

## Chapitre I — Divisibilité

Soient  $\mathbb{N}$  l'ensemble des entiers naturels et  $\mathbb{Z}$  l'ensemble des entiers relatifs. On dispose sur  $\mathbb{Z}$  des trois lois de composition<sup>1</sup>, qui à tout couple  $(x, y)$  de  $\mathbb{Z} \times \mathbb{Z}$  associent la somme  $x + y$ , la différence  $x - y$  et le produit  $xy$ . Nous noterons comme il est d'usage  $\leq$  la relation d'ordre<sup>2</sup> usuelle sur  $\mathbb{Z}$ . Pour tous  $x, y \in \mathbb{Z}$ , si l'on a  $x \leq y$ , on dit que  $x$  est plus petit que  $y$ , ou que  $x$  est inférieur à  $y$ . La relation  $x \leq y$  s'écrit aussi  $y \geq x$ . Si l'on a  $x \leq y$  avec  $x \neq y$ , on écrira parfois que l'on a  $x < y$  ou bien  $y > x$ . Cette relation d'ordre, induite sur  $\mathbb{N}$ , munit  $\mathbb{N}$  d'une structure d'ensemble ordonné, pour laquelle la propriété fondamentale suivante est vérifiée :

**Propriété fondamentale.** *Toute partie non vide de  $\mathbb{N}$  a un plus petit élément<sup>3</sup>.*

On l'utilisera à de nombreuses reprises.

### Table des matières

1. Division euclidienne	1
2. Nombres premiers	3
3. Valuation $p$ -adique d'un entier relatif	7
4. Plus grand commun diviseur	10
5. L'algorithme d'Euclide	12
6. L'équation $ax + by = c$	14
7. Le théorème chinois	15
8. Plus petit commun multiple	18
9. Écriture en base $b$	20

### 1. Division euclidienne

Pour tout  $x \in \mathbb{Z}$ , on note  $|x|$  le plus grand des entiers  $-x$  et  $x$ .

---

<sup>1</sup> Une loi de composition sur un ensemble  $E$  est une application du produit cartésien  $E \times E$  à valeurs dans  $E$ . Si  $E$  est fini de cardinal  $n$ , il y en a  $n^{n^2}$ .

<sup>2</sup> Une relation d'ordre sur un ensemble  $E$  est une relation binaire  $\mathcal{R}$  sur  $E$  telle que pour tous  $x, y$  et  $z$  dans  $E$ , les conditions suivantes soient remplies :

1) on a  $x\mathcal{R}x$  (réflexivité).

**Théorème 1.1 (Division euclidienne).** Soient  $a$  et  $b$  des éléments de  $\mathbb{Z}$  avec  $b \neq 0$ . Il existe un unique couple  $(q, r) \in \mathbb{Z} \times \mathbb{Z}$  tel que l'on ait

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

On dit que  $q$  est le quotient et que  $r$  est le reste de la division euclidienne de  $a$  par  $b$ .

Démonstration : 1) Démontrons l'assertion d'existence. Considérons l'ensemble

$$A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}.$$

Vérifions que  $A$  n'est pas vide. Tel est le cas si  $a \geq 0$ , car alors  $a$  est dans  $A$  (on prend  $k = 0$ ). Supposons  $a < 0$ . Si  $b \geq 1$ , on constate que  $a(1 - b) \in A$  (prendre  $k = a$ ) et si  $b \leq -1$ , alors  $a(1 + b) \in A$  (prendre  $k = -a$ ). D'après la propriété fondamentale satisfaite par  $\mathbb{N}$ , l'ensemble  $A$  possède donc un plus petit élément  $r$ . Parce que  $r$  appartient à  $A$ , on a  $r \geq 0$  et il existe  $q \in \mathbb{Z}$  tel que l'on ait  $r = a - bq$ . Il reste à vérifier que l'on a  $r < |b|$ . Supposons le contraire. On obtient

$$0 \leq r - |b| = a - b(q + \varepsilon) \in A \quad \text{avec} \quad \varepsilon = \pm 1.$$

L'inégalité  $r - |b| < r$  contredit alors le caractère minimal de  $r$ , d'où l'assertion d'existence.

2) Démontrons l'assertion d'unicité. Supposons pour cela qu'il existe deux couples  $(q, r)$  et  $(q', r')$  d'entiers relatifs tels que l'on ait

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

On a  $|q - q'| |b| = |r' - r|$ . Puisque  $r$  et  $r'$  sont positifs,  $|r - r'|$  est inférieur ou égal à  $r$  ou  $r'$ , d'où  $|r - r'| < |b|$ . On obtient  $|q - q'| < 1$ , d'où  $q = q'$ ,  $r = r'$  et le résultat.

**Définition 1.1.** Soient  $a$  et  $b$  deux éléments de  $\mathbb{Z}$ . On dit que  $b$  divise  $a$  ou que  $b$  est un diviseur de  $a$ , ou bien encore que  $a$  est un multiple de  $b$  (dans  $\mathbb{Z}$ ) s'il existe  $k \in \mathbb{Z}$  tel que  $a = kb$ . Si  $b$  est non nul, cette condition signifie que le reste de la division euclidienne de  $a$  par  $b$  est nul.

---

2) Si  $x\mathcal{R}y$  et  $y\mathcal{R}x$ , alors  $x = y$  (antisymétrie).

3) Si  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , alors  $x\mathcal{R}z$  (transitivité).

Une relation d'ordre est souvent notée  $\leq$  par commodité.

<sup>3</sup> Soient  $\leq$  une relation d'ordre sur un ensemble  $E$  et  $F$  une partie de  $E$ . Un élément  $a \in E$  est appelé plus petit élément de  $F$ , si  $a$  appartient à  $F$  et si pour tout  $x \in F$ , on a  $a \leq x$ . D'après la propriété d'antisymétrie, s'il existe un plus petit élément de  $F$ , il est unique. On parle alors du plus petit élément de  $F$ . Par exemple, 0 est le plus petit élément de  $\mathbb{N}$ . Bien entendu, un tel élément n'existe pas toujours. À titre indicatif,  $\mathbb{Z}$  n'a pas de plus petit élément. Il en est de même de l'intervalle  $]0, 1]$  dans l'ensemble des nombres réels muni de sa relation d'ordre usuelle.

### Exemples 1.1.

1) On a  $456567 = 19 \times 24029 + 16$ . Le quotient et le reste de la division euclidienne de 456567 par 19 sont donc respectivement 24029 et 16.

2) Soient  $a$  et  $n$  des entiers naturels non nuls. On a l'égalité

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

En particulier,  $a - 1$  divise  $a^n - 1$ .

Par exemple, l'entier  $N = 1 + 2 + 2^2 + 2^3 + \cdots + 2^{26}$  est divisible par 7. En effet, on a les égalités

$$N = 2^{27} - 1 = (2^3)^9 - 1 = (2^3 - 1)((2^3)^8 + \cdots + 2^3 + 1) = 7 \times 19173961.$$

3) Soit  $n$  un entier naturel tel que  $n + 1$  divise  $n^2 + 1$ . Vérifions que l'on a  $n = 0$  ou  $n = 1$ . On écrit pour cela que l'on a

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

d'où l'on déduit que  $n + 1$  divise 2 et notre assertion.

## 2. Nombres premiers

**Définition 1.2.** On appelle nombre premier tout entier  $p \geq 2$  dont les seuls diviseurs positifs sont 1 et  $p$ .

Par exemple 2, 3, 5, 7, 11, 13,  $\cdots$  sont des nombres premiers.

**Lemme 1.1.** Soit  $p$  un entier  $\geq 2$ . Alors,  $p$  est premier si et seulement si  $p$  n'est pas le produit de deux entiers strictement plus grands que 1.

Démonstration : Si l'on a  $p = ab$  avec  $a$  et  $b$  strictement plus grands que 1, alors  $a$  divise  $p$  et  $a$  est distinct de 1 et  $p$ , donc  $p$  n'est pas premier. Inversement, si  $p$  n'est pas premier, il possède un diviseur positif  $a$  autre que 1 et  $p$ , d'où  $p = ab$  où  $a$  et  $b$  sont  $\geq 2$ .

### Exemples 1.2.

1) Soit  $n$  un entier naturel. Posons  $p = 2n + 1$ . Démontrons que  $p$  est un nombre premier si et seulement si  $n$  ne figure pas dans le tableau infini

$$\begin{pmatrix} 4 & 7 & 10 & 13 & 16 & \cdots \\ 7 & 12 & 17 & 22 & 27 & \cdots \\ 10 & 17 & 24 & 31 & 38 & \cdots \\ 13 & 22 & 31 & 40 & 49 & \cdots \\ 16 & 27 & 38 & 49 & 60 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

dans lequel la première colonne est une suite arithmétique de premier terme 4 et de raison 3 et la  $k$ -ième ligne est une suite arithmétique de raison  $2k + 1$ .

