23

Division euclidienne dans $\mathbb{Z}$

23.1 L'anneau $\mathbb{Z}$ des entiers relatifs

On désigne par $\mathbb{Z}$ l'ensemble des entiers relatifs, soit :

$$\mathbb{Z} = \{\cdots, -n, \cdots, -2, -1, 0, 1, 2, \cdots, n, \cdots\}.$$

On note $\mathbb{Z}^*$ l'ensemble $\mathbb{Z}$ privé de 0.

On rappelle que l'ensemble $(\mathbb{Z}, +, \cdot)$ des entiers relatifs est un anneau unitaire, commutatif et intègre.

En pratique on notera plutôt nm pour $n \cdot m$.

L'ensemble $\mathbb{Z}$ est muni comme l'ensemble $\mathbb{N}$ des entiers naturels d'une relation d'ordre total. C'est la relation $\leq$. Cette relation est :

– réflexive :

$$\forall n \in \mathbb{Z},\ n \leq n,$$

– antisymétrique :

$$\forall n \in \mathbb{Z},\ \forall m \in \mathbb{Z},\ (n \leq m,\ m \leq n) \Leftrightarrow n = m,$$

– transitive :

$$\forall n \in \mathbb{Z},\ \forall m \in \mathbb{Z},\ \forall p \in \mathbb{Z},\ \begin{cases} n \leq m \\ m \leq p \end{cases} \Rightarrow n \leq p.$$

– Deux éléments quelconques de $\mathbb{Z}$ sont comparables (l'ordre est total). C'est-à-dire que pour n, m dans $\mathbb{Z}$ on a soit $n \leq m$ soit $m \leq n$.

On dit qu'une partie A non vide de $\mathbb{Z}$ est minorée s'il existe un entier m tel que :

$$\forall n \in A,\ n \geq m.$$

Si de plus m est dans A on dit alors que c'est un plus petit élément. Dans ce cas il est uniquement déterminé.

On dit qu'une partie A non vide de $\mathbb{Z}$ est majorée s'il existe un entier M tel que :

$$\forall n \in A,\ n \leq M.$$

Si de plus M est dans A on dit alors que c'est un plus grand élément. Dans ce cas il est uniquement déterminé.

L'ensemble $\mathbb{Z}$ est bien ordonné, c'est-à-dire que :

– toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément ;

– toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

23.2 Divisibilité et congruences

Définition 23.1 *On dit que l'entier relatif a est divisible par l'entier relatif d, ou que a est un multiple de d, s'il existe un entier relatif q tel que $a = qd$. On note d/a.*

Remarque 23.1 *Si $d = 0$ alors $a = 0$ et pour $d \neq 0$ l'entier q est uniquement déterminé (une égalité $a = dq = dq'$ entraîne $d(q - q') = 0$ et $q - q' = 0$ puisque $\mathbb{Z}$ est intègre).*
On se limitera donc au cas où $d \in \mathbb{Z}^*$.

Remarque 23.2 *La relation de divisibilité est une relation d'ordre non totale sur $\mathbb{N}$. C'est à dire qu'elle est :*
— réflexive : pour tout $a \in \mathbb{N}$, a/a ;
— antisymétrique : si a/b et b/a dans $\mathbb{N}$ alors $a = b$;
— transitive : si a/b et b/c dans $\mathbb{N}$ alors a/c.
Deux éléments quelconques de $\mathbb{N}$ ne sont pas toujours comparables. Par exemple on n'a aucune relation de divisibilité entre 3 et 5 dans $\mathbb{N}$.

Sur $\mathbb{Z}$ on a les propriétés suivantes :
- les seuls diviseurs de 1 sont 1 et -1 ;
- si d/a et $a \neq 0$, alors $|d| \leq |a|$ (si $a = 0$, on a $0 = 0 \cdot d$ pour tout $d \in \mathbb{Z}$)
- si a/b et b/a dans $\mathbb{Z}$ alors $|a| = |b|$, (*si* $a = 0$, alors $b = 0$), soit $a = \pm b$ (la relation de divisibilité n'est donc pas antisymétrique sur $\mathbb{Z}$, elle est seulement réflexive et transitive et ce n'est pas une relation d'ordre) ;
- si d/a et d/b dans $\mathbb{Z}$ alors $d/(\lambda a + \mu b)$ pour tous λ, μ dans $\mathbb{Z}$.

Pour tout entier relatif n, on note :

$$n\mathbb{Z} = \{n \cdot q \mid q \in \mathbb{Z}\}$$

l'ensemble de tous les multiples de n et :

$$\mathcal{D}_n = \{q \in \mathbb{Z} \mid q \text{ divise } n\}$$

l'ensemble de tous les diviseurs de n.

Exercice 23.1 *Montrer que, pour tout entier relatif n, $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.*

Solution 23.1 *On a $0 = n \cdot 0 \in n\mathbb{Z}$ et pour $a = pn$, $b = qn$ dans $n\mathbb{Z}$, on a, $b - a = (q - p)\, n \in n\mathbb{Z}$. Donc $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

En particulier, on a $0\mathbb{Z} = \{0\}$, $\mathcal{D}_0 = \mathbb{Z}$, $1\mathbb{Z} = \mathbb{Z}$, $\mathcal{D}_1 = \{-1, 1\}$.

Nous verrons plus loin que les $n\mathbb{Z}$ sont les seuls sous-groupes de $(\mathbb{Z}, +)$.

On peut remarquer que pour tout $a = qn \in n\mathbb{Z}$ et tout $b \in \mathbb{Z}$, on a $ab = bqn \in n\mathbb{Z}$, ce qui se traduit en disant que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Exercice 23.2 *Montrer que pour tous a, b dans $\mathbb{Z}$, on a :*

$$a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow b/a \Leftrightarrow \mathcal{D}_b \subset \mathcal{D}_a$$

et :

$$a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b \Leftrightarrow \mathcal{D}_a = \mathcal{D}_b.$$

Solution 23.2 *Si $a\mathbb{Z} \subset b\mathbb{Z}$, on a alors $a \in b\mathbb{Z}$, c'est-à-dire qu'il existe un entier q tel que $a = bq$ et b/a.*
Si b/a, on a alors $a = qb$ avec $q \in \mathbb{Z}$ et tout diviseur δ de b va diviser a, ce qui signifie que $\mathcal{D}_b \subset \mathcal{D}_a$.
Si $\mathcal{D}_b \subset \mathcal{D}_a$, on a alors $b \in \mathcal{D}_a$, c'est-à-dire qu'il existe un entier q tel que $a = bq$ et pour tout pa dans $a\mathbb{Z}$, on a $pa = pqb \in b\mathbb{Z}$, c'est-à-dire que $a\mathbb{Z} \subset b\mathbb{Z}$.
On a donc ainsi montré la première série d'équivalence.
Si $a\mathbb{Z} = b\mathbb{Z}$, on a alors $a\mathbb{Z} \subset b\mathbb{Z}$ et $b\mathbb{Z} \subset a\mathbb{Z}$, donc b/a et a/b et $a = \pm b$.
Si $a = \pm b$, les entiers a et b ont les mêmes diviseurs, ce qui signifie que $\mathcal{D}_a = \mathcal{D}_b$.
Si $\mathcal{D}_a = \mathcal{D}_b$, on a alors $\mathcal{D}_a \subset \mathcal{D}_b$ et $\mathcal{D}_b \subset \mathcal{D}_a$, donc b/a et a/b et $a = \pm b$ qui équivaut à $a\mathbb{Z} = b\mathbb{Z}$.

Exercice 23.3 *Déterminer tous les entiers naturels non nuls n tels que $n+1$ divise n^2+1.*

Solution 23.3 *Pour tout $n \geq 1$, on a :*

$$n^2 + 1 = n(n+1) - (n-1)$$

et si $n+1$ divise n^2+1, il va aussi diviser $n-1$, c'est-à-dire qu'il existe $q \in \mathbb{N}$ tel que $n-1 = q(n+1)$. La seule valeur possible pour q est alors $q = 0$, car $q \geq 1$ entraîne $n-1 \geq n+1$ qui est impossible. On a donc nécessairement $n = 1$ et réciproquement cette valeur convient bien.

Exercice 23.4 *Déterminer tous les entiers relatifs n différents de 3 tels que $n-3$ divise n^3-3.*

Solution 23.4 *Pour tout $n \in \mathbb{Z}$, on a :*

$$\begin{aligned} n^3 - 3 = (n-3+3)^3 - 3 &= q(n-3) + 3^3 - 3 \\ &= q(n-3) + 24 \end{aligned}$$

et si $n-3$ divise n^3-3, il divise alors 24, c'est-à-dire que :

$$n - 3 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$$

et :

$$n \in \{-21, -9, -5, -3, -1, 0, 1, 2, 4, 5, 6, 7, 9, 11, 15, 27\}.$$

Réciproquement ces valeurs conviennent bien.

Définition 23.2 *Soient n un entier naturel et a, b deux entiers relatifs. On dit que a est congru à b modulo n si n divise $a-b$. On note*

$$a \equiv b \ (n)$$

Dire que a est congru à b modulo n équivaut aussi à dire que $a - b \in n\mathbb{Z}$.
Pour $n = 0$, on a $0\mathbb{Z} = \{0\}$ et $a \equiv b \ (0)$ revient à dire que $a = b$.
Pour $n = 1$, on a $1\mathbb{Z} = \mathbb{Z}$ et la relation $a \equiv b \ (1)$ est toujours vérifiée.
On suppose donc, dans ce qui suit que $n \geq 2$.
On peut facilement vérifier que la relation de congruence est une relation d'équivalence. C'est-à-dire que :

- $a \equiv a \ (n)$ $(a - a = 0 \in n\mathbb{Z})$;
- $a \equiv b \ (n) \Rightarrow b \equiv a \ (n)$ ($a - b \in n\mathbb{Z}$ entraîne $b - a \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe) ;
- $(a \equiv b \ (n), \ b \equiv c \ (n)) \Rightarrow a \equiv c \ (n)$ ($a - b \in n\mathbb{Z}$ et $b - c \in n\mathbb{Z}$ entraîne $a - c = (a-b) - (c-b) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe).

Cette relation est compatible avec l'addition et la multiplication sur $\mathbb{Z}$. C'est-à-dire que :

$$(a \equiv b\ (n), c \equiv d\ (n)) \Rightarrow (a+c \equiv b+d\ (n),\ ac \equiv bd\ (n)).$$

En effet $a-b \in n\mathbb{Z}$ et $c-d \in n\mathbb{Z}$ entraîne $a+c-(b+d) = (a-b)+(c-d) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe et $ac-bd = a(c-d)+d(a-b) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Cette compatibilité permet de munir l'ensemble $\mathbb{Z}_n$ des classes d'équivalence modulo n d'une structure d'anneau (voir le chapitre 25).

Exercice 23.5 *Soient x et y dans $\mathbb{Z}$. Montrer que si $3x+7y$ est multiple de 11 alors $4x-9y$ est aussi multiple de 11.*

Solution 23.5 *On a $3x \equiv 7y\ (11)$ donc $15x \equiv -35y\ (11)$ avec $15x \equiv 4x\ (11)$ et $-35y \equiv 9y\ (11)$.*

Exercice 23.6 *Soient a et b dans $\mathbb{Z}$. Montrer que si $p = a^2+b^2$ est impair supérieur ou égal à 3 alors $p-1$ est multiple de 4.*

Solution 23.6 *Tout entier k est congru à $0, 1, 2$ ou 3 modulo 4, donc k^2 est congru à 0 ou 1 modulo 4 et a^2+b^2 est congru à $0, 1$ ou 2 modulo 4. Si p est impair et $p = a^2+b^2$ alors p est congru à 1 modulo 4 et $p-1$ est multiple de 4.*

Exercice 23.7 *Soient p, q deux entiers naturels impairs et $a = 3p+2$, $b = 3q+2$. Déterminer tous les entiers naturels n tels que $a^n - b^{2n}$ soit divisible par 6.*

Solution 23.7 *L'entier $m = a^n - b^{2n}$ est pair comme différence de nombres impairs. Il est donc divisible par 6 si, et seulement si, il est divisible par 3. Avec $a \equiv 2\ (3)$ et $b \equiv 2\ (3)$ on déduit que $m \equiv 2^n - 2^{2n}\ (3)$ et m est divisible par 3 si, et seulement si $2^n - 2^{2n} \equiv 0\ (3)$ ce qui équivaut à $2^n \equiv 1\ (3)$ encore équivalent à dire que n est pair.*

23.3 Le théorème de division euclidienne dans $\mathbb{Z}$

Théorème 23.1 *Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$\begin{cases} a = bq + r, \\ 0 \leq r < |b|. \end{cases} \tag{23.1}$$

Démonstration. On suppose que $b > 0$ et on pose :

$$A = \{k \in \mathbb{Z} \mid bk \leq a\}.$$

Cet ensemble est non vide (pour $a \geq 0$, 0 est dans A et pour $a < 0$, a est dans A) et majoré (pour $a \geq 0$, a majore A et pour $a < 0$, 0 majore A). Il admet donc un plus grand élément q qui vérifie :

$$qb \leq a < (q+1)\, b.$$

Il suffit alors de poser $r = a - bq$.

Pour $b < 0$ on travaille avec $-b$ et on a l'existence de (q', r') vérifiant :

$$\begin{cases} a = -bq' + r', \\ 0 \leq r' < -b. \end{cases}$$

Et il suffit de poser $q = -q'$, $r = r'$.

Supposons qu'il existe deux couples d'entiers (q, r) et (q', r') vérifiant (23.1) avec $q \neq q'$. On a alors :

$$|r - r'| = |b\,(q - q')| \geq |b|$$

avec r et r' dans $]-|b|\,,|b|[$ ce qui est impossible. On a donc $q = q'$ et $r = r'$. Le couple (q, r) vérifiant (23.1) est donc unique. ∎

Définition 23.3 *Avec les notations du théorème 23.1 on dit que a est le dividende, b le diviseur, q le quotient et r le reste dans la division euclidienne de a par b.*

L'anneau $\mathbb{Z}$ est un cas particulier d'anneau euclidien et l'application $n \in \mathbb{Z}^* \mapsto |n|$ est un stathme euclidien.

Dire que le reste dans la division euclidienne de a par b est nul revient aussi à dire que b divise a.

