5 Arithmétique

5.1 Divisibilité et nombres premiers

Définition 5.1 (**Divisibilité**). *Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$. On dit que a divise b, et note $a|b$ s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. On dit alors aussi que b est un multiple de a.*
Pour tout $b \in \mathbb{N}$, on notera $\mathrm{div}(b) = \{a \in \mathbb{N} : a|b\}$ *l'ensemble des diviseurs (positifs) de b.*
Pour tout $a, b \in \mathbb{N}$, on notera $\mathrm{div}(a,b) = \mathrm{div}(a) \cap \mathrm{div}(b)$ *l'ensemble des diviseurs communs (positifs) à a et b.*

Définition 5.2. *On dit que $p \in \mathbb{N}$ est un nombre premier si $p \geq 2$ et* $\mathrm{div}(p) = \{1, p\}$.

Lemme 5.3 (**Existence d'un facteur premier**). *Soit $n \in \mathbb{N}$, $n \geq 2$. Soit p le plus petit diviseur de n supérieur ou égal à 2. Alors p est premier.*

Théorème 5.4 (**Théorème d'Euclide**). *Il existe une infinité de nombres premiers.*

Théorème 5.5 (**Théorème fondamental de l'arithmétique**). *Soit $n \geq 2$ un entier, alors il existe une unique écriture de n sous la forme*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où, pour tout $i \in \{1, ..., k\}$, p_i est un nombre premier, $\alpha_i \in \mathbb{N}^*$ et $p_1 < p_2 < ... < p_k$.

Proposition 5.6 (**Division euclidienne**). *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ d'entiers tels que*

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

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

5.2 PGCD et PPCM et algorithme d'Euclide

Définition 5.7 (**Plus Grand Commun Diviseur (PGCD)**). *Soit $(a, b) \in \mathbb{Z}^2$ tels que $(a, b) \neq (0, 0)$, alors l'ensemble* $\mathrm{div}(a, b)$ *des diviseurs communs à a et b est fini et non-vide (car il contient $n = 1$). Il admet donc un plus grand élément noté* $\mathrm{PGCD}(a, b)$.

Proposition 5.8 (**Homogénéité du PGCD**). *Soient $(a, b) \in \mathbb{Z}^2$ deux entiers non-nuls. Alors,*

$$\forall k \in \mathbb{N}^*, \quad \mathrm{PGCD}(ka, kb) = k \times \mathrm{PGCD}(a, b).$$

Proposition 5.9 (**PGCD et décomposition en facteurs premiers**). *Supposons qu'il existe k nombres premiers distincts $\{p_1, ..., p_k\}$ et $2k$ nombres entiers (éventuellement nuls) $\{\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_k\}$ tels que*

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad \text{et} \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors on a $\mathrm{PGCD}(a, b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$.

Algorithme d'Euclide pour calculer le PGCD.
Remarques préliminaires : $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a - b)$, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a)$ et $\mathrm{PGCD}(a, 0) = a$.
Principe de l'algorithme d'Euclide : quitte à échanger a et b, on peut supposer que $a \geq b$.

- si $b = 0$, alors on a $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a, 0) = a$.
- si $b \neq 0$, alors on effectue la division euclidienne de a par b, $a = bq + r$ et on utilise la remarque préliminaire (q fois) pour dire que $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a - qb) = \mathrm{PGCD}(b, r)$.

On réitère ce principe jusqu'à obtenir $\mathrm{PGCD}(d, 0)$ où d sera donc $d = \mathrm{PGCD}(a, b)$.

Définition 5.10 (**Plus Petit Commun Multiple (PPCM)**). *Soient* $(a,b) \in \mathbb{Z}^2$ *tels que* $(a,b) \neq (0,0)$*, alors l'ensemble des multiples communs à a et b*

$$\{n \in \mathbb{N}^* : a|n \text{ et } b|n\}$$

est non-vide (car il contient ab). Il admet donc un plus petit élément noté $\text{PPCM}(a,b)$.

Proposition 5.11 (**PPCM et décomposition en facteurs premiers**). *Supposons qu'il existe k nombres premiers distincts* $\{p_1,...,p_k\}$ *et* $2k$ *nombres entiers (éventuellement nuls)* $\{\alpha_1,...,\alpha_k,\beta_1,...,\beta_k\}$ *tels que*

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad \text{et} \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors on a $\text{PPCM}(a,b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}$.

