Divisibilité dans $\mathbb{Z}$.

Soient a et b deux entiers relatifs, b étant non nul. On dit que b divise a si et seulement si il existe un entier relatif k tel que $a = kb$. La phrase « a divise b » se note $a|b$.

Propriétés.

- Pour tout entier relatif non nul a, $a|a$.
- Pour tous entiers relatifs non nuls a, b et c, si $a|b$ et $b|c$ alors $a|c$.
- Soient a, b et c trois entiers relatifs, a étant non nul. Si $a|b$ et $a|c$, alors pour tous entiers relatifs λ et μ, $a|(\lambda b + \mu c)$.

Division euclidienne dans $\mathbb{Z}$.

Soient a et b deux entiers naturels, b étant non nul. Il existe un couple (q, r) d'entiers naturels et un seul tel que

$$① \ a = bq + r \text{ et } ② \ 0 \leq r < b.$$

q est le quotient et r le reste de la division euclidienne de a par b.

Congruences dans $\mathbb{Z}$.

Soit n un entier naturel supérieur ou égal à 2. Soient a et b deux entiers relatifs.
On dit que a est congru à b modulo n si et seulement si $b - a$ est divisible par n. On écrit dans ce cas $a \equiv b \ (n)$ ou $a \equiv b$ (modulo n).

Propriétés. Soit n un entier relatif supérieur ou égal à 2.

- Pour tout entier relatif a, $a \equiv a \ (n)$.
- Pour tous entiers relatifs a et b, si $a \equiv b \ (n)$ alors $b \equiv a \ (n)$.
- Pour tous entiers relatifs a, b et c, si $a \equiv b \ (n)$ et $b \equiv c \ (n)$ alors $a \equiv c \ (n)$.
- (Compatibilité avec l'addition) Pour tous entiers relatifs a, b et c, si $a \equiv b \ (n)$ alors $a + c \equiv b + c \ (n)$.
- (Compatibilité avec la multiplication) Pour tous entiers relatifs a, b et c, si $a \equiv b \ (n)$ alors $a \times c \equiv b \times c \ (n)$.

Nombres premiers. Décomposition en facteurs premiers.

Soit n un entier supérieur ou égal à 2. n est premier si et seulement si n admet exactement deux diviseurs à savoir 1 et n.
Il existe une infinité de nombres premiers.
Théorème fondamental de l'arithmétique. Tout entier naturel supérieur ou égal à 2 se décompose en produit de nombres premiers. Cette décomposition est unique à l'ordre près des facteurs.

PPCM, PGCD.

Soient a et b deux entiers naturels supérieurs ou égaux à 2.
On suppose que $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ où $p_1, \dots, p_k$ sont k nombres premiers deux à deux distincts et $\alpha_1, \dots, \alpha_k$, $\beta_1, \dots, \beta_k$ sont des entiers naturels.
On note m_1 le plus petit des deux nombres α_1 et β_1 et M_1 le plus grand. On note m_2 le plus petit des deux nombres α_2 et β_2 et M_2 le plus grand...
Le PGCD (plus grand commun diviseur) de a et b est $p_1^{m_1} \dots p_k^{m_k}$ et le PPCM (plus petit commun multiple) de a et b est $p_1^{M_1} \dots p_k^{M_k}$.
Exemple. $48 = 2^4 \times 3$ et $36 = 2^2 \times 3^2$. Donc $\text{PGCD}(36, 48) = 2^2 \times 3 = 12$ et $\text{PPCM}(36, 48) = 2^4 \times 3^2 = 144$.

Algorithme d'Euclide. On a le résultat préliminaire suivant : si a et b sont deux entiers naturels non nuls tels que $b < a$ et si $a = bq + r$ où q et r sont deux entiers naturels tels que $0 \leq r < b$, alors $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.

On veut maintenant le PGCD de a et de b.
On pose la division euclidienne de a par b. Si $r = 0$, le PGCD de a et de b est $r_0 = r$.
Sinon, on pose la division euclidienne de b par $r_0 = r$: $b = q_1 r + r_1$ avec $0 \leq r_1 < r_0$. Si $r_1 = 0$ le PGCD de b et de r_0 est r_0 et donc le PGCD de a et de b est r_0.
Sinon, on pose la division euclidienne de r_0 par r_1...
Cette algorithme s'arrête quand on trouve un reste nul, ce qui se produit toujours. Le PGCD de a et b est le dernier reste non nul.

Théorèmes de Bézout et Gauss.

Théorème de Bézout. Soient a et b deux entiers relatifs non nuls.
a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.
Théorème de Gauss. Soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.