En utilisant la division euclidienne par un entier naturel non nul n, $a = qn + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, 1, \cdots, n-1\}$, on voit que a est congru modulo n au reste r. Réciproquement, si a est congru à un entier $r \in \{0, 1, \cdots, n-1\}$, alors r est le reste dans la division euclidienne de a par n. C'est-à-dire que le reste dans la division euclidienne de a par n est l'unique entier r vérifiant :

$$\begin{aligned} &a \equiv r \ \ (n)\,, \\ &0 \leq r < n. \end{aligned}$$

Remarque 23.3 *On peut montrer un résultat analogue au théorème 23.1 avec la condition $|r| < b$ (en supposant $b > 0$), mais dans ce cas le couple (q, r) n'est pas unique. Par exemple on a :*

$$12 = 3 \times 5 - 3 = 2 \times 5 + 2.$$

On peut également formuler le théorème de division euclidienne comme suit.

Théorème 23.2 *Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique entier $q \in \mathbb{Z}$ tel que :*

$$0 \leq a - bq < |b|\,. \tag{23.2}$$

Pour $b \in \mathbb{Z}^*$, l'encadrement (23.2) peut aussi s'écrire :

$$\frac{b}{|b|}q \leq \frac{a}{|b|} < \frac{b}{|b|}q + 1$$

ce qui donne

$$q \leq \frac{a}{b} < b + 1$$

pour $b > 0$ et signifie que $q = \left[\frac{a}{b}\right]$ (partie entière de $\frac{a}{b}$).

Pour $b < 0$, on a $-q \leq -\frac{a}{b} < -q + 1$, soit $q - 1 < \frac{a}{b} \leq q$ et $q - 1 = \left[\frac{a}{b}\right]$ si le reste $r = a - bq$ est non nul et $q = \frac{a}{b} = \left[\frac{a}{b}\right]$ si le reste est nul.

Remarque 23.4 *La démonstration précédente du théorème de division euclidienne n'est pas constructive. Un algorithme de détermination du quotient et du reste est donné par la méthode de descente infinie de Fermat qui revient à faire une démonstration par récurrence du théorème 23.1.*

Le principe est le suivant en supposant a et b strictement positifs.
Si $a < b$, on prend alors $(q, r) = (0, a)$.
Si $b \leq a$, il existe alors un entier $q_1 \geq 1$ tel que $q_1 b \leq a$ et on pose $r_1 = a - bq_1$.
Si $r_1 < b$ on prend alors $(q, r) = (q_1, r_1)$.
Si $b \leq r_1$, il existe alors un entier $q_2 \geq 1$ tel que $q_2 b \leq r_1$ et on pose $r_2 = r_1 - bq_2$.
En continuant ainsi de suite on construit deux suites d'entiers (q_n) et (r_n) par la relation de récurrence :
si $r_n < b$ alors $(q_{n+1}, r_{n+1}) = (q_n, r_n)$;
si $b \leq r_n$ alors q_{n+1} est choisi tel que $q_{n+1} b \leq r_n$ et on pose $r_{n+1} = r_n - bq_{n+1}$.
La suite (r_n) est une suite strictement décroissante d'entiers naturels. Le procédé s'arrêtera donc au bout d'un nombre fini d'étapes, c'est-à-dire qu'il existe un entier p tel que $r_p < b$ et dans ce cas le couple :

$$(q, r) = (q_1 + \cdots + q_p, r_p)$$

est la solution cherchée. En effet on a :

$$0 \leq r_p = r_{p-1} - q_p b = a - (q_1 + \cdots + q_p)\, b < b.$$

Exercice 23.8 *Calculer, pour tout entier naturel n, le reste dans la division euclidienne par 13 de l'entier $x_n = 4^{2n+1} + 3^{n+2}$.*

Solution 23.8 *On a :*

$$\begin{aligned} x_n &= 4 \cdot 4^{2n} + 9 \cdot 3^n = 4 \cdot 16^n + 9 \cdot 3^n \\ &= 4\left(16^n - 3^n\right) + (4 + 9)\, 3^n \\ &= 4\,(16 - 3) \sum_{k=1}^{n} 16^{n-k} 3^{k-1} + 13 \cdot 3^n = 13 y_n. \end{aligned}$$

Le reste dans la division euclidienne par 13 de x_n est donc nul, le quotient étant donné par :

$$q_n = 4 \sum_{k=1}^{n} 16^{n-k} 3^{k-1} + 3^n$$

Ce exercice peut en fait se généraliser comme suit.

Exercice 23.9 *Soient a et b deux entiers naturels non nuls tels que $a > b$. Donner une condition suffisante sur les entiers a et b pour que tous les entiers $x_n = a^{2n+1} + b^{n+2}$, où n est un entier naturel, soient divisibles par $a + b^2$.*

Solution 23.9 *On a :*

$$\begin{aligned} x_n &= a \cdot a^{2n} + b^2 \cdot b^n = a \cdot \left(a^2\right)^n + b^2 \cdot b^n \\ &= a\left(\left(a^2\right)^n - b^n\right) + \left(a + b^2\right) b^n \\ &= a\left(a^2 - b\right) \sum_{k=1}^{n} \left(a^2\right)^{n-k} b^{k-1} + \left(a + b^2\right) b^n. \end{aligned}$$

Si $a = b + 1$ (i. e. b et a sont deux entiers consécutifs), alors $a^2 - b = b^2 + b + 1 = a + b^2$ et x_n est divisible par $a + b^2$ pour tout n (la condition $a^2 = b$ n'est pas possible puisqu'on suppose que $b < a$).
Pour $(a, b) = (4, 3)$ on retrouve l'exercice précédent).

Exercice 23.10 *Soient a, b deux entiers relatifs. Montrer que si $a^2 + b^2$ est divisible par 7, alors a et b sont divisibles par 7.*

Solution 23.10 *On a $a = q_1 7 + r_1$ et $b = q_2 7 + r_2$ avec $0 \leq r_1, r_2 \leq 6$ et :*

$$a^2 + b^2 = (q_1 7 + r_1)^2 + (q_2 7 + r_2)^2 = q_3 7 + r_1^2 + r_2^2.$$

Pour $0 \leq r_1, r_2 \leq 6$ et $(r_1, r_2) \neq (0, 0)$, $r_1^2 + r_2^2$ n'est jamais divisible par 7 et donc $a^2 + b^2$ n'est pas divisible par 7. En conclusion, si $a^2 + b^2$ est divisible par 7, alors a et b sont divisibles par 7.

Exercice 23.11 *Calculer le reste dans la division euclidienne de 19^{55} par 7.*

Solution 23.11 *En utilisant la compatibilité de la congruence avec la multiplication on a :*

$$19 = 2 \times 7 + 5 \equiv 5 \ (7)$$

$$19^{55} \equiv 5^{55} \ (7)$$

$$5 \equiv -2 \ (7), \ 5^2 \equiv 4 \ (7), \ 5^4 \equiv 4^2 \equiv 2 \ (7), \ 5^5 \equiv 10 \equiv 3 \ (7)$$

$$5^{55} = \left(5^5\right)^{11} \equiv 3^{11} \ (7)$$

$$3^3 = 27 \equiv -1 \ (7)$$

$$3^{11} = 3^{3\times 3+2} \equiv 5 \ (7)$$

$$19^{55} \equiv 5 \ (7).$$

Exercice 23.12 *Calculer le reste dans la division euclidienne de 17^{51} par 7.*

Solution 23.12 *Laissée au lecteur.*

Les paragraphes qui suivent sont consacrés à quelques applications du théorème de division euclidienne.

23.4 Les systèmes de numération

Une première application importante du théorème de division euclidienne est le théorème de numération dans une base.

Théorème 23.3 *Soit b un entier supérieure ou égal à 2. Pour tout entier $n > 0$ il existe un unique entier p et un unique $(p+1)$-uplet $(n_0, n_1, \cdots, n_p) \in \mathbb{N}^{p+1}$ tels que $n_p \neq 0$, $0 \leq n_k \leq b-1$ pour tout $k \in \{0, 1, \cdots, p\}$ et :*

$$n = \sum_{k=0}^{p} n_k b^k. \tag{23.3}$$

Démonstration. En remarquant que :

$$\mathbb{N}^* = \bigcup_{j=0}^{+\infty} \left[b^j, b^{j+1}\right[$$

il suffit de montrer le résultat pour tout entier n dans $[b^j, b^{j+1}[$ où j décrit $\mathbb{N}$. Pour ce faire on procède par récurrence sur $j \geq 0$.

Pour $j = 0$ tout $n \in [1, b[$ s'écrit sous la forme (23.3) avec $p = 0$ et $n_0 = n$.

Supposons le résultat acquis pour $j \geq 0$ et soit $n \in [b^{j+1}, b^{j+2}[$. En utilisant le théorème de division euclidienne on peut écrire $n = bq + n_0$ avec $0 \leq n_0 \leq b - 1$. On a alors :

$$bq = n - n_0 > b^{j+1} - b = b\left(b^j - 1\right)$$

et donc $q > b^j - 1$, soit $q \geq b^j$. On a également

$$q = \frac{n - n_0}{b} < b^{j+1} - \frac{n_0}{b} \leq b^{j+1}.$$

En définitive $q \in [b^j, b^{j+1}[$ et avec l'hypothèse de récurrence il s'écrit $q = \sum_{k=0}^{p} q_k b^k$ avec $q_p \neq 0$. D'où :

$$n = bq + n_0 = \sum_{k=0}^{p+1} n_k b^k$$

avec $n_k = q_{k-1}$ pour tout $k \in \{1, 2, \cdots, p+1\}$. En particulier $n_{p+1} = q_p \neq 0$.

Supposons que l'on ait deux écritures :

$$n = \sum_{k=0}^{p} n_k b^k = \sum_{k=0}^{p'} n'_k b^k$$

avec $p' \geq p$, $0 \leq n_k \leq b - 1$, $0 \leq n'_k \leq b - 1$, $n_p \neq 0$ et $n'_{p'} \neq 0$. On a alors :

$$b^p \leq n \leq \sum_{k=0}^{p} (b-1)\, b^k = b^{p+1} - 1 < b^{p+1}.$$

De même $b^{p'} \leq n < b^{p'+1}$. Donc $b^{p'} < b^{p+1}$ soit $b^{p'-p} < b$ et nécessairement $p = p'$. En remarquant que n_0 est le reste dans la division euclidienne de n par b, on déduit que $n_0 = n'_0$ puis par récurrence que $n_k = n'_k$ pour tout $k \in \{1, \cdots, p\}$. D'où l'unicité de la décomposition. ■

Remarque 23.5 *Dans la décomposition* (23.3) *on a $b^p \leq n < b^{p+1}$, c'est-à-dire que p est le plus grand entier vérifiant $b^p \leq n$.*

Définition 23.4 *Avec les notations du théorème 23.3 on dit que* (23.3) *est la représentation en base b de l'entier n. On note :*

$$n = \overline{n_p \cdots n_1 n_0}^b$$

et on dit que les n_k sont les chiffres dans l'écriture en base b de n.

Pour les valeurs successives $b = 2, 8, 10$ et 16, les écritures en base b correspondantes sont les systèmes de numération binaire (chiffres $0, 1$), octal (chiffres $0, 1, \cdots, 7$), décimal (chiffres $0, 1, \cdots, 9$) et hexadécimal (chiffres $0, 1, \cdots, 9, A, B, \cdots, F$).

Pour $b = 10$, on écrit plus simplement $n = n_p \cdots n_1 n_0$ la représentation décimale de l'entier n.

Si $n = \overline{n_p \cdots n_1 n_0}^b$, alors n_0 est le reste dans la division euclidienne de n par b et $\overline{n_p \cdots n_1}^b$ est le quotient. Cette remarque nous permet de donner un algorithme de calcul des chiffres dans l'écriture en base b de n : on divise n par b, puis le quotient par b et ainsi de suite, un quotient nul indique la fin du processus et les restes successifs donnent, de droite à gauche, l'écriture en base b de n. Par exemple, l'écriture en base $b = 2$ de $n = 120$ s'obtient comme suit :

n	120	60	30	15	7	3	1
q	60	30	15	7	3	1	0
r	0	0	0	1	1	1	1

ce qui donne $120 = \overline{1111000}^2$.

On peut remarquer que l'écriture en base b de l'entier b est $b = \overline{10}^b$ et plus généralement, pour tout entier $p \geq 1$, l'écriture de l'entier b^p en base b est $b = \overline{10 \cdots 0}^b$ (1 suivi de p zéros).

On peut également remarquer que si $n = \overline{n_p \cdots n_1 n_0}^b$, alors pour tout entier k compris entre 1 et p, $\overline{n_{k-1} \cdots n_1 n_0}^b$ est le reste dans la division euclidienne de n par b^k et $\overline{n_p \cdots n_k}^b$ est le quotient.

L'écriture en base b peut être utilisée pour comparer deux entiers naturels non nuls, en faire la somme ou le produit (voir [**?**], chapitre 1, paragraphe 2).

L'écriture en base $b = 10$ permet d'obtenir les critères classiques de divisibilité résumés avec l'exercice qui suit.

Exercice 23.13 *Soit n un entier naturel et $n = n_p \cdots n_1 n_0$ son écriture décimale. Montrer que :*

- *n est divisible par 2 si, et seulement si, son chiffre des unités n_0 est pair ;*
- *n est divisible par 5 si, et seulement si, son chiffre des unités n_0 est égal à 0 ou 5 ;*
- *n est divisible par 3 si, et seulement si, la somme $\sum_{k=0}^{p} n_k$ de ses chiffres est divisible par 3 ;*
- *n est divisible par 9 si, et seulement si, la somme $\sum_{k=0}^{p} n_k$ de ses chiffres est divisible par 9 ;*
- *n est divisible par 11 si, et seulement si, la somme alternée $\sum_{k=0}^{p} (-1)^k n_k$ de ses chiffres est divisible par 11.*

Solution 23.13 *Ces critères de divisibilité se déduisent de la connaissance du reste dans la division euclidienne de 10 par $2, 3, 5, 9$ et 11 respectivement.*
Comme 10 est congru à 0 modulo 2 et modulo 5, on déduit que n est congru à n_0 modulo 2 et modulo 5 et donc n est divisible par 2 (resp. par 5) si, et seulement si, son chiffre des unités n_0 est pair, c'est-à-dire égal à $0, 2, 4, 6$ ou 8 (resp. multiple de 5, c'est-à-dire égal à 0 où 5).
Du fait que 10 est congru à 1 modulo 3 et modulo 9, on déduit que 10^k est congru à 1 modulo 3 et modulo 9 pour tout entier k et n est congru à $\sum_{k=0}^{p} n_k$ modulo 3 et modulo 9. Donc n est divisible par 3 (resp. par 9) si et seulement si la somme de ses chiffres est divisible par 3 (resp. par 9).
Enfin du fait que 10 est congru à -1 modulo 11 on déduit que 10^k est congru à $(-1)^k$ modulo

11 *pour tout entier* k *et* n *est congru à* $\sum_{k=0}^{p}(-1)^k n_k$ *modulo* 11. *Donc* n *est divisible par* 11 *si et seulement si la somme alternée de ses chiffres est divisible par* 11.

