ENTIERS, RATIONNELS, DECIMAUX

Document de travail pour la préparation au CAPES

François DUMAS

1. $\mathbb{Z}$ comme anneau euclidien

1. Notion de division euclidienne dans $\mathbb{Z}$, méthode de calcul du quotient et du reste, principe de descente de Fermat. – 2. Principales applications: numération, sous-groupes additifs de $\mathbb{Z}$, algorithme d'Euclide. – 3. D'autres applications: applications liées aux congruences, caractérisation des rationnels par la périodicité de leur développement décimal.

2. $\mathbb{Z}$ comme anneau principal

1. Divisibilité et idéaux dans $\mathbb{Z}$: multiples et diviseurs, sous-groupes et idéaux de $\mathbb{Z}$. – 2. PGCD ET PPCM de deux entiers: calcul du PGCD par l'algorithme d'Euclide, entiers premiers entre eux, théorème de Bézout, théorème de Gauss, relation entre PGCD et PPCM, premières applications. – 3. Equations diophantiennes de la forme $ax+by=c$.

3. $\mathbb{Z}$ comme anneau factoriel

1. Notion de nombre premier: premières propriétés, ensembles des nombres premiers. – 2. Décomposition en produit de facteurs premiers: existence et unicité de la décomposition, applications à l'ensemble des diviseurs d'un entier, au calcul du PGCD ET PPCM de deux entiers, à certaines fonctions atithmétiques multiplicatives. – 3. Quelques caractérisation des nombre spremiers et applications: idéaux maximaux de $\mathbb{Z}$, petit théorème de Fermat et nombres pseudo-premiers, théorème de Wilson.

4. Quotients de l'anneau $\mathbb{Z}$

1. Congruences dans $\mathbb{Z}$: compatibilité avec les lois de $\mathbb{Z}$, applications aux critères de divisibilité. – 2. L'anneau $\mathbb{Z}/n\mathbb{Z}$: lois quotients, éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$. – 3. Applications et résultats complémentaires: systèmes de congruences et théorème chinois, indicatrice d'Euler, applications à certains résultats classiques d'arithmétique.

5. Corps des fractions de l'anneau $\mathbb{Z}$

1. L'ensemble $\mathbb{Q}$ des nombres rationnels, injection canonique de $\mathbb{Z}$ dans $\mathbb{Q}$, dénombrabilité de $\mathbb{Q}$. – 2. Opérations et relation d'ordre dans $\mathbb{Q}$, structure de corps ordonné. – 3. Compléments et prolongements: sur le plan algébrique, sur le plan topologique.

6. Anneau des nombres décimaux

1. Notion de nombre décimal, l'anneau $\mathbb{D}$, écriture décimale des nombres décimaux. – 2. Approximations décimales et développement décimal d'un nombre réel. – 3. Exemples d'applications : comparaison de deux réels par leur développement décimal, caractérisation des rationnels par la périodicité de leur développement décimal propre, non dénombrabilité de $\mathbb{R}$.

Leçon 1

$\mathbb{Z}$ comme anneau euclidien

Prérequis: pour les parties 1 et 2, on suppose connus l'ensemble $\mathbb{N}$ des entiers naturels, muni de ses opérations et de sa relation d'ordre, et l'ensemble $\mathbb{Z}$ des entiers relatifs, muni de sa structure d'anneau et de sa relation d'ordre. On utilisera en particulier le fait que $\mathbb{N}$ est bien ordonné (toute partie non-vide de $\mathbb{N}$ admet un plus petit élément, d'où il résulte en particulier qu'il n'existe pas dans $\mathbb{N}$ de suite strictement décroissante), et que toute partie non-vide et majorée de $\mathbb{Z}$ admet un plus grand élément. Les applications de la partie 3 font de plus appel à la notion de congruence, et au développement décimal des nombres réels.

1. Notion de division euclidienne dans $\mathbb{Z}$

1.1 Théorème.

Pour tout couple $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < |b|$.

Preuve. Pour montrer l'unicité, supposons l'existence de deux couples (q,r) et (q',r') dans $\mathbb{Z} \times \mathbb{N}$ satisfaisant aux conditions $a = bq + r$ avec $0 \leq r < |b|$, et $a = bq' + r'$ avec $0 \leq r' < |b|$. On a alors $b(q-q') = r' - r$ et $-|b| < r' - r < |b|$. Donc $-|b| < b(q-q') < |b|$. Comme $b \neq 0$, on en déduit que $-1 < q - q' < 1$, ce qui, puisque $q - q'$ est un entier, implique $q - q' = 0$. Ainsi $q = q'$, d'où $r = r'$.

Pour montrer l'existence, supposons d'abord $b > 0$. Posons $B = \{k \in \mathbb{Z}\,;\, kb \leq a\}$. C'est une partie de $\mathbb{Z}$ qui est non-vide (car $0 \in B$ si $a \geq 0$ et $a \in B$ si $a < 0$) et qui est majorée (par le maximum des entiers a et 0). Donc elle admet un plus grand élément. Notons-le q. On a par définition de q la double inégalité $qb \leq a < (q+1)b$, de sorte que l'entier $r = a - qb$ vérifie $0 \leq r < b$.

Supposons maintenant $b < 0$. D'après ce qui précède, il existe $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = (-b)q + r$ et $0 \leq r < |b|$. Le couple $(-q,r) \in \mathbb{Z} \times \mathbb{N}$ vérifie alors $a = b(-q) + r$ et $0 \leq r < |b|$. □

1.2 Définitions.

L'opération consistant à associer à un couple $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ l'unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ satisfaisant les conditions du théorème s'appelle la *division euclidienne* de a par b.
Dans cette division, a est appelé le *dividende*, b le *diviseur*, q le *quotient*, et r le *reste*.

1.3 Remarques.

1. Si a et b sont deux entiers naturels, avec $b \neq 0$, le quotient q dans la division euclidienne de a par b est lui-même positif. On peut donc parler de la division euclidienne dans $\mathbb{N}$.

   En effet, il suffit d'observer dans la preuve du théorème ci-dessus que, lorsque $a \geq 0$ et $b > 0$, le plus grand élément q de l'ensemble $B = \{k \in \mathbb{Z}\,;\, kb \leq a\}$ est positif.

   Dans les faits, pour effectuer une division euclidienne, il est toujours possible de se ramener au cas où a et b sont tous les deux positifs.

   En effet, supposons $a = bq + r$ avec $0 \leq r < |b|$; on a: $a = (-b)(-q) + r$ avec $0 \leq r < |-b|$, ce qui permet de se ramener toujours au cas où $b > 0$. Supposons donc maintenant $a = bq + r$ avec $b > 0$ et $0 \leq r < b$; si $r = 0$, alors $-a = b(-q)$; si $0 < r < b$, alors $-a = (-q-1)b + (b-r)$ avec $0 \leq b - r < b$. On se ramène donc toujours au cas où $a > 0$.

2. Il résulte du théorème 1.1 que, pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ tel que $a = bq + r$ et $|r| < |b|$. Mais en affaiblissant ainsi la condition sur le reste, on perd l'unicité du quotient et du reste.

   Par exemple, pour $a = 19$ et $b = 3$, on a: $19 = 6 \times 3 + 1 = 7 \times 3 + (-2)$.

   La condition $|r| < |b|$ ci-dessus correspond à la notion générale d'anneau euclidien (en traduisant que la valeur absolue dans $\mathbb{Z}$ définit un stathme), pour laquelle aucune unicité du quotient et du reste n'est a priori requise, ce qui n'empêche pas d'établir certaines propriétés fondamentales (comme le fait que tout idéal est principal). Néanmoins, on verra que pour plusieurs applications spécifiques de la division euclidienne dans $\mathbb{Z}$, l'unicité du quotient et du reste du théorème 1.1 intervient de façon déterminante.

3. En supposant ici connu le corps $\mathbb{Q}$ des rationnels, on déduit aussi du théorème 1.1 que:

   pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe $(q',r') \in \mathbb{Z} \times \mathbb{Z}$ tel que $a = bq' + r'$ et $|r'| \leq \frac{|b|}{2}$.

   En effet, soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Soit (q,r) l'unique couple de $\mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec $0 \leq r < |b|$. Si $r \leq \frac{|b|}{2}$, alors $q' = q$ et $r' = r$ conviennent. Si $r > \frac{|b|}{2}$, distinguons deux cas.

   Ou bien $b > 0$, donc $b > r > \frac{b}{2} > 0$. On écrit $a = b(q+1) - b + r$ avec $|-b+r| = b - r < b - \frac{b}{2} = \frac{b}{2} = \frac{|b|}{2}$. Les entiers $q' = q+1$ et $r' = r - b$ conviennent.

