MATIN cours du 23.11

lundi, 23 novembre 2020 08:18

Dans le monde des modulos, on peut avoir un inverse d'un nombre a, qui est un nombre entier, de sorte que

$$a \times b \equiv_N 1 \quad \text{où} \quad a \in \mathbb{Z}, \; b \in \mathbb{Z}$$

L'existence de **l'inverse** de a "mod N" dépend du PGCD(a,N).

PROPRIETES IMPORTANTES de la congruence $\equiv_N$ avec + et ·

1. Commutatif : $(a+b) \bmod N = (b+a) \bmod N$, ou $a+b \equiv_N b+a$
   $(a \cdot b) \bmod N = (b \cdot a) \bmod N$, ou $a \cdot b \equiv_N b \cdot a$
2. Associatif : $(a+b)+c \equiv_N a+(b+c)$ ou $(a+b)+c \equiv_N a+(b+c)$
   $(a \cdot b) \cdot c \equiv_N a \cdot (b \cdot c)$
3. Distributif : $(a+b) \cdot c \equiv_N a \cdot c + b \cdot c$

Cela s'applique au MODULO !!!!

Mod N est DISTRIBUTIF sur l'addition

$$(a+b) \bmod N \equiv_N (a \bmod N) + (b \bmod N)$$

C'est aussi associatif :

$$(a+b+c) \bmod N \equiv_N (a+b) \bmod N + c \bmod N$$
$$\equiv_N [a \bmod N + b \bmod N] + (c \bmod N)$$

$$\equiv_N \left[a \bmod N + b \bmod N \right] + (c \bmod N)$$

$$\left[a \cdot (b+c) \right] \bmod N \equiv_N (a \bmod N) \cdot \left[b \bmod N + c \bmod N \right]$$

EST-CE UTILE ???

EXEMPLE: calculez 1341 x 679 mod 22 = ? 3

Par distributivité du modulo ?

$1341 \bmod 22 = 21$

$679 \bmod 22 = 19$

$\Big\}$ $(1341 \times 679) \bmod 22 = 21 \cdot 19 \bmod 22$

$= 399 \bmod 22 = 3$

Quelle est la plus grande opération faite (avec les plus grands nombres) ?

Mise à part le modulo, les opérations se font sur des nombres Entre 0 et N-1 !!!

Le plus grand nombre obtenu au cours des calculs sera alors

$(N-1)^2$ pour la multiplication

$a \times b \leq (N-1) \cdot (N-1) = (N-1)^2 = N^2 - 2N + 1$

($a \leq N-1$, $b \leq N-1$)

prend le modulo AVANT le calcul

$a + b \leq (N-1) + (N-1) = 2N - 2$

Donc, sur une machine à précision finie, cela nous permet de faire des calculs de modulo avec de TRES grand nombres (trop grands pour être représentés), sans overflow !

Si on sait factoriser (un ou plusieurs diviseurs suffisent !) un nombre, prendre son modulo devient facile !

$$a = a_1 \cdot a_2 \cdot \dots a_M$$

$$a \bmod N \equiv_N \left(\left(a_1 \bmod N \cdot a_2 \bmod N \right) \bmod N \cdot a_2 \bmod N \right) \dots$$

Exemple: calculez le modulo de 17556 = 2*2*3*7*11*19 Modulo 13 = 6

$84 \bmod 13 = 6$ $\quad 6 \cdot 11$ (66 mod 13 = 1)

$6 \cdot 1 \equiv_{13} 6$

$$17556 \bmod 13 = (2 \cdot 2 \cdot 3) \cdot 7) \cdot (11) \cdot (19) \bmod 13$$

(12 · 7 · 11 · 19 ; 19 mod 13 = 6)

