# Chapitre 2. Divisibilité

**Définition 2.1.** Soit $a, b \in \mathbb{Z}$. On dit que $a$ divise $b$, ou que $b$ est un multiple de $a$, s'il existe $q \in \mathbb{Z}$ tel que $b = aq$. Cela sera noté par $a \mid b$. Le cas où $a$ ne divise pas $b$ sera noté par $a \nmid b$.

**Théorème 2.2.** Soient $a$, $b$ et $c$ des entiers

1) $a \mid b$ implique $a \mid kb$ pour tout entier $k$;
2) $a \mid b$ et $b \mid c$ implique $a \mid c$;
3) $a \mid b$ et $a \mid c$ implique $a \mid (bx + cy)$ pour tous entiers $x$ et $y$;
4) $a \mid b$ et $b \mid a$ implique $a = \pm b$;
5) $a \mid b$, $a > 0$, $b > 0$, implique $a < b$;
6) Si $m \neq 0$ est entier, alors $a \mid b$ ssi $ma \mid mb$.

**Preuve.** Facile à faire.

**Théorème 2.3 (Division euclidienne).** Soit $a$ et $d$ des entiers avec $d \geq 1$. Alors il existe des entiers uniques $q$ et $r$ tels que

$$a = dq + r \ \& \ 0 \leq r \leq d - 1.$$

**Preuve.** Considérons l'ensemble

$$S = \{a - dx \geq 0 : \ x \in \mathbb{Z}\}.$$

$S$ est non vide. En effet; si $a \geq 0$, alors $a = a - d.0 \geq 0$ i.e. $a \in S$. Si $a < 0$, l'entier négatif $x_0 < \dfrac{a}{d}$ vérifie $a - dx_0 > 0$ i.e. $a - dx_0 \in S$. Par l'axiome du bon order, il existe un plus petit élément $r \in S$, $r$ s'écrit sous la forme

$$r = a - dq \geq 0, \, q \in \mathbb{Z}.$$

Si $r \geq d$, alors $0 \leq r - d = a - dq - d = a - d(q + 1) < r$ et $r - d \in S$. Ceci contredit la minimalité de $r$. D'où $r < d$ et par conséquent $r$, $q$ vérifient les conditions du théorème.

Prouvons l'unicité. En effet, supposons qu'ils existent des entiers $q_1$, $r_1$, $q_2$ et $r_2$ vérifient

$$a = dq_1 + r_1 = dq_2 + r_2 \text{ où } 0 \leq r_1, r_2 \leq d - 1.$$

Alors $0 \leq |r_1 - r_2| \leq d - 1$ et $d(q_1 - q_2) = (r_2 - r_1)$. Si $q_1 \neq q_2$, alors $|q_1 - q_2| \geq 1$ et $d \leq d|q_1 - q_2| = |r_1 - r_2| \leq d - 1$. Ceci est impossible.

Alors $q_1 = q_2$ et d'ici $r_1 = r_2$.

**Exemple.**

- Division de 23 par 5 : $23 = 5.4 + 3$. Dans ce cas $d = 5, q = 4$ et $r = 3$.
- Division de $-23$ par 5 : $-23 = 5.(-5) + 2$. Dans ce cas $d = 5, q = -5$ et $r = 2$.

**Plus grand commun diviseur**

Soit $E$ un ensemble non vide d'entiers non tous nuls. On a les définitions suivantes

**1)** Si l'entier $d$ divise chaque élément $a \in E$, alors $d$ est appelé un diviseur commun de $E$.

**2)** L'entier positif $d$ est appelé un plus grand commun diviseur de l'ensemble $E$, noté $d = pgcd(E)$, si $d$ est un diviseur commun de $E$ et que tout diviseur commun de $E$ divise $d$. Si $E = \{a_1, a_2, ..., a_r\} \neq \emptyset$ est un ensemble fini d'entiers non tous nuls, nous écrivons $pgcd(E) = (a_1, a_2, ..., a_r)$.

Le théorème suivant est utile pour la démonstration de l'existence du *pgcd*.

**Théorème 2.4.** Soit $H$ un sous-groupe du groupe $(\mathbb{Z}, +)$. Alors il existe un seul entier non négatif $d$ tel que $H$ s'écrit de la façon suivante

$$H = \{0,\ \pm d,\ \pm 2d,\ ...\}.$$

**Preuve.** Nous avons $0 \in H$ car $H$ est un sous-groupe. Si $H = \{0\}$, alors$H = 0\mathbb{Z}$.

Si $H \neq \{0\}$, alors il existe $a \in H$ avec $a \neq 0$. Du fait que $-a \in H$, il s'ensuit que $H$ contient des entiers positifs. Par le principe du bon order, $H$ contient un plus petit entier positif $d$. D'où $dq \in H$ pour tout entier $q$, et donc $d\mathbb{Z} \subset H$.

