

- La relation « divise » : réflexivité, transitivité, antisymétrie « au signe près ». Propriété d'Archimède. Division euclidienne : étant donnés $a, b \in \mathbb{Z}, b \neq 0$, il existe un unique couple (q, r) d'entiers relatifs tel que

$$\begin{cases} a &= bq + r \\ 0 &\leq r < |b| \end{cases}$$

Application à la détermination des sous-groupes de $\mathbb{Z}$.

- PGCD de deux entiers relatifs. Étant donnés deux entiers relatifs a et b , il existe un entier relatif δ , unique au signe près, vérifiant $\forall d \in \mathbb{Z}, d \mid a \text{ et } d \mid b \iff d \mid \delta$ (démonstration via les sous-groupes de $\mathbb{Z}$).
- Entiers premiers entre-eux. Théorème de Bézout, théorème de Gauss.
- Propriétés de base : un entier est premier avec un produit si et seulement si il est premier avec chacun des facteurs. Des entiers premiers entre-eux deux à deux divisent un entier b si et seulement si leur produit divise b . Étant donnés trois entiers a, b, δ , on a $\delta = a \wedge b$ si et seulement si il existe deux entiers a_1 et b_1 tels que

$$\begin{cases} a &= \delta a_1 \\ b &= \delta b_1 \\ a_1 \wedge b_1 &= 1 \end{cases}$$

- Algorithme d'Euclide. Application au calcul des coefficients de Bézout et à la résolution d'équations du type « $x, y \in \mathbb{Z}, ax + by = c$ ».
 - PPCM de deux entiers relatifs. Étant donnés deux entiers relatifs a et b , il existe un entier relatif μ , unique au signe près, vérifiant $\forall m \in \mathbb{Z}, a \mid m \text{ et } b \mid m \iff \mu \mid m$. On a $\mu = \delta a_1 b_1$ avec les notations données un peu plus haut. Notation $\mu = a \vee b$. Relation $\mu\delta = ab$.
 - Nombres premiers. Deux nombres premiers distincts sont premiers entre-eux. Tout entier ≥ 2 possède un diviseur premier. L'ensemble des nombres premiers est infini. Existence et unicité (à l'ordre près des facteurs) de la décomposition d'un entier naturel supérieur ou égal à 2 en produit de nombres premiers. Valuation p -adique d'un entier ≥ 1 . Application au calcul du pgcd et du ppcm.
 - Relation de congruence modulo un entier sur $\mathbb{Z}$. Opérations sur les congruences : somme, produit. Petit théorème de Fermat.
 - Introduction aux anneaux $\mathbb{Z}/n\mathbb{Z}$. Si n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps. Sinon, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre (et n'est donc pas un corps).
-