   Ou bien $b < 0$, donc $-b > r > \frac{-b}{2} > 0$. On écrit $a = b(q-1)+b+r$ avec $|b+r| = -b-r < -b+\frac{b}{2} = \frac{-b}{2} = \frac{|b|}{2}$. Les entiers $q' = q-1$ et $r' = r + b$ conviennent.

   A noter que, là encore, il n'y a pas unicité du couple (q',r'). Par exemple: $14 = 4 \times 3 + 2 = 4 \times 4 - 2$.

   Les entiers q' solutions sont les entiers les plus proches du nombre rationnel $\frac{a}{b}$.

   En effet, on a avec les notations ci-dessus: $|\frac{a}{b} - q'| = |\frac{r'}{b}| \leq \frac{1}{2}$. Si le rationnel $\frac{a}{b}$ est de la forme $n + \frac{1}{2}$ pour une certain entier $n \in \mathbb{Z}$, alors $q' = n$ ou $q' = n+1$. Sinon, on a $|\frac{a}{b} - q'| < \frac{1}{2}$, et q' est l'(unique) entier le plus proche de $\frac{a}{b}$ dans $\mathbb{Q}$.

4. Pour déterminer explicitement le quotient q et le reste r dont le théorème 1.1 assure l'existence, on peut d'après la remarque 2 ci-dessus supposer sans restriction que a et b sont positifs. Il s'agit alors de trouver le plus grand multiple q de b qui soit inférieur ou égal à a, (on pose ensuite $r = a - bq$). On apprend dans l'enseignement primaire à procéder pour cela par tâtonnements, (on essaie des multiples de b plus ou moins grands par rapport à a), en s'appuyant sur l'écriture décimale des entiers naturels a et b. Donnons un exemple de cette démarche:

   Effectuons la division euclidienne de $a = 9345$ par $b = 16$.

   On a: $9 < b$ et $93 \geq b$; ces inégalités justifie le regroupement $\widehat{93}45$ de la présentation scolaire. On écrit:
   $9345 = 93 \times 100 + 45 = (\mathbf{5 \times 16 + 13}) \times 100 + 45 = 500 \times 16 + 1345$.

   On a: $1 < b$, $13 < b$ et $134 \geq b$; ceci justifie le regroupement $\widehat{134}5$ de la présentation scolaire. On écrit:
   $1345 = 134 \times 10 + 5 = (\mathbf{8 \times 16 + 6}) \times 10 + 5 = 80 \times 16 + 65$.

   On a: $6 < b$ et $65 \geq b$; ceci justifie le regroupement $\widehat{65}$ de la présentation scolaire. On écrit:
   $65 = \mathbf{4 \times 16 + 1}$

   Finalement, on aboutit à: $9345 = (500 + 80 + 4) \times 16 + 1 = \boxed{584 \times 16 + 1}$.

   On présente les calculs sous la forme bien connue ci-contre.
   On y retrouve les trois divisions euclidiennes intermédiaires (en gras dans les calculs ci-dessus) permettant d'aboutir au résultat final (encadré).

$\widehat{93}45$	16
$\widehat{134}5$	584
$\widehat{65}$	
1	

   La méthode proposée ci-dessous ne repose pas sur une recherche intuitive de q mais sur un procédé algorithmique systématique.

1.4 Méthode de calcul du quotient et du reste (principe de descente de Fermat).

D'après la remarque 1.3.1, on peut sans restriction se limiter au cas où a et b sont positifs. On a alors:

PROPOSITION. *Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$. On définit une suite d'entiers relatifs (x_n) en posant $x_n = a - (n+1)b$ pour tout $n \in \mathbb{N}$. Alors:*

(i) *la suite (x_n) est strictement décroissante;*

(ii) *il existe un entier naturel m tel que, pour tout $n \geq m$, on ait $x_n < 0$;*

(iii) *si l'on note N le plus petit entier naturel tel que $x_N < 0$, alors le quotient q et le reste r dans la division euclidienne de a par b sont donnés par $q = N$ et $r = a - bN$.*

Preuve. Le point (i) est clair. Le (ii) résulte du fait qu'il n'existe pas de suite strictement décroissante d'entiers naturels. Pour le (iii), distinguons deux cas. Si $N = 0$, alors $x_0 = a - b < 0$, donc $q = 0$ et $r = a$ vérifient bien $a = bq + r$ avec $0 \leq a < b$. Si $N > 0$, il résulte de la définition de N que $x_N < 0$ et $x_{N-1} \geq 0$. Donc $a - (N+1)b < 0$ et $a - Nb \geq 0$. En posant $r = x_{N-1} = a - Nb$, on a bien $0 \leq r < b$, et $q = N$ vérifie alors $a = qb + r$ □

Exemple. Considérons $a = 144$ et $b = 31$. On calcule $x_0 = a - b = 113$, $x_1 = a - 2b = 82$, $x_2 = a - 3b = 51$, $x_3 = a - 4b = 20$ et $x_4 = a - 5b = -11$; donc $N = q = 4$ et $r = x_{N-1} = x_3 = 20$; on a: $144 = 31 \times 4 + 20$.

2. Principales applications

2.1 Numération.

Remarque préliminaire. Nous avons donné précédemment pour illustrer diverses propriétés des exemples numériques utilisant l'écriture décimale des entiers. En toute rigueur, ces exemples numériques ne pourraient être introduits qu'après avoir traité la question de l'écriture d'un entier dans une base donnée. Ce résultat fondamental, qui permet d'écrire tous les entiers à partir d'un nombre fini de symboles, est rappelé dans le théorème ci-dessous, dont la preuve utilise la division euclidienne.

Théorème. *Soit b un entier naturel ≥ 2. Pour tout entier naturel a non-nul, il existe unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \ldots, a_n)$ d'entiers naturels strictement inférieurs à b vérifiant:*

$$a = \sum_{i=0}^{n} a_i b^i \quad \text{et} \quad a_n \neq 0.$$

Preuve. Montrons d'abord l'unicité. Supposons pour cela que $a = \sum_{i=0}^{n} a_i b^i$ et $a = \sum_{i=0}^{m} \alpha_i b^i$, avec n et m deux entiers naturels, $(a_0, a_1, \ldots, a_n)$ un $(n+1)$-uplet d'entiers naturels strictement inférieurs à b tel que $a_n \neq 0$, et $(\alpha_0, \alpha_1, \ldots, \alpha_m)$ un $(m+1)$-uplet d'entiers naturels strictement inférieurs à b tel que $\alpha_m \neq 0$.

Comme $a_i \leq b-1$ pour tout $0 \leq i \leq n$, on a: $a \leq \sum_{i=0}^{n} (b-1) b^i = (b-1) \sum_{i=0}^{n} b^i = b^{n+1} - 1$.

Comme $a_n \geq 1$, on a: $a \geq b^n$. Donc, $b^n \leq a \leq b^{n+1} - 1$, et de même: $b^m \leq a \leq b^{m+1} - 1$.

Si l'on avait $n < m$, on aurait $b^{n+1} \leq b^m$, d'où avec les inégalités ci-dessus: $b^m \leq a \leq b^m - 1$, contradiction ! Donc $n \geq m$. On conclut en échangeant les rôles de n et m que $n = m$.

Ainsi: $a = \sum_{i=0}^{n} a_i b^i = \sum_{i=0}^{n} \alpha_i b^i$. On montre par récurrence sur n que $a_i = \alpha_i$ pour tout $0 \leq i \leq n$.

C'est clair si $n = 0$. Si $n \geq 1$, il résulte de l'égalité ci-dessus que $a_0 - \alpha_0 = b \sum_{i=0}^{n-1} (\alpha_i - a_i) b^i$.

Comme $0 \leq a_0 < b$ et $0 \leq \alpha_0 < b$, on a $|a_0 - \alpha_0| < b$; l'égalité précédente implique donc $a_0 = \alpha_0$ et $\sum_{i=0}^{n-1} a_i b^i = \sum_{i=0}^{n-1} \alpha_i b^i$. On applique l'hypothèse de récurrence pour conclure.

Montrons maintenant l'existence de la décomposition. On procède par récurrence sur a. Si $a = 1$, on a le résultat voulu avec $n = 0$ et $a_0 = 1$. Supposons le théorème vrai pour tous les entiers naturels strictement inférieurs à un entier $a \geq 1$. Par division euclidienne de a par b, il existe $q \in \mathbb{N}$ et $r \in \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$. Si $a < b$, on a le résultat voulu avec $n = 0$ et $a_0 = 1$. Sinon, $a \geq b$, donc $1 \leq q < a$; on applique alors à q l'hypothèse de récurrence: il s'écrit $q = \sum_{i=0}^{m} q_i b^i$ avec $m \in \mathbb{N}$, $0 \leq q_i < b$ pour tout $0 \leq i \leq m$ et $q_m \neq 0$. Donc $a = \sum_{i=0}^{m} q_i b^{i+1} + r$, d'où le résultat voulu avec $n = m+1$, $a_i = q_{i-1}$ pour $1 \leq i \leq n$ et $a_0 = r$. □

Définitions et notation. Avec les données et hypothèses du théorème ci-dessus, on note $a = \overline{a_n \cdots a_1 a_0}^{\,b}$. Cette écriture s'appelle la représentation de a dans la base (de numération) b. L'entier $n+1$ s'appelle la longueur de cette représentation. Les entiers a_i compris entre 0 et $b-1$ s'appellent les chiffres de cette représentation.

