Après-midi COURS du 23.11.2020

lundi, 23 novembre 2020 13:03

Arithmétique modulaire : propriétés suivantes par rapport à l'addition et la multiplication en MODULO N $\in \mathbb{N}^*$

1. Commutatif : $(a+b) \bmod N = (b+a) \bmod N$ $\quad a+b \equiv_N b+a$

   $a \cdot b \equiv_N b \cdot a$

2. Associatif : $(a+b+c) \bmod N = [(a+b)+c] \bmod N = [a+(b+c)] \bmod N$

   $a+(b+c) \equiv_N (a+b)+c$ $\quad$ idem $(a \cdot b) \cdot c \equiv_N a(b \cdot c)$

3. + est Distributif sur ·

   $a \cdot (b+c) \equiv_N a \cdot b + a \cdot c$

4. Modulo est lui aussi ASSOCIATIF, COMMUTATIF et DISTRIBUTIF par rapport à + et · en CONGRUENCE

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

⚠ " $\equiv_N$ " et pas " $=$ "

Exemple : $(\underbrace{13+14}_{27}) \bmod 25 = 2$ $\quad 2 \neq 27$

?!!? $\quad$!\?!?! $\quad$ MAIS $2 \equiv_{25} 27$!

$13 \bmod 25 + 14 \bmod 25 = 13+14 = 27$

$13 = 0 \cdot 25 + 13$

RAPPEL : Définition du modulo $\quad a \bmod N = r$

Donc $\quad a = q \cdot N + r \quad$ où $r \in [0, \dots, N-1]$

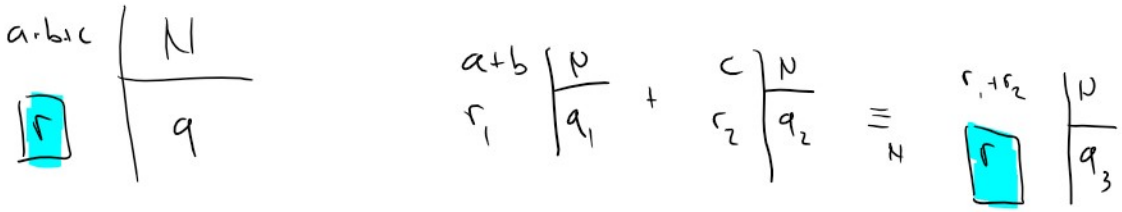
Via division Euclidienne :

a	N
r	q

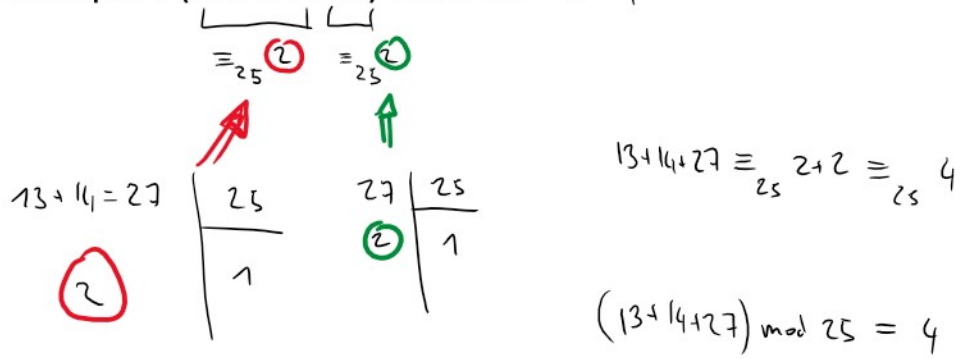
Via division Euclidienne :

Propriétés qui en suivent :

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



Exemple : (13+14+27) mod 25 = ? 4

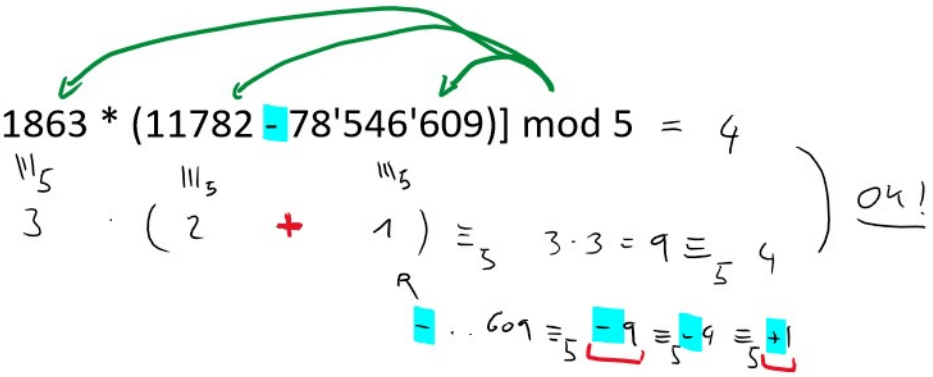


$13+14+27 \equiv_{25} 2+2 \equiv_{25} 4$

$(13+14+27) \bmod 25 = 4$

Idem pour la multiplication ET la combinaison des deux

Calculez [1863 * (11782 - 78'546'609)] mod 5 = 4



Si on décompose ainsi les modules par opérations 2 à 2,
que se passe-t-il ???
On ne travaille plus qu'avec des nombres compris entre 0

et N - 1.