De manière un peu plus générale, on a les résultats suivants.

Exercice 23.14 *Soit* n *un entier naturel et* $n = \overline{n_p \cdots n_1 n_0}^b$ *son écriture dans une base* $b \geq 2$. *Montrer que :*

- *si* d *est un diviseur premier de* $b \geq 2$ *(les nombres premiers sont définis au chapitre 24), alors* n *est divisible par* d *si, et seulement si,* n_0 *est divisible par* d *;*
- *si* $b \geq 3$ *et* d *est un diviseur premier de* $b-1$, *alors* n *est divisible par* d *si, et seulement si,* $\sum_{k=0}^{p} n_k$ *est divisible par* d *;*
- *si* d *est un diviseur premier de* $b+1$, *alors* n *est divisible par* d *si, et seulement si,* $\sum_{k=0}^{p}(-1)^k n_k$ *est divisible par* d.

Solution 23.14 *Laissée au lecteur.*

Exercice 23.15 *Déterminer le reste dans la division euclidienne de* k^{100} *par* 10 *pour tout* k *compris entre* 1 *et* 10. *En déduire le dernier chiffre dans l'écriture en base* 10 *de* $\sum_{k=1}^{10} k^{100}$.

Solution 23.15 *On a :*

$$2^{100} = \left(2^5\right)^{20} = (30+2)^{20} \equiv 2^{20} = \left(2^5\right)^4 \equiv 2^4 = 16 \equiv 6 \ (10)$$

$$3^{100} = \left(3^4\right)^{25} \equiv 1^{25} \equiv 1 \ (10)$$

$$4^{100} = \left(2^{100}\right)^2 \equiv 36 \equiv 6 \ (10)$$

$$5^{100} \equiv 5 \ (10)$$

$$6^{100} \equiv (-4)^{100} \equiv 6 \ (10)$$

$$7^{100} \equiv (-3)^{100} \equiv 1 \ (10)$$

$$8^{100} \equiv (-2)^{100} \equiv 6 \ (10)$$

$$9^{100} \equiv (-1)^{100} \equiv 1 \ (10)$$

et donc $S \equiv 3 \ (10)$.

Exercice 23.16 *Pour tout entier naturel* n, *on désigne par* a_n *et* b_n *les entiers définis par* $a_0 = 16$, $b_0 = 4$ *et pour* $n \geq 1$, $a_n = 11\cdots1155\cdots56$, *où le chiffre* 1 *est répété* $n+1$ *fois et le chiffre* 5 *répété* n *fois et* $b_n = 33\cdots34$ *où le chiffre* 3 *est répété* n *fois.*
Montrer que $a_n = b_n^2$ *pour tout* n. *Généraliser.*

Solution 23.16 *Pour les premières valeurs de* n, *on peut constater que* $a_0 = 16 = 4^2 = b_0^2$, $a_1 = 1156 = 34^2 = b_1^2$, $a_2 = 111556 = 334^2 = b_2^2$.
De manière plus générale, pour $n \geq 1$, *on a :*

$$\begin{aligned} b_n &= 4 + 3\cdot 10 + \cdots + 3\cdot 10^n \\ &= 4 + 3\cdot 10\frac{10^n - 1}{10-1} = 4 + \frac{10}{3}\left(10^n - 1\right) \\ &= \frac{2}{3} + \frac{1}{3}10^{n+1} \end{aligned}$$

et :

$$\begin{aligned} a_n &= 6 + 5 \cdot 10 + \cdots + 5 \cdot 10^n + 10^{n+1} + \cdots + 10^{2n+1} \\ &= 6 + 5 \cdot 10 \frac{10^n - 1}{10 - 1} + 10^{n+1} \frac{10^{n+1} - 1}{10 - 1} \\ &= 6 + \frac{5 \cdot 10}{9} \left(10^n - 1\right) + \frac{10^{n+1}}{9} \left(10^{n+1} - 1\right) \\ &= \frac{4}{9} + \frac{4}{9} 10^{n+1} + \frac{1}{9} 10^{2n+2} = \left(\frac{2}{3} + \frac{1}{3} 10^{n+1}\right)^2 = b_n^2. \end{aligned}$$

On peut remarquer que :

$$(2b_n)^2 = 66 \cdots 68^2 = 4a_n = 44 \cdots 4622 \cdots 24.$$

On peut aussi montrer ce résultat par récurrence sur $n \geq 0$.
On peut essayer de généraliser. Soit $b_n = bb \cdots bc$ *où le chiffre* b *compris entre* 1 *et* 9 *est répété* n *fois et* c *est compris entre* 0 *et* 9. *On a :*

$$\begin{aligned} b_n &= c + b \cdot 10 + \cdots + b \cdot 10^n \\ &= c + b \cdot 10 \frac{10^n - 1}{10 - 1} = c + \frac{10b}{9} \left(10^n - 1\right) \\ &= c - \frac{10b}{9} + \frac{b}{9} 10^{n+1} \end{aligned}$$

et :

$$\begin{aligned} b_n^2 &= \left(c - \frac{10b}{9}\right)^2 + \frac{2b}{9} \left(c - \frac{10b}{9}\right) 10^{n+1} + \frac{b^2}{9^2} 10^{2n+2} \\ &= \left(c - \frac{10b}{9}\right)^2 + \frac{2b}{9} \left(c - \frac{10b}{9}\right) 10^{n+1} + \frac{b^2}{9} 10^{n+1} \frac{10^{n+1} - 1}{9} + \frac{b^2}{9^2} 10^{n+1} \\ &= \left(c - \frac{10b}{9}\right)^2 + b \left(2c - \frac{19}{9} b\right) \frac{10^{n+1}}{9} + \frac{b^2}{9} 10^{n+1} \frac{10^{n+1} - 1}{9} \\ &= \left(c - \frac{10b}{9}\right)^2 + b \left(2c - \frac{19}{9} b\right) 10 \frac{10^n - 1}{9} + \frac{10b}{9} \left(2c - \frac{19}{9} b\right) \\ &\qquad + \frac{b^2}{9} 10^{n+1} \frac{10^{n+1} - 1}{9} \\ &= c^2 - \frac{10}{9} b^2 + b \left(2c - \frac{19}{9} b\right) \left(10 + \cdots + 10^n\right) + \frac{b^2}{9} \left(10^{n+1} + \cdots + 10^{2n+1}\right) \end{aligned}$$

Il s'agit alors de choisir b *et* c *tels que* $\alpha = c^2 - \dfrac{10}{9} b^2$ *et* $\beta = b \left(2c - \dfrac{19}{9} b\right)$ *soient entiers compris entre* 0 *et* 9 *et* $\gamma = \dfrac{b^2}{9}$ *est entier compris entre* 1 *et* 9. *Si* $b \in \{1, 2, 4, 5, 7, 8\}$, *alors* $\dfrac{b^2}{9}$ *n'est pas entier.*
Pour $b = 3$, *on a* $\gamma = 1$, $\alpha = c^2 - 10$ *et* $\beta = 6c - 19$, *ce qui impose* $c = 4$ *(*$c \leq 3$ *donne* $\alpha < 0$ *et* $c \geq 5$ *donne* $\alpha > 9$*), c'est l'énoncé initiale avec* $\alpha = 6$, $\beta = 5$ *et* $\gamma = 1$.
Pour $b = 6$, *on a* $\gamma = 4$, $\alpha = c^2 - 40$ *et* $\beta = 12c - 76$, *ce qui impose* $c = 7$. *On a alors* $\alpha = 9$, $\beta = 8$ *et* $\gamma = 4$, *soit* $b_n^2 = a_n$ *avec* $a_n = 44 \cdots 4488 \cdots 89$ *et* $b_n = 66 \cdots 67$.
Pour $b = 9$ *on a* $\gamma = 9$, $\alpha = c^2 - 90$ *qui est toujours négatif, ce cas est donc exclu.*

23.5 Sous-groupes additifs de $\mathbb{Z}$

Le théorème de division euclidienne permet de caractériser les sous-groupes additifs de $\mathbb{Z}$.

On a déjà vu que pour tout entier naturel n, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe additif de $\mathbb{Z}$. En réalité ce sont les seuls.

Théorème 23.4 *Si G est un sous-groupe de $(\mathbb{Z},+)$, il existe alors un unique entier naturel n tel que $G=n\mathbb{Z}$.*

Démonstration. Si $G=\{0\}$, on a $G=0\mathbb{Z}$.

Si $G\neq\{0\}$, il existe dans G un entier a non nul et l'un des entiers a ou $-a$ est dans $G^+=G\cap\mathbb{N}^*$. L'ensemble G^+ est donc une partie non vide de $\mathbb{N}^*$ et en conséquence admet un plus petit élément $n\geq 1$. Comme $n\in G$ et G est un groupe additif, on a $n\mathbb{Z}\subset G$. D'autre part, pour tout $x\in G$, la division euclidienne par n donne $x=qn+r$ avec $r=x-nq\in G^+$ et $r\leq n-1$, ce qui impose $r=0$ par définition de n. On a donc $G\subset n\mathbb{Z}$ et $G=n\mathbb{Z}$.

L'unicité provient du fait que $n\mathbb{Z}=m\mathbb{Z}$ si, et seulement si, $n=\pm m$ et pour n,m positifs, on a nécessairement $n=m$. ∎

Le résultat précédent peut se traduire en disant que l'anneau $\mathbb{Z}$ est principal et a de nombreuses applications.

23.5.1 Ordre d'un élément dans un groupe

Comme première application, nous allons voir que cette caractérisation des sous-groupes de $(\mathbb{Z},+)$ peut être utilisée pour définir l'ordre d'un élément dans un groupe.

Étant donné un groupe multiplicatif G et un élément a de G, l'application :

$$\begin{array}{rccc}\varphi_a: & \mathbb{Z} & \to & G\\ & k & \mapsto & a^k\end{array}$$

est un morphisme de groupes et son noyau est un sous-groupe de $\mathbb{Z}$. En effet, pour j,k dans $\mathbb{Z}$, on a $\varphi_a(j+k)=a^{j+k}=a^ja^k=\varphi_a(j)\,\varphi_a(k)$, donc φ_a est un morphisme de groupes et le théorème 20.7 nous dit que $\ker(\varphi_a)$ est un sous-groupe de $\mathbb{Z}$. Il existe donc un unique entier $n\geq 0$ tel que $\ker(\varphi_a)=n\mathbb{Z}$.

Le théorème 20.7 nous dit aussi que $\mathrm{Im}(\varphi_a)$ est un sous-groupe de G, il est défini par :

$$\mathrm{Im}(\varphi_a)=\left\{a^k\mid k\in\mathbb{Z}\right\}$$

et est noté $\langle a\rangle$. On dit que c'est le sous-groupe de G engendré par a.

On aura $n=0$ si, et seulement si, φ_a est injective, ce qui revient à dire que $\varphi_a(k)=a^k\neq 1$ pour tout $k\in\mathbb{Z}^*$ ou encore que $\varphi_a(k)=a^k\neq\varphi_a(j)=a^j$ pour tous $j\neq k$ dans $\mathbb{Z}$ encore équivalent à dire que le sous-groupe $\langle a\rangle=\mathrm{Im}(\varphi_a)$ de G est infini.

On dira alors, dans le cas où $n=0$, que a est un élément d'ordre infini dans G.

Si $n\geq 1$, en effectuant, pour $k\in\mathbb{Z}$, la division euclidienne de k par n, on a $k=qn+r$ avec $0\leq r\leq n-1$ et $a^k=(a^n)^q\,a^r=a^r$. On a donc :

$$\langle a\rangle=\mathrm{Im}(\varphi_a)=\{a^r\mid 0\leq r\leq n-1\}$$

De plus pour $1\leq r\leq n-1$, on a $a^r\neq 1$ puisque $a^r=1$ entraîne $r\in\ker(\varphi_a)=n\mathbb{Z}$, soit $r=qn$, ce qui est impossible avec $0<r<n$. Il en résulte que si r et s sont deux entiers distincts compris entre 0 et $n-1$, on a alors $a^r\neq a^s$. En effet, en supposant que $r\leq s$, l'égalité $a^r=a^s$ équivaut à $a^{s-r}=1$ avec $s-r$ compris entre 0 et $n-1$, ce qui équivaut à $r=s$. Le groupe $\langle a\rangle$ a donc exactement n éléments. On dit alors que a est d'ordre n dans G.

En définitive, on donne les définitions suivantes.

Définition 23.5 *Soient G un groupe multiplicatif et a un élément de G. L'ordre de a est l'élément $\theta(a) \in \mathbb{N}^* \cup \{+\infty\}$ défini par :*

$$\theta(a) = \operatorname{card}(\langle a \rangle).$$

Si $\theta(a)$ est dans $\mathbb{N}^*$, on dit alors que a est d'ordre fini, sinon on dit qu'il est d'ordre infini.

Remarque 23.6 *Seul l'unité 1 est d'ordre 1 dans G. En effet, si $a = 1$, alors $\langle a \rangle = \{1\}$ et si $a \neq 1$, alors $a^0 \neq a^1$ et $\langle a \rangle$ a au moins deux éléments.*

L'étude préliminaire que nous avons faite se traduit par le résultat suivant.