Remarque. Les chiffres $a_0, a_1, \ldots, a_n$ sont obtenus par divisions euclidiennes successives par b, à partir de a.

Plus précisément, prenons a et b dans $\mathbb{N}^*$ et considérons les divisions euclidiennes:

$$a = bq_0 + a_0,\ q_0 = bq_1 + a_1,\ q_1 = bq_2 + a_2, \ldots,\ q_i = bq_{i+1} + a_{i+1},\ \ldots.$$

Si tous les q_i étaient non-nuls, ils formeraient une suite strictement décroissante d'entiers naturels, ce qui est impossible. Il existe donc $n \in \mathbb{N}^*$ tel que $q_n = 0$ et $q_{n-1} \neq 0$. On a donc:

$$a = bq_0 + a_0 = b^2 q_1 + ba_1 + a_0 = b^3 q_2 + b^2 a_2 + ba_1 + a_0 = \cdots = \sum_{i=0}^{n} b^i a_i, \text{ où } a_n = q_{n-1} \neq 0.$$

Exemple: écrivons 3310 en base 8. On a:
$3310 = 8 \times 413 + 6$, $413 = 8 \times 51 + 5$, $51 = 8 \times 6 + 3$, $6 = 8 \times 0 + 6$,
d'où: $3310 = 8 \times 413 + 6 = 8 \times (8 \times 51 + 5) + 6 = 8 \times (8 \times (8 \times 6 + 3) + 5) + 6 = 8^3 \times 6 + 8^2 \times 3 + 8 \times 5 + 6$.
On conclut que $3310 = \overline{6356}^{8}$.

2.2 Sous-groupes additifs de $\mathbb{Z}$.

Définition et notation. Soit $a \in \mathbb{Z}$. On appelle multiple de a tout entier $n \in \mathbb{Z}$ pour lequel il existe un entier $k \in \mathbb{Z}$ tel que $n = ak$. Le sous-ensemble de $\mathbb{Z}$ formé des mutiples de a est noté $a\mathbb{Z}$.
En particulier $0\mathbb{Z} = \{0\}$ et $1\mathbb{Z} = \mathbb{Z}$.

Remarques. On vérifie aisément que:

(i) pour tout $(a, b) \in \mathbb{Z}^2$, $a\mathbb{Z} = b\mathbb{Z}$ si et seulement si $a = b$ ou $a = -b$;

(ii) pour tout $a \in \mathbb{Z}$, $a\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.

Réciproquement, on a:

THÉORÈME. *Soit G un sous-groupe additif de $\mathbb{Z}$. Alors, il existe un unique entier naturel a tel que $G = a\mathbb{Z}$.*

Preuve. L'unicité est claire d'après la remarque (i) ci-dessus. Montrons l'existence. Soit G un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$, alors $G = 0\mathbb{Z}$. Sinon, G contient au moins un élément $g \neq 0$. Comme G est un sous-groupe, on a nécessairement $-g \in G$, de sorte que l'un des deux éléments g ou $-g$ est strictement positif. Donc $G \cap \mathbb{N}^*$ est non-vide. Parce que $\mathbb{N}$ est bien ordonné, on en déduit que $G \cap \mathbb{N}^*$ admet un plus petit élément. Notons-le a.

Vérifions que $a\mathbb{Z} \subseteq G$. Comme G est stable par l'addition et que $a \in G$, on a $a + a \in G$, et par récurrence $ka \in G$ pour tout entier $k > 0$. Comme G est stable par passage à l'opposé, on en déduit que $ka \in G$ pour tout entier $k < 0$. Comme enfin $0 \in G$, on conclut que G contient l'entier ka pour tout $k \in \mathbb{Z}$.

Vérifions que $G \subseteq a\mathbb{Z}$. Soit $x \in G$ quelconque. Comme $a \neq 0$, on peut effectuer la division euclidienne de x par a. Il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $x = aq + r$ et $0 \leq r < a$. L'entier $r = x - aq$ appartient à G car $x \in G$ et $aq \in a\mathbb{Z} \subseteq G$ d'après ce qui précède. Puisque a est le plus petit élément de $G \cap \mathbb{N}^*$ et que $r \in G$ vérifie $0 \leq r < a$, on a forcément $r = 0$, et donc $x \in a\mathbb{Z}$. On a ainsi vérifié que $G = a\mathbb{Z}$, ce qui prouve le résultat voulu. □

Remarque. Il est facile de vérifier que, pour tout $a \in \mathbb{Z}$, le sous-groupe $a\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$. Il résulte alors du théorème ci-dessus que tout idéal de $\mathbb{Z}$ est principal (c'est-à-dire du type $a\mathbb{Z}$ pour un élément a de $\mathbb{Z}$). En d'autres termes, l'anneau $\mathbb{Z}$ est principal.

Les conséquences pratiques de cette propriété pour l'étude de la divisibilité dans $\mathbb{Z}$ sont nombreuses et importantes. Elles seront détaillées dans la leçon suivante. Bornons-nous à remarquer ici que c'est l'existence du quotient et du reste dans la division euclidienne qui est à la base du théorème fondamental ci-dessus, dont la preuve n'est que la traduction pour $\mathbb{Z}$ de la démonstration du fait que tout anneau euclidien est principal.

2.3 Algorithme d'Euclide.

Définition et notation. Soit $a \in \mathbb{Z}$. On appelle diviseur de a tout entier $n \in \mathbb{Z}$ pour lequel il existe un entier $k \in \mathbb{Z}$ tel que $a = nk$. Le sous-ensemble de $\mathbb{Z}$ formé des diviseurs de a est noté D_a.

Remarques. On vérifie aisément que:

(i) $D_0 = \mathbb{Z}$ et $D_1 = \{-1, 1\}$;

(ii) pour tout $(a, b) \in \mathbb{Z}^2$, on a: $(a \in D_b) \Leftrightarrow (b \in a\mathbb{Z}) \Leftrightarrow (b\mathbb{Z} \subset a\mathbb{Z}) \Leftrightarrow (D_a \subset D_b)$;

(iii) pour tout $(a, b) \in \mathbb{Z}^2$, $D_a = D_b$ si et seulement si $a = b$ ou $a = -b$;

(iv) pour tout $a \in \mathbb{Z}^*$, D_a est fini et son plus grand élément est $|a|$.

Définition. Soit $(a, b) \in \mathbb{Z}^2$. On appelle diviseur commun de a et b tout élément de $D_a \cap D_b$.

Lemme et définition. Soit $(a, b) \in \mathbb{Z}^2$ deux entiers. Si l'un au moins des deux entiers a et b est non-nul, l'ensemble $D_a \cap D_b$ des diviseurs communs de a et b admet un plus grand élément (pour l'ordre usuel dans $\mathbb{Z}$), qui est un entier naturel. On l'appelle le plus grand commun diviseur de a et b et on le note $\mathrm{pgcd}(a, b)$.

Preuve. L'ensemble $D_a \cap D_b$ des diviseurs communs de a et b est une partie non-vide de $\mathbb{Z}$ (elle contient au moins 1) et fini (car d'après la remarque (iv), D_a ou D_b est fini puisque $a \neq 0$ ou $b \neq 0$). Il admet donc un plus grand élément, qui est un entier naturel. □

Remarque. Si $a = 0$ et $b \neq 0$, on a $D_a \cap D_b = D_b$ et donc $\mathrm{pgcd}(0, b) = |b|$; de même $\mathrm{pgcd}(a, 0) = |a|$ pour $a \neq 0$ et $b = 0$. On convient par ailleurs de poser $\mathrm{pgcd}(0, 0) = 0$.

On donne ci-dessous, grâce à la division euclidienne, un procédé pour déterminer les diviseurs communs de deux entiers, et en particulier leur pgcd. D'après la dernière remarque ci-dessus et la remarque (iii) précédente, on peut sans restriction se limiter à prendre a et b dans $\mathbb{N}^*$.