Proposition 5.12 (**Lien entre le PGCD et le PPCM**). *Pour tout* $(a,b) \in \mathbb{Z}^2$ *tels que* $(a,b) \neq (0,0)$*,*

$$\text{PGCD}(a,b) \times \text{PPCM}(a,b) = ab.$$

Définition 5.13 (**Nombres premiers entre eux**). *Soient* $(a,b) \in \mathbb{Z}^2$*. On dit que a et b sont premiers entre eux si* $\text{PGCD}(a,b) = 1$*, c'est-à-dire si le seul diviseur commun positif de a et b est 1.*

Proposition 5.14. *Soient* $(a,b) \in \mathbb{N}^2$ *deux entiers non-nuls. Soit d un diviseur commun à a et b et posons* $a = da'$ *ainsi que* $b = db'$ *avec* $(a',b') \in \mathbb{N}$*. On a*

$$\text{PGCD}(a,b) = d \iff a' \text{ et } b' \text{ sont premiers entre eux.}$$

5.3 Coefficients de Bézout et équations diophantiennes

Théorème 5.15 (**Identité de Bézout**). *Soient a et b deux entiers non nuls, alors il existe* $(u,v) \in \mathbb{Z}^2$*, appelés coefficients de Bézout, tels que*

$$au + bv = \text{PGCD}(a,b).$$

En particulier,

$$a \text{ et } b \text{ sont premiers entre eux} \iff \exists (u,v) \in \mathbb{Z}^2, au + bv = 1.$$

Théorème 5.16 (**Lemme de Gauss**). *Soient* $a,b,c \in \mathbb{Z}^*$ *tels que a et b soient premiers entre eux. Si* $a|bc$ *alors* $a|c$.

Définition 5.17 (**Equation diophantienne**). *On appelle équation diophantienne toute équation de la forme* $ax + by = c$ *avec* $(a,b,c) \in \mathbb{Z}^3$ *et d'inconnues* $(x,y) \in \mathbb{Z}^2$.

Théorème 5.18 (**Solutions d'une équation diophantienne**). *Soient* $a,b,c \in \mathbb{Z}$*, alors :*

1. *L'équation* $ax + by = c$ *admet une solution* $(x,y) \in \mathbb{Z}^2$ *si et seulement si* $\text{PGCD}(a,b)|c$.
2. *Si a et b sont premiers entre eux et* (x_0,y_0) *est une solution particulière de l'équation* $ax + by = c$*, alors l'ensemble des solutions de cette équation est* $S = \{(x_0 + kb, y_0 - ka) \in \mathbb{Z}^2 : k \in \mathbb{Z}\}$.

5.4 Congruences

Définition 5.19 (**Congruences**). *Soit $n \in \mathbb{N}^*$. On dit que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont congrus modulo n si $n|a-b$, c'est-à-dire si $\exists k \in \mathbb{Z}, \quad a = b + kn$. On écrit $a \equiv b\ [n]$.*
C'est aussi équivalent à dire que les divisions euclidiennes de a par n et de b par n donnent le même reste.

Proposition 5.20 (**Opérations sur les congruences**). *Soit $n \in \mathbb{N}^*$ et $(a,b,c,d) \in \mathbb{Z}^4$.*

1. *Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$.*
2. *Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $ac \equiv bd\ [n]$.*
3. *Si $a \equiv b\ [n]$, alors $\forall k \in \mathbb{N}^*$, $a^k \equiv b^k\ [n]$.*

Théorème 5.21 (**Petit théorème de Fermat**). *Soit p un nombre premier et $a \in \mathbb{N}$ tel que $p \nmid a$, alors $a^{p-1} \equiv 1\ [p]$.*

Théorème 5.22 (**Théorème des restes chinois**). *Soient a, b deux entiers naturels non-nuls premiers entre eux et soient $y, z \in \mathbb{Z}$. Alors le système d'inconnue $x \in \mathbb{Z}$*

$$\begin{cases} x \equiv y\ [a] \\ x \equiv z\ [b] \end{cases}$$

admet une unique solution x_0 dans $\{0, 1, ..., ab-1\}$ et l'ensemble des solutions dans $\mathbb{Z}$ de ce système est

$$S = \{x_0 + kab : k \in \mathbb{Z}\}.$$

5.5 Bases de numération

Théorème 5.23 (**Base de numération**). *Soit $b \geq 2$. Tout entier $x \in \mathbb{N}$ peut s'écrire d'une manière unique sous la forme*

$$x = a_n b^n + a_{n-1} b^{n-1} + ... + a_1 b + a_0,$$

où $n \in \mathbb{N}$ et $\forall i \in \{0, ...n\}$, $a_i \in \{0, ..., b-1\}$. On dit alors que $x = \overline{a_n a_{n-1} ... a_0}^b$ (aussi noté $x = (a_n a_{n-1} ... a_0)_b$) est l'écriture de x en base b.