N$

Tant que e > 0 :

$X_i = e \bmod 2$

$e = e / 2$ (Division ENTIÈRE) !!!

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

$b = (b \cdot b) \bmod N$

$i = i+1$

Fin

$a^X \bmod N = R.$

Plus gros calcul possible

$(N-1) \cdot (N-1)$

Exercice : $5^{209} \bmod 11$

Init:

$i = 0$

$R = 1$

$e = 209$

$b = 5$

X_0: $e = 209 \Rightarrow$ continue

$X_0 = 209 \bmod 2 = 1$

$e = 209/2 = 104$

$R = (1 \cdot 5^1) \bmod 11 = 5$

$b = b^2 \bmod 11 = 3$

x_1: $e = 104$ Ok.-

$x_1 = 104 \bmod 2 = 0$

$e = 52$

$R = (5 \cdot 3^0) \bmod 11 = 5$

$b = b^2 \bmod 11 = 3^2 \bmod 11 = 9$

x_2: $e = 52$ → ok

$x_2 = 52 \bmod 2 = 0$

$e = 52/2 = 26$

$R = (R \cdot 9^0) \bmod 11 = 5$

$b = b^2 \bmod 11 = 9^2 \bmod 11 = 4$

x_3:

$x_3 = 26 \bmod 2 = \boxed{0}$

$e = 13$

$R = (5 \cdot 4^{\boxed{0}}) \bmod 11 = 5$

$b = 4^2 \bmod 11 = 5$

x_4: $x_4 = 13 \bmod 2 = \boxed{1}$

$e = 6$

$R = (5 \cdot 5^{\boxed{1}}) \bmod 11 = 3$

$b = 5^2 \bmod 11 = 3$

x_5:

$x_5 = 6 \bmod 2 = \boxed{0}$

$e = 3$

$R = (3 \cdot 3^{\boxed{0}}) = 3$

$b = 3^2 \equiv_{11} 9$

$x_6 = 3 \bmod 2 = 1$

$e = 1$

$R = (3 \cdot 9^1) \bmod 11 = 5$

$b = 9^2 \bmod 11 = 4$

$x_7 = 1$

$e = 0$

$R = (5 \cdot 4) \bmod 11 = \boxed{9}$

$b = 4^2 \bmod 11 = 5$

→ STOP

→ $5^{209} \bmod 11 = R = \boxed{9}$

Avantages :

1. Algorithme en performance logarithmique
   (exponent * 2 => +1 itération)

2. Pas d'overflow car calcul maximum :

$$(n-1)\cdot(n-1) = (n-1)^2 = n^2 - 2n + 1$$

Notion Inverse Modulaire

Dans les REELS $\mathbb{R}$

$X \neq 0$, il existe un <u>unique</u> inverse $x^{-1} = \frac{1}{x}$

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

Et dans l'arithmétique modulaire ???

2 a-t-il un inverse modulo 5 ?

$2 \cdot X \equiv_5 1$ est-ce possible ? ($X \in \mathbb{Z}$)

<u>OUI</u> $2 \cdot 3 = 6 \equiv_5 1$ ✓

3 est l'inverse modulaire (modulo 5) de 2 et vice-versa !!

Est-ce que l'inverse de 2 modulo 5 est unique ???

$2 \cdot 8 = 16 \equiv_5 1$ 8 est aussi inverse de 2 (mod 5)

$2 \cdot 13 = 26 \equiv_5 1$

$2 \cdot (-2) = -4 \equiv_5 1$ Tout nombre de la forme $3 + k \cdot 5$ ($k \in \mathbb{Z}$) est un inverse de 2 mod 5 !

Si c'est vrai

$$(3+k\cdot 5)\cdot 2 \equiv_5 1 \quad \text{pour } k \in \mathbb{Z}$$

Par distrib. du modulo :

$$(3+k\cdot 5)\cdot 2 \equiv_5 (6)^{\text{mod } 5} + \underbrace{((2k)\cdot 5)}_{\substack{\text{multiple de } 5 \\ \Rightarrow \equiv_5 0}} \text{mod } 5 \equiv_5 6 \text{ mod } 5 + 0$$

$$\equiv_5 1 \qquad \text{CQFD !}$$

Propriété : l'inverse modulaire, s'il existe, est UNIQUE mod N (il est unique entre 0 et N-1).

$$3\cdot 7 \equiv_{10} 1$$

$3 \in [0,9]$ et $7 \in [0,9]$ } ils sont inverses l'un de l'autre modulo 10 et aucun autre (0,1,2,4,5,6,8 et 9) ne le sont !

ATTENTION : parfois l'inverse modulaire n'existe pas !!!!!

p. ex. 2 n'a pas d'inverse mod 10

$$\underbrace{2\cdot X}_{\text{PAIR}} = \underbrace{k\cdot 10 + 1}_{\text{IMPAIR}} \equiv_{10} 1 \qquad \text{PAS POSSIBLE !}$$

Quand est-ce que l'inverse modulaire de a mod N existe ???

Il existe TOUJOURS un inverse modulaire si

$$PGCD(a, N) = 1$$

BONUS DU JOUR : COMMENT CALCULER L'INVERSE MODULAIRE N

Théorème de Bachet-Bézout nous dit que

$PGCD(a, N) = 1 \equiv_N (a \cdot x + N \cdot y) \bmod N$ $\quad x, y \in \mathbb{Z}$ coeff. de Bézout.

$$1 \equiv_N (a \cdot x) \bmod N + \underbrace{(N \cdot y) \bmod N}_{0}$$

$a \cdot x \equiv_N 1$ donc x est l'inverse modulaire de a mod N

a et x sont inverses mod N et mod y !

$$1 \equiv_{\cancel{a}} (a \cdot x + N \cdot y) \bmod \cancel{a}$$

$\equiv_a N \cdot y$ $\quad$ N et y sont inverses mod $\cancel{a}$