LEMME D'EUCLIDE. *Soient a et b deux entiers naturels tel que $b \neq 0$. Soit r le reste de la division euclidienne de a par b. Alors les diviseurs communs à a et b sont les diviseurs communs à b et r.*

En d'autres termes, $D_a \cap D_b = D_b \cap D_r$. Il en résulte en particulier que $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

Preuve. Soient q et r le quotient et le reste dans la division euclidienne de a par b. On a donc $a = bq + r$. Soit $d \in D_a \cap D_b$. Il existe n et m dans $\mathbb{Z}$ tel que $a = nd$ et $b = md$. Dans ce cas, $r = a - bq = (n - mq)d$, d'où $d \in D_r$, et donc $d \in D_b \cap D_r$. Réciproquement, soit $d \in D_b \cap D_r$. Il existe m et p dans $\mathbb{Z}$ tels que $b = md$ et $r = pd$. Dans ce cas, $a = bq + r = (mq + p)d$, d'où $d \in D_a$, et donc $d \in D_a \cap D_b$. □

THÉORÈME (ALGORITHME D'EUCLIDE). *Soit $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$.*

(i) il existe $k \in \mathbb{N}^*$, $(q_1, \ldots, q_k) \in \mathbb{N}^k$, et $(r_0, r_1, \ldots, r_k) \in \mathbb{N}^{k+1}$ uniques vérifiant
$$0 = r_k < r_{k-1} < r_{k-2} < \cdots < r_2 < r_1 < r_0 = b,$$
et les égalités:
$$\begin{aligned} a &= bq_1 + r_1 = r_0 q_1 + r_1, \\ r_0 &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\cdots\cdots\cdots \\ r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, \\ r_{k-2} &= r_{k-1} q_k + r_k = r_{k-1} q_k. \end{aligned}$$

(ii) $D_a \cap D_b = D_{r_{k-1}}$, et donc en particulier $\text{pgcd}(a,b) = r_{k-1}$.

Preuve. On effectue la division euclidienne de a par b. Notons $a = bq_1 + r_1$ avec $0 \leq r_1 < b$.
Si $r_1 = 0$, on arrête.
Si $r_1 \neq 0$, on effectue la division euclidienne de b par r_1. Notons $b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$.
Si $r_2 = 0$, on arrête.
Si $r_2 \neq 0$, on effectue la division euclidienne de r_1 par r_2. Notons $r_1 = r_2 q_3 + r_3$ avec $0 \leq r_3 < r_2$.
Si $r_3 = 0$, on arrête.
Si $r_3 \neq 0$, on effectue la division euclidienne de r_2 par r_3.
On itère ainsi le processus. Comme il n'existe pas de suite strictement décroissante dans $\mathbb{N}$, il existe un rang $k \in \mathbb{N}^*$ tel que $r_k = 0$. En notant $r_0 = b$ pour la cohérence des notations, ceci prouve l'existence dans le point (i). L'unicité est claire par unicité du quotient et du reste dans la division euclidienne.

Pour (ii), remarquons que le lemme d'Euclide appliqué dans la première égalité de (i) donne $D_a \cap D_b = D_b \cap D_{r_1} = D_{r_0} \cap D_{r_1}$. De même dans la deuxième égalité, on obtient $D_{r_0} \cap D_{r_1} = D_{r_1} \cap D_{r_2}$. Puis $D_{r_1} \cap D_{r_2} = D_{r_2} \cap D_{r_3}$, et par une récurrence évidente, $D_a \cap D_b = D_{r_{k-1}} \cap D_{r_k}$. Or puisque r_k est nul, $D_{r_{k-1}} \cap D_{r_k} = D_{r_{k-1}}$, ce qui achève la preuve. □

On traduit le point (ii) en disant que le pgcd de a et b est le dernier reste non-nul dans la suite des divisions successives de a par b.

Exemple. Soient $a = 33810$ et $b = 4116$. La suite des divisions successives donne:

$$\underbrace{33810}_{a} = \underbrace{4116}_{b=r_0} \times 8 + \underbrace{882}_{r_1} \quad ; \quad \underbrace{4116}_{r_0} = \underbrace{882}_{r_1} \times 4 + \underbrace{588}_{r_2} \quad ; \quad \underbrace{882}_{r_1} = \underbrace{588}_{r_2} \times 1 + \underbrace{294}_{r_3} \quad ; \quad \underbrace{588}_{r_2} = \underbrace{294}_{r_3} \times 2 + 0$$

On conclut que $\text{pgcd}(a,b) = r_3$ donc $\text{pgcd}(33810, 4116) = 294$.

COROLLAIRE (FONDAMENTAL). $D_a \cap D_b = D_{\text{pgcd}(a,b)}$.

REMARQUE. On verra plus loin une autre façon de présenter et définir le pgcd; il est tout à fait crucial de bien dominer l'équivalence de ces deux définitions (voir en particulier le paragraphe 2.1 de la leçon suivante).

3. D'autres applications

3.1 Applications liées aux congruences

Rappels. Soit $n \in \mathbb{N}$; deux entiers a et b sont dits congrus modulo n lorsqu'il existe $q \in \mathbb{Z}$ tel que $a - b = qn$. On note alors $a \equiv b\ [n]$. En d'autres termes: $a \equiv b\ [n] \Leftrightarrow a - b \in n\mathbb{Z}$.
La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$, compatible avec l'addition et la multiplication; l'ensemble quotient est noté $\mathbb{Z}/n\mathbb{Z}$.
Si $n = 0$, la congruence modulo 0 est l'égalité dans $\mathbb{Z}$ et $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$. Dans toute la suite, on prendra $n \in \mathbb{N}^*$.

Les applications que l'on va donner ici de la division euclidienne reposent toutes sur l'observation suivante.

Proposition (évidente mais importante). *Soit $n \in \mathbb{N}^*$.*

(i) *Tout entier a est congru modulo n au reste de la division euclidienne de a par n.*

(ii) *Deux entiers a et b sont congrus modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.*

(iii) *En particulier, si deux entiers a et r sont congrus modulo n et si $0 \leq r < n$, alors r est le reste de la division euclidienne par de a par n.*

Preuve. (i) est évident puisque $a = nq + r$ implique $a \equiv r\ [n]$. Pour (ii), notons $a = nq + r$ et $b = nq' + r'$ avec $0 \leq r < n$ et $0 \leq r' < n$. On a: $a \equiv b\ [n] \Leftrightarrow n(q - q') + (r - r') \in n\mathbb{Z} \Leftrightarrow r - r' \in n\mathbb{Z}$. Or comme $0 \leq r < n$ et $0 \leq r' < n$, on a: $r - r' \in n\mathbb{Z} \Leftrightarrow r = r'$. Le point (iii) découle directemment de (ii). □

Cette proposition a plusieurs conséquences importantes (parmi lesquelles les critères de divisibilité dits "de Pascal", et le fait que l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n) qui seront détaillées plus loin dans la leçon sur les anneaux $\mathbb{Z}/n\mathbb{Z}$.

3.2 Caractérisation des rationnels par la périodicité de leur développement décimal

(voir la leçon sur les nombres décimaux)

Leçon 2

$\mathbb{Z}$ comme anneau principal

Prérequis: on suppose connu l'anneau $\mathbb{Z}$ des entiers relatifs, et la division euclidienne dans $\mathbb{Z}$.

Rappel. Soit A un anneau commutatif. Soit I une partie non-vide de A. On dit que I est un idéal de A lorsque I est un sous-groupe additif de A (ie. $x-y \in I$ pour tous x et y dans I) vérifiant de plus la condition: $ax \in I$ pour tous $a \in A$ et $x \in I$. Si I et J sont deux idéaux de A, alors l'intersection $I \cap J$ et la somme $I+J = \{x+y\,;\, x \in I, y \in J\}$ sont des idéaux de A.

1. Divisibilité et idéaux dans $\mathbb{Z}$

1.1 Multiples et diviseurs.

Définition. Soit $(a,b) \in \mathbb{Z}^2$. On dit que a divise b, ou que a est un diviseur b, ou encore que b est multiple de a, lorsqu'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$.

Remarque. Par unicité du quotient et du reste dans la division euclidienne, dire que a divise b équivaut à dire que le reste de la division euclidienne de b par a est nul. □

Notation. Soit $a \in \mathbb{Z}$. On note $a\mathbb{Z}$ l'ensemble des multiples de a. Donc: $a\mathbb{Z} = \{ka\ ;\ k \in \mathbb{Z}\}$.
Soit $b \in \mathbb{Z}$. On note D_b l'ensemble des diviseurs de b. Donc: $D_b = \{a \in \mathbb{Z}\ ; \exists k \in \mathbb{Z},\ b = ka\}$.

