Arithmétique dans $\mathbb{Z}$

Chapitre 16

Divisibilité dans $\mathbb{Z}$

On étend les notions de TC à tout $\mathbb{Z}$.

Définition
Pour $a, b \in \mathbb{Z}$ avec $b \neq 0$, on dit que b *divise* a, noté $b \mid a$, s'il existe $k \in \mathbb{Z}$ tel que $a = bk$.

Propriété
- $a \mid a$, $1 \mid a$, $a \mid 0$ pour tout $a \neq 0$.
- Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
- Si $a \mid b$ et $a \mid c$, alors $a \mid (ub + vc)$ pour tous $u, v \in \mathbb{Z}$.
- Si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$.

Division euclidienne dans $\mathbb{Z}$

Théorème
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r, \quad 0 \leq r < |b|.$$

PGCD et algorithme d'Euclide

Définition
Pour $a, b \in \mathbb{Z}$ non tous deux nuls, le $\mathrm{PGCD}(a, b)$ est le plus grand entier positif divisant à la fois a et b.

Théorème — Algorithme d'Euclide
Si $a = bq + r$, alors $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$. En itérant, on arrive à un reste nul ; le dernier reste non nul est le PGCD.

Nombres premiers entre eux

Définition
$a, b \in \mathbb{Z}$ sont *premiers entre eux* si $\text{PGCD}(a, b) = 1$.

Théorème — Bézout — version élémentaire
Si a, b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$.

Cette identité de Bézout est admise au niveau 1BAC SM, formellement démontrée en 2BAC SM. On peut aussi la voir comme conséquence de l'algorithme d'Euclide étendu.

Théorème — Théorème de Gauss
Si $a \mid bc$ et a premier avec b, alors $a \mid c$.

Nombres premiers

Définition
Un entier $p > 1$ est *premier* si ses seuls diviseurs positifs sont 1 et p.

Théorème — Décomposition unique
Tout entier $n \geq 2$ s'écrit de manière unique (à l'ordre près) comme produit de nombres premiers.

Propriété — PGCD et PPCM via factorisation
Si $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$:

$$\text{PGCD} = \prod p_i^{\min(\alpha_i, \beta_i)}, \quad \text{PPCM} = \prod p_i^{\max(\alpha_i, \beta_i)}.$$

Et $\text{PGCD}(a, b) \times \text{PPCM}(a, b) = |ab|$.

Congruences modulo n (introduction)

Définition
Pour $n \in \mathbb{N}^*$, on dit que $a \equiv b \bmod n$ (lu « a congru à b modulo n ») si $n \mid (b - a)$. C'est une relation d'équivalence.

Propriété — Compatibilité
Si $a \equiv a' \bmod n$ et $b \equiv b' \bmod n$:
- $a + b \equiv a' + b' \bmod n$.

- $ab \equiv a'b' \bmod n$.
- Pour tout $k \in \mathbb{N}$, $a^k \equiv a'^k \bmod n$.

Exemple. Modulo 7 : $10 \equiv 3 \bmod 7$. Donc $10^3 = 1000 \equiv 3^3 = 27 \equiv 6 \bmod 7$ (car $27 = 7 \times 3 + 6$).

Applications

Problèmes de divisibilité

Exemple. Démontrer que $7 \mid \left(2^{\{3n\}} - 1\right)$ pour tout $n \in \mathbb{N}$. En effet $2^3 = 8 \equiv 1 \bmod 7$, donc $2^{\{3n\}} = \left(2^3\right)^n \equiv 1^n = 1 \bmod 7$.

Critères de divisibilité

Modulo 9 : $10 \equiv 1$, donc tout nombre est congru à la somme de ses chiffres modulo 9. Un nombre est divisible par 9 ssi la somme de ses chiffres l'est.