Théorème 23.5 *Soient G un groupe multiplicatif et a un élément de G. Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que $a^n = 1$ et $a^k \neq 1$ si k est compris entre 1 et $n-1$ (n est le plus petit entier naturel non nul tel que $a^n = 1$).*

Démonstration. Supposons que a soit d'ordre $n \geq 1$. Si $a^k \neq 1$ pour tout $k \in \mathbb{N}^*$, on a alors $a^j \neq a^j$ pour tous $j \neq k$ dans $\mathbb{Z}$ et $\langle a \rangle$ est infini, ce qui est contraire à l'hypothèse. Il existe donc des entiers $k \geq 1$ tels que $a^k = 1$ et peut définir le plus petit de ces entiers, notons le m. On a donc $a^m = 1$, $a^k \neq 1$ si k est compris entre 1 et $m-1$ et l'ensemble $H = \{a^r \mid 0 \leq r \leq m-1\}$ est de cardinal m contenu dans $\langle a \rangle$ qui est de cardinal n, donc $m \leq n$. Par division euclidienne tout entier relatif k s'écrit $k = qm + r$ avec $0 \leq r \leq m-1$ et $a^k = (a^m)^q a^r = a^r \in H$, donc $\langle a \rangle$ est contenu dans H et $n \leq m$. On a donc $n = m$ et $H = \langle a \rangle$. L'entier n vérifie donc bien la propriété annoncée.

Réciproquement supposons qu'il existe un entier $n \geq 1$ tel que $a^n = 1$ et $a^k \neq 1$ si k est compris entre 1 et $n-1$. Les mêmes arguments nous donnent :

$$\begin{aligned} H &= \{a^r \mid 0 \leq r \leq n-1\} \\ \subset \langle a \rangle &= \left\{a^{qn+r} \mid q \in \mathbb{Z},\ 0 \leq r \leq n-1\right\} = H \end{aligned}$$

et $\langle a \rangle = H$ est de cardinal n, ce qui signifie que a est d'ordre n. ∎

Corollaire 23.1 *Soient G un groupe multiplicatif et a un élément de G. Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que, pour $k \in \mathbb{Z}$, on a $a^k = 1$ si, et seulement si, k est multiple de n.*

Démonstration. Si a est d'ordre n, alors $a^n = 1$ et pour $k = qn + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$ (division euclidienne), on a $a^k = a^r = 1$ si, et seulement si $r = 0$.

Réciproquement supposons que $a^k = 1$ si, et seulement si, k est multiple de n. On a alors $a^n = 1$ et $a^k \neq 1$ si k est compris entre 1 et $n-1$, ce qui signifie que a est d'ordre n. ∎

Remarque 23.7 *Dans le cas où le groupe G est additif, l'ordre de $a \in G$ est défini comme le plus petit entier $n \geq 1$ tel que $na = 0$, quand cet ordre est fini. L'égalité $ma = 0$ équivaut alors à dire que m est multiple de n. Le groupe engendré par a est alors :*

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\} = \{ra \mid 0 \leq r \leq n-1\}.$$

Dans le cas où le groupe G est fini, le théorème de Lagrange (théorème 20.9) nous dit que, pour tout $a \in G$, l'ordre de a divise l'ordre de G.

23.5.2 Caractéristique d'un anneau ou d'un corps commutatif

Comme deuxième application, nous allons voir que cette la caractérisation des sous-groupes de $(\mathbb{Z},+)$ peut être utilisée pour définir la caractéristique d'un anneau ou d'un corps commutatif.

Si $(A,+,\cdot)$ est un anneau commutatif unitaire, alors l'application $\varphi : n \mapsto n\cdot 1$ est un morphisme d'anneaux de $\mathbb{Z}$ dans A et son noyau $\ker(\varphi)$ est un sous-groupe de $\mathbb{Z}$ (c'est même un sous-anneau), il existe donc un unique entier naturel p tel que :

$$\ker(\varphi) = \{n \in \mathbb{Z} \mid n\cdot 1 = 0\} = p\mathbb{Z}$$

et on peut alors donner la définition suivante.

Définition 23.6 *Si $(A,+,\cdot)$ est un anneau commutatif unitaire, la caractéristique de A est l'entier naturel p qui vérifie* $\ker(\varphi) = p\mathbb{Z}$*, où φ est le morphisme d'anneaux de $\mathbb{Z}$ dans A défini par $\varphi(n) = n\cdot 1$ pour tout $n \in \mathbb{Z}$.*

Dire que la caractéristique d'un anneau commutatif unitaire A est nulle équivaut à dire que l'application φ est injective et dans ce cas $\varphi(\mathbb{Z})$ est un sous-anneau de A isomorphe à $\mathbb{Z}$, il est donc en particulier infini. On identifie ce sous-anneau $\varphi(\mathbb{Z})$ à $\mathbb{Z}$.

Un anneau de caractéristique nul est donc infini et contient $\mathbb{Z}$ comme sous-anneau.

Dans le cas où $A = \mathbb{K}$ est un corps commutatif, si sa caractéristique est nulle, il contient non seulement $\mathbb{Z}$, mais aussi le corps $\mathbb{Q}$ des rationnels, puisque pour tout entier non nul n, on a $(n\cdot 1)^{-1} = \dfrac{1}{n} \in \mathbb{K}$ et en conséquence tout $r = p\dfrac{1}{q}$ (où $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$) est aussi dans $\mathbb{K}$.

Nous verrons plus loin que la caractéristique d'un anneau commutatif unitaire et intègre est soit nulle soit un nombre premier. C'est le cas en particulier pour un corps commutatif.

Le théorème 23.4 combiné avec le fait que la somme et l'intersection de deux sous groupes de $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$ (voir l'exercice 20.22 pour la somme de deux sous-groupes) nous permet de donner une définition du pgcd et du ppcm de deux entiers relatifs.

23.5.3 Plus grand commun diviseur

La caractérisation des sous-groupes de $(\mathbb{Z},+)$ peut être utilisée pour définir le pgcd de deux ou plusieurs entiers relatifs, non tous nuls.

Théorème 23.6 *Soient a,b deux entiers relatifs non tous deux nuls. Il existe un unique entier naturel δ tel que :*

$$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}.$$

Cet entier s'écrit $\delta = au + bv$ avec $(u,v) \in \mathbb{Z}^2$ et c'est le plus grand entier naturel qui divise a et b.

Démonstration. $a\mathbb{Z} + b\mathbb{Z}$ étant un sous groupe de $(\mathbb{Z},+)$, le théorème 23.4 nous dit qu'il existe un unique entier naturel δ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$.

Comme $\delta \in \delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $\delta = au + bv$.

De $a\mathbb{Z} \subset \delta\mathbb{Z}$ et $b\mathbb{Z} \subset \delta\mathbb{Z}$, on déduit que δ un diviseur commun à a et b. Si $d \in \mathbb{N}$ est un diviseur commun à a et b, il divise aussi $\delta = au + bv$ et $d \leq \delta$ (a et b n'étant pas tous les deux nuls, on a $\delta \neq 0$). Donc δ est bien le plus grand entier naturel qui divise a et b. ■

On peut donc donner la définition suivante.

Définition 23.7 *Soient a,b deux entiers relatifs non tous deux nuls. On appelle plus grand commun diviseur de a et b le plus grand entier naturel qui divise a et b. On le note* $\operatorname{pgcd}(a,b)$ *ou $a \wedge b$.*

La relation $a \wedge b = au + bv$ avec $(u, v) \in \mathbb{Z}^2$ est l'identité de Bézout.

Exercice 23.17 *Soient a, b deux entiers relatifs non tous deux nuls et $\mathcal{D}_{a,b}$ l'ensemble des diviseurs communs à a et b dans $\mathbb{N}^*$, c'est-à-dire :*

$$\mathcal{D}_{a,b} = \{d \in \mathbb{N}^* \mid d/a \text{ et } d/b\}.$$

Montrer que $a \wedge b$ est le plus grand élément pour l'ordre de la division dans $\mathbb{N}$ de $\mathcal{D}_{a,b}$ et que $\mathcal{D}_{a,b} = \mathcal{D}_{a\wedge b}$ (ensemble des diviseurs strictement positifs de $a \wedge b$).

Solution 23.17 *On sait déjà que $\delta = a \wedge b$ divise a et b, donc $\delta \in \mathcal{D}_{a,b}$ et tout entier $d \in \mathcal{D}_{a,b}$ divisant a et b va diviser $\delta = au + bv$.*
Comme tout $d \in \mathcal{D}_{a,b}$ divise δ, on a $\mathcal{D}_{a,b} \subset \mathcal{D}_\delta$ et comme tout $d \in \mathcal{D}_\delta$ divise δ qui divise lui même a et b, d va diviser a et b, soit $d \in \mathcal{D}_{a,b}$. On a donc $\mathcal{D}_{a,b} = \mathcal{D}_{a\wedge b}$.

On peut aussi donner une définition de $\text{pgcd}\,(a, b)$ sans référence directe aux sous-groupes de $\mathbb{Z}$ comme indiqué dans l'exercice suivant.

Exercice 23.18 *Montrer, sans référence directe aux sous-groupes de $\mathbb{Z}$, que l'ensemble $\mathcal{D}_{a,b}$ défini à l'exercice précédent admet donc un plus grand élément δ (δ est alors le plus grand diviseur communs à a et b).*

Solution 23.18 *L'ensemble $\mathcal{D}_{a,b}$ est non vide car il contient* 1. *Comme a et b ne sont pas tous deux nuls, cet ensemble est fini puisqu'un entier relatif non nul n'a qu'un nombre fini de diviseurs dans $\mathbb{N}^*$. L'ensemble $\mathcal{D}_{a,b}$ est donc non vide et majoré dans $\mathbb{N}^*$, il admet donc un plus grand élément $\delta \in \mathbb{N}^*$ qui est bien le plus diviseur communs à a et b.*

Exercice 23.19 *Vérifier les propriétés suivantes du* pgcd *:*
- $\forall\,(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}\,,\ a \wedge b \in \mathbb{N}^*$;
- $\forall a \in \mathbb{Z}^*,\ a \wedge 0 = a \wedge a = |a|$;
- $\forall a \in \mathbb{Z},\ a \wedge 1 = 1$;
- $\forall\,(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}\,,\ a \wedge b = |a| \wedge |b| = |a| \wedge b = a \wedge |b|$;
- $\forall\,(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}\,,\ a \wedge b = b \wedge a$ *(commutativité du* pgcd*)* ;
- *pour $b \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$, on a $a \wedge b = |b|$ si, et seulement si, b divise a* ;
- $\forall\,(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}\,,\ \forall c \in \mathbb{Z}^*,\ (ac) \wedge (bc) = |c|\,(b \wedge a)$;
- *si $d \in \mathbb{Z}^*$ est un diviseur commun de a et b non tous deux nuls, alors* $\dfrac{a}{d} \wedge \dfrac{b}{d} = \dfrac{a \wedge b}{|d|}$;
- *pour a, b, c non tous nuls dans $\mathbb{Z}$, on a $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (associativité du* pgcd*).*

Solution 23.19 *Laissée au lecteur.*

Exercice 23.20 *Soient a, b deux entiers naturels non nuls. Montrer que :*

$$a \wedge b = \begin{cases} (a - b) \wedge b & \text{si } a \geq b \\ a \wedge (b - a) & \text{si } b > a \end{cases}$$

En déduire un algorithme simple de calcul de $a \wedge b$.

Solution 23.20 *Si $a = b$, alors $a \wedge b = a \wedge a = a = 0 \wedge a$. Si $a > b$, on note $\delta = a \wedge b$ et $\delta' = (a-b) \wedge b$. Comme δ divise a et b, il divise $a-b$ et b, donc il divise leur* pgcd *δ'. De même δ' qui divise $a-b$ et b va diviser $a = (a-b)+b$ et b, il divise donc δ et $\delta = \delta'$. Pour $a < b$, on a $a \wedge b = b \wedge a = a \wedge (b-a)$.*
Un algorithme simple de calcul de $a \wedge b$, pour a, b entiers relatifs est donc le suivant :
Début
Lecture de a et b ;
$a = |a|$; $b = |b|$;
Tant que $a \neq b$ Faire
Début
Si $a > b$ Alors
remplacer a par $a - b$;
Sinon
remplacer b par $b - a$;
Fin si ;
Fin ;
pgcd $= a$;
Fin.
Par exemple, pour $(a, b) = (128, 28)$, on a :

$$\begin{aligned} a \wedge b = 100 \wedge 28 = 72 \wedge 28 = 44 \wedge 28 \\ = 16 \wedge 28 = 16 \wedge 12 = 4 \wedge 12 = 4 \wedge 8 \\ = 4 \wedge 4 = 4. \end{aligned}$$

Cet algorithme n'est évidemment pas très performant, il sera amélioré par l'algorithme d'Euclide.

Exercice 23.21 *Soient a et b deux entiers relatifs non tous deux nuls. Montrer que :*

$$a \wedge b = a \wedge (a+b) = b \wedge (a+b).$$

Solution 23.21 *On remarque que si $(a, b) \neq (0, 0)$, alors $(a, a+b) \neq (0, 0)$ et $(b, a+b) \neq (0, 0)$.*
En notant $\delta = a \wedge b$ et $\delta' = a \wedge (a+b)$, on a :

$$\begin{aligned} \delta = au + bv = a(u-v) + (a+b)v \\ \in a\mathbb{Z} + (a+b)\mathbb{Z} = \delta'\mathbb{Z} \end{aligned}$$

donc $\delta\mathbb{Z} \subset \delta'\mathbb{Z}$ et :

$$\begin{aligned} \delta' = au' + (a+b)v' = a(u'+v') + bv' \\ \in a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z} \end{aligned}$$

donc $\delta'\mathbb{Z} \subset \delta\mathbb{Z}$ et donc $\delta\mathbb{Z} = \delta'\mathbb{Z}$, ce qui équivaut à $\delta = \delta'$.
On peut aussi dire que comme δ divise a et b, il divise a et $a+b$, donc il divise leur pgcd *δ'. De même δ' qui divise a et $a+b$ va diviser a et $b = (a+b) - a$, il divise donc δ et $\delta = \delta'$.*
On a donc, en permutant les rôles de a et b :

$$a \wedge b = a \wedge (a+b) = b \wedge (a+b).$$

Exercice 23.22 *Soient a, b deux entiers naturels non nuls. Calculer $(5a+3b) \wedge (7a+4b)$ en fonction de $a \wedge b$.*

Solution 23.22 *En utilisant la relation $a \wedge b = (a-b) \wedge b$ pour $a \geq b$, on a :*

$$\begin{aligned}(5a+3b) \wedge (7a+4b) &= (5a+3b) \wedge (2a+b) \\ &= (3a+2b) \wedge (2a+b) \\ &= (a+b) \wedge (2a+b) \\ &= (a+b) \wedge a \\ &= a \wedge b.\end{aligned}$$

On définit de manière analogue le pgcd d'une famille $a_1, \cdots, a_p$ formée de p entiers non tous nuls comme le plus grand des diviseurs communs à $a_1, \cdots, a_p$. On le note $\text{pgcd}(a_1, \cdots, a_p)$ ou $a_1 \wedge a_2 \wedge \cdots \wedge a_p$ et c'est un entier supérieur ou égal à 1. Cette définition est justifiée par le théorème suivant.