Remarques. On a de façon évidente les propriétés suivantes:
- Pour tout $(a,b) \in \mathbb{Z}^2$, $b \in a\mathbb{Z}$ si et seulement si $a \in D_b$.
- $0\mathbb{Z} = \{0\}$ et $1\mathbb{Z} = \mathbb{Z}$. Il est clair que si $a \neq 0$, alors $a\mathbb{Z}$ est infini.
- $D_0 = \mathbb{Z}$ et $D_1 = \{-1, 1\}$. Il est clair que si $b \neq 0$, alors D_b est fini, majoré par $|b|$.

Proposition. *Soit $(a,b) \in \mathbb{Z}^2$. On a:*

(i) (a divise b) $\Leftrightarrow$ ($b \in a\mathbb{Z}$) $\Leftrightarrow$ ($b\mathbb{Z} \subset a\mathbb{Z}$) $\Leftrightarrow$ ($D_a \subset D_b$)

(ii) (a divise b et b divise a) $\Leftrightarrow$ ($b\mathbb{Z} = a\mathbb{Z}$) $\Leftrightarrow$ ($D_a = D_b$) $\Leftrightarrow$ ($a = b$ ou $a = -b$)

Preuve. Les équivalences du point (i) se déduisent directement des définitions précédentes. Pour le (ii), supposons d'abord que a divise b et b divise a. Il existe alors $(k,k') \in \mathbb{Z}^2$ tels que $a = kb$ et $b = k'a$, donc $(1-kk')a = 0$. Si $a = 0$, alors $b = k' \times 0 = 0$. Si $a \neq 0$, alors $kk' = 1$ par intégrité de $\mathbb{Z}$, donc $k = k' = \pm 1$ puisque les seuls inversibles de l'anneau $\mathbb{Z}$ sont 1 et -1, d'où finalement $a = \pm b$. Le reste de la preuve est clair. □

Remarque. Si a et b sont deux entiers naturels, on dit que a divise b dans $\mathbb{N}$ lorsqu'il existe un entier naturel k tel que $b = ka$. Dans ce cas, a est évidemment aussi un diviseur de b dans $\mathbb{Z}$. Il est clair que la relation "est un diviseur de" est une relation d'ordre dans $\mathbb{N}$, alors que, dans $\mathbb{Z}$, elle n'est pas antisymétrique (voir point (ii) de la proposition ci-dessus).

1.2 Sous-groupes et idéaux de l'anneau $\mathbb{Z}$.

Théorème. *Pour toute partie I de $\mathbb{Z}$, les conditions suivantes sont équivalentes:*

(i) *I est un idéal de l'anneau $\mathbb{Z}$;*

(ii) *I est un sous-groupe du groupe additif $\mathbb{Z}$;*

(iii) *il existe $a \in \mathbb{N}$ unique tel que $I = a\mathbb{Z}$;*

(iv) *il existe $a \in \mathbb{Z}$ tel que $I = a\mathbb{Z}$.*

Preuve. Supposons (iv). $I = a\mathbb{Z}$ n'est pas vide (il contient 0). Si x et y sont deux éléments quelconques de $I = a\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $x = ak$ et $k' \in \mathbb{Z}$ tel que $y = ak'$, donc $x - y = a(k-k')$, d'où $x - y \in I$; ce qui prouve que I est un sous-groupe additif de $\mathbb{Z}$. Soient maintenant $x = ak$ un élément quelconque de I, avec $k \in \mathbb{Z}$, et b un élément quelconque de $\mathbb{Z}$. On a $bx = b(ak) = a(kb)$, donc $bx \in I$. On conclut que $I = a\mathbb{Z}$ est un idéal de $\mathbb{Z}$. On a ainsi prouvé que (iv) implique (i). Il est clair que (i) implique (ii). Comme (iii) implique trivialement (iv), il reste seulement à montrer que (ii) implique (iii).

Pour cela, considérons I un sous-groupe de $\mathbb{Z}$. Si $I = \{0\}$, alors $I = 0\mathbb{Z}$. Sinon, I contient au moins un élément $y \neq 0$. Comme I est un sous-groupe additif, on a nécessairement $-y \in I$, de sorte que l'un des deux éléments y ou $-y$ est strictement positif. Donc $I \cap \mathbb{N}^*$ est non-vide. Parce que $\mathbb{N}$ est bien ordonné, on en déduit que $I \cap \mathbb{N}^*$ admet un plus petit élément. Notons-le a.

Vérifions que $a\mathbb{Z} \subseteq I$. Comme I est stable par l'addition et que $a \in I$, on a $a + a \in I$, et par récurrence $ka \in I$ pour tout entier $k > 0$. Comme I est stable par passage à l'opposé, on en déduit que $ka \in I$ pour tout entier $k < 0$. Comme enfin $0 \in I$, on conclut que I contient l'entier ka pour tout $k \in \mathbb{Z}$.

Vérifions que $I \subseteq a\mathbb{Z}$. Soit $x \in I$ quelconque. Comme $a \neq 0$, on peut effectuer la division euclidienne de x par a. Il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $x = aq + r$ et $0 \leq r < a$. L'entier $r = x - aq$ appartient à I, car $x \in I$, $aq \in a\mathbb{Z} \subseteq I$ d'après ce qui précède, et I est un sous-groupe additif. Puisque a est le plus petit élément de $I \cap \mathbb{N}^*$ et que $r \in I$ vérifie $0 \leq r < a$, on a forcément $r = 0$, et donc $x \in a\mathbb{Z}$. On a ainsi vérifié que $I = a\mathbb{Z}$. L'unicité de a découle du point (ii) de la proposition de 1.1. □

Remarque. Il est facile de vérifier que, pour tout anneau commutatif A et tout élément $a \in A$, la partie $aA = \{ax; x \in A\}$ est un idéal de A. Un tel idéal est dit principal. Un anneau A dont tous les idéaux sont principaux est dit anneau principal. Le théorème ci-dessus traduit donc que l'anneau $\mathbb{Z}$ est un anneau principal.

2. PGCD ET PPCM DE DEUX ENTIERS

2.1 Plus grand commun diviseur de deux entiers.

PROPOSITION ET DÉFINITION. *Pour tout $(a, b) \in \mathbb{Z}^2$, il existe un unique entier naturel d tel que $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$. On l'appelle le plus grand commun diviseur de a et b. On note $d = \text{pgcd}(a, b)$ ou $d = a \wedge b$.*

Preuve. Comme on l'a rappelé au début du chapitre, $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Donc d'après le point (iii) du théorème de 1.2, il existe $d \in \mathbb{N}$ unique tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. □

THÉORÈME. *Soit a et b deux entiers quelconques.*

(i) *L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de leur pgcd. En d'autres termes: $D_a \cap D_b = D_{\text{pgcd}(a,b)}$.*

(ii) *Le pgcd de a et b est le seul entier naturel vérifiant cette propriété.*

Preuve. Posons $d = \text{pgcd}(a, b)$. On a donc $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. En particulier $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$, c'est-à-dire $D_d \subset D_a$ et $D_d \subset D_b$, d'où $D_d \subset D_a \cap D_b$. Réciproquement, soit $c \in D_a \cap D_b$ quelconque. Donc $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$. Comme $c\mathbb{Z}$ est stable par addition, on en déduit que $a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$, c'est-à-dire $d\mathbb{Z} \subset c\mathbb{Z}$. En d'autres termes, $c \in D_d$. Ceci prouve l'inclusion $D_d \supset D_a \cap D_b$ et donc le point (i). Pour (ii), considérons un entier naturel x vérifiant $D_a \cap D_b = D_x$. D'après (i), on a donc $D_x = D_d$, d'où $x = \pm d$ (proposition 1.1), et finalement $x = d$ puisque x et d sont tous les deux positifs. □

REMARQUE FONDAMENTALE (justifiant la terminologie)

Si a ou b est non-nul, l'ensemble $D_a \cap D_b$ est fini, et il résulte du théorème ci-dessus que le pgcd de a et b est le plus grand élément de $D_a \cap D_b$ (pour l'ordre usuel des entiers).

On peut choisir comme définition du pgcd de deux entiers naturels non-nuls le plus grand élément de l'ensemble de leurs diviseurs communs (c'est ce que l'on fait dans l'enseignement secondaire). Mais le point crucial est alors de vérifier que le plus grand élément d de $D_a \cap D_b$ vérifie bien la propriété arithmétique fondamentale $D_a \cap D_b = D_d$; ceci utilise l'algorithme d'Euclide. On renvoie pour plus de détails au paragraphe 2.3 de la leçon sur la division euclidienne, où nous avons développé cette présentation alternative, afin d'avoir les deux points de vue.