Le premier terme de la  $k$ -ième ligne est  $3k + 1$ . Le coefficient de la  $k$ -ième ligne et de la  $j$ -ième colonne du tableau est donc  $3k + 1 + (j - 1)(2k + 1) = 2kj + k + j$ . Supposons  $p$  non premier. Il existe alors  $k$  et  $j$  au moins égaux à 1 tels que l'on ait  $p = (2k + 1)(2j + 1)$  ( $p$  est impair), d'où

$$n = \frac{p - 1}{2} = 2kj + k + j$$

et  $n$  apparaît donc dans le tableau. Inversement, si  $n$  apparaît dans le tableau, il existe  $k, j \geq 1$  tels que  $n = 2kj + k + j$ , ce qui conduit à l'égalité  $p = (2k + 1)(2j + 1)$  et  $p$  n'est pas premier, d'où notre assertion.

2) Pour tout  $n \geq 1$ , posons  $R_n = 1 \cdots 1$ , l'entier constitué de  $n$  chiffres 1. Démontrons que si  $R_n$  est premier, alors  $n$  est premier. Soit  $n$  un entier non premier. Il existe deux entiers  $a$  et  $b$  strictement plus grands que 1 tels que l'on ait  $n = ab$ . Par ailleurs, on a l'égalité

$$R_n = \frac{10^n - 1}{9}.$$

On a ainsi

$$R_n = \frac{10^{ab} - 1}{9} = \frac{10^{ab} - 1}{10^a - 1} \times \frac{10^a - 1}{9},$$

et  $R_n$  est donc le produit de deux entiers strictement plus grands que 1, autrement dit,  $R_n$  n'est pas premier, d'où le résultat.

Les seules valeurs de  $n$  pour lesquelles on sache que  $R_n$  est premier sont 2, 19, 23, 317, 1031. Il est probable que pour  $n = 49081, 86453, 109297, 270343$ ,  $R_n$  soit premier. On ne sait pas s'il existe une infinité d'entiers  $R_n$  premiers. Remarquons que si  $n$  est multiple de 3, alors  $R_n$  est divisible par 3, car la somme de ses chiffres l'est (voir le paragraphe 9).

**Théorème 1.2.** *Tout entier  $n \geq 1$  est un produit de nombres premiers. En particulier, tout entier  $n \geq 2$  possède un diviseur premier.*

Démonstration : On procède par récurrence sur  $n$ <sup>4</sup>. Notons  $P(n)$  la propriété :  $n$  est un produit de nombres premiers. La propriété  $P(1)$  est vraie car 1 est le produit vide des nombres premiers. Considérons un entier  $n \geq 2$  tel que  $P(k)$  soit vraie pour tout entier  $k$  tel que  $1 \leq k < n$ . Il s'agit de démontrer que  $P(n)$  est vraie. Tel est le cas si  $n$  est premier. Si  $n$  n'est pas premier, il existe des entiers  $a$  et  $b$  strictement plus grands que 1 tels que  $n = ab$ . On a  $1 \leq a < n$  et  $1 \leq b < n$ , donc  $P(a)$  et  $P(b)$  sont vraies, d'où le résultat.

---

<sup>4</sup> Rappelons le principe du raisonnement par récurrence. Soit  $n_0$  un entier naturel. Il s'agit de démontrer qu'une certaine propriété  $P(n)$  de l'entier  $n$  est vraie pour tout  $n \geq n_0$ . Supposons vérifiées les deux assertions suivantes :

1) la propriété  $P(n_0)$  est vraie.

**Notation.** On notera  $\mathbf{P}$  l'ensemble des nombres premiers.

**Théorème 1.3.** *L'ensemble  $\mathbf{P}$  est infini.*

Démonstration : Supposons que  $\mathbf{P}$  soit fini de cardinal  $n$ . Soient  $p_1, \dots, p_n$  ses éléments. Posons  $N = 1 + p_1 \cdots p_n$ . On a  $N \geq 2$ , donc  $N$  possède un diviseur premier  $p$ . L'entier  $p$  divise  $p_1 \cdots p_n$ , d'où l'on déduit que  $p$  divise 1, ce qui conduit à une contradiction.

**Théorème 1.4 (Lemme d'Euclide<sup>5</sup>).** *Soient  $a, b$  des entiers naturels et  $p$  un nombre premier tels que  $p$  divise  $ab$ . Alors,  $p$  divise l'un des entiers  $a$  et  $b$ .*

Démonstration. La démonstration qui suit est due à Gauss<sup>6</sup>. Supposons que  $p$  ne divise pas  $a$ . Il s'agit de montrer que  $p$  divise  $b$ . Considérons pour cela l'ensemble

$$A = \{n \geq 1 \mid p \text{ divise } an\}.$$

Il est non vide, car  $p$  appartient à  $A$ . Soit  $m$  le plus petit élément de  $A$ . D'après l'hypothèse faite sur  $a$ , on a l'inégalité

$$(1) \quad m \geq 2.$$

Soit  $n$  un élément de  $A$ . Vérifions que  $m$  divise  $n$ . D'après le théorème de la division euclidienne, il existe deux entiers  $q$  et  $r$  tels que l'on ait  $n = mq + r$  avec  $0 \leq r < m$ . On a l'égalité  $an - (am)q = ar$ , d'où l'on déduit que  $p$  divise  $ar$  (car  $n$  et  $m$  sont dans  $A$ ). Puisque l'on a  $r < m$ ,  $r$  n'est pas dans  $A$ , d'où  $r = 0$  et notre assertion. L'entier  $p$  est dans  $A$ . Par ailleurs, on peut supposer  $b \geq 1$ , auquel cas  $b$  est aussi dans  $A$ . Il en résulte que  $m$

---

2) Pour tout  $n \geq n_0$ , si la propriété  $P(n)$  est vraie, alors  $P(n+1)$  l'est aussi.  
Sous ces hypothèses, la propriété  $P(n)$  est vraie pour tout  $n \geq n_0$ .

Une variante consiste à remplacer la deuxième condition par la suivante, qui est parfois plus facile à utiliser, et qui, avec la première condition, conduit à la même conclusion :

2') Pour tout  $n > n_0$ , si la propriété  $P(k)$  est vraie pour tout  $k$  tel que  $n_0 \leq k < n$ , alors  $P(n)$  l'est aussi.

<sup>5</sup> Euclide était un mathématicien grec qui vécut vraisemblablement au troisième siècle avant notre ère. Il est l'auteur d'un ouvrage de treize volumes, Les Éléments de Mathématiques, consacrés entre autres à la géométrie et à la notion de nombre entier. La définition qu'il donne d'un nombre premier est «un nombre mesuré par une seule unité». Son oeuvre, dont une partie seulement nous est parvenue, est fondatrice en mathématiques.

<sup>6</sup> Carl Friedrich Gauss, surnommé le prince des mathématiciens, est né à Brunswick en 1777 et décède à Göttingen en 1855. On lui doit une quantité massive de résultats en arithmétique, ainsi que dans d'autres domaines. Son ouvrage, Disquisitiones Arithmeticae, est resté célèbre en théorie des nombres. On pourra trouver les arguments de la démonstration du théorème 1.4 à la page 6 de ce livre. À dix ans, le maître d'école lui demanda de calculer la somme des cent premiers entiers naturels. Il donna de façon surprenante la réponse très rapidement, à savoir  $50 \times 101 = 5050$ . Quelle formule avait-il utilisée ?

divise  $p$  et  $b$ . L'inégalité (1) et le fait que  $p$  soit premier entraînent alors  $p = m$ . Par suite,  $p$  divise  $b$ .

**Corollaire 1.1.** *Si un nombre premier divise un produit d'entiers relatifs, il divise l'un de ces entiers. En particulier, si un nombre premier divise un produit de nombres premiers, il est égal à l'un d'eux.*

Démonstration : C'est une conséquence directe du théorème 1.4, en procédant par récurrence sur le nombre de facteurs du produit.