Théorème 23.7 *Soient $a_1, \cdots, a_p$ des entiers relatifs non tous nuls. Il existe un unique entier naturel δ tel que :*

$$a_1\mathbb{Z} + \cdots + a_p\mathbb{Z} = \delta\mathbb{Z}.$$

Cet entier s'écrit $\delta = \sum_{k=1}^{p} u_k a_k$ avec $(u_1, \cdots, u_p) \in \mathbb{Z}^p$ et c'est le plus grand entier naturel qui divise $a_1, \cdots, a_p$.

Démonstration. Analogue au cas où $p = 2$. ∎

Comme dans le cas où $p = 2$, on vérifie que $a_1 \wedge \cdots \wedge a_p$ est aussi le plus grand élément pour l'ordre de la division dans $\mathbb{N}$ de l'ensemble des diviseurs positifs communs à $a_1, \cdots, a_p$.

L'égalité $\delta = \sum_{k=1}^{p} u_k a_k$ est l'identité de Bézout.

La notation $a_1 \wedge a_2 \wedge \cdots \wedge a_p$ ne pose pas de problème du fait de la commutativité et l'associativité du pgcd (elle est indépendante de l'ordre des a_k).

23.5.4 Plus petit commun multiple

La caractérisation des sous-groupes de $(\mathbb{Z}, +)$ peut être utilisée pour définir le ppcm de deux ou plusieurs entiers relatifs, non tous nuls.

Théorème 23.8 *Soient a, b sont deux entiers relatifs. Il existe un unique entier naturel μ tel que :*

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}.$$

Si $a = 0$ ou $b = 0$, alors $\mu = 0$. Si $a \neq 0$ et $b \neq 0$, alors μ est le plus petit entier naturel non nul multiple de a et de b.

Démonstration. $a\mathbb{Z} \cap b\mathbb{Z}$ étant un sous groupe de $(\mathbb{Z}, +)$, l'existence et l'unicité de μ se déduit du théorème 23.4.

Si $a = 0$ ou $b = 0$, on a $\mu\mathbb{Z} \subset 0\mathbb{Z} = \{0\}$ et $\mu = 0$.

Si $a \neq 0$ et $b \neq 0$, de $\mu\mathbb{Z} \subset a\mathbb{Z}$ et $\mu\mathbb{Z} \subset b\mathbb{Z}$, on déduit que μ est multiple de a et b. Si $m \in \mathbb{N}$ est un multiple commun à a et b, il est dans $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ et c'est donc un multiple de μ, ce qui implique $m \geq \mu$. Donc, μ est bien le plus petit entier naturel non nul multiple de a et de b. ∎

On peut donc donner la définition qui suit.

Définition 23.8 *Soient a, b deux entiers relatifs. On appelle plus petit commun multiple de a et b le plus petit entier naturel multiple de a et b. On le note* $\operatorname{ppcm}(a,b)$ *ou* $a \vee b$.

Remarque 23.8 *La définition de* $\operatorname{ppcm}(a,b)$ *peut aussi se justifier directement sans référence directe aux sous-groupes de $\mathbb{Z}$. Pour ce faire, on désigne par $\mathcal{M}_{a,b}$ l'ensemble des multiples communs à a et b. Si $a \neq 0$ et $b \neq 0$, alors l'ensemble $\mathcal{M}_{a,b} \cap \mathbb{N}^*$ des multiples communs à a et b qui sont strictement positifs est non vide car il contient $|ab|$, il admet donc un plus petit élément μ qui est bien plus petit commun multiple de a et b. Pour $a = 0$ ou $b = 0$, on a $\mathcal{M}_{a,b} = \{0\}$ et $\mu = 0$.*

Remarque 23.9 *Le* ppcm *de a et b est aussi le plus petit élément pour l'ordre de la division dans $\mathbb{Z}$ de l'ensemble $\mathcal{M}_{a,b}$ des multiples communs à a et b. En effet, $a \vee b$ est un multiple de a et b et tout multiple commun m à a et b qui est dans $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ est un multiple de $a \vee b$.*

On vérifie facilement les propriétés suivantes.

Exercice 23.23 *Vérifier les propriétés suivantes du* ppcm *:*
- $\forall (a,b) \in (\mathbb{Z}^*)^2$, $a \vee b \in \mathbb{N}^*$;
- $\forall a \in \mathbb{Z}^*$, $a \vee 1 = a \vee a = |a|$;
- $\forall (a,b) \in \mathbb{Z}^2$, $a \vee b = |a| \vee |b| = |a| \vee b = a \vee |b|$;
- $\forall (a,b) \in \mathbb{Z}^2$, $a \vee b = b \vee a$ *(commutativité du* ppcm*)* ;
- *pour $b \in \mathbb{Z}$ et $a \in \mathbb{Z}$, on a $a \vee b = |b|$ si, et seulement si, b est multiple de a ;*
- $\forall (a,b,c) \in \mathbb{Z}^3$, $(ac) \vee (bc) = |c|\,(b \vee a)$;
- *si $d \in \mathbb{Z}^*$ est un diviseur commun de a et b, alors* $\dfrac{a}{d} \vee \dfrac{b}{d} = \dfrac{a \vee b}{|d|}$;
- *pour a, b, c non tous nuls dans $\mathbb{Z}$, on a $a \vee (b \vee c) = (a \vee b) \vee c$ (associativité du* ppcm*).*

Solution 23.23 *Laissée au lecteur.*

Lemme 23.1 *Soient a, b deux entiers relatifs premiers entre eux. On a alors :*

$$a \vee b = |ab|.$$

Démonstration. Du fait que $|ab|$ est un multiple de a et b on déduit que $\mu = a \vee b$ divise ab.

D'autre part il existe deux entiers k, k' tels que $\mu = ka = k'b$ et comme a est premier avec b et divise $k'b$, il divise k' (théorème de Gauss). Ce qui donne $\mu = k''ab$ et ab divise μ. D'où l'égalité $\mu = ab$. ∎

Nous verrons que la réciproque du résultat précédent est vraie.

Théorème 23.9 *Soient a, b deux entiers relatifs. On a alors :*

$$(a \wedge b)(a \vee b) = |ab|.$$

Démonstration. On note $\delta = a \wedge b$ et on a $|a| = \delta a'$, $|b| = \delta b'$ avec a' et b' premiers entre eux. Ce qui donne :

$$\mu = a \vee b = (\delta a') \vee (\delta b') = \delta\,(a' \vee b') = \delta a' b'$$

et $\delta\mu = \delta a' \delta b' = |ab|$. ∎

Du lemme et du théorème précédent, on déduit que :

$$a \wedge b = 1 \Leftrightarrow a \vee b = |ab|.$$

On a donc pour a, b dans $\mathbb{Z}^*$ $a \vee b = \dfrac{|ab|}{a \wedge b}$.

On peut donc définir de manière naturelle le ppcm de deux entiers relatifs non tous deux nuls par :

$$a \vee b = \frac{|ab|}{a \wedge b}.$$

On peut aussi utiliser cette relation pour calculer le ppcm de deux entiers. On calcule d'abord le pgcd en utilisant l'algorithme d'Euclide (paragraphe 23.6), puis on divise $|ab|$ par ce pgcd .

On définit de manière analogue le ppcm d'une famille $a_1, \cdots, a_p$ formée de p entiers non tous nuls comme le plus petit des multiples communs à $a_1, \cdots, a_p$. On le note ppcm $(a_1, \cdots, a_p)$ ou $a_1 \vee a_2 \vee \cdots \vee a_p$ et c'est un entier supérieur ou égal à 1. Cette définition est justifiée par le théorème suivant.

Théorème 23.10 *Soient $a_1, \cdots, a_p$ des entiers relatifs non tous nuls. Il existe un unique entier naturel μ tel que :*

$$a_1\mathbb{Z} \cap \cdots \cap a_p\mathbb{Z} = \mu\mathbb{Z}.$$

μ est le plus petit entier naturel divisible par $a_1, a_2, \cdots$ et a_p.

Démonstration. Analogue au cas où $p = 2$. ∎

La notation $a_1 \vee a_2 \vee \cdots \vee a_p$ ne pose pas de problème du fait de la commutativité et l'associativité du ppcm (elle est indépendante de l'ordre des a_k).

Comme dans le cas où $p = 2$, on vérifie que $a_1 \vee \cdots \vee a_p$ est aussi le plus petit élément pour l'ordre de la division dans $\mathbb{N}$ de l'ensemble des multiples positifs communs à $a_1, \cdots, a_p$.

Exercice 23.24 *Montrer que si $a_1, \cdots, a_p$ sont des entiers relatifs non nuls deux à deux premiers entre eux alors $a_1 \vee \cdots \vee a_p = |a_1 \cdots a_p|$. Ce résultat est-il encore valable si on suppose que $a_1, \cdots, a_p$ sont premiers entre eux dans leur ensemble.*

Solution 23.24 *On sait déjà que si a_1 et a_2 sont premiers entre eux alors $a_1 \vee a_2 = |a_1 a_2|$. Supposons le résultat acquis pour $p - 1 \geq 2$ et soient $a_1, \cdots, a_p$ deux à deux premiers entre eux. Les entiers $a_1 \cdots a_{p-1}$ et a_p sont alors premiers entre eux (corollaire 23.3) et en utilisant l'associativité du* ppcm, *on a :*

$$\begin{aligned} a_1 \vee \cdots \vee a_p &= (a_1 \vee \cdots \vee a_{p-1}) \vee a_p \\ &= |a_1 \cdots a_{p-1}| \vee a_p = |a_1 \cdots a_p| . \end{aligned}$$

Ce résultat n'est plus valable si on suppose seulement que les a_k sont premiers entre eux dans leur ensemble comme le montre l'exemple suivant :

$$2 \vee 3 \vee 4 = 12 \neq 2 \cdot 3 \cdot 4 = 24$$

Exercice 23.25 *A-t-on $(a_1 \wedge \cdots \wedge a_p)(a_1 \vee \cdots \vee a_p) = |a_1 \cdots a_p|$ dans $\mathbb{Z}^*$?*

Solution 23.25 *La réponse est non pour $n \geq 3$ comme le montre l'exercice précédent.*

Exercice 23.26 *Peut-on trouver des entiers a, b tels que $a \wedge b = 7$ et $a \vee b = 36$.*

Solution 23.26 *Comme $a \wedge b = 7$ divise a et b, il divise $a \vee b$ et $a \vee b = 36$ est alors impossible.*

Exercice 23.27 *Déterminer tous les couples (a, b) d'entiers naturels non nuls tels que $a \wedge b = 3$ et $a \vee b = 12$.*

Solution 23.27 *De $a \vee b = 12$ on déduit que a, b sont des diviseurs de 12 donc dans $\{1,2,3,4,6,12\}$. de $a \wedge b = 3$, on déduit que a et b sont multiples de 3, donc dans $\{3,6,12\}$. De $ab = (a \wedge b)(a \vee b) = 36$, on déduit que :*

- *$a = 3$ [resp. $b = 3$] donne $b = 12$ [resp. $a = 12$] et $(3,12), (12,3)$ sont deux solutions possibles ;*
- *$a = 6$ [resp. $b = 6$] donne $b = 6$ [resp. $a = 6$] et $a \wedge b = 6 \neq 3$.*

En définitive, $(a,b) \in \{(3,12),(12,3)\}$.

Exercice 23.28 *On se propose de montrer que pour tout entier naturel $n \geqslant 2$, on a :*

$$\mu_n = \text{ppcm}(1,2,\cdots,n) \geq 2^{n-2}.$$

1. *Montrer le résultat pour $n = 2$ et $n = 3$.*
2. *Pour tout entier naturel n, on, note :*

$$I_n = \int_0^1 x^n (1-x)^n \, dx.$$

   (a) *Montrer que :*

$$\forall n \in \mathbb{N},\ 0 < I_n \leq \frac{1}{4^n}.$$

   (b) *Montrer que, pour tout $n \in \mathbb{N}^*$, il existe un entier naturel non nul a_n tel que $I_n = \dfrac{a_n}{\mu_{2n+1}}$.*

   (c) *En déduire que :*

$$\forall n \in \mathbb{N}^*,\ \mu_{2n+1} \geq 2^{2n}.$$

   (d) *En déduire le résultat annoncé.*

Solution 23.28

1. *On a :*

$$\mu_2 = \text{ppcm}(1,2) = 2 \geq 1 \text{ et } \mu_3 = \text{ppcm}(1,2,3) = 6 \geq 2.$$

2.

   (a) *Pour $0 < x < 1$, on a $0 < x(x-1) \leq \sup_{[0,1]} x(1-x) = \dfrac{1}{4}$, ce qui donne le résultat.*

   (b) *On a :*

$$\begin{aligned} I_n &= \int_0^1 x^n \left(\sum_{k=0}^n C_n^k (-1)^k x^k \right) dx \\ &= \sum_{k=0}^n C_n^k (-1)^k \int_0^1 x^{n+k} dx \\ &= \sum_{k=0}^n C_n^k \frac{(-1)^k}{n+k+1} \end{aligned}$$

   et en réduisant au même dénominateur $I_n = \dfrac{a_n}{\mu_{2n+1}}$, où $a_n \in \mathbb{N}^*$.

(c) On a alors $\mu_{2n+1} I_n = a_n \geq 1$ *et :*

$$\mu_{2n+1} \geq \frac{1}{I_n} \geq 4^n = 2^{2n}.$$

(d) Pour $n \in \mathbb{N}^*$*, on a :*

$$\mu_{2n+2} = \mu_{2n+1} \vee (2n+2) \geq 2^{2n}.$$

On a donc montré que $\mu_n \geq 2^{n-2}$ *pour tout* $n \geq 4$.

On peut en fait montrer que $\mu_n \geq 2^n$ *pour tout* $n \geq 7$.

23.6 L'algorithme d'Euclide.

Le lemme qui suit permet de déduire du théorème de division euclidienne un algorithme de calcul du pgcd de deux entiers positifs. C'est l'algorithme d'Euclide.