mod 13 PARTOUT

$$= (12 \cdot 7 \cdot 11 \cdot 6) \bmod 13$$

$$= (12 \cdot 11 \cdot (42 \bmod 13)) \bmod 13$$

$42 \bmod 13 = 3$

$$= (12 \cdot 11 \cdot 3) \bmod 13 = (12 \cdot (33 \bmod 13)) \bmod 13$$

$33 \bmod 13 = 7$

$$= 12 \cdot 7 \bmod 13 = 84 \bmod 13 = 6$$

$84 = 6 \cdot 13 + 6$

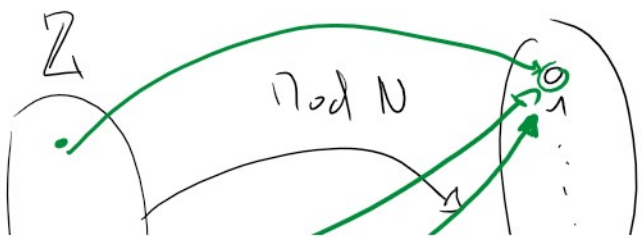
Def: Modulo

$x \bmod N = r$

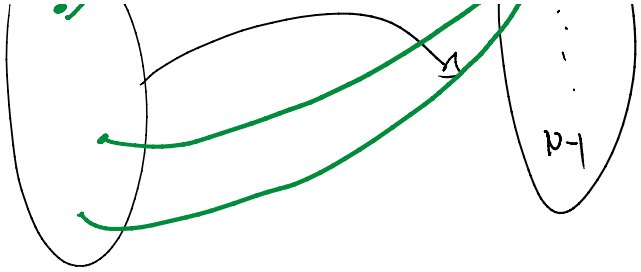
$x \mid N$

$r \mid q$

L'opérateur modulo PAS bijectif



0 a une INFINITÉ de préimages!



de préimages!

PAS bijectif

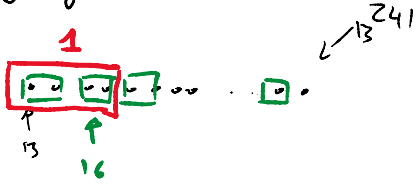
Surjectif => tous les éléments de l'ensemble d'arrivée ont au moins une préimage
Injectif => tous les éléments de l'ensemble de départ ont au moins une image
BIJECTIF => l'image ET la préimage sont uniques (nécessaire pour l'existence de l'inverse).

L'algorithme d'exponentiation rapide

Calculez $13^{241} \bmod 17 = 13$

trop grand pour ordi 64 bits

calculette de M. Eggenberg ?



$13^{241} = (13 \cdot 13 \cdot \ldots) \bmod 17 = ?$

$13 \cdot 13 \equiv_{17} 169 \equiv_{17} 16$

$16 \cdot 16 \equiv_{17} 1$

$13^7 \bmod 17 \times 13^7 \bmod 17$

$13^{14} \bmod 17 = 1$

$13^{241} = (13^2)^{120} \cdot 13$

$\equiv_{17} (16)^{120} \cdot 13$

$13^2 \bmod 17$

$\equiv_{17} (16 \cdot 16)^{60} \cdot 13$

$16^2 \bmod 17$

$\equiv_{17} \underbrace{(1)^{60}}_{1} \cdot 13 \equiv_{17} 13$

Si on calcule $a^x \bmod N$

Calcule $a \bmod N = \bullet$

$\downarrow \cdot^2$

$a^2 \bmod N = \square$

$\downarrow$

$a^4 \bmod N = \square^2 \bmod N = \triangle$

$a^8 \bmod N = \triangle^2 \bmod N = \bigstar$

$\vdots$

} Puissances de puissance de 2 de a : a^{2^i} $i = 0, 1, \ldots$

Objectif : calculer $a^x \bmod N$

L'idée: 1) écrire $(x)_{10} = (\quad)_2$

2) Calculer itérativement $a^{2^i} \bmod N$ pour i bit de poids fort

3) Si le bit i est 1 alors on retient $a^{2^i} \bmod N$ dans le calcul final.

$13^{241} \bmod 17$:

$(241)_{10} = (11110001)_2$ (2^7)

$13^{241} = 13^{128 \cdot 1} \cdot 13^{64 \cdot 1} \cdot 13^{32 \cdot 1} \cdot 13^{16 \cdot 1} \cdot 13^{1 \cdot 1}$

$13^{8 \cdot 0}$

$13^1 \bmod 17 = 13$

$(\,)^2$ → $13^2 \bmod 17 = 16$

$(\,)^2$ → $13^4 \bmod 17 = 16^2 \bmod 17 = 1$

$13^8 \bmod 17 = 1^2 \bmod 17 = 1$

13^{16} ... 13^{32} ... 13^{64} ... 13^{128}

$13^{241} \equiv_{17} 13^{128} \cdot 13^{64} \cdot 13^{32} \cdot 13^{16} \cdot 13^1$

$\equiv_{17} 1 \cdot 1 \cdot 1 \cdot 1 \cdot 13 \equiv_{17} 13$!

$13^8 \bmod 17 = 1^7 \bmod 17 = 1$

$13^{16} \equiv_{17} 13^{32} \equiv_{17} 13^{64} \equiv_{17} 13^{128} \equiv_{17} 1$

$\equiv_{17} 1 \cdot 1 \cdot 1 \cdot 1 \cdot 13 \equiv_{17} 13$!