Le théorème suivant s'appelle parfois le théorème fondamental de l'arithmétique :

**Théorème 1.5.** *Tout entier  $n \geq 2$  s'écrit de façon unique sous la forme*

$$(2) \quad n = p_1^{n_1} \cdots p_r^{n_r},$$

où les  $n_i$  sont des entiers naturels non nuls, et où les  $p_i$  sont des nombres premiers vérifiant  $p_{i-1} < p_i$  pour tout  $i = 2, \dots, r$ . On dit que l'égalité (2) est la décomposition de  $n$  en produit de nombres premiers.

Démonstration : L'assertion d'existence provient du théorème 1.2 en regroupant les facteurs égaux par ordre croissant. Prouvons l'assertion d'unicité. Supposons que l'on ait

$$n = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

où les  $p_i$  et  $q_i$  sont premiers tels que  $p_1 < \cdots < p_r$ ,  $q_1 < \cdots < q_s$  et où les  $n_i$  et  $m_i$  sont des entiers naturels non nuls. On déduit du corollaire 1.1 que l'on a

$$\{p_1, \dots, p_r\} = \{q_1, \dots, q_s\}.$$

Par suite, on a  $r = s$ . De plus,  $p_1$  est le plus petit élément de  $\{p_1, \dots, p_r\}$  et  $q_1$  est le plus petit élément de  $\{q_1, \dots, q_r\}$ , d'où  $p_1 = q_1$ , puis  $p_i = q_i$  pour tout  $i$ . Par ailleurs, s'il existe un indice  $i$  tel que  $n_i \neq m_i$ , par exemple  $n_i < m_i$ , alors  $p_i$  divise un produit de nombres premiers tous distincts de lui même, ce qui contredit le corollaire 1.1 et établit le résultat.

Un problème naturel qui se pose est le suivant :

**Problème.** *Soit  $n$  un entier  $\geq 2$ . Comment décider si  $n$  est un nombre premier ou non ?*

Il existe de nombreux tests permettant parfois de reconnaître si un entier  $n$  est premier. Nous n'aborderons quasiment pas cette étude. C'est la théorie des tests et critères de primalité. Signalons à ce sujet le résultat ci-dessous :

**Lemme 1.2.** *Soit  $n$  un entier  $\geq 2$ . Si  $n$  n'est pas premier, alors  $n$  possède un diviseur premier  $p$  vérifiant l'inégalité  $p^2 \leq n$ .*

Démonstration : Si  $n$  n'est pas premier, il existe deux entiers  $a$  et  $b$  strictement plus grands que 1 tels que  $n = ab$  (lemme 1.1). Supposons par exemple  $a \leq b$ . Puisque  $a \geq 2$ ,  $a$  possède un diviseur premier  $p$  (th. 1.2). Ainsi  $p$  divise  $n$  et on a  $p^2 \leq n$ .

En utilisant ce résultat, on constate par exemple que 641 est premier. En effet, s'il ne l'était pas, il devrait exister un nombre premier  $p < 25$  divisant 641. Les nombres premiers plus petits que 25 sont 2, 3, 5, 7, 11, 13, 17, 19 et 23. On vérifie alors qu'aucun de ces nombres ne divise 641 en utilisant le théorème de la division euclidienne.

**Crible d'Ératosthène**<sup>7</sup>. Un criblage est un procédé de triage. Étant donné un entier  $N$ , ce crible permet de déterminer tous les nombres premiers inférieurs à  $N$ . Son principe est le suivant. On écrit dans un tableau tous les entiers jusqu'à  $N$ . On raye ensuite tous les multiples de 2, autres que 2, puis tous les multiples de 3, autres que 3, etc, autrement dit, à chaque étape on raye tous les multiples du plus petit entier qui n'a pas encore été rayé. Pour démontrer que  $N$  est premier, si tel est le cas, il suffit d'après le lemme 1.2 de cribler tous les entiers plus petits que  $\sqrt{N}$ . Par exemple, en rayant tous les multiples de 2, 3, 5 et 7, on constate que 101 est premier. Signalons que l'on peut facilement repérer et stocker sur machine tous les nombres premiers plus petits que  $10^9$ .

### 3. Valuation $p$ -adique d'un entier relatif

On considère dans ce paragraphe l'ensemble  $\mathbb{N} \cup \{+\infty\}$  obtenu en adjoignant à  $\mathbb{N}$  un élément noté  $+\infty$ , que l'on munit de la structure d'ensemble ordonné qui induit l'ordre usuel sur  $\mathbb{N}$  et telle que  $+\infty \geq n$  pour tout entier naturel  $n$ . On prolonge par ailleurs la loi additive de  $\mathbb{N}$  à cet ensemble en posant  $(+\infty) + n = n + (+\infty) = +\infty$  et  $(+\infty) + (+\infty) = +\infty$ . Pour tout nombre premier  $p$ , on va définir ici une application, appelée valuation  $p$ -adique,

$$v_p : \mathbb{Z} \rightarrow \mathbb{N} \cup \{+\infty\}.$$

**Définition 1.2.** Soient  $n$  un entier relatif et  $p$  un nombre premier.

1) Si l'on a  $n \geq 2$ , alors  $v_p(n)$  est l'exposant de  $p$  dans la décomposition de  $n$  en produit de nombres premiers. Autrement dit :

1.1) si  $p$  ne divise pas  $n$ , on a  $v_p(n) = 0$ .

1.2) Si  $n = p_1^{n_1} \cdots p_r^{n_r}$  est la décomposition de  $n$  en produit de nombres premiers ( $n_i \geq 1$ ), on a

$$v_{p_i}(n) = n_i \quad \text{pour } i = 1, \dots, r.$$

2) On pose  $v_p(0) = +\infty$  et  $v_p(1) = 0$ .

3) Pour tout  $n \geq 1$ , on pose  $v_p(-n) = v_p(n)$ .

On dit que  $v_p(n)$  est la valuation  $p$ -adique de  $n$ .

---

<sup>7</sup> Ératosthène était un astronome, géographe, philosophe et mathématicien grec qui vécut au troisième siècle avant notre ère. Il est resté célèbre en mathématiques principalement pour son procédé de criblage des nombres premiers.

Pour tout nombre premier  $p$  et tout entier  $n \geq 1$ , zéro est divisible par  $p^n$ , ce qui justifie l'égalité  $v_p(0) = +\infty$ .

**Exemple 1.3.** Posons  $n = 539000$ . On a  $n = 2^3 \cdot 5^3 \cdot 7^2 \cdot 11$ , d'où  $v_2(n) = 3$ ,  $v_5(n) = 3$ ,  $v_7(n) = 2$ ,  $v_{11}(n) = 1$  et pour tout nombre premier  $p$  distinct de 2, 5, 7 et 11, on a  $v_p(n) = 0$ .

Avec cette définition, le théorème 1.5 s'écrit comme suit :

**Théorème 1.6.** *Tout entier relatif  $n$  non nul s'écrit de manière unique, à l'ordre près des facteurs, sous la forme*

$$(3) \quad n = \varepsilon \prod_{p \in \mathbf{P}} p^{v_p(n)} \quad \text{avec} \quad \varepsilon = \pm 1.$$

On a  $\varepsilon = 1$  si  $n \geq 1$  et  $\varepsilon = -1$  si  $n \leq -1$ . Contrairement à ce que laisse supposer cette formule, il s'agit d'un produit fini car on a  $v_p(n) = 0$  pour presque tout  $p \in \mathbf{P}$  (au sens tous sauf un nombre fini). En effet, pour tout  $n \in \mathbb{Z}$ , on a l'équivalence

$$(4) \quad v_p(n) \geq 1 \iff p \text{ divise } n.$$

Pour tous  $x$  et  $y$  dans  $\mathbb{Z}$ , on note dans la suite  $\text{Min}(x, y)$  le plus petit d'entre eux.

**Proposition 1.1.** *Soient  $a$  et  $b$  deux entiers relatifs et  $p$  un nombre premier.*

- 1) *On a  $v_p(ab) = v_p(a) + v_p(b)$ .*
- 2) *On a  $v_p(a + b) \geq \text{Min}(v_p(a), v_p(b))$ . De plus, si  $v_p(a) \neq v_p(b)$ , alors on a l'égalité  $v_p(a + b) = \text{Min}(v_p(a), v_p(b))$ .*
- 3) *Pour que  $a$  divise  $b$ , il faut et il suffit que l'on ait  $v_p(a) \leq v_p(b)$  pour tout  $p \in \mathbf{P}$ .*

Démonstration : On vérifie directement que ces assertions sont vraies si  $ab = 0$ . Supposons donc  $ab \neq 0$ .