Soit $a \in H$. Par le Théorème 2.3, on peut écrire $a = dq + r$, où $q$ et $r$ sont des entiers tels que $0 \leq r \leq d - 1$. Puisque $dq \in H$ et $H$ est stable sous soustraction, il s'ensuit que $r = a - dq \in H$. Puisque $0 \leq r < d$ et $d$ est le plus petit entier positif de $H$, nous devons avoir $r = 0$, c'est-à-dire $a = dq \in d\mathbb{Z}$ . Ainsi $H \subset d\mathbb{Z}$. Par conséquent, de ceci et de ce que précède, $H = d\mathbb{Z}$.

Démontrons maintenant l'unicité de $d$. Supposons $H = d\mathbb{Z} = \overline{d}\mathbb{Z}$, où $d$ et $\overline{d}$ sont des entiers positifs, alors $d \in \overline{d}\mathbb{Z}$ ce qui signifie que $d = \overline{d}\overline{q}$ pour un entier $\overline{q}$, et $\overline{d} \in d\mathbb{Z}$ ce qui implique que $\overline{d} = dq$ pour un entier $q$. Par conséquent, $d = \overline{d}\overline{q} = dq\overline{q}$, et donc $q\overline{q} = 1$, d'où $q = \overline{q} = \pm 1$ et $d = \pm\overline{d}$. Puisque $d$ et $\overline{d}$ sont positifs, nous avons $d = \overline{d}$.

**Exemple.** Soit $H$ le sous groupe de tous les entiers $26x + 39y$. Alors $13 = 26 \times (2) + 39 \times (-1) \in H$. D'où $H = 13\mathbb{Z}$.

Nous montrons dans le théorème suivant que tout ensemble non vide d'entiers non tous nuls a un plus grand commun diviseur.

**Théorème 2.5.** Soit $E \neq \emptyset$ un ensemble d'entiers non tous nuls. Alors $E$ a un unique plus grand commun diviseur et il existe des entiers $a_1$, $a_2$, ...,$a_k$ $\in E$ et des entiers $x_1$, $x_2$, ...,$x_k$ tels que

$$pgcd(E) = a_1x_1 + a_2x_2 + ... + a_kx_k.$$

**Proof.** Soit $H \subset \mathbb{Z}$ formée par les entiers qui sont de la forme $a_1x_1 + a_2x_2 + ... + a_kx_k$, avec $a_1$, $a_2$, ...,$a_k \in E$ et $x_1$, $x_2$, ...,$x_k \in \mathbb{Z}$. Alors $H$ est sous groupe de $\mathbb{Z}$ et $E \subset H$. Par le Théorème 2.4, il existe un unique entier positif $d$ tel que $H = d\mathbb{Z}$. Ceci signifie que $H$ est exactement l'ensemble des multiples de $d$. D'où chaque élément $a \in E$ est un multiple de $d$ et donc $d$ est un diviseur commun de $E$. Comme $d \in H$, alors il existe des entiers $a_1$, $a_2$, ...,$a_k \in E$ et des entiers $x_1$, $x_2$, ...,$x_k$ tels que

$$d = a_1x_1 + a_2x_2 + ... + a_kx_k.$$

Il suit que tout diviseur commun de $E$ divise $d$. D'où $d$ est un plus grand commun diviseur de l'ensemble $E$.

Si les nombres entiers positifs $d$ et $d'$ sont tous les deux des plus grands communs diviseurs, alors $d \mid d'$ et $d' \mid d$, et donc $d = d'$. Il s'ensuit que $E$ a un unique plus grand commun diviseur.

**Exemple.** $(35, 65) = 5 = (2) \times 35 + (-1) \times 65$.

**Théorème 2.6.** Soient $a_1$, $a_2$, ...,$a_k$ des entiers non tous nuls. Alors $(a_1, a_2, ..., a_k) = 1$ si et seulement s'il existe des $x_1$, $x_2$, ...,$x_k$ tels que

$$a_1x_1 + a_2x_2 + ... + a_kx_k = 1.$$

**Preuve.**
( $\Longrightarrow$ ) D'après le Théorème 2.5, il existe des entiers $x_1$, $x_2$, ...,$x_k$ tels que $a_1x_1 + a_2x_2 + ... + a_kx_k = 1$.
( $\Longleftarrow$ ) De l'hypothèse, le seule diviseur commun est 1. C'est -à-dire $(a_1, a_2, ..., a_k) = 1$.