Cet algorithme permet également de déterminer des entiers u et v tels que $au + bv = a \wedge b$.

Théorème 23.11 *Soient* a, b *deux entiers naturels non nuls et* r *le reste dans la division euclidienne de* a *par* b*. On a alors* $a \wedge b = b \wedge r$.

Démonstration. Par division euclidienne, on a $a = bq + r$ avec $0 \leq r < b$. L'entier naturel $\delta = a \wedge b$ qui est un diviseur commun à a et b va diviser $r = a - bq$, c'est donc un diviseur commun à b et r et $\delta \leq \delta' = b \wedge r$.

L'entier naturel $\delta' = b \wedge r$ qui est un diviseur commun à b et r va diviser $a = bq + r$, c'est donc un diviseur commun à a et b et $\delta' \leq \delta$. On a donc bien $\delta = \delta'$. ∎

Le principe de l'algorithme d'Euclide est le suivant pour $a > b$ dans $\mathbb{N}^*$ (par symétrie, on peut supposer que $a \geq b$ et pour $a = b$, on a $a \wedge a = a$).

On note $r_0 = b$ et on désigne par r_1 le reste dans la division euclidienne de a par b.

On a alors $0 \leq r_1 < r_0$ et d'après le lemme précédent :

$$a \wedge b = r_0 \wedge r_1.$$

Si $r_1 = 0$ alors $r_0 \wedge r_1 = r_0 = b$ et c'est terminé.

Si $r_1 \neq 0$ on désigne alors par r_2 le reste dans la division euclidienne de r_0 par r_1 et on a $0 \leq r_2 < r_1$ et :

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2.$$

Si $r_2 = 0$ alors $r_1 \wedge r_2 = r_1$ et c'est terminé. Sinon on continu.

On définit donc ainsi une suite d'entiers $(r_n)_{n \geq 0}$ par :

- $r_0 = b$;
- r_1 est le reste dans la division euclidienne de a par b ; on a donc $0 \leq r_1 < b$;
- pour $n \geq 2$, si $r_{n-1} = 0$ alors $r_n = 0$ et sinon r_n est le reste dans la division euclidienne de r_{n-2} par r_{n-1} et on a $0 \leq r_n < r_{n-1}$. Dans tous les cas on $r_n \leq r_{n-1}$ l'égalité étant réalisée si et seulement si les deux termes sont nuls.

La suite $(r_n)_{n \geq -1}$ ainsi construite est donc une suite décroissante d'entiers positifs, elle est donc stationnaire à partir d'un certain rang. Précisément il existe un entier $p \geq 1$ tel que $r_p = 0 < r_{p-1} < \cdots < r_1 < r_0$ et :

$$a \wedge b = r_0 \wedge r_1 = \cdots = r_{p-1} \wedge r_p = r_{p-1}.$$

C'est à dire que $a \wedge b$ est le dernier reste non nul dans cette suite de divisions euclidiennes.

Par exemple pour calculer le pgcd de $a = 128$ et $b = 28$, on procède comme suit :

$$\begin{cases} a = 128 = 4 \cdot 28 + 16 = q_1 r_0 + r_1 \\ r_0 = 28 = 1 \cdot 16 + 12 = q_2 r_1 + r_2 \\ r_1 = 16 = 1 \cdot 12 + 4 = q_3 r_2 + r_3 \\ r_2 = 12 = 3 \cdot 4 + 0 = q_4 r_3 + r_4 \\ r_4 = 0,\ r_3 = 4 = 128 \wedge 28 \end{cases} \tag{23.4}$$

On peut utiliser un tableau pour effectuer la suite des calculs. Sur la deuxième ligne, on place d'abord a et b, puis sur la première ligne on place au dessus de b le quotient q_1 et sur la troisième ligne, on place au dessous de a le reste r_1, ce même reste r_1 étant aussi placé en deuxième ligne après b. On recommence alors avec le couple (b, r_1). Sur la première ligne apparaissent les quotients successifs sur la troisième les restes successifs. Le dernier reste non nul, qui apparaît en fin de deuxième ligne, donne alors le pgcd.

	q_1	q_2	q_3	q_4		4	1	1	3
a	b	r_1	r_2	$\mathbf{r}_3$	128	28	16	12	**4**
r_1	r_2	r_3	$r_4 = 0$		16	12	4	$r_4 = 0$	

On a donc construit, avec l'algorithme d'Euclide, deux suites d'entiers $(r_n)_{0 \leq n \leq p}$ et $(q_n)_{1 \leq n \leq p}$ de la manière suivante :

$$\begin{cases} a = q_1 r_0 + r_1 \ \ (0 < r_1 < r_0 = b) \\ r_0 = q_2 r_1 + r_2 \ \ (0 < r_2 < r_1) \\ r_1 = q_3 r_2 + r_3 \ \ (0 < r_3 < r_2) \\ \vdots \\ r_{p-3} = q_{p-1} r_{p-2} + r_{p-1} \ \ (0 < r_{p-1} < r_{p-2}) \\ r_{p-2} = q_p r_{p-1} + r_p \ \ (r_p = 0) \end{cases}$$

On vérifie alors, par récurrence finie sur $n \in \{0, 1, \cdots, p-1\}$, qu'il existe des entiers u_n et v_n tels que $r_n = a u_n + b v_n$.

Pour $n = 0$ et $n = 1$ on a :

$$\begin{aligned} r_0 &= b = a \cdot 0 + b \cdot 1, \\ r_1 &= a \cdot 1 + b\,(-q_1)\,. \end{aligned}$$

En supposant le résultat acquis jusqu'à l'ordre $n-1$ pour $0 \leq n-1 \leq p-2$ on a :

$$\begin{aligned} r_n &= -q_n r_{n-1} + r_{n-2} \\ &= -q_n\,(a u_{n-1} + b v_{n-1}) + a u_{n-2} + b v_{n-2} \\ &= a\,(u_{n-2} - q_n u_{n-1}) + b\,(v_{n-2} - q_n v_{n-1}) = a u_n + b v_n. \end{aligned}$$

En particulier pour $n = p-1$ on a $a \wedge b = r_{p-1} = a u_{p-1} + b v_{p-1} = au + bv$.

Un tel couple d'entiers (u, v) n'est pas unique puisque si (u, v) est une solution, pour tout entier λ, le couple $(u', v') = (u + \lambda v, v - \lambda a)$ est aussi solution. On a en effet :

$$a\,(u + \lambda b) + b\,(v - \lambda a) = au + bv = a \wedge b.$$

Une équation dans $\mathbb{Z}$ de la forme $au + bv = \delta$, où a, b, δ sont donnés et u, v sont les inconnues est une équation diophantienne. Ce type d'équation est étudié plus en détails au paragraphe suivant.

Les suites $(r_n)_{0\leq n\leq p-1}$ $(u_n)_{0\leq n\leq p-1}$ et $(v_n)_{0\leq n\leq p-1}$ vérifient la même relation de récurrence :

$$x_n = x_{n-2} - q_n x_{n-1} \ (2 \leq n \leq p-1)$$

avec les conditions initiales :

$$(r_0, r_1) = (b, 1)\,,\ (u_0, u_1) = (0, 1)\,,\ (v_0, v_1) = (1, -q_1)$$

où q_1, r_1 sont, respectivement, le quotient et le reste dans la division euclidienne de a par b.

On peut donner une interprétation matricielle de ces calculs comme suit. On a :

$$\begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} -q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \end{pmatrix} \ (2 \leq n \leq p-1)$$

et :

$$\begin{aligned} \begin{pmatrix} x_{p-1} \\ x_{p-2} \end{pmatrix} &= \begin{pmatrix} -q_{p-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -q_{p-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_0 \end{pmatrix} \\ &= A_{p-1} \begin{pmatrix} x_1 \\ x_0 \end{pmatrix}. \end{aligned}$$

Pour l'exemple précédent, la suite de calculs (23.4) donne :

$$p - 1 = 3,\ (q_1, q_2, q_3) = (4, 1, 1)$$

et :

$$\begin{aligned} A_3 &= \begin{pmatrix} -q_3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \end{aligned}$$

d'où :

$$\begin{pmatrix} u_3 \\ u_2 \end{pmatrix} = A_3 \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix},$$
$$\begin{pmatrix} v_3 \\ v_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -q_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -4 \\ 1 \end{pmatrix} = \begin{pmatrix} -9 \\ 5 \end{pmatrix}$$

soit $(u, v) = (u_3, v_3) = (2, -9)$.

Si on veut se passer du calcul matriciel, on peut procéder comme suit. Les divisions successives :

$$\begin{cases} a = q_1 r_0 + r_1 \\ r_0 = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ r_2 = q_4 r_3 \end{cases}$$

donne :

$$\begin{aligned} a \wedge b = r_3 &= r_1 - q_3 r_2 = r_1 - q_3 (r_0 - q_2 r_1) \\ &= r_1 (1 + q_3 q_2) - q_3 r_0 = (a - q_1 r_0)(1 + q_3 q_2) - q_3 r_0 \\ &= (a - q_1 b)(1 + q_3 q_2) - q_3 b = au + bv \end{aligned}$$

(on commence par la fin), soit pour les valeurs particulières 128 et 28 :

$$\begin{cases} 128 = 4 \cdot 28 + 16 \\ 28 = 1 \cdot 16 + 12 \\ 16 = 1 \cdot 12 + 4 \\ 12 = 3 \cdot 4 \end{cases}$$

qui donne :

$$\begin{aligned} 128 \wedge 28 = 4 &= 16 - 12 = 16 - (28 - 16) = 2 \cdot 16 - 28 \\ &= 2\,(128 - 4 \cdot 28) - 28 \\ &= 2 \cdot 128 - 9 \cdot 28 = ua + vb \end{aligned}$$

23.7 Equations diophantiennes $ax + by = c$

Soient a, b, c trois entiers relatifs, avec a et b non nuls. On s'intéresse ici à l'équation diophantienne dans $\mathbb{Z}^2$:

$$ax + by = c. \tag{23.5}$$

En notant δ le pgcd de a et b, on a $a = \delta a'$, $b = \delta b'$ avec a' et b' premiers entre eux.

Lemme 23.2 *L'équation diophantienne* (23.5) *a des solutions entières si, et seulement si, δ divise c.*

Démonstration. Si c n'est pas un multiple de δ, comme δ divise $ax + by$ pour tous entiers x, y, l'équation (23.5) n'a pas de solutions.

Si $c = \delta c'$ est un multiple de δ, en écrivant que $\delta = au_0 + bv_0$ avec u_0, v_0 dans $\mathbb{Z}$ (théorème de Bézout) on déduit que $(x_0, y_0) = (u_0 c', v_0 c')$ est une solution de (23.5) . ■

Théorème 23.12 *Si c est multiple de δ, alors l'ensemble des solutions de* (23.5) *est :*

$$S = \{(x_0 - kb', y_0 + ka') \mid k \in \mathbb{Z}\}$$

où (x_0, y_0) est une solution particulière.

Démonstration. Si (x, y) est une solution de (23.5) , on a alors :

$$\begin{cases} ax_0 + by_0 = c, \\ ax + by = c, \end{cases}$$

ce qui donne par soustraction :

$$a\,(x_0 - x) = b\,(y - y_0)$$

et divisant par δ, on obtient :

$$a'\,(x_0 - x) = b'\,(y - y_0)\,.$$

Avec le théorème de Gauss on en déduit alors que a' divise $y - y_0$. On a donc $y - y_0 = ka'$ avec $k \in \mathbb{Z}$, ce qui entraîne $a'\,(x_0 - x) = b'ka'$ et $x_0 - x = kb'$. En définitive on a :

$$(x, y) = (x_0 - kb', y_0 + ka')$$

avec $k \in \mathbb{Z}$. Réciproquement on vérifie que pour tout $k \in \mathbb{Z}$, $(x_0 - kb', y_0 + ka')$ est bien solution de (23.5) . En effet on a :

$$ax + by = ax_0 + by_0 + k\left(a'b - ab'\right) = c + k\delta\left(a'b' - a'b'\right) = c.$$

■

L'algorithme d'Euclide vu au paragraphe précédent nous permet d'obtenir une solution particulière $(x_0, y_0) = \left(u_0\frac{c}{\delta}, v_0\frac{c}{\delta}\right)$.

Exemple 23.1 *Soit à résoudre l'équation :*

$$370x + 45y = 15.$$

Le pgcd *de* 370 *et* 45 *est égal à* 5 *qui divise* 15.
On cherche tout d'abord une solution particulière de $74x + 9y = 1$. *En utilisant l'algorithme d'Euclide, on a :*

$$\begin{aligned} 74 &= 8 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

et donc :

$$\begin{aligned} 1 = 9 - 4 \cdot 2 &= 9 - 4 \cdot (74 - 8 \cdot 9) \\ &= 74 \cdot (-4) + 9 \cdot 33 \end{aligned}$$

Le couple $(-12, 99)$ *est solution de* $74x + 9y = 3$ *et de* $370x + 45y = 15$.

D'un point de vue géométrique l'ensemble des solutions de (23.5) est formé de la suite de points de $\mathbb{Z}^2$ définie par :

$$\begin{cases} M_0 = \begin{pmatrix} x_0 \\ x_0 \end{pmatrix}, \\ M_k = M_0 + k \begin{pmatrix} -b' \\ a' \end{pmatrix}, \ k \in \mathbb{Z}. \end{cases}$$

Les points M_k sont sur la droite passant par M_0 et dirigée par le vecteur $\overrightarrow{v'} = \begin{pmatrix} -b' \\ a' \end{pmatrix}$ ou encore par le vecteur colinéaire $\overrightarrow{v} = \begin{pmatrix} -b \\ a \end{pmatrix}$. Ces vecteurs sont orthogonaux au vecteur $\overrightarrow{u} = \begin{pmatrix} a \\ b \end{pmatrix}$.

Exercice 23.29 *Résoudre dans* $\mathbb{Z}^2$ *l'équation diophantienne :*

$$128x + 28y = 8.$$

Solution 23.29 *En notant* $(a, b) = (128, 28)$, $c = 8$ *et* $\delta = a \wedge b$, *on a vu au paragraphe précédent que :*

$$\delta = 4 = 2 \cdot 128 - 9 \cdot 28 = au_0 + bv_0$$

et $(x_0, y_0) = \left(u_0\frac{c}{\delta}, v_0\frac{c}{\delta}\right) = (4, -18)$ *est une solution particulière de notre équations. Toutes les solutions étant données par :*

$$(x, y) = (x_0 - kb', y_0 + ka') = (4 - 7k, -18 + 32k)$$

où k *décrit* $\mathbb{Z}$.