- 1) Il résulte du théorème 1.6 que l'on a les égalités

$$ab = \varepsilon \prod_{p \in \mathbf{P}} p^{v_p(ab)} = \varepsilon \prod_{p \in \mathbf{P}} p^{v_p(a) + v_p(b)} \quad \text{avec} \quad \varepsilon = \pm 1.$$

L'unicité de la décomposition d'un entier sous la forme (3) entraîne alors l'égalité annoncée.

- 2) Il existe des entiers  $r$  et  $s$ , qui ne sont pas divisibles par  $p$ , tels que l'on ait

$$a = p^{v_p(a)} r \quad \text{et} \quad b = p^{v_p(b)} s.$$

Supposons par exemple  $v_p(a) \geq v_p(b)$ . On a

$$(5) \quad a + b = p^{v_p(b)} (p^{v_p(a) - v_p(b)} r + s),$$



d'où l'on déduit, d'après la première assertion, que l'on a

$$v_p(a+b) = v_p(b) + v_p(p^{v_p(a)-v_p(b)}r + s) \geq v_p(b) = \text{Min}(v_p(a), v_p(b)).$$

Supposons de plus  $v_p(a) > v_p(b)$ . Dans ce cas,  $p$  ne divise pas  $p^{v_p(a)-v_p(b)}r + s$ . D'après (5), cela conduit à l'égalité  $v_p(a+b) = v_p(b)$ .

3) Supposons que  $a$  divise  $b$ . Il existe  $k \in \mathbb{Z}$  tel que  $b = ak$ . Pour tout nombre premier  $p$ , on a  $v_p(b) = v_p(a) + v_p(k)$ , d'où  $v_p(b) \geq v_p(a)$ . Inversement, d'après l'hypothèse faite, pour tout  $p \in \mathbf{P}$  il existe  $t_p \geq 0$  tel que l'on ait  $v_p(b) = v_p(a) + t_p$ . Pour presque tout  $p$ , on a  $v_p(a) = v_p(b) = t_p = 0$ . Posons

$$t = \prod_{p \in \mathbf{P}} p^{t_p}.$$

Pour tout  $p \in \mathbf{P}$ , on a donc  $v_p(b) = v_p(at)$ , d'où  $b = \pm at$  et  $a$  divise  $b$ .

**Exemple 1.4.** Démontrons que  $\sqrt{2}$  est irrationnel i.e. n'est pas dans  $\mathbb{Q}$ . Procédons par l'absurde, en supposant qu'il existe des entiers naturels  $a$  et  $b$  tels que l'on ait

$$\sqrt{2} = \frac{a}{b}.$$

On a alors  $2b^2 = a^2$ . La valuation 2-adique de  $2b^2$  est  $1 + 2v_2(b)$ . Elle est impaire. Celle de  $a^2$  est  $2v_2(a)$ . Elle est paire, d'où une contradiction et le résultat. Il semble qu'il a été démontré pour la première fois par un membre de l'école philosophique de Pythagore, au cinquième siècle avant notre ère. On établit de la même façon que pour tout  $n \in \mathbb{N}$ , qui n'est pas un carré,  $\sqrt{n}$  est irrationnel.

Signalons que d'autres nombres célèbres comme  $e$  ou  $\pi$  sont irrationnels. On peut l'établir en utilisant des arguments issus de l'analyse relevant des programmes des deux premières années d'université. Cela étant, il est souvent très difficile de prouver qu'un nombre réel est irrationnel, si tel est le cas. Par exemple, on pense que  $e + \pi$  est irrationnel, mais on ne sait pas le démontrer.

**Définition 1.3.** Soient  $a$  et  $b$  deux entiers relatifs. On dit que  $a$  et  $b$  sont premiers entre eux s'il n'existe pas de nombres premiers divisant à la fois  $a$  et  $b$ , autrement dit, si pour tout nombre premier  $p$ , on a  $\text{Min}(v_p(a), v_p(b)) = 0$ . Dans ce cas, on dit aussi que  $a$  est premier avec  $b$ .

**Exemple 1.5.** Soit  $n$  un entier relatif. Vérifions que les entiers  $5n + 2$  et  $12n + 5$  sont premiers entre eux. Supposons qu'il existe un nombre premier  $p$  divisant  $5n + 2$  et  $12n + 5$ . Dans ce cas,  $p$  divise  $12(5n + 2)$  et  $5(12n + 5)$ , donc  $p$  divise la différence de ces deux nombres, autrement dit  $p$  divise 1, d'où une contradiction et l'assertion.

**Théorème 1.7 (Lemme de Gauss).** Soient  $a, b, c$  trois entiers relatifs tels que  $a$  divise  $bc$  et que  $a$  soit premier avec  $b$ . Alors,  $a$  divise  $c$ .

Démonstration : Soit  $p$  un nombre premier. Compte tenu de l'assertion 3 de la proposition 1.1, il s'agit de démontrer que l'on a l'inégalité  $v_p(a) \leq v_p(c)$ . Elle est évidente si  $v_p(a) = 0$ . Supposons  $v_p(a) \geq 1$  i.e. que  $p$  divise  $a$ . L'entier  $a$  étant premier avec  $b$ , on a alors  $v_p(b) = 0$ . Puisque  $a$  divise  $bc$ , on a  $v_p(a) \leq v_p(bc)$ , d'où  $v_p(a) \leq v_p(c)$  et le résultat.

**Corollaire 1.2.** Soient  $a$  un entier relatif et  $r, s$  deux entiers premiers entre eux. Si  $a$  est divisible par  $r$  et  $s$ , alors  $a$  est divisible par  $rs$ .

Démonstration : Il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que l'on ait les égalités  $a = ur = vs$ . D'après le lemme de Gauss,  $r$  divise donc  $v$ , d'où l'assertion.

#### 4. Plus grand commun diviseur

On considère dans ce paragraphe deux entiers relatifs  $a$  et  $b$  non tous les deux nuls.

**Théorème 1.8.** Il existe un unique entier  $d \geq 1$  vérifiant les deux conditions suivantes :

- 1) l'entier  $d$  est un diviseur commun à  $a$  et  $b$ .
- 2) Tout diviseur commun à  $a$  et  $b$  divise  $d$ .

On a l'égalité

$$(6) \quad d = \prod_{p \in \mathbf{P}} p^{\min(v_p(a), v_p(b))}.$$

**Définition 1.4.** L'entier  $d$  défini par l'égalité (6) est appelé le plus grand commun diviseur de  $a$  et  $b$ , ou en abrégé le pgcd de  $a$  et  $b$ . On le note  $\text{pgcd}(a, b)$  ou parfois  $a \wedge b$ .

Démonstration : Considérons l'entier  $d$  défini par l'égalité (6) ( $d$  est bien défini car  $a$  et  $b$  ne sont pas tous les deux nuls). Pour tout nombre premier  $p$ ,  $v_p(a)$  et  $v_p(b)$  sont plus grands que  $\min(v_p(a), v_p(b))$ , donc  $d$  est un diviseur commun à  $a$  et  $b$  (assertion 3 de la prop. 1.1). Par ailleurs, si  $c$  est un diviseur commun à  $a$  et  $b$ , alors pour tout nombre premier  $p$  on a  $v_p(c) \leq v_p(a)$  et  $v_p(c) \leq v_p(b)$ , d'où  $v_p(c) \leq \min(v_p(a), v_p(b))$ , donc  $c$  divise  $d$  (*loc. cit.*). Ainsi  $d$  vérifie les conditions 1 et 2. Par ailleurs, si  $d'$  est un entier naturel non nul vérifiant ces conditions, alors  $d$  divise  $d'$  et  $d'$  divise  $d$ , d'où  $d = d'$ .

**Lemme 1.3.** Les entiers  $\frac{a}{d}$  et  $\frac{b}{d}$  sont premiers entre eux.

Démonstration : Pour tout  $p \in \mathbf{P}$ ,  $v_p(d)$  est égal à  $v_p(a)$  ou  $v_p(b)$ . Par ailleurs, on a  $v_p(a/d) = v_p(a) - v_p(d)$  et  $v_p(b/d) = v_p(b) - v_p(d)$ , donc le minimum de  $v_p(a/d)$  et  $v_p(b/d)$  est nul, d'où le lemme.

**Lemme 1.4.** *Les entiers  $a$  et  $b$  sont premiers entre eux si et seulement si leur pgcd est 1.*

Démonstration : Les entiers  $a$  et  $b$  sont premiers entre eux si et seulement si pour tout  $p \in \mathbf{P}$ , on a  $\text{Min}(v_p(a), v_p(b)) = 0$ . D'après (6), cela est équivalent à l'égalité  $\text{pgcd}(a, b) = 1$ .