**Définition 2.7.**
**1)** Les entiers $a_1$, $a_2$, ...,$a_k$ sont appelés relativement premiers si $(a_1, a_2, ..., a_k) = 1$.
**2)** Les entiers $a_1$, $a_2$, ...,$a_k$ sont appelés deux à deux relativement premiers si $(a_i, a_j) = 1$ pour tout $i, j$ avec $i \neq j$.

**Exemple.** $(12, 21, 14) = 1$, $(12, 21) = 3$, $(21, 14) = 7$, $(14, 12) = 2$.

Le théorème suivant donne une caractérisation très utile du plus grand diviseur commun de $a$ et $b$.

**Théorème 2.8.** Supposons $a$, $b \in \mathbb{Z}$ non tous deux nuls et soit $d = (a, b)$. Alors $d$ est le plus petit entier positif qui peut être exprimé comme combinaison linéaire de $a$ et $b$.
**Preuve.** Soit $\mathcal{C}$ l'ensemble de toutes les combinaisons linéaires de $a$ et $b$. Alors $\mathcal{C}$ contient des entiers positifs. Soit $m$ le plus petit élément de la partie de $\mathcal{C}$ formée uniquement par les entiers positif. Alors $m$ est un entier positif et son existence est assurée par l'axiome du bon ordre. Mettons $m = sa + tb$. Par la division euclidienne de $a$ par $m$ on a $a = qm + r$ où $0 \leq r < m$. Alors

$$\begin{aligned} r = a - qm &= a - q(sa + tb) \\ &= a(1 - qs) + (-qt)b. \end{aligned}$$

D'où $r$ est aussi combinaison linéaire de $a$ et $b$. Comme $r < m$, il vient de la définition de $m$ que $r = 0$. Ainsi $a = qm$ c'est-à-dire $m \mid a$. Par la même méthode on obtient $m \mid b$. Alors $m$ est un diviseur commun de $a$ et $b$.

Vu que $d$ divise $a$ et $b$, $d$ divise toute combinaison linéaire de $a$ et $b$. Donc $d$ divise $m$ et ainsi $d \leq m$. Comme $d$ est le $p\,\mathrm{gcd}\,(a, b)$, $d = m$.

**Théorème 2.9.** Soient $a$ et $b$ deux entiers. Alors

1) $(ca, cb) = c\,(a, b)$ pour tout entier positif $c$.

2) $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$ si $d = (a, b)$.

**Preuve.** 1) De l'égalité $s\,(ca) + t\,(cb) = c\,(sa + tb)$ et du fait que $c$ est un entier positif, on déduit que le plus petit entier positif qui peut être exprimé comme combinaison linéaire de $ca$ et $cb$ égal'à $c$ fois le plus petit entier positif qui peut être exprimé comme combinaison linéaire de $a$ et $b$. D'où, par le Théorème 2.8, $(ca, cb) = c\,(a, b)$.

2) De la partie 1) on a

$d = (a, b) = \left(d\dfrac{a}{d}, d\dfrac{b}{d}\right) = d\left(\dfrac{a}{d}, \dfrac{b}{d}\right)$. D'où $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

**Théorème 2.10 (Euclid).** Si $a$ divise $bc$ et $(a, b) = 1$, alors $a \mid c$.

**Preuve.** Le Théorème 2.9, permet d'écrire $(ac, bc) = c(a, b) = c$. Comme $a$ est un diviseur de $ac$ et de $bc$ (par hypothèse), alors $a$ divise $c$ car $(ac, bc) = c$.

**Théorème 2.11 (Euclid).** Soient $a$, $b$ et $c$ sont des entiers.

**1)** Si $(a, b) = (a, c) = 1$ alors $(a, bc) = 1$.

**2)** Si $a \mid c$, $b \mid c$, et $(a, b) = 1$, alors $ab \mid c$.

**Preuve.** 1) Par le Théorème 2.8, on écrit $sa + tb = 1$ et $ua + vc = 1$ pour les entiers $s$, $t$, $u$, et $v$. Alors $tb.vc = (1 - sa)(1 - ua) = 1 - ma$, où $m = s + u - sua$. D'où $ma + tv(bc) = 1$, et donc le résultat découle par le Théorème 2.6 ou le Théorème 2.8.

