Cours du 07.12.2020

lundi, 7 décembre 2020 18:33

Récapitualatif : L'algorithme d'exponentiation rapide

$$8^{67} \bmod 13 = \underbrace{(8^{64}) \bmod 13}_{1} \times \underbrace{(8^{2}) \bmod 13}_{12} \cdot \underbrace{8 \bmod 13}_{8}$$

$$8^{67} = (8^{64})^{1} (8^{2})^{1} \cdot (8^{1})^{1} \cdot \underbrace{(8^{32})^{0}}_{=1}$$

$$(67)_{10} = (1000011)_{2}$$

$8 \bmod 13 = 8$

$8^2 \bmod 13 = 12$

$8^4 \bmod 13 \equiv_{13} 12^2 \equiv_{13} 1$

$8^8 \bmod 13 = (1)^2 \bmod 13 = 1$

$8^{16} \bmod 13 = 1$

$8^{32} \bmod 13 = 1$

$8^{64} \bmod 13 = 1$

$$8^{67} \bmod 13 = (1 \cdot 12 \cdot 8) \bmod 13 = 5$$

12^2 le plus grand calcul possible

Inverse modulaire :

Si a et $n \in \mathbb{Z}^*$, alors il existe $b \in \mathbb{Z}^*$ tel que $a \cdot b \equiv_n 1$ si et seulement si : $PGCD(a, n) = 1$.

(A) ⟺ (B)

(A) => (B) :

Je sais que $a \cdot b \equiv_n 1$

Par définition du modulo : $a \cdot b = y' \cdot n + 1 \quad y' \in \mathbb{Z}^*$

$a \cdot b - y' \cdot n = 1$

$ax + yn = 1$ Bachet-Bézout

$= PGCD(a, n)$

Coeff. Bézout sont x et y

$= b \quad = -y'$

On a trouvé 2 coeff de Bézout (b et $-y'$)

$\Rightarrow PGCD(a, n) = 1$

Cela prouve (A) => (B).

(B) => (A): Nous savons que $PGCD(a, n) = 1$.

Thé. De Bachet-Bézout nous qu'il existe x et y tels que

$$PGCD(a, n) = 1 = a \cdot x + n \cdot y$$

Prenons le modulo n des deux côtés ci-dessus

$$1 \bmod n = (a \cdot x + n \cdot y) \bmod n$$

$$= (a \cdot x \bmod n + n \cdot y \bmod n) \bmod n$$

↑ distrib. du modulo

$n \cdot y \bmod n = 0$ (par déf. du modulo)

$1 = a \cdot x \bmod n \Rightarrow$ il existe $b = x \in \mathbb{Z}$

tel que $a \cdot x \bmod n = 1$.

Cela prouve B => A.

CQFD !

Conjecture de Fermat : $a^n + b^n = c^n$ n'a pas de solution dans $\mathbb{Z}^*$ si $n \geq 3$.

Petit Théorème de Fermat : (XVIIe s)

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

1. $a^p \bmod p = a \bmod p$
2. $a^{p-1} \bmod p = 1$
3. Il existe un entier $k \in \mathbb{N}^*$ tel que $a^k \bmod p = 1$. Le plus petit de de ces k > 0 vérifiant l'égalité divise p-1.

Exemples : $p = 3 \quad a = 8$

1. $8^3 \bmod 3 = 2 = 8 \bmod 3$ ✓

$8^{127} \bmod 3 = \left((8^3)^{42} \cdot 8^1\right) \bmod 3 \equiv_3 \left(\underbrace{8^3 \bmod 3}_{8 \bmod 3 \,=\, 2}\right)^{42} \cdot 2 \equiv_3 (2^{42} \cdot 2) \bmod 3$

$127 = 3 \cdot 42 + 1$

$3-1$

2. $8^{3-1} \bmod 3 = 64 \bmod 3 = 1$ ✓

3. $8^2 \bmod 3 = 1$ $k=2$ fonctionne et c'est le plus petit (il ne resterait que 1) $\Rightarrow k=2$ divise $p-1=3-1=2$!

Contre exemple : a = 9 et p = 3
(cela viole "p ne divise pas a")

1. $9^3 \equiv_3 0 \equiv 9^1 \bmod 3$ ✓

2. $9^{3-1} \bmod 3 = 9^2 \bmod 3 = 0 \neq 1$ ✗ ERREUR !