**Théorème 1.9 (Théorème de Bézout<sup>8</sup>).** *Il existe deux entiers relatifs  $u$  et  $v$  tels que l'on ait*

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

Démonstration : Considérons l'ensemble

$$A = \{au + bv \mid u, v \in \mathbb{Z}\} \cap (\mathbb{N} - \{0\}).$$

C'est une partie non vide de  $\mathbb{N}$ . Soit  $c$  son plus petit élément. On a  $c \geq 1$ . Vérifions que l'on a

$$(7) \quad A = \{ck \mid k \geq 1\}.$$

D'abord,  $c$  étant dans  $A$ , les éléments de la forme  $ck$ , avec  $k \geq 1$ , sont aussi dans  $A$ . Inversement, soit  $n$  un élément de  $A$ . D'après le théorème de la division euclidienne, il existe  $q, r \in \mathbb{Z}$  tels que l'on ait  $n = cq + r$  avec  $0 \leq r < c$ . Supposons  $r \neq 0$ . On a alors  $r = n - cq \geq 1$ . Les entiers  $n$  et  $c$  étant dans  $A$ ,  $n - cq$  est aussi de la forme  $a\alpha + b\beta$  avec  $\alpha, \beta \in \mathbb{Z}$ , donc  $r$  appartient à  $A$ . Le caractère minimal de  $c$  conduit alors à une contradiction. Ainsi, on a  $r = 0$ , puis  $n = cq$  avec  $q \geq 1$ , d'où l'égalité (7). Démontrons alors que l'on a

$$(8) \quad \text{pgcd}(a, b) = c,$$

ce qui entraînera le résultat. Si  $ab \neq 0$  les entiers  $|a|$  et  $|b|$  sont dans  $A$ , et d'après (7),  $c$  divise donc  $a$  et  $b$ . On a la même conclusion si  $ab = 0$ . Ainsi,  $c$  est un diviseur commun à  $a$  et  $b$ . Par ailleurs, il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que  $c = au + bv$ , de sorte que tout diviseur commun à  $a$  et  $b$  divise  $c$ . L'égalité (8) en résulte, car  $c$  vérifie les deux conditions du théorème 1.8.

On en déduit l'énoncé suivant :

**Corollaire 1.3.** *Les entiers  $a$  et  $b$  sont premiers entre eux si et seulement si il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que l'on ait  $1 = au + bv$ .*

---

<sup>8</sup> Étienne Bézout fut un mathématicien français qui vécut de 1730 à 1783. Il fut chargé de l'enseignement des élèves du corps de l'artillerie. Il publia une théorie générale des équations algébriques à Paris en 1779. Outre le théorème 1.9, un autre théorème célèbre porte son nom concernant l'intersection de deux « courbes algébriques ».

**Remarque 1.1.** On peut généraliser la notion de pgcd au cas d'une famille finie d'entiers relatifs non tous nuls, et les résultats de ce paragraphe s'étendent à cette situation. Si  $(x_i)_{1 \leq i \leq n}$  est une famille d'entiers relatifs non tous nuls, le pgcd des  $x_i$  est l'unique entier  $d > 0$  tel que  $d$  divise tous les  $x_i$  et que tout diviseur commun aux  $x_i$  divise  $d$ . Pour tout nombre premier  $p$ , on vérifie que l'on a (avec la notation évidente)

$$v_p(d) = \text{Min}(v_p(x_1), \dots, v_p(x_n)).$$

On démontre que  $d$  peut s'écrire sous la forme  $d = u_1x_1 + \dots + u_nx_n$  pour des entiers  $u_i$  convenablement choisis. On dit que les  $x_i$  sont premiers entre eux dans leur ensemble s'ils n'ont pas de diviseurs premiers communs, ce qui signifie que leur pgcd vaut 1. Il convient de noter que cela ne signifie pas qu'ils soient premiers entre eux deux à deux. En pratique, le calcul du pgcd d'une famille d'entiers se ramène à des calculs de pgcd de deux entiers. Par exemple, le pgcd de trois entiers non nuls  $a, b, c$  n'est autre que  $(a \wedge b) \wedge c$ .

### Exemples 1.6.

1) Démontrons que tout entier  $n \geq 7$  peut s'écrire sous la forme

$$n = a + b \quad \text{avec} \quad \text{pgcd}(a, b) = 1 \quad \text{et} \quad a \geq 2, b \geq 2.$$

Si  $n$  est impair, la décomposition  $n = a + b$  avec  $a = 2$  et  $b = n - 2$  convient. Supposons  $n$  multiple de 4. En posant  $n = 4k$ , on a  $n = a + b$  avec  $a = 2k - 1$  et  $b = 2k + 1$ . Deux nombres impairs consécutifs étant premiers entre eux, on obtient l'assertion dans ce cas. Supposons qu'il existe  $k \in \mathbb{N}$  tel que  $n = 4k + 2$ . On a alors  $n = a + b$  avec  $a = 2k + 3$  et  $b = 2k - 1$ . L'inégalité  $n \geq 7$  entraîne  $k \geq 2$ , donc  $a$  et  $b$  sont au moins égaux à 2. On a  $a - b = 4$ , donc le pgcd de  $a$  et  $b$  divise 4. Puisque  $a$  et  $b$  sont impairs, ils sont donc premiers entre eux, d'où le résultat.

2) Soient  $a$  et  $b$  des entiers relatifs tels que  $a > b$ . Il existe une infinité d'entiers  $n \in \mathbb{N}$  tels que  $a + n$  et  $b + n$  soient premiers entre eux. Tel est le cas des entiers  $n$  de la forme

$$n = (a - b)k + 1 - b,$$

où  $k$  est un entier plus grand que  $\frac{b-1}{a-b}$ . En effet, si  $d$  est un diviseur positif de  $a + n$  et  $b + n$ , alors  $d$  divise  $a - b$ , et l'égalité  $b + n = (a - b)k + 1$  implique  $d = 1$ .

## 5. L'algorithme d'Euclide

Considérons dans ce paragraphe deux entiers naturels  $a$  et  $b$  non nuls tels que  $a \geq b$ . On va détailler ici un algorithme, qui utilise seulement le théorème de la division euclidienne, permettant d'une part de déterminer le pgcd de  $a$  et  $b$ , et d'autre part d'expliciter une relation de Bézout entre  $a$  et  $b$ , autrement dit, de déterminer deux entiers relatifs  $u$  et  $v$  tels que l'on ait  $\text{pgcd}(a, b) = au + bv$ .

On construit pour cela une suite finie d'entiers naturels  $(r_i)_{i \geq 0}$ , que l'on appelle la suite des restes (associée à  $a$  et  $b$ ), par le procédé suivant : on pose d'abord

$$r_0 = a \quad \text{et} \quad r_1 = b.$$

Soit  $i$  un entier  $\geq 1$ . Si  $r_i \neq 0$ , on définit  $r_{i+1}$  comme étant le reste de la division euclidienne de  $r_{i-1}$  par  $r_i$ . Si  $r_i = 0$ , le procédé s'arrête et la suite des restes est alors formée des entiers  $r_0, r_1, \dots, r_{i-1}, r_i = 0$ . Il existe un unique indice  $n \geq 1$  tel que la condition suivante soit satisfaite :

$$0 < r_n < r_{n-1} < \dots < r_1 \leq r_0 \quad \text{et} \quad r_{n+1} = 0.$$

**Proposition 1.2.** On a  $r_n = \text{pgcd}(a, b)$ .

Démonstration : Soit  $i$  un entier tel que  $1 \leq i \leq n$ . Il existe  $q_i \in \mathbb{Z}$  tel que l'on ait

$$(9) \quad r_{i-1} = q_i r_i + r_{i+1} \quad \text{avec} \quad 0 \leq r_{i+1} < r_i.$$

Il résulte directement du théorème 1.8 que l'on a

$$\text{pgcd}(r_{i-1}, r_i) = \text{pgcd}(r_i, r_{i+1}).$$

Par suite, on a  $\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$ .

On a ainsi démontré que le pgcd de  $a$  et  $b$  est le dernier reste non nul  $r_n$  dans la suite des restes que l'on a construite. Il existe donc  $u$  et  $v$  dans  $\mathbb{Z}$  tels que l'on ait

$$r_n = au + bv.$$

Le problème qui nous intéresse maintenant est d'explicitier un tel couple  $(u, v)$ . On construit pour cela deux suites d'entiers  $(u_i)_{0 \leq i \leq n}$  et  $(v_i)_{0 \leq i \leq n}$  en posant

$$u_0 = 1, \quad u_1 = 0 \quad \text{et} \quad v_0 = 0, \quad v_1 = 1,$$

$$u_{i+1} = u_{i-1} - u_i q_i \quad \text{et} \quad v_{i+1} = v_{i-1} - v_i q_i \quad \text{pour tout } i = 1, \dots, n-1,$$

où  $q_i$  est défini par l'égalité (9), autrement dit, où  $q_i$  est le quotient de la division euclidienne de  $r_{i-1}$  par  $r_i$ .