2) Soit $c = mb$. Puisque $a \mid mb$ et $(a, b) = 1$, il découle du Théorème 2.10, que $a \mid m$.

Si $m = na$, alors $c = nab$ et donc $ab \mid c$.

**Theorem 2.12.** Soit $k \geq 2$, et soient $a$, $b_1$, $b_2$,..., $b_k$ des entiers. Si $(a, b_i) = 1$ pour tout $i = 1, 2, ..., k$, alors $(a,\ b_1 b_2 ... b_k) = 1$.

**Preuve.** On utilise la récurrence et le le Théorème 2.10.

Donnons maintenant la définition du plus petit commun multiple

**Définition 2.13.** Soient $a_1$, $a_2$, ..., $a_k$ $(k \geq 2)$ des entiers non nuls.

- Un entier $m$ est appelé un commun multiple de $a_1$, $a_2$,..., $a_k$ s'il est multiple de $a_i$ pour tout $i = 1, ..., k$, i.e., chaque entier $a_i$ divise $m$.

- Le plus petit commun multiple de $a_1$, $a_2$, ..., $a_k$ est un entier positif

$m$ qui est un commun multiple de $a_1$, $a_2$, ..., $a_k$, et qui divise tout commun multiple de $a_1$, $a_2$, ..., $a_k$. Nous notons le plus petit commun multiple de $a_1$, $a_2$, ..., $a_k$ par $[a_1, a_2, ..., a_k]$.

**The Fundamental Theorem of Arithmetic.**

**Nombres premiers**

**Définition 2.14.**
- Un nombre entier $n > 1$ est premier si ses seules diviseurs sont $n$ et 1.
- Un entier $n > 1$ qui n'est pas premier est appelé composé.
- L'entier 1 n'est ni premier ni composé.

Nous notons, généralement, un entier premier par $p$.

**Théorème 2.15 (Euclid).** Il existe une infinité d'entiers premiers.

Il existe de nombreuses preuves pour ce théorème. Nous en donnons ici la preuve d'Euclid car elle est facile et simple.
**Preuve.** Supposons que $p_1 = 2 < p_2 = 3 < p_3 = ... < p_r$ sont tous les entiers naturels premiers. Considérons l'entier $P = p_1 p_2 p_3 ... p_r + 1$. Soit $p$ un entier premier divisant $P$. Alors $p$ ne peut être l'un des entiers premiers $p_1$, $p_2$, $p_3$,..., $p_r$ car sinon $p$ divise $P - p_1 p_2 p_3 ... p_r = 1$, ce qui est impossible. D'où $p$ est autre premier par conséquent $\{p_1, p_2, p_3, ..., p_r\}$ ne contient pas tous les entiers naturels premiers.

**Theorem 2.16.** Si un nombre premier $p$ divise un produit d'entiers, alors $p$ divise l'un des facteurs.
**Preuve.** La preuve se fait par récurrence. Le théorème est, par le Théorème 2.10, vrai pour un produit de deux facteurs. Supposons que le théorème est vrai pour un produit de $k \geq 2$ facteurs et le démontrons pour $k + 1$. Soit alors $b_1 b_2 ... b_k b_{k+1}$ un produit d'entiers tel que $p \mid b_1 b_2 ... b_k b_{k+1}$ i.e. $p \mid (b_1 b_2 ... b_k)\, b_{k+1}$. Maintenant, si $p \nmid (b_1 b_2 ... b_k)$, alors d'après le Théorème 2.10, $p \mid b_{k+1}$ et si $p \mid b_1 b_2 .. b_k$ alors $p$ divise, par l'hypothèse de récurrence, l'un des entiers $b_1$, $b_2$, .., $b_k$. Ceci achève la preuve.
**Theorem 2.17 (Le théorème fondamental de l'arithmétique).** Tout entier $n > 1$ peut être écrit comme un produit de nombres premiers. Cette représentation, à l'exception de l'ordre des facteurs, est unique.

Le théorème fondamental de l'arithmétique permet d'écrire tout entier $n > 1$ selon la forme

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r} = \prod_{i=1}^{r} p_i^{a_i},$$

où les nombres premiers $p_i$ sont distincts et les exposants sont positifs. De plus il fournit, pour deux entiers donnés $m$ et $n$, des formules pour calculer le plus grand commun diviseur et le plus petit commun multiple. Pour ce but nous utilisons dans la représentons de $m$ et $n$ les mêmes nombres premiers, où certains des exposants doivent être égaux à zéro si nécessaire.