Contre exemple 2 : a = 9 et p = 4

1. $9^4 \bmod 4 = 1 = 9 \bmod 4$ ✓

2. $9^3 \bmod 4 = 1 \bmod 4$ ✓

3. Le plus petit k > 0 qui vérifie $9^4 \bmod 4 = 1$ c'est $k=1$

k divise bien $4-1=3$. ✓ c'est ok

Contre exemple 3 : a = 7, p = 4

pas ok !

1. $7^4 \bmod 4 = 1 \neq \underbrace{7 \bmod 4}_{3}$

Résultat découlant directement du Théorème de Fermat est que si *a* est un nombre quelconque et *n* est premier avec *a*,

$a, n \in \mathbb{N}^*$

$\varphi(n)$

$a^{\varphi(n)} \bmod n = 1$ n premier avec a

$a, n \in \mathbb{N}$

n premier avec a

$a^{\varphi(n)} \bmod n = 1$

alors

$$a^{\varphi(n)} \bmod n = 1$$

$\varphi(n)$ est l'indice d'Euler : c'est le nombre de facteurs premiers avec n compris entre 1 et n.

Exemple : $\varphi(18)$ comptons le nombre de facteurs $a \in [1, 18]$ tels que $PGCD(a, 18) = 1$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
PGCD :	1	2	3	2	1	6	1	2	9	2	1	6	1	2	3	2	1	18

$18 = 2 \cdot 3 \cdot 3$

$\varphi(18) = 6$ (facteurs sont $1, 5, 7, 11, 13, 17$)

Exercice : que valent $\varphi(17) = 16$ (si p premier $\varphi(p) = p-1$)

$\varphi(14) = 6$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
PGCD(a,14)	1	2	1	2	1	2	7	2	1	2	1	2	1	14

$14 = 2 \cdot 7$

Exercice : Prouvez que si n > 1 est un nombre premier alors

$\varphi(n) = n-1$.

Bonus : Montrez que si p et q sont des nombres premiers, alors

$$\varphi(p \cdot q) = (p-1) \cdot (q-1).$$

Preuve 1:

Si p premier $\Rightarrow$ il n'a que 2 diviseurs 1 et p

Donc tous les autres $\underbrace{(2,3,\dots,p-1)}_{+\boxed{p-2}}$ sont premiers avec p

De plus $PGCD(1,n)=1 \Rightarrow$ il compte aussi $\boxed{+1}$

$PGCD(n,n)=n \neq 1$ il ne compte pas $\boxed{+0}$

$$\varphi(n) = \underbrace{(p-2)}_{2,\dots,p-2} + \underbrace{1}_{1} + \underbrace{0}_{n} = p-1$$

CQFD !

Preuve 2 : p et q sont premiers

Les seuls diviseurs de $p \times q$ sont $1, p, q$ et $p \cdot q$

Il y a $p \cdot q$ candidats

or tous les multiples de p ne sont <u>PAS</u> premiers avec $p \cdot q$

Combien de ces multiples y a-t-il entre 1 et $p \cdot q$

$1 \times p, 2 \times p, 3 \times p, \dots (q-1) \times p, \boxed{q \cdot p}$

$p=3$
$q=7$ $\}p \cdot q = 21$

$$1 \times p, \quad 2 \times p, \quad 3 \times p, \quad \ldots \quad (q-1) \times p, \quad q \cdot p$$

(les $q-1$ premiers termes, jusqu'à $(q-1) \times p$, sont regroupés sous une accolade marquée $q-1$)

[illegible]
$q = 7$ } $p \cdot q = 21$

$3, 6, 9, 12, 15, 18$ et 21
ont $PGCD(x, 21) \geqslant 3$

Idem pour les multiples de q

$$1 \cdot q, \quad 2 \cdot q \quad \ldots, \quad (p-1) \cdot q, \quad p \cdot q$$

<u>Au total :</u> $\quad p \cdot q$ candidats

$-\quad p \quad$ candidats multiples de q (sont pas premiers avec $p \cdot q$)

$-\quad q \quad$ candidats (multiples de p)

$+\quad 1 \quad$ (compté $p \cdot q$ 2 fois)

$$p \cdot q - p - q + 1 = (p-1) \cdot (q-1)$$

(QFD)