Programme de Colle 13

Chapitre 13 : Arithmétique dans $\mathbb{Z}$

Dans ce qui suit, les lettres a, b, c, d, α et β désignent, sauf mention contraire, des entiers relatifs.

- notions de diviseur et de multiple, notation $a \mid b$, l'ensemble des multiples de a est $a\mathbb{Z}$, l'ensemble des diviseurs de b est $\mathscr{D}(b) = \left\{d \in \mathbb{Z} \,\middle|\, d \mid b\right\}$
- dans $\mathbb{Z}$, $a \mid b$ et $b \mid a$ si et seulement si $|a| = |b|$ (les entiers a et b sont dits *associés*) ; la relation $\mid$ est une relation d'ordre sur $\mathbb{N}$
- si $d \mid a$ et $d \mid b$, alors $d \mid \alpha a + \beta b$
- si $c \in \mathbb{Z}^*$, alors $a \mid b$ si et seulement si $ac \mid bc$
- théorème de la division euclidienne (application : les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$)
- plus grand diviseur commun (PGCD) de deux entiers relatifs a et b, notation $a \wedge b$ (si $a = b = 0$, alors $a \wedge b = 0$ et, sinon, $a \wedge b = \max(\mathscr{D}(a) \cap \mathscr{D}(b)) \in \mathbb{N}^*$)
- algorithme d'Euclide, algorithme d'Euclide étendu pour la détermination pratique du PGCD, les diviseurs communs à a et à b sont les diviseurs de $a \wedge b$
- si $k \in \mathbb{N}^*$, alors $(ka) \wedge (kb) = k(a \wedge b)$
- relation de Bézout :
$$\exists\, u, v \in \mathbb{Z}, \qquad au + bv = a \wedge b,$$
on obtient le couple de coefficients de Bézout (u, v) par l'algorithme d'Euclide *étendu*
- entiers premiers entre eux, théorème de Bézout :
$$a \wedge b = 1 \iff (\exists\, u, v \in \mathbb{Z},\ au + bv = 1)$$
- si $a \neq 0$ ou $b \neq 0$, alors les entiers $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux, application : tout nombre rationnel peut-être mis sous *une* forme irréductible
- si $a \wedge c = 1$ et $b \wedge c = 1$, alors $ab \wedge c = 1$
- lemme de Gauss : si $a \wedge b = 1$ et si $a \mid bc$, alors $a \mid c$, applications :
  — pour tout $r \in \mathbb{Q}$, il existe un unique couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $a \wedge b = 1$ et $r = \frac{a}{b}$ (unicité de la forme irréductible d'un nombre rationnel)
  — résolution d'équations diophantiennes $ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$
- si a et b sont premiers entre eux et si a et b divisent c, alors ab divise c
- plus petit multiple commun (PPCM) de deux entiers relatifs a et b, notation $a \vee b$ (si $a = b = 0$, alors $a \vee b = 0$ et, sinon, $a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*)$)
- relation $|ab| = (a \wedge b)(a \vee b)$, si a et b sont premiers entre eux, alors $a \vee b = |ab|$
- PGCD d'un nombre fini d'entiers $a_1, \ldots, a_n$, notation $a_1 \wedge \cdots \wedge a_n$, relation de Bézout
- les entiers $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$, si les entiers sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble (et la réciproque est fausse)
- nombres premiers (ensemble noté $\mathscr{P}$), si $p \in \mathscr{P}$ divise ab, alors $p \mid a$ ou $p \mid b$, tout entier $n \geqslant 2$ admet un diviseur premier, l'ensemble $\mathscr{P}$ est infini
- théorème fondamental de l'arithmétique : pour tout $n \in \mathbb{N} \setminus \{0, 1\}$, il existe un unique entier $r \in \mathbb{N}^*$, une unique famille de nombres premiers distincts (à l'ordre près des facteurs) $p_1, \ldots, p_r$ et une unique famille d'entiers naturels non nuls $\alpha_1, \ldots, \alpha_r$ tels que $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$

- pour $p \in \mathscr{P}$, valuation p-adique d'un entier, notée $v_p(a)$:

$$v_p(a) = \max\left\{k \in \mathbb{N} \,\middle|\, p^k \mid n\right\}$$

- formule $v_p(ab) = v_p(a) + v_p(b)$, b divise a si et seulement si $v_p(b) \leqslant v_p(a)$ pour tout $p \in \mathscr{P}$, décomposition en produit de facteurs premiers du PGCD et du PPCM :

$$a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))} \qquad \text{et} \qquad a \vee b = \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$$

- relation de congruence modulo un entier, compatibilité de la congruence avec l'addition, la multiplication et l'exponentiation positive entière
- notion d'élément inversible modulo $n \in \mathbb{N}^*$ (un entier $a \in \mathbb{Z}$ est inversible modulo n s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1\,[n]$), un entier a est inversible modulo n si et seulement si $a \wedge n = 1$
- petit théorème de Fermat

Questions de cours

- Énoncer et démontrer le théorème de Bézout.
- Si $a, b, c \in \mathbb{Z}$ sont tels que $a \wedge c = 1$ et $b \wedge c = 1$, alors $(ab) \wedge c = 1$.
- L'ensemble $\mathscr{P}$ des nombres premiers est infini.
- Soit $p \in \mathscr{P}$. Pour tout $k \in [\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$. De plus $(a+b)^p \equiv a^p + b^p\,[p]$.
- Énoncer et démontrer le petit théorème de Fermat.

Remarques aux colleurs

- **Merci d'être très exigeants sur la rédaction.**