**Théorème 2.18.** Soient $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$ où $\alpha_i \geq 0$, $\beta_i \geq 0$ pour $i = 1, 2, ..., r$. Alors

$$(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad [a, b] = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

Dans le lême contexte ce théorème se généralise au cas de plus de deux entiers; par exemple pour trois entiers $a$, $b$ et $c$ avec $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, $b = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$ et $c = p_1^{\gamma_1} p_2^{\gamma_2} ... p_r^{\gamma_r}$, on a

$$(a, b, c) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i, \gamma_i)} \quad \text{et} \quad [a, b] = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i, \gamma_i)}.$$

**Exemple.** Calculer $(72, 60, 84)$, $[72, 60, 84]$.

$72 = 2^3 \times 3^2$, $60 = 2^2 \times 3 \times 5$, $84 = 2^2 \times 3 \times 7$. D'où

$$\left\{ \begin{array}{lclcl} (72, 60, 84) & = & 2^2 \times 3 & = & 12 \\ [72, 60, 84] & = & 2^3 \times 3^2 \times 5 \times 7 & = & 2520 \end{array} \right. .$$

$(72, 60, 84) = 2^2 \times 3 = 12.$

**Equations Diophantiennes linéaires**

**Algorithme d'Euclid.** Soient $a$ et $b$ deux entiers positifs. Par l'utilisation de l'algorithme de division d'une façon répétée, nous obtenons une suite d'égalités

$$\begin{array}{rcccl} a & = & bq_1 + r_2 & , & 0 < r_2 < b \\ b & = & r_2 q_2 + r_3 & , & 0 < r_3 < r_2 \\ r_2 & = & r_3 q_3 + r_4 & , & 0 < r_4 < r_3 \\ & .. & .. & & .. \\ & .. & .. & & .. \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n & , & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n . & & \end{array} \qquad (*)$$

Comme $b > r_2 > r_3 > ... > r_n > r_{n+1} = 0$, on peut prouver que

$$(a, b) = (b, r_2) = (r_2, r_3) = ... = (r_{n-1}, r_n) = r_n.$$

D'où on a

**Théorème 2.19.** Si $r_n$ est le dernier reste non nul dans le processus d'algorithme d'Euclid, alors $(a, b) = r_n$.
**Preuve.** From $(*)$, on a

$$\begin{array}{rcl} r_2 & = & a - bq_1 \\ r_3 & = & b - r_2 q_2 \\ r_4 & = & r_2 - r_3 q_3 \\ .. & .. & .. \\ .. & .. & .. \\ r_n & = & r_{n-2} - r_{n-1} q_{n-1}. \end{array} \qquad (**)$$

Soit $r = (a, b)$. De $(**)$, on observe que de sa première équation $r \mid r_2$ et de sa deuxième équation $r \mid r_3$. Ainsi en itérant ces observations on trouve que $r \mid r_n$. Maintenant en remontant dans $(*)$ de la dernière équation, on observe que

$$r_n \mid r_{n-1},\ r_n \mid r_{n-2}, ...,\ r_n \mid r_2,\ r_n \mid b,\ r_n \mid a.$$

Alors $r_n$ est un diviseur commun de $a$ et $b$. D'où $r_n \mid (a, b)$ i.e. $r_n \mid r$. Par conséquent $r = r_n$.

**Exemples.**
1) Trouver $(228, 66)$.
Solution. D'après l'algorithme d'Euclid

$$\begin{array}{rcl} 228 & = & 66 \times 3 + 30 \\ 66 & = & 30 \times 2 + 6 \\ 30 & = & 6 \times 5 + 0. \end{array}$$

Doù $(228, 66) = 6$.

2) Montrer que si $a$, $b$ sont des entiers positifs, alors

$$(a, b) = (a + nb, b)\,.$$

Solution. Posons $d = (a\ ,\ b)$, $c = (a + nb\ ,\ b)$. Comme $d \mid a$ et $d \mid b$, alors $d \mid a + nb$. C'est-à-dire $d$ est un diviseur commun de $a + nb$ et de $b$. Ceci implique

$$d \mid c. \tag{1}$$

D'autre part $c \mid a + nb$ et $c \mid b$. Alors $c \mid (a + nb - nb)$ i.e. $c \mid a$. D'où $c$ est un diviseur commun de $a$ et $b$. Donc

$$c \mid d. \tag{2}$$

De (1) et (2) on a $d = c$.

