Division Euclidienne – Congruences

Soit a , b entiers , avec $b \leq a$, alors $a = bq + r$ de façon unique, avec $0 \leq r < b$.

a = dividende , b = diviseur , q = quotient , r = reste.

Ainsi : $29 = 2\times13 + 3$ (division euclidienne de 29 par 13 : $a = 29$, $b = 13$, $q = 2$, $r = 3$).

Deux nombres sont dits *congrus modulo n* si et seulement si ils ont même reste dans la division par n .

Notation : $a \equiv b\ [\ n\ ] \Leftrightarrow a , b$ même reste en division par $n \Leftrightarrow a = nq + r$ et $b = nq' + r$.

Ainsi : $29 = 2\times13 + 3$ et $16 = 1\times13 + 3 \Rightarrow 29 \equiv 16\ [13]$.

La congruence est compatible avec l'addition et la multiplication :

$a \equiv a'\ [\ n\ ]$ et $b \equiv b'\ [\ n\ ] \Rightarrow a + b \equiv a' + b'\ [\ n\ ]$ et $a \times b \equiv a' \times b'\ [\ n\ ]$

Les congruences modulo n des puissances d'un nombre (leurs restes en division par n) sont cycliques, puisque le nombre de restes est limité ($0 \leq r < n$).

Ainsi, en division par 5 :

$2^1 \equiv 2\ [\ 5\ ]$, $2^2 \equiv 4\ [\ 5\ ]$, $2^3 \equiv 3\ [\ 5\ ]$, $\mathbf{2^4 \equiv 1\ [\ 5\ ]} \Rightarrow 2^5 \equiv 2\ [\ 5\ ]$, $2^6 \equiv 4\ [\ 5\ ]$, $2^7 \equiv 3\ [\ 5\ ]$, $2^8 \equiv 1\ [\ 5\ ]$ …

$p = 4k \Rightarrow 2^p \equiv 2\ [\ 5\ ]$, ainsi 2^{20} admet un reste 1 dans la division par 5.

$p = 4k + 1 \Rightarrow 2^p \equiv 4\ [\ 5\ ]$, ainsi 2^{13} admet un reste 2 dans la division par 5……