23.8 Equations $ax \equiv b\ (n)$

Soient n un entier supérieur ou égal à 2, a un entier supérieur ou égal à 1 et b un entier relatif. On veut résoudre dans $\mathbb{Z}$ l'équation diophantienne :

$$ax \equiv b\ (n) \tag{23.6}$$

On s'intéresse tout d'abord au cas où $b = 1$.

Lemme 23.3 *Soient n un entier supérieur ou égal à 2, a un entier supérieur ou égal à 1. L'équation*

$$ax \equiv 1\ (n) \tag{23.7}$$

a des solutions dans $\mathbb{Z}$ si et seulement si a est premier avec n.

Démonstration. Le théorème de Bézout nous dit que a est premier avec n si, et seulement si, il existe des entiers relatifs x et k tels que $ax - kn = 1$, ce qui équivaut à dire que $x \in \mathbb{Z}$ est solution de (23.7). ■

Si a et n sont premiers entre eux alors l'algorithme d'Euclide nous permet de trouver une solution $x_0 \in \mathbb{Z}$ de (23.7). Et pour tout autre solution $x \in \mathbb{Z}$ l'entier $a(x - x_0)$ est divisible par n. Comme n est premier avec a, le théorème de Gauss nous dit que nécessairement n divise $x - x_0$. Il est clair que réciproquement pour tout $k \in \mathbb{Z}$, $x_0 + kn$ est solution de (23.7). En définitive, l'ensemble des solutions de (23.7) est :

$$S = \{x_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.7).

Remarque 23.10 *Si a et n sont premiers entre eux alors il existe une unique solution de* (23.7) *dans $\{1, \cdots, n-1\}$. En effet, si S est l'ensemble des solutions de* (23.7) *alors $S \cap \mathbb{N}^*$ est non vide et donc admet un plus petit élément $x > 0$. Si $x \geq n$ on a alors $x = qn + r$ avec $q \geq 1$ et $0 \leq r < n$. Comme $ar \equiv ax \equiv 1$ modulo n, on a $r \in S \cap \mathbb{N}$ et nécessairement $r = 0$. Mais $x = qn$ entraîne $ax \equiv 0$ modulo n en contradiction avec $x \in S$. On a donc $x < n$.*

On s'intéresse maintenant au cas où les entiers a et n sont premiers entre eux et b est un entier relatif. Dans ce cas on peut trouver une solution x_0 de l'équation (23.7) et pour tout entier relatif k, $x = bx_0 + kn$ est solution de (23.6). Réciproquement si x est solution de (23.6) alors $a(x - bx_0)$ est divisible par n avec n premier avec a. Le théorème de Gauss nous dit alors que $x - bx_0$ est divisible par n. En définitive, pour a et n premiers entre eux, l'ensemble des solutions de (23.6) est :

$$S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.7).

Considérons maintenant le cas où $\delta = a \wedge n$ n'est pas nécessairement égal à 1 et b est un entier relatif.

On a alors $a = \delta a'$, $n = \delta n'$ et si l'équation (23.6) admet une solution $x \in \mathbb{Z}$ alors $\delta n'$ divise $\delta a' - b$, donc δ divise $\delta a' - b$ et δ divise b. En conclusion si b n'est pas un multiple de δ alors l'équation (23.6) n'a pas de solution dans $\mathbb{Z}$.

On suppose donc que b est un multiple de δ, soit $b = \delta b'$. Si $x \in \mathbb{Z}$ est solution de (23.6) alors x est solution de :

$$a'x \equiv b'\ (n')$$

avec a' et n' premiers entre eux. On sait alors que x est de la forme $x = b'x'_0 + kn'$ où x'_0 est une solution de $a'x \equiv 1$ modulo n' et k est un entier relatif. Réciproquement on peut vérifier que pour tout entier $k \in \mathbb{Z}$, $x = b'x'_0 + kn'$ est solution de (23.6) . En effet on a :

$$\begin{aligned} ax &= a'x'_0\delta b' + a'k\delta n' = (1 + k'n')\,\delta b' + a'kn \\ &= b + n\,(k'b' + ka') \equiv b \ (n)\,. \end{aligned}$$

En définitive, si $b = \delta b'$ où $\delta = a \wedge n$, alors l'ensemble des solutions de (23.6) est :

$$S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$$

où x'_0 est une solution particulière de $a'x \equiv 1$ modulo n', où $a = \delta a'$, $n = \delta n'$.

23.9 Le théorème Chinois

On s'intéresse ici aux système d'équations diophantiennes :

$$\begin{cases} x \equiv a \ (n) \\ x \equiv b \ (m) \end{cases} \tag{23.8}$$

où n, m sont deux entiers naturels supérieur ou égal à 2.

Théorème 23.13 (chinois) *Soient n, m deux entier supérieur ou égal à 2 premiers entre eux. Quels que soient les entiers relatifs a et b le système* (23.8) *a une infinité de solutions dans $\mathbb{Z}$.*

Démonstration. Comme n et m sont premiers entre eux on peut trouver une infinité de couples d'entiers relatifs (u, v) tels que :

$$nu + mv = 1.$$

En posant $x = bnu + amv$ on obtient une infinité de solutions de (23.8) . ∎

Dans le cas où n et m sont premiers entre eux on vient de voir que si (u_0, v_0) est solution de $nu + mv = 1$ (un tel couple peut être obtenu par l'algorithme d'Euclide) alors $x_0 = bnu_0 + amv_0$ est une solution particulière de (23.8) .

Si $x \in \mathbb{Z}$ est solution de (23.8) alors x est congru à x_0 modulo n et modulo m, soit :

$$x - x_0 = pn = qm.$$

Mais m est premier avec n, le théorème de Gauss nous dit alors que m divise p. On a donc $x = x_0 + knm$ avec $k \in \mathbb{Z}$. Et réciproquement on vérifie que pour tout entier relatif k, $x_0 + knm$ est solution de (23.8) . En définitive, si n et m sont premiers entre eux, alors l'ensemble des solutions de (23.8) est :

$$S = \{x_0 + knm \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.8) .

Dans le cas général où m et n ne sont pas nécessairement premiers entre eux on note $\delta = m \wedge n$, $n = \delta n'$, $m = \delta m'$ avec n', m' premiers entre eux et $\mu = m \vee n$.

Si $x \in \mathbb{Z}$ est une solution de (23.8) alors δ qui divise n et m va diviser $x - a$ et $x - b$, il divise donc $a - b$. Donc si $a - b$ n'est pas un multiple de $\delta = m \wedge n$ le système d'équations (23.8) n'a pas de solutions.

On suppose donc que $a-b$ est multiple de δ, c'est-à-dire que $b-a=\delta c'$. Les entiers n' et m' étant premiers entre eux, le théorème de Bézout nous dit qu'il existe des entiers u_0 et v_0 tels que $n'u_0+m'v_0=1$. En posant :

$$x_0=bn'u_0+am'v_0$$

on a :

$$\begin{aligned}x_0&=b\,(1-m'v_0)+am'v_0=b-m'v_0\,(b-a)\\&=b-m'v_0\delta c'=b-mv_0c'\equiv b\ \ (m)\,.\end{aligned}$$

Et de manière analogue on voit que x_0 est congru à a modulo n. L'entier x_0 est donc solution de (23.8) .

Si $x\in\mathbb{Z}$ est solution de (23.8) alors x est congru à x_0 modulo n et modulo m, soit :

$$x-x_0=pn=qm=p\delta n'=q\delta m'.$$

On déduit donc que $\dfrac{x-x_0}{\delta}$ est un entier et :

$$\frac{x-x_0}{\delta}=pn'=qm'.$$

Mais m' est premier avec n', le théorème de Gauss nous dit alors que m' divise p. On a donc :

$$\frac{x-x_0}{\delta}=kn'm'$$

avec $k\in\mathbb{Z}$. Ce qui peut aussi s'écrire :

$$x-x_0=knm'=k\frac{nm}{\delta}=k\mu$$

avec $k\in\mathbb{Z}$.

Et réciproquement on vérifie facilement que pour tout entier relatif k, $x_0+k\mu$ est solution de (23.8) . En définitive, l'ensemble des solutions de (23.8) est :

$$S=\{x_0+k\,(m\vee n)\mid k\in\mathbb{Z}\}$$

où x_0 est une solution particulière de (23.8) .

23.10 Nombres premiers entre eux. Les théorèmes de Bézout et de Gauss

On a vu que, par définition du pgcd, on a $a\wedge b=au+bv$ avec u,v entiers relatifs, mais en général la réciproque est fausse, c'est-à-dire que si δ est entier naturel tel que $\delta=au+bv$ avec u,v entiers relatifs, il n'y a aucune raison pour que δ soit le pgcd de a et b. Par exemple $2=3\cdot2+2\cdot(-2)$ et $3\wedge2=1$. Mais pour $\delta=1$, cette réciproque est vrai et ce résultat est très souvent utilisé.

Définition 23.9 *Soient* $(a,b)\in\mathbb{Z}^2-\{(0,0)\}$. *On dit que* a *et* b *sont premiers entre eux (ou étrangers) si leur* pgcd *est égal à* 1.

De manière équivalente, on peut dire que a et b sont premiers entre eux si, et seulement si, -1 et 1 sont leurs seuls diviseurs communs, ce qui est encore équivalent à dire que $\mathcal{D}_a \cap \mathcal{D}_b = \{-1, 1\}$ ou encore que le dernier reste non nul dans l'algorithme d'Euclide vaut 1.

Exercice 23.30 *Soient $(a_k)_{1\leq k\leq p}$ et $(b_k)_{1\leq k\leq q}$ deux suites finies d'entiers relatifs non nuls. Montrer que si $n = \prod_{k=1}^{p} a_k$ et $m = \prod_{k=1}^{q} b_k$ sont premiers entre eux, alors chaque a_k, pour k compris entre 1 et p, est premier avec chacun des b_j, pour j compris entre 1 et q.*

Solution 23.30 *Soit $\delta = a_k \wedge b_j$ où $1 \leq k \leq p$ et $1 \leq j \leq q$. Comme δ est un entier naturel non nul qui divise a_k et b_j, il divise n et m et vaut nécessairement* 1.

De manière plus générale, on peut donner la définition suivante.

Définition 23.10 *Soient $a_1, \cdots, a_p$ des entiers relatifs non tous nuls. On dit que $a_1, \cdots, a_p$ sont premiers entre eux dans leur ensemble si leur* pgcd *est égal à* 1.

Exercice 23.31 *Est-il équivalent de dire $a_1, \cdots, a_p$ sont premiers entre eux dans leur ensemble et $a_1, \cdots, a_p$ sont deux à deux premiers entre eux ?*

Solution 23.31 *On vérifie immédiatement que la réponse est négative en considérant le triplet* $(2, 3, 8)$.

Théorème 23.14 *Soient $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$ et $\delta = a \wedge b$. Il existe deux entiers p et q premiers entre eux tels que $a = \delta p$ et $b = \delta q$.*

Démonstration. Comme δ divise a et b il existe deux entiers p et q tels que $a = \delta p$ et $b = \delta q$. Le pgcd $\delta' = p \wedge q$ est un diviseur de p et q, donc l'entier naturel $\delta\delta'$ divise $a = \delta p$ et $b = \delta q$ et nécessairement $\delta\delta' \leq \delta$, soit $\delta(1 - \delta') \geq 0$ avec $\delta > 0$. On a donc $\delta' \leq 1$. Mais δ' est supérieur ou égal à 1 comme tout pgcd qui se respecte. En définitive, on a $\delta' = 1$, c'est-à-dire que p et q sont premiers entre eux. ∎

De manière plus générale, on a le résultat suivant.

Théorème 23.15 *Soient $a_1, \cdots, a_p$ des entiers relatifs non tous nuls. et $\delta = a_1 \wedge a_2 \wedge \cdots \wedge a_p$. Il existe des entiers $a'_1, \cdots, a'_p$ premiers entre eux dans leur ensemble tels que $a_k = \delta a'_k$ pour tout k compris entre 1 et p.*

Démonstration. Analogue au cas où $p = 2$. ∎

Exercice 23.32 *Déterminer tous les couples (a, b) d'entiers naturels non nuls tels que $a \wedge b = 3$ et $a + b = 12$.*

Solution 23.32 *On a $a = 3p$, et $b = 3q$ où p, q sont des entiers naturels non nuls premiers entre eux et $a + b = 12$ équivaut à $p + q = 4$.*
Réciproquement si $a = 3p$, $b = 3q$ où p, q sont des entiers naturels non nuls premiers entre eux tels que $p + q = 4$, alors $a \wedge b = 3$ et $a + b = 12$.
Les seuls couples (p, q) possibles sont $(1, 3)$ et $(3, 1)$. Donc $(a, b) = (3, 9)$ ou $(a, b) = (9, 3)$.

Exercice 23.33 *Soient a, n deux entiers naturels non nuls. Montrer que :*

$$\frac{(a+1)^n - 1}{a} \wedge a = a \wedge n.$$

Solution 23.33 *On remarque d'abord que :*

$$(a+1)^n - 1 = a\sum_{k=0}^{n-1}(a+1)^k$$

est divisible par a, donc $\dfrac{(a+1)^n-1}{a}$ est un entier.
Soit $\delta = \dfrac{(a+1)^n-1}{a} \wedge a$. Pour tout $k \geq 0$, on a :

$$(a+1)^k \equiv 1 \pmod{a}$$

(pour $k = 0$, c'est clair et pour $k \geq 1$, on utilise la formule du binôme) et donc :

$$b = \frac{(a+1)^n-1}{a} = \sum_{k=0}^{n-1}(a+1)^k \equiv n \pmod{a}$$

de sorte que δ qui divise a et b divise aussi $n = b - pa$ ($p \in \mathbb{Z}$). Il en résulte que δ divise $\delta' = a \wedge n$. Comme δ' divise a et n, il divise aussi $b = n + pa$ et en conséquence δ' divise δ. On a donc bien $\delta = \delta'$.