Remarques. Il résulte immédiatement de la définition du pgcd que, pour tout $(a, b) \in \mathbb{Z}^2$, on a:

1. $\text{pgcd}(a, b) = \text{pgcd}(b, a)$.
2. $\text{pgcd}(a, b) = |a|$ si et seulement si a divise b.
3. $\text{pgcd}(a, 0) = |a|$ et $\text{pgcd}(a, 1) = 1$.
4. $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$,
   et donc on peut toujours se ramener à considérer le pgcd de deux entiers naturels.

EXERCICE. Montrer que, pour tous $(a, b, c) \in \mathbb{Z}^3$, on a:

$$\text{pgcd}(\text{pgcd}(a, b)\ ,\ c) = \text{pgcd}(a\ ,\ \text{pgcd}(b, c)) \quad \textit{et} \quad \text{pgcd}(ca, cb) = |c|\,\text{pgcd}(a, b).$$

2.2 Calcul du pgcd à l'aide de l'algorithme d'Euclide.

Comme on l'a vu aux remarques 3 et 4 de 2.1, on peut sans restriction supposer a et b dans $\mathbb{N}^*$.

LEMME D'EUCLIDE. *Soient a et b deux entiers naturels tel que $b \neq 0$. Soit r le reste de la division euclidienne de a par b. Alors* $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

Preuve. Soient q et r le quotient et le reste dans la division euclidienne de a par b. Il résulte de l'égalité $a = bq + r$ que $a \in b\mathbb{Z} + r\mathbb{Z}$; comme $b\mathbb{Z} + r\mathbb{Z}$ est un idéal, on en déduit que $ax \in b\mathbb{Z} + r\mathbb{Z}$ pour tout $x \in \mathbb{Z}$, c'est-à-dire $a\mathbb{Z} \subset b\mathbb{Z} + r\mathbb{Z}$. Comme par ailleurs $b\mathbb{Z} \subset b\mathbb{Z} + r\mathbb{Z}$, la stabilité de $b\mathbb{Z} + r\mathbb{Z}$ pour l'addition implique alors $a\mathbb{Z} + b\mathbb{Z} \subset b\mathbb{Z} + r\mathbb{Z}$. En écrivant ensuite $r = a - bq$, on montre de même que $b\mathbb{Z} + r\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. Finalement $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$, et donc $\text{pgcd}(a,b) = \text{pgcd}(b,r)$. □

Une variante de rédaction de la preuve. Soient q et r le quotient et le reste dans la division euclidienne de a par b. On a donc $a = bq + r$. Posons $d = \text{pgcd}(a,b)$ et $d' = \text{pgcd}(b,r)$. Comme $d \in D_a \cap D_b$, il existe des entiers n et m tels que $a = nd$ et $b = md$. On a alors $r = a - bq = nd - mdq = (n - mq)d$, d'où $d \in D_r$. Donc $d \in D_b \cap D_r$, ce qui d'après le théorème 2.1 implique que d divise d'. De même, comme $d' \in D_b \cap D_r$, il existe des entiers m et p tels que $b = md'$ et $r = pd'$. On a alors $a = bq + r = md'q + pd' = (mq + p)d'$, d'où $d' \in D_a$. Donc $d' \in D_a \cap D_b$, ce qui d'après le théorème 2.1 implique que d' divise d. Les deux entiers d et d' étant positifs, le fait que d divise d' et d' divise d implique $d = d'$. □

THÉORÈME (ALGORITHME D'EUCLIDE). *Soit $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$.*

(i) il existe $k \in \mathbb{N}^*$, $(q_1, \ldots, q_k) \in \mathbb{N}^k$, et $(r_0, r_1, \ldots, r_k) \in \mathbb{N}^{k+1}$ uniques vérifiant

$$0 = r_k < r_{k-1} < r_{k-2} < \cdots < r_2 < r_1 < r_0 = b,$$

et les égalités:

$$\begin{aligned}
a &= bq_1 + r_1 = r_0 q_1 + r_1,\\
r_0 &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\cdots\cdots\cdots\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1},\\
r_{k-2} &= r_{k-1} q_k + r_k = r_{k-1} q_k.
\end{aligned}$$

(ii) On a alors: $\text{pgcd}(a,b) = r_{k-1}$.

Preuve. On effectue la division euclidienne de a par b. Notons $a = bq_1 + r_1$ avec $0 \leq r_1 < b$.
Si $r_1 = 0$, on arrête.
Si $r_1 \neq 0$, on effectue la division euclidienne de b par r_1. Notons $b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$.
Si $r_2 = 0$, on arrête.
Si $r_2 \neq 0$, on effectue la division euclidienne de r_1 par r_2. Notons $r_1 = r_2 q_3 + r_3$ avec $0 \leq r_3 < r_2$.
Si $r_3 = 0$, on arrête.
Si $r_3 \neq 0$, on effectue la division euclidienne de r_2 par r_3.

On itère ainsi le processus. Comme il n'existe pas de suite strictement décroissante dans $\mathbb{N}$, il existe un rang $k \in \mathbb{N}^*$ tel que $r_k = 0$. En notant $r_0 = b$ pour la cohérence des notations, ceci prouve l'existence dans le point (i). L'unicité est claire d'après l'unicité du quotient et du reste dans la division euclidienne.

Pour (ii), remarquons que le lemme d'Euclide appliqué dans la première égalité de (i) donne $\text{pgcd}(a,b) = \text{pgcd}(b,r_1) = \text{pgcd}(r_0,r_1)$. De même dans la deuxième égalité, on obtient $\text{pgcd}(r_0,r_1) = \text{pgcd}(r_1,r_2)$. Puis $\text{pgcd}(r_1,r_2) = \text{pgcd}(r_2,r_3)$, et par une récurrence évidente, $\text{pgcd}(a,b) = \text{pgcd}(r_{k-1},r_k)$. Or puisque r_k est nul, $\text{pgcd}(r_{k-1},r_k) = r_{k-1}$, ce qui achève la preuve. □

On traduit le point (ii) en disant que le pgcd de a et b est le dernier reste non-nul dans la suite des divisions successives de a par b.

Exemple. Soient $a = 33810$ et $b = 4116$. La suite des divisions successives donne:

$$\underbrace{33810}_{a} = \underbrace{4116}_{b=r_0} \times 8 + \underbrace{882}_{r_1} \quad ; \quad \underbrace{4116}_{r_0} = \underbrace{882}_{r_1} \times 4 + \underbrace{588}_{r_2} \quad ; \quad \underbrace{882}_{r_1} = \underbrace{588}_{r_2} \times 1 + \underbrace{294}_{r_3} \quad ; \quad \underbrace{588}_{r_2} = \underbrace{294}_{r_3} \times 2 + 0$$

On conclut que $\text{pgcd}(a,b) = r_3$ donc $\text{pgcd}(33810, 4116) = 294$.

Remarques.

(i) L'algorithme d'Euclide permet non seulement de calculer $d = \text{pgcd}(a,b)$ mais aussi, en remontant les calculs dans la suite des divisions successives, de déterminer un couple (u,v) d'entiers tel que $d = au + bv$, apparaissant ainsi effectivement comme un élément de $a\mathbb{Z} + b\mathbb{Z}$.

Par exemple, en reprenant l'exemple ci-dessus, on a:

$d = 294 = 882 - 588 = 882 + (4 \times 882) - 4116 = 5 \times (33810 - 8 \times 4116) - 4116 = 5 \times 33810 - 41 \times 4116.$

Comme on le verra plus loin, c'est un point crucial pour une bonne compréhension du théorème de Bézout et la résolution de certaines équations diophantiennes.

(ii) Nous avions déja donné dans la leçon sur la division euclidienne une présentation de l'algorithme d'Euclide adaptée à la définition du pgcd comme plus grand élément de l'ensemble des diviseurs communs de deux entiers non-nuls. La rédaction légèrement modifiée que nous avons détaillée ci-dessus est plus adaptée à la définition du pgcd comme unique générateur positif de l'idéal somme.

(iii) On verra dans la leçon sur les nombres premiers une méthode de calcul du pgcd de deux entiers utilisant la décomposition en facteurs premiers. Ce sera donc une méthode reposant, non pas sur le caractère euclidien de l'anneau $\mathbb{Z}$, mais sur son caractère factoriel.

2.3 Entiers premiers entre eux.

Définition. Deux entiers a et b sont dits premiers entre eux lorsque leur pgcd est égal à 1.

En d'autres termes, d'après le théorème 2.1, a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1.

