Arithmétique

Divisibilité, congruences, PGCD, Bézout, Gauss, nombres premiers et petit théorème de Fermat

Divisibilité

Tle exp.

a, b, c sont des entiers relatifs.

- b divise a (on note $b \mid a$) s'il existe un entier k tel que $a = kb$: a est un **multiple** de b.
- Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
- Si $a \mid b$ et $a \mid c$, alors a divise toute combinaison $bu + cv$ (u et v entiers).

Exemple : si d divise $n+3$ et n, alors d divise leur différence, 3.

Division euclidienne

Tle exp.

Pour a entier et b entier naturel non nul, il existe un unique couple d'entiers $(q ; r)$ tel que

$$a = bq + r \quad \text{avec} \quad 0 \leqslant r < b$$

q est le quotient et r le reste ; b divise a si et seulement si $r = 0$.

Exemples : $47 = 6 \times 7 + 5$; $-47 = 6 \times (-8) + 1$ (le reste est toujours positif).

Congruences

Tle exp.

Pour $n \geqslant 2$: $a \equiv b\ [n]$ (« a congru à b modulo n ») signifie que n divise $a - b$, c'est-à-dire que a et b ont le même reste dans la division par n.

Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors :

- $a + c \equiv b + d\ [n]$ et $a - c \equiv b - d\ [n]$;
- $ac \equiv bd\ [n]$;
- $a^k \equiv b^k\ [n]$ pour tout entier naturel k.

Grandes puissances : chercher une puissance congrue à 1. Comme $2^3 = 8 \equiv 1\ [7]$: $2^{100} = (2^3)^{33} \times 2 \equiv 1^{33} \times 2 \equiv 2\ [7]$.

Un entier est congru à la somme de ses chiffres modulo 9 : $1\,234 \equiv 1 + 2 + 3 + 4 = 10 \equiv 1\ [9]$.

> **Attention :** On ne simplifie pas une congruence : $2 \times 3 \equiv 2 \times 8\ [10]$, mais $3 \not\equiv 8\ [10]$.

PGCD et algorithme d'Euclide

Tle exp.

$\text{PGCD}(a ; b)$ est le plus grand diviseur commun de a et b. Si $a = bq + r$, alors $\text{PGCD}(a ; b) = \text{PGCD}(b ; r)$.

Algorithme d'Euclide : on enchaîne les divisions euclidiennes ; le PGCD est le **dernier reste non nul**.

Division	Reste
$252 = 1 \times 198 + 54$	54
$198 = 3 \times 54 + 36$	36
$54 = 1 \times 36 + 18$	18
$36 = 2 \times 18 + 0$	0

Donc $\text{PGCD}(252 ; 198) = 18$. Deux entiers sont **premiers entre eux** si leur PGCD vaut 1.

Théorèmes de Bézout et de Gauss

Tle exp.

- Identité de Bézout : il existe des entiers u et v tels que $au + bv = \text{PGCD}(a ; b)$ (on les trouve en remontant l'algorithme d'Euclide).
- Théorème de Bézout : a et b sont premiers entre eux $\iff$ il existe des entiers u et v tels que $au + bv = 1$.
- Théorème de Gauss : si $a \mid bc$ et si a et b sont premiers entre eux, alors $a \mid c$.
- Si $a \mid c$, $b \mid c$ et si a et b sont premiers entre eux, alors $ab \mid c$.

Exemple : $5 \times (-7) + 12 \times 3 = 1$, donc 5 et 12 sont premiers entre eux.

Équations $ax + by = c$ et inverse modulo n

Tle exp.

- $ax + by = c$ a des solutions entières si et seulement si $\text{PGCD}(a ; b)$ divise c.
- Si a et b sont premiers entre eux et si $(x_0 ; y_0)$ est une solution, les solutions sont $x = x_0 + bk$ et $y = y_0 - ak$, k entier (on soustrait, puis on applique Gauss).
- Inverse modulo n : si $\text{PGCD}(a ; n) = 1$, il existe a' tel que $aa' \equiv 1\ [n]$; alors $ax \equiv b\ [n] \iff x \equiv a'b\ [n]$.

Exemples : les solutions de $5x + 12y = 1$ sont $x = -7 + 12k$ et $y = 3 - 5k$. Comme $3 \times 5 = 15 \equiv 1\ [7]$, $3x \equiv 4\ [7] \iff x \equiv 5 \times 4 \equiv 6\ [7]$.

Nombres premiers

Tle exp.

- p est premier s'il a exactement deux diviseurs positifs, 1 et p (1 n'est pas premier). Il y a une infinité de nombres premiers.
- Test : si $n \geqslant 2$ n'est divisible par aucun nombre premier p tel que $p^2 \leqslant n$, alors n est premier.
- Lemme d'Euclide : si un nombre premier p divise ab, alors $p \mid a$ ou $p \mid b$.
- Décomposition : tout entier $n \geqslant 2$ s'écrit de façon unique (à l'ordre près) $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$.
- Nombre de diviseurs positifs : $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.
- PGCD : produit des facteurs premiers communs, chacun avec son **plus petit** exposant.

Exemple : $360 = 2^3 \times 3^2 \times 5$ a $(3+1)(2+1)(1+1) = 24$ diviseurs positifs.

Petit théorème de Fermat

Tle exp.

Si p est premier et a entier : $a^p \equiv a \ [p]$. Si de plus p ne divise pas a : $a^{p-1} \equiv 1 \ [p]$.

Exemple : 7 est premier et ne divise pas 3, donc $3^6 \equiv 1 \ [7]$. Comme $100 = 6 \times 16 + 4$: $3^{100} = (3^6)^{16} \times 3^4 \equiv 3^4 \equiv 4 \ [7]$, car $3^4 = 81 = 7 \times 11 + 4$.