**Proposition 1.3.** On a  $r_n = au_n + bv_n$ .

Démonstration : Il suffit de vérifier que pour tout  $i$  tel que  $0 \leq i \leq n$ , on a l'égalité  $r_i = au_i + bv_i$ . Elle est vraie si  $i = 0$  et  $i = 1$ . Considérons un entier  $k$  vérifiant les inégalités  $1 \leq k < n$  tel que l'on ait  $r_i = au_i + bv_i$  pour tout  $i \leq k$ . On a alors

$$r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1}a + v_{k-1}b) - q_k(u_k a + v_k b) = au_{k+1} + bv_{k+1},$$

d'où l'égalité annoncée.

Il peut être commode de présenter les étapes de calculs sous la forme du tableau suivant :

	$q_1$	$q_2$	$\cdots$	$q_{n-1}$	$q_n$
$r_0 = a$	$r_1 = b$	$r_2$	$\cdots$	$r_{n-1}$	$r_n$
1	0	$u_2$	$\cdots$	$u_{n-1}$	$u_n$
0	1	$v_2$	$\cdots$	$v_{n-1}$	$v_n$

**Exemple 1.7.** Appliquons ce qui précède au calcul du pgcd des entiers  $a = 17640$  et  $b = 525$ . On obtient le tableau :

	33	1	1	2
17640	525	315	210	105
1	0	1	-1	2
0	1	-33	34	-67

Ainsi  $105 = \text{pgcd}(a, b)$  et l'on obtient la relation de Bézout

$$105 = 2 \times 17640 - 67 \times 525.$$

Bien entendu, on peut aussi expliciter les décompositions de  $a$  et  $b$  en produit de nombres premiers. On trouve  $a = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$  et  $b = 3 \cdot 5^2 \cdot 7$ , d'où  $\text{pgcd}(a, b) = 3 \cdot 5 \cdot 7 = 105$  comme attendu (th. 1.8).

## 6. L'équation $ax + by = c$

Considérons des entiers relatifs non nuls  $a, b$  et  $c$ . On se propose ici de décrire l'ensemble  $S$  formé des couples  $(x, y) \in \mathbb{Z}^2$  tels que l'on ait

$$(10) \quad ax + by = c.$$

**Proposition 1.4.** Soit  $d$  le pgcd de  $a$  et  $b$ . Posons  $a' = \frac{a}{d}$  et  $b' = \frac{b}{d}$ .

- 1) L'ensemble  $S$  est non vide si et seulement si  $d$  divise  $c$ .
- 2) Supposons que  $d$  divise  $c$ . Soit  $(x_0, y_0)$  un élément de  $\mathbb{Z}^2$  tel que  $ax_0 + by_0 = c$ . On a

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

Démonstration : 1) S'il existe des entiers  $x$  et  $y$  vérifiant (10),  $d$  doit diviser  $c$  vu que  $d$  est un diviseur de  $a$  et  $b$ . Inversement, supposons que  $d$  divise  $c$ . Il existe  $c'$  dans  $\mathbb{Z}$  tel

que  $c = dc'$ . Puisque  $a'$  et  $b'$  sont premiers entre eux (lemme 1.3), il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que  $a'u + b'v = 1$  (cor. 1.3). On obtient alors l'égalité  $c = a(c'u) + b(c'v)$ , ce qui prouve que  $S$  n'est pas vide.

2) Soit  $(x, y)$  un élément de  $S$ . On a l'égalité

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

Puisque  $a'$  est premier avec  $b'$ , on déduit du lemme de Gauss que  $a'$  divise  $y_0 - y$ . Il existe donc  $k \in \mathbb{Z}$  tel que l'on ait  $y = y_0 - ka'$ , puis  $x = x_0 + kb'$ . Inversement, pour tout  $k \in \mathbb{Z}$ , on a  $a(x_0 + kb') + b(y_0 - ka') = c$ , d'où le résultat.

**Exemple 1.8.** Déterminons l'ensemble  $S$  des couples  $(x, y) \in \mathbb{Z}^2$  tels que

$$47x + 111y = 1.$$

Il n'est pas vide car 47 et 111 sont premiers entre eux. On peut le constater directement ou le vérifier avec l'algorithme d'Euclide. On détermine ensuite une solution particulière de cette équation, autrement dit on explicite une relation de Bézout entre 47 et 111. En utilisant cet algorithme, on obtient le tableau suivant :

	2	2	1	3	
111	47	17	13	4	1
1	0	1	-2	3	-11
0	1	-2	5	-7	26

On en déduit l'égalité  $26 \times 47 - 11 \times 111 = 1$ . Il en résulte que  $S$  est formé des couples  $(26 + 111k, -11 - 47k)$  où  $k \in \mathbb{Z}$ .

## 7. Le théorème chinois

Commençons par définir la notion de congruence.

### 1. Congruence modulo un entier

**Définition 1.5.** Soient  $n$  un entier naturel et  $a, b$  des entiers relatifs. On dit que  $a$  et  $b$  sont congrus modulo  $n$  si  $n$  divise  $a - b$ .

**Notation.** Pour signifier que  $a$  et  $b$  sont congrus modulo  $n$ , on note souvent

$$a \equiv b \pmod{n}.$$

On dit que c'est une congruence modulo  $n$ . Par définition, on a donc  $a \equiv b \pmod{n}$  si et seulement si il existe  $k \in \mathbb{Z}$  tel que l'on ait  $a = b + kn$ .

**Lemme 1.4.** Soit  $n$  un entier  $\geq 1$ . Pour tout  $a \in \mathbb{Z}$ , le reste de la division euclidienne de  $a$  par  $n$  est l'unique entier  $r$  tel que l'on ait

$$a \equiv r \pmod{n} \quad \text{et} \quad 0 \leq r \leq n-1.$$

Démonstration : Par définition, le reste de la division euclidienne de  $a$  par  $n$  vérifie cette condition. Si elle est satisfaite par deux entiers naturels  $r$  et  $r'$ , alors on a  $r \equiv r' \pmod{n}$ , puis  $r = r'$ , car  $r$  et  $r'$  sont plus petits que  $n-1$ .

### Exemples 1.9.

1) Soient  $a, b, c$  trois entiers relatifs. On a  $a + b + c \equiv 0 \pmod{6}$  si et seulement si  $a^3 + b^3 + c^3 \equiv 0 \pmod{6}$ . En effet, pour tout  $k \in \mathbb{Z}$ , on a  $k^3 \equiv k \pmod{6}$ , d'où la congruence  $a^3 + b^3 + c^3 \equiv (a + b + c) \pmod{6}$ , puis l'assertion.

2) Vérifions que 3 est le seul nombre premier  $p$  tels que  $p+2$  et  $p+4$  soient premiers. Soit  $p$  un nombre premier tel que  $p+2$  et  $p+4$  soient premiers. Tout nombre premier, autre que 3, est congru à 1 ou 2 modulo 3. Si l'on a  $p \equiv 1 \pmod{3}$ , (resp.  $p \equiv 2 \pmod{3}$ ), alors  $p+2$  (resp.  $p+4$ ) est divisible par 3. Les entiers  $p+2$  et  $p+4$  étant distincts de 3, on a donc  $p \equiv 0 \pmod{3}$ , puis  $p = 3$ . Par ailleurs, 5 et 7 sont premiers.

On pense qu'il existe une infinité de nombres premiers  $p$  tels que  $p+2$  soit aussi premier. Des tests sur machine permettent facilement de s'en convaincre, mais on ne sait pas le démontrer. C'est la célèbre conjecture des nombres premiers jumeaux.

3) Démontrons qu'il existe une infinité de nombres premiers congrus à 3 modulo 4. Supposons le contraire et considérons l'ensemble  $\{p_1, \dots, p_k\}$  des nombres premiers congrus à 3 modulo 4. Posons

$$N = 4(p_1 \cdots p_k) - 1.$$

On a  $N \geq 2$  et  $N \equiv -1 \pmod{4}$ . Il existe donc un diviseur premier  $p$  de  $N$  qui est congru à 3 modulo 4. En effet, tout nombre premier, autre que 2, est congru à 1 ou 3 modulo 4. Si tous les diviseurs premiers de  $N$  étaient congrus à 1 modulo 4, alors  $N$  le serait aussi, ce qui n'est pas. D'après l'hypothèse faite,  $p$  est l'un des  $p_i$ , ce qui entraîne que  $p$  divise  $-1$ , d'où une contradiction. On notera la similitude de cette démonstration avec celle du théorème 1.3.