Le résultat indiqué dans cette partie (partie 2 de ces exemples) nous aide à faire des calculs effectifs comme dans ce qui suit

3) Trouver $(3456, 246)$.
Solution. $3456 = 246 \times 14 + 12$. D'où

$$\begin{array}{rcc} (3456\ ,\ 246) & = & (3456 - 246 \times 14\ ,\ 246) \\ & = & (12\ ,\ 246) \\ & = & (12\ ,\ 246 - 20 \times 12) \\ & = & (12\ ,\ 6) \\ & = & 6. \end{array}$$

**Théorème (Bachet-Bezout) 2.20.** Soient $a_1$, $a_2$,..., $a_k$ des entiers non tous nuls. Pour tout entier $b$, il existe des entiers $x_1$, $x_2$,..., $x_k$ tels que

$$a_1x_1 + a_2x_2 + ... + a_kx_k = b \qquad (*)$$

si et seulement si $b$ est un multiple de $(a_1, a_2, ..., a_k)$. En particulier, l'équation $(*)$ a une solution pour tout entier $b$ si et seulement si $(a_1, a_2, ..., a_k) = 1$.
**Preuve.** Soit $d = (a_1, a_2, ..., a_k)$. Si $(*)$ admet une solution en $x_i$ $(i = 1, 2, .., k)$, alors $d \mid b$ i.e. $b$ est un multiple de $d = (a_1, a_2, ..., a_k)$.

Réciproquement, si $d \mid b$ alors $b = dq$ $(q \in \mathbb{Z})$. Par un théorème précédent il existent des entiers $y_1, y_2, ..., y_k$ tels que

$$a_1y_1 + a_2y_2 + ... + a_ky_k = d.$$

Soit, pour $i = 1, 2, .., k$, $x_i = y_iq$. Alors

$$\begin{array}{rcc} a_1x_1 + a_2x_2 + ... + a_kx_k & = & a_1(y_1q) + a_2(y_2q) + ... + a_k(y_kq) \\ & = & dq \\ & = & b. \end{array}$$

C'est-à-dire $(x_1, x_2, ..., x_k)$ est une solution pour $(*)$.

Il suit que $(*)$ admet solution en entiers pour tout $b$ si et seulement si $(a_1, a_2, ..., a_k) = 1$.

L'algorithme d'Euclid est un outil efficace pour résoudre les équations du type

$$ax + by = c.$$

**Exemple.**
1) Trouver $x$, $y$ tels que: $23x + 29y = 1$.
Solution. D'après l'algorithme d'Euclid

$$\begin{array}{rcl} 29 & = & 23 \times 1 + 6 \\ 23 & = & 6 \times 3 + 5 \\ 6 & = & 5 \times 1 + 1 \\ 5 & = & 5 \times 1 + 0 \end{array} \quad \Longrightarrow \quad \begin{array}{rcc} 1 & = & 6 - 5 \times 1 \\ & = & 6 - (23 - 6 \times 3) \\ & = & 4 \times 6 - 23 \times 1 \\ & = & 4 \times (29 - 23) - 23 \\ & = & 4 \times 29 - 5 \times 23 \end{array}$$

D'où $x = -5$ et $y = 4$.

2) Trouver les solutions de $23x + 29y = 7$.
Solution. De la première partie $23\,(-5) + 29\,(4) = 1$. D'où $23\,(-35) + 29\,(28) = 7$.

**Théorème 2.21.** Supposons que $a$, $b$ et $c$ sont des entiers tels que $(a, b) \mid c$. Si $(x_0, y_0)$ est une solution de $ax + by = c$, alors toute autre solution de cette équation est donnée par

$$\begin{cases} x &= x_0 + t\dfrac{b}{d} \\ y &= y_0 - t\dfrac{a}{d} \end{cases}$$

où $d = (a, b)$ et $t \in \mathbb{Z}$.

**Références.**


[1] A Adler, J E Coury, *The theory of numbers: A text and source book of problems*,
Jones and Bartlett Publ., Boston (1995); ISBN-10:0867204729.
[2] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 1991 by John Wiley & Sons, Inc. .
[3] Kenneth H. Rosen, *Elementary Number Theory & Its Applications*, 2011, Library of Congress Cataloging-in-Publication Data.
[4] Melvyn B. Nathanson, *Elementary Methods in Number Theory, Springer 2000.*
[5] Jean-Marie De Koninck and Armel Mercier, 1001 problems in classical number theory, AMS 2007.
[6] David A. Santos, Elementary Number Theory Notes, January 15, 2004.