COURS • 4ÈME ANNÉE MATHÉMATIQUES

Chapitre 14 — Arithmétique

◆ Sommaire

1. Divisibilité dans Z
2. Division euclidienne
3. Congruences
4. PGCD, PPCM
5. Théorèmes de Bézout, de Gauss et de Fermat
6. Équations ax+by=c

◆ Objectifs du chapitre

– Utiliser la division euclidienne et les congruences pour calculer un reste, un chiffre des unités ou des dizaines, et démontrer une divisibilité.

– Dresser une table de congruences pour étudier tous les cas possibles modulo n.

– Calculer un PGCD par l'algorithme d'Euclide et en déduire des coefficients de Bézout.

– Utiliser le lemme de Gauss, le théorème de Bézout et le petit théorème de Fermat.

– Résoudre les équations diophantiennes $ax+by=c$ et les systèmes de congruences simples ; traiter des problèmes concrets (partages, codage).

Le plan du cours suit celui du manuel officiel (Tome 2, chapitres 7 et 8 : *Divisibilité dans* $\mathbb{Z}$; *Identité de Bézout*). Les lettres a, b, c, n désignent des entiers relatifs.

1 Divisibilité dans Z

◆ Définition

Soit d un entier non nul. On dit que d **divise** a (ou que a est un multiple de d) s'il existe un entier q tel que $a=dq$. On note $d \mid a$.

Un entier naturel $p \geq 2$ est **premier** si ses seuls diviseurs positifs sont 1 et p.

◆ Propriétés

Pour des entiers non nuls a, b et un entier c :

– si $d \mid a$, alors $-d \mid a$;

– si $a \mid b$ et $b \mid a$, alors $a=b$ ou $a=-b$;

– si $a \mid b$ et $b \mid c$, alors $a \mid c$;

– si $a \mid b$ et $a \mid c$, alors $a \mid xb + yc$ pour tous entiers x, y.

◆ **Factorisations utiles**

Pour tout entier $n \geq 1$:

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}\right),$$

$$a^n + b^n = (a+b)\left(a^{n-1} - a^{n-2}b + \ldots + b^{n-1}\right) \text{si } n \text{ est impair.}$$

En particulier $a - b \mid a^n - b^n$.

2 Division euclidienne

◆ **Théorème**

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

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

q est le **quotient** et r le **reste** de la division euclidienne de a par b. Le reste appartient à $\{0, 1, \ldots, |b| - 1\}$.

3 Congruences

◆ **Définition**

Soit n un entier naturel non nul. On dit que a est **congru à** b **modulo** n, et on note $a \equiv b\,[n]$, si $a - b$ est un multiple de n.

Pour tout entier a, il existe un unique $r \in \{0, \ldots, n-1\}$ tel que $a \equiv r\,[n]$: c'est le reste de a modulo n. Deux entiers sont congrus modulo n si et seulement s'ils ont le même reste modulo n.

◆ **Propriétés**

La congruence modulo n est réflexive, symétrique et transitive. Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors

$$a + c \equiv b + d\,[n], ac \equiv bd\,[n], ha \equiv hb\,[n] (h \in \mathbb{Z}), a^m \equiv b^m\,[n] (m \in \mathbb{N}^*).$$

◆ **Méthode**

Méthode — calculer a^N modulo n. On cherche une petite puissance $a^k \equiv 1\,[n]$ (ou $\equiv -1$), on écrit la division euclidienne $N = kq + r$, et alors $a^N = \left(a^k\right)^q a^r \equiv a^r\,[n]$.

◆ **Méthode — table de congruences**

Pour étudier une expression polynomiale en x modulo n, on examine les n restes possibles de x (ou de chaque variable) dans un tableau.

4 PGCD, PPCM

◆ **Théorème et définition**

Pour a, b non nuls, il existe un unique entier naturel d tel que : $d \mid a$, $d \mid b$, et tout diviseur commun de a et b divise d. On le note $a \wedge b$ (PGCD). Deux entiers sont **premiers entre eux** si $a \wedge b = 1$.

Il existe un unique entier $m > 0$ multiple de a et de b qui divise tout multiple commun : c'est le PPCM, noté $a \vee b$.

◆ **Propriétés**

– $a \wedge b = |a| \wedge |b|$; si $b \mid a$, $a \wedge b = |b|$; $(ka) \wedge (kb) = |k|(a \wedge b)$.

– **Algorithme d'Euclide :** si $a = bq + r$ avec $r \neq 0$, alors $a \wedge b = b \wedge r$; le PGCD est le dernier reste non nul.

– Il existe un unique couple (a', b') tel que $a = (a \wedge b)a'$, $b = (a \wedge b)b'$ et $a' \wedge b' = 1$.

– $(a \wedge b) \times (a \vee b) = |ab|$.

5 Théorèmes de Bézout, de Gauss et de Fermat

◆ **Théorème de Bézout**

$a \wedge b = 1$ si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$.

◆ **Corollaire**

Si $d = a \wedge b$, il existe deux entiers u, v tels que $au + bv = d$.

◆ **Lemme de Gauss**

Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

◆ **Conséquences**

– Si $a \wedge b = 1$, $a \mid n$ et $b \mid n$, alors $ab \mid n$.

– (**Lemme d'Euclide**) Si un nombre premier p divise bc, alors $p \mid b$ ou $p \mid c$.

– **Inverse modulo b.** Si $b \geq 2$ et $a \wedge b = 1$, il existe un unique $u \in \{1, \ldots, b-1\}$ tel que $au \equiv 1 [b]$.

◆ Petit théorème de Fermat

Soit p un nombre premier et a un entier non divisible par p. Alors $a^{p-1} \equiv 1 [p]$.

Pour tout entier a : $a^p \equiv a [p]$.

6 Équations ax+by=c

◆ Théorème

Soit $d = a \wedge b$. L'équation $ax + by = c$ admet des solutions dans $\mathbb{Z} \times \mathbb{Z}$ si et seulement si $d \mid c$.

◆ Méthode

Méthode de résolution (cas $a \wedge b = 1$, sinon on divise d'abord par d).

1. On trouve une solution particulière (x_0, y_0) (évidente, ou par l'algorithme d'Euclide « remonté »).
2. Par différence : $a(x - x_0) = -b(y - y_0)$. D'après le lemme de Gauss, $b \mid x - x_0$; on obtient
$$x = x_0 + bk, y = y_0 - ak, k \in \mathbb{Z}.$$
3. On vérifie que ces couples sont bien solutions.

◆ Attention

Dans une équation à inconnues **naturelles** (nombres de pièces, d'objets…), on termine en sélectionnant les valeurs de k compatibles avec les contraintes de signe ou d'encadrement.