Signalons que si  $d \geq 2$  et  $a \neq 0$  sont des entiers premiers entre eux, il existe une infinité de nombres premiers dans la progression arithmétique

$$a, \quad a + d, \quad a + 2d, \quad a + 3d, \dots$$

Ce résultat été démontré en 1837 par Dirichlet<sup>9</sup>. Il peut être exposé dans un cours de théorie des nombres en quatrième année d'université.

---

<sup>9</sup> Gustave Lejeune Dirichlet était un mathématicien allemand qui vécut de 1805 à 1859. Il fut l'un des premiers à utiliser des résultats issus de l'analyse pour aborder des problèmes d'arithmétique, inaugurant ainsi la voie de la théorie analytique des nombres. Ses travaux ont principalement concerné l'arithmétique et les séries de Fourier.



## 2. Le théorème

On l'appelle aussi le théorème des restes chinois. Il semble qu'il a été découvert vers le cinquième siècle avant notre ère par le mathématicien chinois Sun Tzu.

**Théorème 1.10.** *Soient  $m$  et  $n$  des entiers naturels non nuls premiers entre eux. Quels que soient  $a$  et  $b$  dans  $\mathbb{Z}$ , il existe  $c \in \mathbb{Z}$  tel que l'on ait*

$$(11) \quad c \equiv a \pmod{m} \quad \text{et} \quad c \equiv b \pmod{n}.$$

*De plus,  $c$  étant un entier comme ci-dessus, l'ensemble des entiers satisfaisant (11) est*

$$\{c + kmn \mid k \in \mathbb{Z}\}.$$

Démonstration : Parce que  $m$  et  $n$  sont premiers entre eux, il existe des entiers  $u$  et  $v$  tels que l'on ait (cor. 1.3)

$$(12) \quad mu + nv = 1.$$

Posons alors

$$(13) \quad c = b(mu) + a(nv).$$

On vérifie que l'on a  $c \equiv a \pmod{m}$  et  $c \equiv b \pmod{n}$ , d'où l'assertion d'existence.

Par ailleurs, un entier congru à  $c$  modulo  $mn$  satisfait la condition (11). Considérons alors un entier  $c'$  vérifiant (11). On a  $c \equiv c' \pmod{m}$  et  $c \equiv c' \pmod{n}$ , autrement dit  $m$  et  $n$  divisent  $c - c'$ . Parce que  $m$  et  $n$  sont premiers entre eux,  $mn$  divise donc  $c - c'$  (cor. 1.2) d'où le résultat.

**Remarque 1.2.** La démonstration précédente est effective, au sens où si  $a$  et  $b$  sont deux entiers relatifs donnés, elle permet d'expliciter un entier  $c$  vérifiant les congruences (11). Il suffit pour cela de déterminer des entiers  $u$  et  $v$  vérifiant l'égalité (12), ce que l'on peut faire en utilisant l'algorithme d'Euclide. On peut alors prendre pour  $c$  l'entier défini par l'égalité (13).

**Exemple 1.10.** Déterminons l'ensemble des entiers  $k \in \mathbb{Z}$  tels que l'on ait

$$(14) \quad k \equiv 1 \pmod{19} \quad \text{et} \quad k \equiv 2 \pmod{23}.$$

On commence par chercher une solution particulière de (14). On explicite pour cela une relation de Bézout entre 19 et 23. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	4	1	3	
23	19	4	3	1	0
1	0	1	-4	5	
0	1	-1	5	-6	

On en déduit l'égalité  $5 \times 23 - 6 \times 19 = 1$ , puis que l'entier

$$5 \times 23 - 2 \times (6 \times 19) = -113$$

vérifie les congruences (14). L'ensemble cherché est donc formé des entiers congrus à  $-113$  modulo 437.

## 8. Plus petit commun multiple

Soient  $a$  et  $b$  deux entiers relatifs non nuls. Pour tous  $x, y \in \mathbb{Z}$ , on note  $\text{Max}(x, y)$  le plus grand d'entre eux.

**Théorème 1.11.** *Il existe un unique entier  $m \geq 1$  vérifiant les deux conditions suivantes :*

- 1) *l'entier  $m$  est un multiple commun à  $a$  et  $b$ .*
- 2) *Tout multiple commun à  $a$  et  $b$  est un multiple de  $m$ .*

On a l'égalité

$$(15) \quad m = \prod_{p \in \mathbf{P}} p^{\text{Max}(v_p(a), v_p(b))}.$$

**Définition 1.6.** *L'entier  $m$  défini par l'égalité (11) est appelé le plus petit commun multiple de  $a$  et  $b$ , ou en abrégé le ppcm de  $a$  et  $b$ . On le note  $\text{ppcm}(a, b)$  ou parfois  $a \vee b$ .*

Démonstration : Considérons l'entier  $m$  défini par l'égalité (15). Pour tout  $p \in \mathbf{P}$ , on a  $\text{Max}(v_p(a), v_p(b)) \geq v_p(a), v_p(b)$ . Ainsi,  $m$  est un multiple commun à  $a$  et  $b$  (prop. 1.1). Par ailleurs, si  $c$  est un multiple commun à  $a$  et  $b$ , on a pour tout  $p \in \mathbf{P}$  les inégalités  $v_p(c) \geq v_p(a)$  et  $v_p(c) \geq v_p(b)$ , d'où  $v_p(c) \geq \text{Max}(v_p(a), v_p(b))$ , donc  $c$  est un multiple de  $m$  (loc. cit.). L'entier  $m$  vérifie donc les conditions 1 et 2. Si  $m'$  est un entier  $\geq 1$  vérifiant ces conditions, alors  $m'$  est un multiple de  $m$  et  $m$  est un multiple de  $m'$ , d'où  $m = m'$ .

**Proposition 1.5.** *On a l'égalité  $\text{pgcd}(a, b) \text{ppcm}(a, b) = |ab|$ .*

Démonstration : Pour tout  $p \in \mathbf{P}$ , on a

$$v_p(ab) = v_p(a) + v_p(b) = \text{Max}(v_p(a), v_p(b)) + \text{Min}(v_p(a), v_p(b)).$$

Les théorèmes 1.8 et 1.11 entraînent alors le résultat.

**Remarque 1.3.** On peut, comme pour le pgcd, généraliser la notion de ppcm au cas d'une famille finie d'entiers. Étant donnés des entiers non nuls  $x_1, \dots, x_n$  leur ppcm est l'unique entier  $m > 0$  multiple des  $x_i$ , tel que tout multiple des  $x_i$  soit multiple de  $m$ . Pour tout  $p \in \mathbf{P}$ , on a comme attendu

$$v_p(m) = \text{Max}(v_p(x_1), \dots, v_p(x_n)).$$

Cela étant, on notera que la proposition 1.5 est fausse dans ce cadre général, ce qui s'explique par le fait que l'entier  $\text{Min}(v_p(x_1), \dots, v_p(x_n)) + \text{Max}(v_p(x_1), \dots, v_p(x_n))$  n'est pas en général la somme des  $v_p(x_i)$  : prendre par exemple  $(x_1, x_2, x_3) = (2, 3, 4)$  et  $p = 2$ . Le pgcd des  $x_i$  est 1, leur ppcm est 12 et leur produit vaut 24.

### Exemples 1.11.

1) Déterminons le plus petit entier naturel multiple de 7 et congru à 1 modulo 2, 3, 4, 5 et 6. Un entier est multiple de 2, 3, 4, 5 et 6 si et seulement si il est multiple du ppcm de ces entiers i.e. de 60. Il s'agit donc de déterminer le plus petit entier naturel  $n$  vérifiant les congruences

$$n \equiv 0 \pmod{7} \quad \text{et} \quad n \equiv 1 \pmod{60}.$$

En utilisant l'algorithme d'Euclide, on obtient l'égalité

$$-17 \times 7 + 2 \times 60 = 1,$$

de sorte que l'ensemble des entiers satisfaisant ces congruences sont ceux de la forme  $-119 + 420k$  où  $k \in \mathbb{Z}$ . L'entier cherché est donc 301.