PROPOSITION. *Soient a et b deux entiers non tous les deux nuls, et d leur pgcd. Alors $d \neq 0$, et les entiers uniques a' et b' définis par $a = da'$ et $b = db'$ sont premiers entres eux.*

Preuve. Si on avait $d = 0$, alors on aurait $a\mathbb{Z} + b\mathbb{Z} = \{0\}$, ce qui contredirait $(a, b) \neq (0, 0)$. Donc $d \neq 0$. Il existe donc $(a', b') \in \mathbb{Z}^2$ unique tel que $a = da'$ et $b = db'$. Il en résulte que, pour tout diviseur commun c de a' et b', l'entier cd est un diviseur commun de a et b, donc un diviseur de d d'après le théorème 2.1, d'où $c = \pm 1$. On conclut que $\text{pgcd}(a', b') = 1$. (On peut aussi appliquer le second point de la dernière proposition de 2.1). □

THÉORÈME DE BÉZOUT. *Deux entiers a et b sont premiers entre eux si et seulement s'il existe (au moins) un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.*

Preuve. Posons $d = \text{pgcd}(a, b)$; on a donc $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$. Si $d = 1$, il en résulte que $1 \in a\mathbb{Z}+b\mathbb{Z}$, et donc il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Supposons réciproquement qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$; alors 1 appartient à $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc d divise 1, d'où $d = 1$. □

Remarques.

(i) Attention, pour $d \neq 0$, l'existence d'un couple (u, v) tel que $au + bv = d$ n'implique pas que d est le pgcd de a et b. Par exemple $3 \times 10 + (-2) \times 14 = 2$, mais 2 n'est pas le pgcd de 3 et -2.

(ii) Attention, dans le théorème de Bézout, il n'y a pas unicité du couple (u, v); on verra au corollaire 3.3 comment déterminer tous les couples (u, v) solutions.

THÉORÈME DE GAUSS. *Soient a, b, c trois entiers. Si a divise bc, et si a et b sont premiers entre eux, alors a divise c.*

Preuve. Comme $\text{pgcd}(a, b) = 1$, il existe d'après le théorème de Bézout un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Donc $c = cau + cbv$. Comme a divise bc, on a $bc \in a\mathbb{Z}$, donc $bcv \in a\mathbb{Z}$. Par ailleurs il est clair que $acu \in a\mathbb{Z}$. Par stabilité de l'idéal $a\mathbb{Z}$ pour l'addition, on conclut que $c = acu + bcv \in a\mathbb{Z}$. Ce qui achève la preuve. □

PROPOSITION. (Une autre application du théorème de Bézout) *Soient a, b, c trois entiers;*

(i) *a et bc sont premiers entre eux si et seulement si a et b sont premiers entre eux, et a et c sont premiers entre eux;*

(ii) *si a divise c et b divise c, et si a et b sont premiers entre eux, alors ab divise c.*

Preuve. Laissée au lecteur à titre d'exercice. □

2.4 Plus petit commun multiple de deux entiers.

PROPOSITION ET DÉFINITION. *Pour tout $(a, b) \in \mathbb{Z}^2$, il existe un unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On l'appelle le plus petit commun multiple de a et b. On note $m = \text{ppcm}(a, b)$ ou $m = a \vee b$.*

Preuve. Comme on l'a rappelé au début de ce chapitre, $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Donc d'après le pont (ii) du théorème de 1.2, il existe $m \in \mathbb{N}$ unique tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. □

Remarque. Par définition, l'ensemble des multiples communs à a et b est égal à l'ensemble des multiples de leur ppcm. Il résulte immédiatement du point (ii) du lemme 1.1 que le ppcm de a et b est le seul entier naturel vérifiant cette propriété. Si a ou b est non-nul, c'est aussi le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$, ce qui justifie la terminologie.

Remarques. Il résulte de la définition précédente que, pour tout $(a, b) \in \mathbb{Z}^2$, on a:

1. $\text{ppcm}(a, b) = \text{ppcm}(b, a)$.
2. $\text{ppcm}(a, b) = |a|$ si et seulement si b divise a.
3. $\text{ppcm}(a, 0) = 0$ et $\text{ppcm}(a, 1) = |a|$.
4. $\text{ppcm}(a, b) = \text{ppcm}(|a|, |b|)$,
   et donc on peut toujours se ramener à considérer le ppcm de deux entiers naturels.

EXERCICE. Montrer que, pour tous $(a, b, c) \in \mathbb{Z}^3$, on a:
$$\text{ppcm}(\text{ppcm}(a, b)\,,\, c) = \text{ppcm}(a\,,\, \text{ppcm}(b, c)) \quad \textit{et} \quad \text{ppcm}(ca, cb) = |c|\,\text{ppcm}(a, b).$$

2.5 Relations entre pgcd et ppcm.

Lemme préliminaire. Si a et b sont deux entiers premiers entre eux, alors $\text{ppcm}(a, b) = |ab|$.

Preuve. Notons $m = \text{ppcm}(a, b)$; il existe donc $(r, q) \in \mathbb{Z}^2$ tels que $m = ar = bq$. Ainsi a divise bq en étant premier avec b, donc d'après le théorème de Gauss, il existe $u \in \mathbb{Z}$ tel que $q = ua$. Mais alors $m = bq = abu$ est un multiple de ab. Comme par ailleurs ab est toujours un multiple de m en tant que mutiple commun de a et b, il résulte du point (ii) de la proposition 1.1 que $m = \pm ab$. Comme m est positif, on conclut que $m = |ab|$. □

THÉORÈME. *Soient a et b deux entiers quelconques. On a:* $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$

Preuve. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$. D'après la première proposition de 2.3, il existe des entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$. D'après le second point de l'exercice de 2.4, on a alors $\text{ppcm}(a, b) = d\,\text{ppcm}(a', b')$. Mais d'après le lemme ci-dessus, $\text{ppcm}(a', b') = |a'b'|$. Donc $m = d|a'b'|$, d'où $md = |da'db'| = |ab|$. □

Remarque. Ainsi, il suffit de savoir calculer le pgcd de deux entiers pour connaître leur ppcm, et réciproquement. Mais attention, bien que l'on puisse naturellement définir le pgcd et le ppcm d'un nombre quelconque d'entiers, la relation du théorème ci-dessus n'est vraie que dans le cas de deux entiers.

Exemple. Si a, b, c sont trois entiers, leur pgcd d et leur ppcm m sont respectivement définis par $a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z} = m\mathbb{Z}$, mais on n'a pas forcément $dm = abc$. Par exemple, pour $a = 6$, $b = 15$, $c = 10$, on a $d = 1$ et $m = 30$, alors que $abc = 900$. On pourra vérifier que l'on en fait la relation plus complexe:
$$\text{ppcm}(a, b, c) = \frac{abc\,\text{pgcd}(a, b, c)}{\text{pgcd}(a, b)\,\text{pgcd}(b, c)\,\text{pgcd}(c, a)}$$

Exercice. Montrer que, pour tout $(a, b, c) \in \mathbb{Z}^3$, on a: (1) $\text{pgcd}(a, \text{ppcm}(a, b)) = \text{ppcm}(a, \text{pgcd}(a, b)) = a$,
(2) $\text{pgcd}(a, \text{ppcm}(b, c)) = \text{ppcm}(\text{pgcd}(a, b), \text{pgcd}(a, c))$, (3) $\text{ppcm}(a, \text{pgcd}(b, c)) = \text{pgcd}(\text{ppcm}(a, b), \text{ppcm}(a, c))$.

2.6 Premières applications.

(i) Au niveau élémentaire, une application importante des pgcd et ppcm est le calcul des fractions.

La première proposition de 2.3 permet d'exprimer toute fraction $\frac{a}{b}$ sous forme irréductible $\frac{a'}{b'}$, avec a' et b' premiers entre eux, après simplification par $d = \text{pgcd}(a, b)$. Le ppcm des dénominateurs de deux fractions est un dénominateur commun minimal permettant d'effectuer la somme de ces deux fractions.

(ii) On verra dans la leçon sur les anneaux quotients $\mathbb{Z}/n\mathbb{Z}$ l'importance de la recherche des entiers premiers avec un entier non-nul donné.

Cependant, l'application principale développée dans cette leçon est la résolution en nombres entiers de certaines équations, qui fait l'objet de la partie suivante.

3. Equations diophantiennes de la forme $ax + by = c$.

3.1 Données et notations.

On fixe trois entiers α, β, γ. On suppose $\alpha \neq 0$ et $\beta \neq 0$. On considère l'équation:

$$\alpha x + \beta y = \gamma. \qquad (1)$$

On pose $d = \text{pgcd}(\alpha, \beta)$. On a: $d \in \mathbb{N}^*$. D'après le lemme de 2.3, il existe deux entiers a et b non-nuls et premiers entre eux tels que $\alpha = ad$ et $\beta = bd$. On considère l'équation:

$$ax + by = 1. \qquad (2)$$

Le problème est de déterminer l'ensemble des solutions dans $\mathbb{Z}^2$ de l'équation (1).

Remarque. On exclut dès le départ de notre étude le cas où l'un au moins des coefficients α et β est nul; la résolution dans $\mathbb{Z}^2$ de l'équation (1) est alors évidente et laissée au lecteur.

