

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

1. Commutatif :  $(a + b) \bmod N = (b + a) \bmod N$        $a + b \equiv_N b + a$   
 $a \cdot b \equiv_N b \cdot a$
2. Associatif :  $(a + b + c) \bmod N = [(a + b) + c] \bmod N = [a + (b + c)] \bmod N$   
 $a + (b + c) \equiv_N (a + b) + c$       idem  $(a \cdot b) \cdot c \equiv_N a \cdot (b \cdot c)$
3. + est Distributif sur  $\cdot$   
 $a \cdot (b + c) \equiv_N a \cdot b + a \cdot c$

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

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

⚠  $\equiv_N$  et  $\equiv$

Exemple :  $(13 + 14) \bmod 25 = 2$

?..?

\\???

$2 \neq 27$

MAIS  $2 \equiv_{25} 27$  !

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

$$13 = 0 \cdot 25 + 13$$

RAPPEL : Définition du modulo

$$a \bmod N = r$$

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

Via division Euclidienne:

$$\begin{array}{r} a \\ \hline N \end{array}$$

Via division Euclidienne:

$$\begin{array}{r|l} a & N \\ \hline r & q \end{array}$$

Propriétés qui en suivent :

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

$$\begin{array}{r|l} a+b+c & N \\ \hline r & q \end{array}$$

$$\begin{array}{r|l} a+b & N \\ \hline r_1 & q_1 \end{array}$$

$$+ \begin{array}{r|l} c & N \\ \hline r_2 & q_2 \end{array}$$

$$\equiv_N \begin{array}{r|l} r_1+r_2 & N \\ \hline r & q_3 \end{array}$$

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

$$\begin{array}{r|l} 13+14=27 & 25 \\ \hline 2 & 1 \end{array} \quad \begin{array}{r|l} 27 & 25 \\ \hline 2 & 1 \end{array}$$

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

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

Idem pour la multiplication ET la combinaison des deux

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

$$\begin{array}{l} \text{||}_5 \quad \text{||}_5 \quad \text{||}_5 \\ 3 \quad (2 + 1) \equiv_5 3 \cdot 3 = 9 \equiv_5 4 \end{array} \quad \text{ou!}$$

$$\begin{array}{l} \dots 609 \equiv_5 -9 \equiv_5 -4 \equiv_5 +1 \end{array}$$

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

$$\begin{matrix} \wedge & \wedge \\ (N-1) & + & (N-1) \end{matrix}$$

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

$$\begin{matrix} \wedge & \wedge \\ (N-1) & \cdot & (N-1) \end{matrix}$$

Exemple :  $17556 \bmod 13 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \bmod 13 = \underline{\underline{6}}$  ?

$$\begin{array}{ccccccc} 2 & \cdot & 2 & \cdot & 3 & \cdot & 7 & \cdot & 11 & \cdot & 19 \\ \hline 12 & \cdot & 7 & \cdot & 11 & \cdot & 6 \\ \hline 6 & & & & & & 1 \\ \hline 6 \end{array} \bmod 13$$

CHALLENGE : calculer  $13^{241} \bmod 17 = 13$  direct 1705!

Esl. est VRAI ?

$$\begin{aligned} 13^{241} &= \overbrace{13 \cdot 13 \cdot 13 \cdot \dots \cdot 13 \cdot 13}^{241} \\ &= \overbrace{13^2 \cdot 13^2 \cdot \dots \cdot 13^2 \cdot 13}^{120} \cdot 13 \\ &= \overbrace{13^4 \cdot 13^4 \cdot \dots \cdot 13^4 \cdot 13}^{60} \cdot 13 \end{aligned}$$

Diagram illustrating the reduction of the exponent 241 modulo 16 (since  $\phi(17) = 16$ ):

$$\begin{array}{r} 241 \\ 2 \\ \hline 120 \\ 121 \\ 2 \\ \hline 60 \\ 61 \\ 2 \\ \hline 30 \\ 31 \\ 2 \\ \hline 15 \\ 16 \\ 2 \\ \hline 7 \end{array}$$

Arrows indicate the reduction steps:  $241 \equiv 1 \pmod{16}$ ,  $121 \equiv 1 \pmod{16}$ ,  $61 \equiv 5 \pmod{16}$ ,  $31 \equiv 15 \pmod{16}$ ,  $1 \pmod{16}$ .

$$\begin{aligned}
 &= \underbrace{13^8 \cdot 13^8 \cdot \dots \cdot 13^8}_{30} \cdot 13 \cdot (13^4) \quad \checkmark \\
 &= \dots \\
 &= \underbrace{13^{32} \cdot \dots \cdot 13^{32}}_7 \cdot 13^{16} \cdot 13^1 \\
 &= \underbrace{13^{128} \cdot 13^{64} \cdot 13^{32} \cdot 13^{16} \cdot 13^1}_{13^{241}} = 13^{241} \\
 &\quad (13)^{2^8} \cdot (13)^{2^7} \cdot (13)^{2^6} \cdot \dots
 \end{aligned}$$

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

$$\begin{aligned}
 ( )^2 \left( \begin{array}{l} 13 \bmod 17 = 13 \\ 13^2 \bmod 17 = 16 \end{array} \right) & \downarrow ( )^2 \\
 ( )^2 \left( \begin{array}{l} 13^4 \bmod 17 = 1 \\ 13^8 \bmod 17 = 1 \end{array} \right) & \downarrow ( )^2 \\
 ( )^2 \left( \begin{array}{l} 13^{16} \bmod 17 = 1 \\ 13^{32} \bmod 17 = 1 \\ 13^{64} \bmod 17 = 1 \\ 13^{128} \bmod 17 = 1 \end{array} \right) & \downarrow ( )^2
 \end{aligned}$$

$$\begin{aligned}
 13^4 \bmod 17 &\equiv_{17} 13^2 \bmod 17 \cdot 13^2 \bmod 17 \\
 &\equiv_{17} 16 \cdot 16 \equiv_{17} 1
 \end{aligned}$$

$$\begin{aligned}
 13^{241} \bmod 17 &\equiv_{17} \underbrace{13^{128} \bmod 17}_1 \cdot \underbrace{13^{64} \bmod 17}_1 \cdot \underbrace{13^{32} \bmod 17}_1 \cdot \underbrace{13^{16} \bmod 17}_1 \cdot \underbrace{13^1 \bmod 17}_{13} \\
 &= 1 \cdot 13 = \underline{\underline{13}}
 \end{aligned}$$

$(741)_{10} = (11110001)_2$

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

1. Ecrire  $(x)_{10} = (x_h x_{h-1} \dots x_1 x_0)_{10} \Rightarrow (x)_{10} = x_h \cdot 10^h + x_{h-1} \cdot 10^{h-1} + \dots + x_0 \cdot 10^0$   
 $x_i \in \{0, 1\}$

$$a^x = a^{2^h \cdot x_h} \cdot a^{2^{h-1} \cdot x_{h-1}} \cdot \dots \cdot a^{2^1 \cdot x_1} \cdot a^{2^0 \cdot x_0}$$

2. Calculer les valeurs de  $\underbrace{a^{2^i} \bmod N}_{\text{pour } i=0,1,\dots,h}$

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

3. On multiplie les résultats intermédiaires dans

$$a^x \bmod N = \underbrace{a^{2^h \cdot x_h} \bmod N}_{\text{calculé en } 2} \cdot \underbrace{a^{2^{h-1} \cdot x_{h-1}} \bmod N} \cdot \dots \cdot \underbrace{a^{2^0 \cdot x_0} \bmod N}$$