2) Explicitons tous les couples  $(a, b)$  d'entiers naturels non nuls tels que l'on ait

$$\text{pgcd}(a, b) + 10 \text{ppcm}(a, b) = 341 \quad \text{avec} \quad a \leq b.$$

Soient  $a$  et  $b$  deux entiers naturels non nuls vérifiant la condition demandée. Soient  $d$  leur pgcd et  $m$  leur ppcm. L'entier  $d$  divise  $m$ , donc  $d$  divise  $341 = 11 \times 31$ . Puisque  $m$  n'est pas nul, on a  $d < 341$ , d'où  $d = 1, 11, 31$ . Par ailleurs, on a  $md = ab$  (prop. 1.5). Si  $d = 1$ , on a  $m = 34$ , d'où  $ab = 34$ , puis  $(a, b) = (1, 34)$  ou  $(2, 17)$ . Si  $d = 11$ , on a  $m = 33$ , d'où  $ab = 3 \times 11^2$ , puis  $(a, b) = (11, 33)$ . Si  $d = 31$ , on a  $m = 31$ ,  $ab = 31^2$ , d'où  $(a, b) = (31, 31)$ . On obtient ainsi les couples

$$(1, 34), \quad (2, 17), \quad (11, 33), \quad (31, 31),$$

et on vérifie qu'ils satisfont la condition annoncée.

## 9. Écriture en base $b$

Considérons un entier  $b \geq 2$ .

**Théorème 1.12.** *Soit  $n$  un entier naturel non nul. On peut écrire  $n$  de manière unique sous la forme*

$$(16) \quad n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

où  $k$  est un entier naturel, où  $a_0, \dots, a_k$  sont des entiers tels que  $0 \leq a_i \leq b-1$  et où  $a_k$  est non nul. On dit que  $n = a_k a_{k-1} \cdots a_1 a_0$  est l'écriture de  $n$  en base  $b$  et l'on écrit parfois  $n = (a_k \cdots a_0)_b$ .

Démonstration : Démontrons l'assertion d'existence. Notons pour cela  $P(n)$  la propriété :  $n$  possède une écriture de la forme (16). La propriété  $P(1)$  est vraie, avec  $k = 0$  et  $a_0 = 1$ . Considérons un entier  $n \geq 2$  et supposons que la propriété  $P(j)$  soit vraie pour tout entier  $j$  tel que  $1 \leq j < n$ . Il s'agit de démontrer que  $P(n)$  est vraie. Tel est le cas si l'on a  $n < b$ , en prenant  $k = 0$  et  $a_0 = n$  dans (16). Supposons donc  $n \geq b$ . Il existe des entiers  $q$  et  $a_0$  tels que l'on ait  $n = bq + a_0$  avec  $0 \leq a_0 < b$ . L'inégalité  $n \geq b$  entraîne  $q \geq 1$ . Par suite, on a  $q < bq \leq n$ . La propriété  $P(q)$  étant vraie, il existe un entier  $k \geq 1$  tel que l'on ait  $q = a_k b^{k-1} + \cdots + a_2 b + a_1$ , où les  $a_i$  sont entiers vérifiant les inégalités  $0 \leq a_i \leq b-1$  et où  $a_k \neq 0$ . L'égalité  $n = bq + a_0$  entraîne alors que  $P(n)$  est vraie, d'où l'assertion d'existence.

Prouvons l'assertion d'unicité. On remarque pour cela que l'entier  $k$  intervenant dans (16) vérifie les inégalités

$$(17) \quad b^k \leq n < b^{k+1}.$$

En effet, la première inégalité est immédiate et le fait que les  $a_i$  soient compris entre 0 et  $b-1$  entraîne que l'on a  $n \leq (b-1)(b^k + b^{k-1} + \cdots + b + 1) = b^{k+1} - 1 < b^{k+1}$ . Par ailleurs, les inégalités (17) caractérisent l'entier  $k$  : c'est le plus grand entier inférieur ou égal à  $\frac{\log n}{\log b}$ . Tout revient donc à démontrer que si l'on a

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

avec  $a_k c_k \neq 0$  et  $0 \leq a_i, c_i \leq b-1$ , alors  $a_i = c_i$  pour tout  $i$ . Vu le caractère d'unicité du reste de la division euclidienne de  $n$  par  $b$ , on a  $a_0 = c_0$ . On en déduit ensuite l'assertion en procédant par récurrence finie sur les indices des coefficients.

**Remarque 1.4.** Rappelons que pour tout nombre réel  $x$ , il existe un unique entier relatif  $E(x)$  vérifiant les inégalités

$$E(x) \leq x < E(x) + 1.$$

L'entier  $E(x)$  s'appelle la partie entière de  $x$ . Il ressort de cette démonstration que le nombre de chiffres intervenant dans l'écriture d'un entier  $n \geq 1$  en base  $b$  est

$$1 + E\left(\frac{\log n}{\log b}\right).$$

**Exemples 1.12.**

1) On vérifie que l'on a  $101 = 2^6 + 2^5 + 2^2 + 1$ , de sorte que l'écriture de 101 en base deux est 1100101 i.e. on a  $101 = (1100101)_2$ .

2) Voyons quelques critères de divisibilité. Soit  $n$  un entier naturel non nul. Notons

$$n = a_k a_{k-1} \cdots a_1 a_0$$

son écriture en base dix.

Tout d'abord,  $n$  est pair si et seulement si  $a_0$  l'est. Par ailleurs, on a

$$n \equiv 10a_1 + a_0 \pmod{100},$$

donc, 100 étant divisible par 4, on a

$$n \equiv 0 \pmod{4} \iff a_1 a_0 \equiv 0 \pmod{4}.$$

De même,  $n$  est divisible par 5 si et seulement si  $a_0 = 0$  ou  $a_0 = 5$ . On a  $10 \equiv 1 \pmod{9}$  (en particulier  $10 \equiv 1 \pmod{3}$ ), d'où les équivalences

$$n \equiv 0 \pmod{3} \iff \sum_{i=0}^k a_i \equiv 0 \pmod{3},$$

$$n \equiv 0 \pmod{9} \iff \sum_{i=0}^k a_i \equiv 0 \pmod{9}.$$

On a  $10 \equiv -1 \pmod{11}$ , d'où l'on déduit que l'on a

$$n \equiv 0 \pmod{11} \iff \sum_{i=0}^k (-1)^i a_i \equiv 0 \pmod{11}.$$

3) Vérifions que les nombres de deux chiffres qui s'écrivent  $uv$  en base dix et  $vu$  en base sept sont 23 et 46. Soit  $uv$  un tel nombre. On a  $v + 10u = u + 7v$  avec  $0 \leq u, v \leq 6$ . On obtient  $3u = 2v$ , d'où  $u = 2$  ou  $u = 4$  et l'assertion.

Terminons ce chapitre en donnant une application du théorème 1.12.

**Calcul «rapide» de la puissance d'un entier.** L'existence de l'écriture en base deux des entiers permet d'accélérer le calcul de la puissance d'un entier. Plus précisément, considérons deux entiers  $x \geq 1$  et  $n \geq 1$ . Afin de calculer  $x^n$ , il faut a priori effectuer  $n - 1$  multiplications. En fait, la détermination de l'écriture de  $n$  en base deux permet de calculer  $x^n$  en effectuant au plus

$$\frac{2 \log n}{\log 2}$$

multiplications. On procède comme suit. Soit

$$n = 2^{i_k} + 2^{i_{k-1}} + \dots + 2^{i_1} + 2^{i_0},$$

le développement de  $n$  en base deux avec  $i_0 < i_1 < \dots < i_k$ . On a l'égalité

$$x^n = x^{2^{i_k}} \times x^{2^{i_{k-1}}} \times \dots \times x^{2^{i_1}} \times x^{2^{i_0}}.$$

On peut effectuer le calcul de  $x^{2^{i_k}}$  avec  $i_k$  multiplications, ce qui fournit aussi le calcul des autres termes  $x^{2^{i_j}}$  pour  $0 \leq j \leq k$ . Il en résulte que l'on peut calculer  $x^n$  avec  $i_k + k$  multiplications. Par ailleurs, on a

$$k \leq i_k \quad \text{et} \quad 2^{i_k} \leq n \quad \text{i.e.} \quad i_k \leq \frac{\log n}{\log 2}.$$

On en déduit que

$$i_k + k \leq \frac{2 \log n}{\log 2},$$

ce qui établit notre assertion.

**Exemple 1.13.** On a vu que l'on a  $101 = 2^6 + 2^5 + 2^2 + 1$ . Le calcul de  $x^{101}$  peut donc se faire avec neuf multiplications, au lieu de cent a priori.