Exercice 23.34 *On se donne un entier naturel $a \geq 2$ et on définit la suite $(u_n)_{n\in\mathbb{N}}$ par :*

$$\forall n \in \mathbb{N},\ u_n = a^{2^n} + 1.$$

1. Montrer que :
$$\forall n \in \mathbb{N},\ u_{n+1} = (u_n - 1)^2 + 1.$$
2. Montrer que :
$$\forall n \in \mathbb{N},\ u_{n+1} = (a-1)\prod_{k=0}^{n} u_k + 2.$$
3. Montrer que, pour $n \neq m$ dans $\mathbb{N}$, on a :
$$u_n \wedge u_m = \begin{cases} 1 \text{ si } a \text{ est pair} \\ 2 \text{ si } a \text{ est impair} \end{cases}$$
4. Calculer $u_n^p \wedge u_m^p$ pour $n \neq m$ dans $\mathbb{N}$ et p dans $\mathbb{N}^*$.

Solution 23.34

1. On a :
$$u_{n+1} = a^{2^{n+1}} + 1 = \left(a^{2^n}\right)^2 + 1 = (u_n - 1)^2 + 1.$$
2. On procède par récurrence sur $n \geq 0$.
Pour $n = 0$, on a :
$$\begin{aligned} u_1 = a^2 + 1 &= \left(a^2 - 1\right) + 2 \\ &= (a-1)\,u_0 + 2. \end{aligned}$$
En supposant le résultat acquis pour $n - 1 \geq 0$, on a :
$$u_{n+1} = u_n\,(u_n - 2) + 2 = u_n\,(a-1)\prod_{k=0}^{n-1} u_k + 2 = (a-1)\prod_{k=0}^{n} u_k + 2.$$

3. Supposons que $m > n$.
   On a :
$$u_m = (a-1)\prod_{k=0}^{m-1} u_k + 2 = (a-1)\,u_n \prod_{\substack{k=0\\k\neq n}}^{m-1} u_k + 2$$
$$= qu_n + 2$$
   Le pgcd de u_n et u_m divise alors 2 et il vaut 2 ou 1.
   Si a est pair, alors u_n est impair et $\delta = 1$ puisqu'il divise u_n, ce qui signifie que u_n et u_n sont premiers entre eux (pour $a = 2$, c'est le cas des nombres de Fermat).
   Si a est impair, alors tous les u_n sont pairs et δ vaut 2.
4. En utilisant le résultat de l'exercice 24.6, on a :
$$u_n^p \wedge u_m^p = (u_n \wedge u_m)^p = \begin{cases} 1 \text{ si } a \text{ est pair} \\ 2^p \text{ si } a \text{ est impair} \end{cases}$$

Théorème 23.16 (Bézout) *Deux entiers relatifs a et b non tous deux nuls sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.*

Démonstration. On sait déjà, par définition, que la condition est nécessaire.
Réciproquement s'il existe deux entiers relatifs u et v tels que $au + bv = 1$ alors $\delta = a \wedge b$ est un entier naturel qui divise a et b, il divise donc $1 = au + bv$ et $\delta = 1$, c'est-à-dire que a et b sont premiers entre eux. ■

Remarque 23.11 *La relation de Bézout $au + bv = 1$ implique que u et v sont aussi premiers entre eux. On a aussi $|a| \wedge |b| = |a| \wedge b = a \wedge |b| = a \wedge b = 1$.*

Ce théorème peut se généraliser comme suit.

Théorème 23.17 (Bézout) *Des entiers relatifs $a_1, a_2, \cdots, a_p$ non tous nuls sont premiers entre eux dans leur ensemble si et seulement si il existe deux entiers relatifs $u_1, u_2, \cdots, u_p$ tels que $\displaystyle\sum_{k=1}^{p} u_k a_k = 1$.*

Démonstration. On sait déjà, par définition, que la condition est nécessaire.
Réciproquement s'il existe deux entiers relatifs $u_1, u_2, \cdots, u_p$ tels que $\displaystyle\sum_{k=1}^{p} u_k a_k = 1$ alors $\delta = a_1 \wedge a_2 \wedge \cdots \wedge a_p$ est un entier naturel qui divise tous les a_k, il divise donc $1 = \displaystyle\sum_{k=1}^{p} u_k a_k$ et $\delta = 1$, c'est-à-dire que $a_1, a_2, \cdots, a_p$ sont premiers entre eux dans leur ensemble. ■

Corollaire 23.2 *Soient a, b, c des entiers relatifs non nuls. Si c est premier avec a alors $a \wedge b = a \wedge (bc)$ (le* pgcd *de deux entiers est inchangé si on multiplie l'un d'eux par un nombre premier avec l'autre).*

Démonstration. Soient $\delta = a \wedge b$ et $\delta' = a \wedge (bc)$. Comme δ divise a et b, il divise a et bc ainsi que leur pgcd δ'. De $au + cv = 1$, on déduit que $abu + bcv = b$ et δ' qui divise a et bc va diviser a et b ainsi que leur pgcd δ. On a donc $\delta = \delta'$. ■

Corollaire 23.3 *Soient $a_1, a_2, \cdots, a_p$ et c des entiers relatifs non nuls. Si c est premier avec chacun des a_k, pour k compris entre 1 et p, il est alors premier avec leur produit $\prod_{k=1}^{p} a_k$.*

Démonstration. En utilisant le corollaire précédent, on a :

$$c \wedge \prod_{k=1}^{p} a_k = c \wedge \left(a_1 \prod_{k=2}^{p} a_k \right) = c \wedge \prod_{k=2}^{p} a_k$$

puisque a_1 est premier avec c et par récurrence finie, on déduit que :

$$c \wedge \prod_{k=1}^{p} a_k = c \wedge \prod_{k=2}^{p} a_k = c \wedge \prod_{k=3}^{p} a_k = \cdots = c \wedge a_p = 1$$

puisque chaque a_k, pour k compris entre 1 et p, est premier avec c. ■

Une conséquence importante du théorème de Bézout est le résultat suivant.

Théorème 23.18 (Gauss) *Soient a, b, c des entiers relatifs non nuls. Si a divise bc et a est premier avec b alors a divise c.*

Démonstration. Comme a et b sont premiers entre eux, il existe deux entiers u, v tels que $au + bv = 1$ et pour tout entier c, on a $acu + bcv = c$, de sorte que si a divise bc, il va diviser $c = acu + bcv$. ■

Ce résultat peut être utilisé pour donner une unique représentation des nombres rationnels non nuls.

Corollaire 23.4 *Tout nombre rationnel non nul r s'écrit de manière unique $r = \dfrac{p}{q}$ avec $p \in \mathbb{Z}^*$ et $q \in \mathbb{N}^*$ premiers entre eux.*

Démonstration. Un nombre rationnel non nul r s'écrit $r = \dfrac{a}{b}$ avec (a, b) dans $\mathbb{Z}^* \times \mathbb{N}^*$. En notant $\delta = a \wedge b$ on a $a = \delta p$, $b = \delta q$ et $r = \dfrac{p}{q}$ avec p et q premiers entre eux. Si $r = \dfrac{p}{q} = \dfrac{p'}{q'}$ avec (p, q) , (p', q') dans $\mathbb{Z}^* \times \mathbb{N}^*$ tels que $p \wedge q = p' \wedge q' = 1$, on a alors $pq' = p'q$ avec q premier avec p et q qui divise pq', donc q divise q' d'après le théorème de Gauss. De manière analogue, on voit que q' divise q. On a donc $q = q'$ (q, q' sont des entiers naturels non nuls) et $p = p'$. L'écriture est donc unique. ■

Corollaire 23.5 *Si un entier relatif non nul n est divisible par des entiers $a_1, a_2, \cdots, a_p$ deux à deux premiers entre eux, il est alors divisible par leur produit.*

Démonstration. On procède par récurrence sur $p \geq 2$.

Supposons que n soit divisible par a_1 et a_2 premiers entre eux. On a alors $n = a_1 q_1$ et a_2 divise n en étant premier avec a_2, il va donc diviser q_1 (théorème de Gauss), c'est-à-dire que $q_1 = q_2 a_2$ et $n = a_1 a_2 q_2$ est divisible par $a_1 a_2$.

En supposons le résultat acquis au rang $p-1 \geq 2$, soient $a_1, a_2, \cdots, a_p$ deux à deux premiers entre eux qui divisent n. L'hypothèse de récurrence nous dit que n est divisible par $a = \prod_{k=1}^{p-1} a_k$. Comme a_p est premier avec chacun des a_k, pour k compris entre 1 et $p-1$, il est premier avec leur produit a (corollaire 23.3) et n qui est divisible par a et a_p est aussi divisible par leur produit $\prod_{k=1}^{p} a_k$. ■

Exercice 23.35

1. *Montrer que pour tout entier naturel n, il existe deux entiers p_n et q_n premiers entre eux tels que :*
$$\left(\sqrt{2}+1\right)^n = p_n + q_n\sqrt{2}.$$
2. *En utilisant l'application φ définie sur l'anneau $\mathbb{Z}\left[\sqrt{2}\right]$ par $\varphi\left(a+b\sqrt{2}\right) = a - b\sqrt{2}$ pour tout $(a,b) \in \mathbb{Z}^2$, montrer que, pour tout $n \in \mathbb{N}$, on a :*
$$\left(\sqrt{2}-1\right)^n = (-1)^n\left(p_n - q_n\sqrt{2}\right).$$
3. *En déduire que, pour tout $n \in \mathbb{N}$, il existe un entier naturel r_n tel que :*
$$\begin{cases} \left(\sqrt{2}+1\right)^n = \sqrt{r_n} + \sqrt{r_n - 1} \\ \left(\sqrt{2}-1\right)^n = \sqrt{r_n} - \sqrt{r_n - 1} \end{cases}.$$

Solution 23.35

1. *Le réel $\theta = \sqrt{2}+1$ est dans l'anneau $\mathbb{Z}\left[\sqrt{2}\right]$, il en est donc de même de θ^n pour tout $n \in \mathbb{N}$, ce qui prouve l'existence des suites d'entiers $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$.*
On peut aussi retrouver ce résultat par récurrence en écrivant que pour tout $n \in \mathbb{N}$, on a :
$$\theta^{n+1} = \left(\sqrt{2}+1\right)\left(p_n + q_n\sqrt{2}\right) = (p_n + 2q_n) + (p_n + q_n)\sqrt{2}$$
ce qui donne :
$$\begin{cases} p_{n+1} = p_n + 2q_n \\ q_{n+1} = p_n + q_n \end{cases}$$
et montre en outre que les p_n et q_n sont des entiers naturels non nuls sauf $q_0 = 0$.
On a alors :
$$p_{n+1} \wedge q_{n+1} = (p_n + 2q_n) \wedge (p_n + q_n).$$
En utilisant la relation $a \wedge b = a \wedge (a+b) = b \wedge (a+b)$ (exercice 23.21), on a :
$$\begin{aligned} p_n \wedge q_n &= q_n \wedge (p_n + q_n) = (q_n + p_n) \wedge q_n \\ &= (q_n + p_n) \wedge (p_n + q_n + q_n) = p_{n+1} \wedge q_{n+1}. \end{aligned}$$
On a donc, pour tout $n \in \mathbb{N}$:
$$p_n \wedge q_n = p_0 \wedge q_0 = 1 \wedge 0 = 1.$$
2. *L'application φ réalise un automorphisme de l'anneau $A = \mathbb{Z}\left[\sqrt{2}\right]$. En effet, pour tous $x = a + b\sqrt{2}$ et $x' = a' + b'\sqrt{2}$ dans A, on a :*
$$\begin{cases} \varphi(x + x') = (a + a') - (b + b')\sqrt{2} = \varphi(x) + \varphi(x') \\ \varphi(xx') = (aa' + 2bb') - (ab' + a'b)\sqrt{2} = \varphi(x)\,\varphi(x') \end{cases}$$
et $x = a + b\sqrt{2}$ a pour unique antécédent $a - b\sqrt{2}$ par φ.
On a donc, pour tout $n \in \mathbb{N}$:
$$\begin{aligned} \left(\sqrt{2}-1\right)^n &= (-1)^n\left(1-\sqrt{2}\right)^n = (-1)^n\left(\varphi\left(\sqrt{2}+1\right)\right)^n \\ &= (-1)^n\,\varphi\left(\left(\sqrt{2}+1\right)^n\right) = (-1)^n\,\varphi\left(p_n + q_n\sqrt{2}\right) \\ &= (-1)^n\left(p_n - q_n\sqrt{2}\right) \end{aligned}$$

3. Pour tout $n \in \mathbb{N}$, on a $\left(\sqrt{2}+1\right)^n \left(\sqrt{2}-1\right)^n = 1$, soit :

$$(-1)^n \left(p_n + q_n\sqrt{2}\right)\left(p_n - q_n\sqrt{2}\right) = 1$$

ou encore :

$$p_n^2 - 2q_n^2 = (-1)^n$$

(c'est une relation de Bézout pour p_n et q_n qui sont premiers entre eux) et :

$$\begin{cases} \left(\sqrt{2}+1\right)^n = p_n + q_n\sqrt{2} = p_n + \sqrt{p_n^2 - (-1)^n} \\ \left(\sqrt{2}-1\right)^n = (-1)^n\left(p_n - q_n\sqrt{2}\right) = (-1)^n\left(p_n - \sqrt{p_n^2 - (-1)^n}\right) \end{cases}$$

En posant $s_n = p_n^2$, on a :

$$\begin{cases} \left(\sqrt{2}+1\right)^n = \sqrt{s_n} + \sqrt{s_n - (-1)^n} \\ \left(\sqrt{2}-1\right)^n = (-1)^n\left(\sqrt{s_n} - \sqrt{s_n - (-1)^n}\right) \end{cases}$$

Pour n pair, cela s'écrit :

$$\begin{cases} \left(\sqrt{2}+1\right)^n = \sqrt{s_n} + \sqrt{s_n - 1} = \sqrt{r_n} + \sqrt{r_n - 1} \\ \left(\sqrt{2}-1\right)^n = \sqrt{s_n} - \sqrt{s_n - 1} = \sqrt{r_n} - \sqrt{r_n - 1} \end{cases}$$

avec $r_n = s_n$ et pour n impair :

$$\begin{cases} \left(\sqrt{2}+1\right)^n = \sqrt{s_n + 1} + \sqrt{s_n} = \sqrt{r_n} + \sqrt{r_n - 1} \\ \left(\sqrt{2}-1\right)^n = \sqrt{s_n + 1} - \sqrt{s_n} = \sqrt{r_n} - \sqrt{r_n - 1} \end{cases}$$

avec $r_n = s_n - 1$.