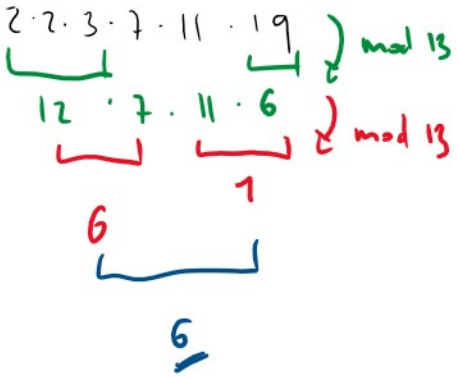
ADDITION: $a + b \leq 2N - 2$

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

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

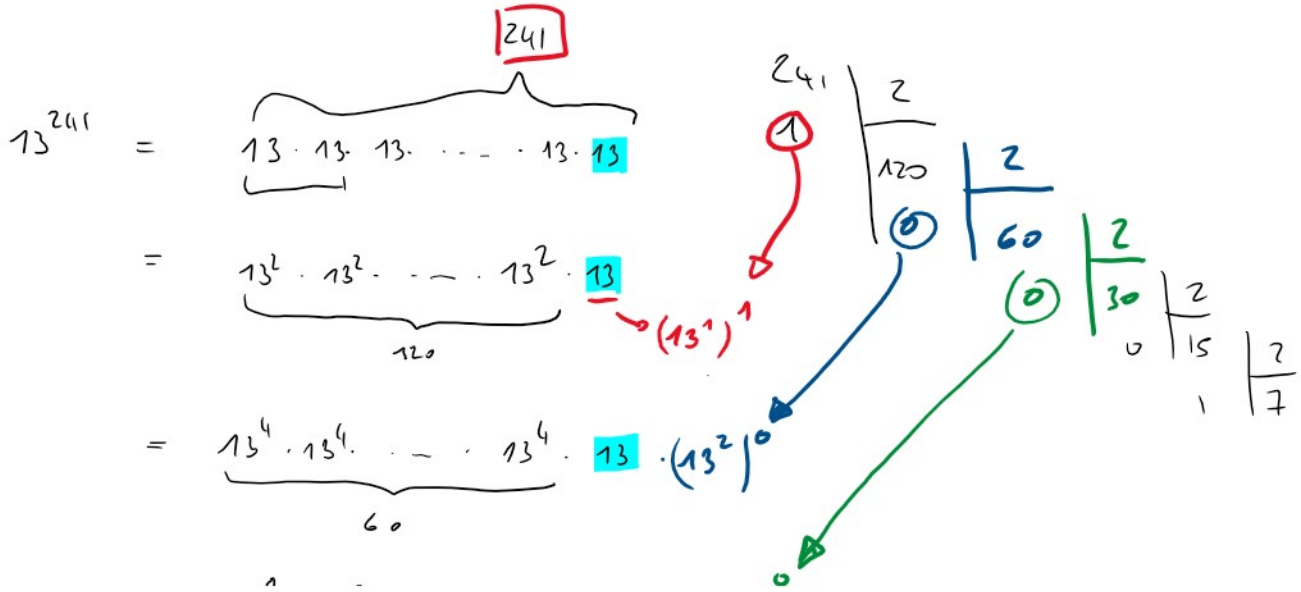
$a \leq (N-1)$ et $b \leq (N-1)$

Exemple : 17556 mod 13 = 2*2*3*7*11*19 mod 13 = 6 ?



CHALLENGE : calculer $13^{241} \bmod 17 = 13$ dixit 17OI!

Est-ce VRAI ?



60

$= \underbrace{13^8 \cdot 13^8 \cdot \dots \cdot 13^8}_{30} \cdot 13 \cdot (13^4)^0$

$= \dots$

$= \underbrace{13^{32} \cdot \dots \cdot 13^{32}}_{7} \cdot 13^{16} \cdot 13^1$

$(1\ 1\ 1\ 1\ 0001)_2 = (241)_{10}$ ($13^{2^0} = 13^1$)

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

$(13)^{2^8} \cdot (13)^{2^7} \cdot (13)^{2^6} \dots$

$\equiv_{17} \underbrace{(13^{128} \bmod 17)}_{=1} \cdot \underbrace{(13^{64} \bmod 17)}_{=1} \cdot \dots \cdot (13^1 \bmod 17)$

$()^2$: $13 \bmod 17 = 13$ → $13^2 \bmod 17 = 16$

$()^2$: $13^4 \bmod 17 = 1$

$()^2$: $13^8 \bmod 17 \equiv_{17} 1^2 \bmod 17 = 1$

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

$13^4 \bmod 17 \equiv_{17} \underbrace{13^2 \bmod 17}_{16} \cdot 13^2 \bmod 17$

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

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

$= 1 \cdot 13 = \underline{\underline{13}}$

$(241)_{10} = (11110001)_2$

Algorithme d'exponentiation rapide pour calculer $a^x \bmod N$

1. Ecrire $(x)_{10} = (x_k x_{k-1} \cdots x_1 x_0)_{2^k}$ $\Rightarrow (x)_{10} = x_k \cdot 2^k + x_{k-1} \cdot 2^{k-1} + \ldots + x_1 \cdot 2^0$

$x_k \in \{0,1\}$

$$a^x = a^{2^k \cdot x_k} \cdot a^{2^{k-1} \cdot x_{k-1}} \cdot \ldots \cdot a^{2^1 \cdot x_1} \cdot a^{2^0 \cdot x_0}$$

2. Calculer les valeurs de $a^{2^i} \bmod N$ pour $i = 0, 1, \ldots, k$

Il suffit de mettre au carré le résultat de l'étape précédente à chaque fois

3. On multiplie les résultats intermédiaires dans

$$a^x \bmod N = \underbrace{a^{2^k \cdot x_k} \bmod N}_{\text{calculé en 2.}} \cdot \underbrace{a^{2^{k-1} \cdot x_{k-1}} \bmod N}_{} \cdot \ldots \cdot \underbrace{a^{2^0 \cdot x_0} \bmod N}_{}$$