

Chapitre 17 : Arithmétique

Dans ces lignes, le terme “entier” est synonyme “d’entier relatif”.

1 – Divisibilité dans $\mathbb{Z}$

Définitions : diviseur et multiple. Exemples : pour tout $n \in \mathbb{Z}$, $1|n$ et $(-1)|n$; si $n \in \mathbb{Z} \setminus \{\pm 1\}$, n admet au moins quatre diviseurs : ± 1 et $\pm n$. 0 ne divise aucun entier non nul, et est multiple de tout entier.

Propriétés. Soient a, b, c et d entiers.

$$1/ (\forall (n, m) \in \mathbb{Z}^2, a|b \text{ et } a|c \implies (a|nb + mc))$$

$$2/ (a|c \text{ et } b|d \implies (ab|cd))$$

Notation. Soit a un entier. On note $a\mathbb{Z} = \{ka / k \in \mathbb{Z}\}$.

Propriétés. Soient a, b et c dans $\mathbb{Z}$.

$$\text{Alors : } 1/ a|a \quad 2/ [a|b \text{ et } b|a] \implies |a| = |b| \quad [a|b \text{ et } b|c] \implies a|c$$

Conséquence : la relation de divisibilité est une relation d’ordre dans $\mathbb{N}$.

2 – Division euclidienne dans $\mathbb{Z}$ et PGCD

Théorème (division euclidienne). Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d’entiers tels que : $a = bq + r$ et $0 \leq r < b$.
Conséquence : $b|a \iff r = 0$.

PGCD. Définition et propriétés.

Algorithme d’Euclide pour le calcul du PGCD de deux entiers.

Théorème (Bezout). $\forall (a, b) \in \mathbb{Z}^2, \exists (u, v) \in \mathbb{Z}^2, au + bv = a \wedge b$.

Corollaire. Soient a et b deux entiers. On a : $[d|a \text{ et } d|b] \iff [d| a \wedge b]$.

Ainsi, $a \wedge b$ est aussi le plus grand commun diviseur à a et b pour la relation (d’ordre, dans $\mathbb{N}$) de divisibilité.

Corollaire. Soient a et b deux entiers. On a : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Corollaire. Soient a et b deux entiers. S’il existe deux entiers u et v tels que $au + bv = 1$, alors $a \wedge b = 1$

3 – Congruences

Définition. Soient a, b et n trois entiers relatifs. On dit que a est **congru à b modulo n** si $b - a$ est multiple de n , c’est à dire s’il existe $k \in \mathbb{Z}$ tel que : $b = a + kn$. On le note $a \equiv b [n]$.

Rq : $a \equiv 0 [n]$ si et seulement si a est multiple de n .

Lemme : la relation de congruence est une relation d’équivalence ; propriétés algébriques des congruences.

Lemme. Soit n un entier, $n \geq 2$, et a un entier quelconque. On a : $a \equiv r [n]$, où r est le reste dans la division euclidienne de a par n .

Définition. Soit a et n deux entiers, avec $n \neq 0$. On appelle **inverse de a modulo n** un entier b tel que $ab \equiv 1 [n]$.

Exemples. 3 a pour inverse 5 modulo 7. Mais 12 et -2 sont aussi des inverses de 3 modulo 7. Plus généralement : si b est un inverse de a modulo n , alors $b + kn$ est un inverse de a modulo n (pour tout $k \in \mathbb{Z}$).

Propriété. Soient a et b deux entiers, avec $b \neq 0$. L’entier a est inversible modulo b si et seulement si $a \wedge b = 1$.

4 – Entiers premiers entre eux, Lemme de Gauss

Définition. Deux entiers a et b sont **premiers entre eux** si $a \wedge b = 1$.

Lemme. Soient a et b deux entiers non nuls. On note $d = a \wedge b$.

Alors : $\exists ! (a', b') \in \mathbb{Z}^2$ tel que : $a = da', b = db'$ et $a' \wedge b' = 1$.

Théorème (Lemme de Gauss). Soient a, b et c trois entiers.

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

Propriété. Si $a \wedge b = 1$, alors : $a|c$ et $b|c$ impliquent $ab|c$.

5 – Nombres premiers

Définition. Un nombre **premier** est un entier admettant exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

Notation. On note $\mathcal{P}$ l’ensemble des nombres premiers.

Observation. Tout entier $n \geq 2$ composé admet au moins un diviseur compris entre 2 et $\lfloor \sqrt{n} \rfloor$.

Théorème. Soit $p \in \mathbb{N}$. LASSE :

1/ p est premier

2/ p est premier avec tout entier qu’il ne divise pas.

3/ p est premier avec tout entier compris entre 2 et $p - 1$.

► Théorème de Fermat

Lemme. Soit $p \in \mathcal{P}$. Alors : $\forall k \in \llbracket 1, p-1 \rrbracket, \quad p \mid \binom{p}{k}$

“Petit” théorème de Fermat. $\forall p \in \mathcal{P}, \forall m \in \mathbb{Z}, m^p \equiv m \pmod{p}$.

Corollaire. $\forall p \in \mathcal{P}, \forall m \in \mathbb{Z} \setminus p\mathbb{Z}, m^{p-1} \equiv 1 \pmod{p}$.

QUESTIONS DE COURS

- **Théorème (division euclidienne).** Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que : $a = bq + r$ et $0 \leq r < b$.
- **Propriété.** Soient a et b deux entiers. On a : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.
- **Propriété.** Soit a et b deux entiers, $b \neq 0$. L'entier a est inversible modulo b si et seulement si $a \wedge b = 1$.

- **Théorème (Lemme de Gauss).** Soient a, b et c trois entiers. Si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.
- **Propriété.** $\forall p \in \mathcal{P}, \forall k \in \llbracket 1, p-1 \rrbracket, \quad p \mid \binom{p}{k}$
- **Théorème (Fermat).** Soit p un nombre premier. Alors : $\forall m \in \mathbb{Z}, m^p \equiv m \pmod{p}$.