Arithmétique dans $\mathbb{Z}$

Chapitre 9

Rappels et identité de Bézout

En 2e Bac SM on reprend l'arithmétique de 1BAC SM avec plus de rigueur.

Théorème — Identité de Bézout
Soient $a, b \in \mathbb{Z}$ non tous deux nuls et $d = \text{PGCD}(a, b)$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$. En particulier : a, b premiers entre eux ssi il existe u, v tels que $au + bv = 1$.

L'algorithme d'Euclide étendu fournit une méthode algorithmique pour trouver u, v.

Théorèmes de Gauss et applications

Théorème — Gauss
Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $\text{PGCD}(a, b) = 1$, alors $a \mid c$.

Démonstration. Par Bézout, $au + bv = 1$. Multiplier par c : $auc + bvc = c$. $a \mid auc$ et $a \mid bc$ donc $a \mid bvc$, donc $a \mid c$. ∎

Propriété
Si $a \mid c$, $b \mid c$ et $\text{PGCD}(a, b) = 1$, alors $ab \mid c$.

Équations diophantiennes linéaires

Théorème — Équations $a x + b y = c$
Soient $a, b, c \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$ et $d = \text{PGCD}(a, b)$.

- L'équation $ax + by = c$ admet des solutions entières ssi $d \mid c$.
- Si (x_0, y_0) est une solution particulière, l'ensemble des solutions est : $x = x_0 + \left(\frac{b}{d}\right)k$, $y = y_0 - \left(\frac{a}{d}\right)k$, $k \in \mathbb{Z}$.

Exemple. Résoudre $15x + 6y = 9$. $d = 3$ divise 9. Solution particulière : $15 \times 1 + 6 \times (-1) = 9$. Général : $x = 1 + 2k, y = -1 - 5k$.

Congruences

Définition
$a \equiv b \bmod n$ si $n \mid (a-b)$. Relation d'équivalence.

Propriété — Opérations
Si $a \equiv a'$ et $b \equiv b'$ (tous modulo n) : $a+b \equiv a'+b'$, $ab \equiv a'b'$, $a^k \equiv a'^k$.

Théorème — Petit théorème de Fermat
Si p est premier et $a \in \mathbb{Z}$ non multiple de p, alors :

$$a^{p-1} \equiv 1 \bmod p.$$

Plus généralement, $a^p \equiv a \bmod p$ pour tout $a \in \mathbb{Z}$.

Résolution d'équations modulo n

Pour résoudre $ax \equiv b \bmod n$:

- Si $d = \text{PGCD}(a, n)$ ne divise pas b, pas de solution.
- Sinon, simplifier par d pour obtenir $a'x \equiv b' \bmod n'$ avec $\text{PGCD}(a', n') = 1$, puis utiliser l'inverse de a' modulo n' (fourni par Bézout).

Exemple. Résoudre $5x \equiv 3 \bmod 11$. Inverse de 5 modulo 11 : par Bézout, $5 \times 9 = 45 = 4 \times 11 + 1$, donc 9 est l'inverse. $x \equiv 27 \equiv 5 \bmod 11$.

Applications en cryptographie

Les congruences et le petit théorème de Fermat sont les fondations de la cryptographie moderne (RSA en particulier). À ce niveau, on se limite à des exercices de manipulation.