Divisibilité dans $\mathbb{Z}$

1) Congruence de deux entiers

Définition 1

Deux nombres entiers a et b sont dits congrus modulo n lorsque leurs restes dans la division euclidienne par n sont égaux.
On écrit alors :

$$a \equiv b\ [n]$$

Exemples :

- *Modulo 7, les nombres 3, 10, 17, 38 sont congrus.*
- *Les nombres pairs sont congrus modulo 2 (à 0).*
- *Les nombres impairs sont congrus modulo 2 (à 1).*

Propriété 2

$a \equiv b\ [n]$ si, et seulement si il existe un entier k tel que $a = b + k \times n$

Propriété 3

$a \equiv b\ [n]$ si, et seulement si $a - b$ est divisible par n.

2) Opérations

Propriété 4

Soient a, b, a', b' et n des nombres entiers tels que $a \equiv b\ (n)$ et $a' \equiv b'\ (n)$.
Alors :

- $a + a' \equiv b + b'\ [n]$
- $a - a' \equiv b - b'\ [n]$
- $aa' \equiv bb'\ [n]$
- $a^k \equiv b^k\ [n]$ pour toute puissance k entière.

Exemples :

- *Le chiffre des unités de* 1024×493 *est 2*
- *Le nombre* $6509 + 497 \times 3133$ *est divisible par 10*
- *Le nombre* $324 \times 729 - 964$ *est divisible par 8*
- *Si* $n^3 - 1$ *est divisible par* p *alors* $n^6 - 1$ *aussi*

Propriété 5

Soient a, b et n des nombres entiers tels que $a \equiv b\ (n)$ et c un entier.
Alors :

- $a + c \equiv b + c\ [n]$
- $a - c \equiv b - c\ [n]$
- $ac \equiv bc\ [n]$

Remarque :

Attention, la réciproque du troisième point est fausse (trouver des contre-exemples et comprendre pourquoi).

3) Démonstrations

Propriété 4

- $a + a' \equiv b + b'\ [n]$
- $a - a' \equiv b - b'\ [n]$
- $aa' \equiv bb'\ [n]$
- $a^k \equiv b^k\ [n]$ pour toute puissance k entière.