Interprétation graphique. Déterminer l'ensemble des solutions dans $\mathbb{Z}^2$ de l'équation (1) équivaut à rechercher dans le plan réel les points à coefficients entiers par lesquels passe la droite d'équation (1).

3.2 Théorème.

Avec les donnés et hypothèses ci-dessus, on a:

(i) *L'équation* (2) *admet toujours des solutions dans* $\mathbb{Z}^2$.

(ii) *L'équation* (1) *admet des solutions dans* $\mathbb{Z}^2$ *si et seulement si* d *divise* γ.

(iii) *Si l'on suppose que* d *divise* γ *et si on pose* $\gamma = dc$ *avec* $c \in \mathbb{Z}$, *alors l'ensemble des solutions dans* $\mathbb{Z}^2$ *de l'équation* (1) *est égal à l'ensemble des solutions dans* $\mathbb{Z}^2$ *de l'équation:*

$$ax + by = c, \qquad (1')$$

et est égal à l'ensemble de tous les couples $(x, y) \in \mathbb{Z}^2$ *de la forme:*

$$(x, y) = c(u, v) + \lambda(-b, a),$$

où (u, v) *est une solution de l'équation* (2) *et* $\lambda \in \mathbb{Z}$ *quelconque.*

Preuve. Puisque a et b sont premiers entre eux, le point (i) résulte du théorème de Bézout. Pour le point (ii), observons que l'existence d'un couple $(x, y) \in \mathbb{Z}^2$ tel que $\gamma = \alpha x + \beta y$ équivaut à la condition $\gamma \in \alpha\mathbb{Z} + \beta\mathbb{Z}$. Or $\alpha\mathbb{Z} + \beta\mathbb{Z} = d\mathbb{Z}$ par définition de d, et donc (1) admet (au moins) une solution dans $\mathbb{Z}^2$ si et seulement si $\gamma \in d\mathbb{Z}$, ce qui prouve (ii).

Pour montrer (iii), on suppose désormais que $\gamma = cd$. L'équivalence de (1) et (1') est claire. Soit (u, v) une solution quelconque de (2) et λ un entier quelconque. Posons $(x, y) = c(u, v) + \lambda(-b, a)$. On a alors: $ax + by = acu - a\lambda b + bcv + b\lambda a = c(au + bv) = c$. Donc (x, y) est une solution de (1') dans $\mathbb{Z}^2$. Le problème est de montrer que toute solution de (1') est de ce type.

Soit (x, y) une solution de (1'). Pour toute solution (u, v) de (2), on a: $ax + by = c = c(au + bv)$, d'où $a(cu - x) = b(y - cv)$. Comme a et b sont premiers entre eux, il résulte du théorème de Gauss que a divise $y - cv$. Il existe donc $\lambda \in \mathbb{Z}$ tel que $y - cv = \lambda a$. On a alors: $\lambda ab = b(y - cv) = a(cu - x)$. Comme $a \neq 0$, on déduit que $cu - x = \lambda b$. On a bien obtenu $x = cu - \lambda b$ et $y = cv + \lambda a$. □

3.3 Corollaire. (Une précision importante sur le théorème de Bézout)

Soient a *et* b *deux entiers premiers entre eux. Pour tout couple* $(u, v) \in \mathbb{Z}^2$ *tel que* $au + bv = 1$, *l'ensemble de tous les couples* $(x, y) \in \mathbb{Z}^2$ *tels que* $ax + by = 1$ *est égal à* $\{(u, v) + \lambda(-b, a)\,;\, \lambda \in \mathbb{Z}\}$.

3.4 Remarques, exemples, compléments.

(i) Comme on l'a déjà observé à la remarque (i) de 2.2, l'algorithme d'Euclide permet de trouver une solution de (2), et donc d'après le théorème 3.2, toutes les solutions de (1).

(ii) Illustrons la méthode par un exemple.

Exemple. Considérons l'équation: $198198x + 87856y = 194 \qquad (1)$

Posons $\alpha = 198198$, $\beta = 87856$, $\gamma = 194$. Ces trois entiers sont divisibles par 2. Donc l'équation (1) équivaut à:

$$99099x + 43928y = 97 \qquad (1')$$

On va montrer que $d = 2$ est en fait le pgcd de α et β, c'est-à-dire que les entiers $a = 99099$ et $b = 43928$ sont premiers entre eux. On utilise pour cela l'algorithme d'Euclide.

$$\begin{array}{lcl}
\underbrace{99099}_{a} = \underbrace{43928}_{b}\times 2 + \underbrace{11243}_{r_1} & & r_1 = a - 2b \\
\underbrace{43928}_{b} = \underbrace{11243}_{r_1}\times 3 + \underbrace{10199}_{r_2} & & r_2 = b - 3r_1 = -3a + 7b \\
\underbrace{11243}_{r_1} = \underbrace{10199}_{r_2}\times 1 + \underbrace{1044}_{r_3} & & r_3 = r_1 - r_2 = 4a - 9b \\
\underbrace{10199}_{r_2} = \underbrace{1044}_{r_3}\times 9 + \underbrace{803}_{r_4} & & r_4 = r_2 - 9r_3 = -39a + 88b \\
\underbrace{1044}_{r_3} = \underbrace{803}_{r_4}\times 1 + \underbrace{241}_{r_5} & & r_5 = r_3 - r_4 = 43a - 97b \\
\underbrace{803}_{r_4} = \underbrace{241}_{r_5}\times 3 + \underbrace{80}_{r_6} & & r_6 = r_4 - 3r_5 = -168a + 379b \\
\underbrace{241}_{r_5} = \underbrace{80}_{r_6}\times 3 + \underbrace{1}_{r_7} & & r_7 = r_5 - 3r_6 = 547a - 1234b
\end{array}$$

Ceci prouve, d'une part que $\text{pgcd}(a, b) = 1$ comme on l'avait annoncé, d'autre part que $547a - 1234b = 1$. Donc $(u, v) = (547, -1234)$ est une solution de l'équation:

$$99099x + 43928y = 1 \qquad (2)$$

Donc l'ensemble des solutions entières de (2) est: $S_2 = \{(547 - 43928\lambda, -1234 + 99099\lambda)\,;\, \lambda \in \mathbb{Z}\}$.

En calculant $97 \times 547 = 53059$ et $97 \times 1234 = 119698$, on conclut que l'ensemble des solutions entières de (1) est:

$$S_1 = \{(53059 - 43928\lambda, -119698 + 99099\lambda)\,;\, \lambda \in \mathbb{Z}\}.$$

Une autre expression de cet ensemble est par exemple: $S_1 = \{(9131 - 43928\mu, -20599 + 99099\mu)\,;\, \mu \in \mathbb{Z}\}$

(iii) Le lemme ci-dessous, parfois appelé théorème de Bézout dans $\mathbb{N}$, donne des conditions suffisantes pour l'existence d'un couple (u, v) unique, satisfaisant certaines propriétés supplémentaires, dans le théorème de Bézout et le corollaire 3.3.

LEMME. *Soient a et b deux entiers strictement supérieurs à 1. On suppose a et b premiers entre eux. Il existe alors un unique couple (u, v) d'entiers naturels tels que:*

$$au - bv = 1, \qquad 0 < u < b, \qquad 0 < v < a.$$

Preuve. Soit $S = \{(x, y) \in \mathbb{Z}^2\,;\, ax + by = 1\}$. D'après le théorème de Bézout, $S \neq \emptyset$. Fixons donc un couple (x, y) quelconque dans S. Soit (q, r) le couple d'entiers tels que $x = bq + r$ avec $0 \leq r < b$. On a donc $r = x - bq$. Posons par ailleurs $s = y + qa$. On a $(r, s) = (x, y) + q(-b, a)$, de sorte que $(r, s) \in S$. Si l'on avait $r = 0$, on aurait $bs = ar + bs = 1$, ce qui contredirait l'hypothèse $b > 1$. C'est donc que $0 < r < b$. Il en résulte que $-bs = ar - 1$ vérifie $ar - 1 \geq 2 \times 1 - 1 > 0$ et $ar - 1 \leq a(b - 1) - 1 < ab$, et donc $0 < -s < a$. En posant $u = r$ et $v = -s$, le couple (u, v) vérifie: $0 < u < b$, $0 < v < a$ et $au - bv = 1$.

Pour l'unicité, supposons qu'il existe un autre couple $(u', v') \in S$ d'entiers tels que $0 < u' < b$ et $0 < v' < a$. D'après le corollaire 3.3, il existe un entier λ tel que $(u', v') = (u, v) + (-\lambda b, \lambda a)$. Ceci implique en particulier que $|u' - u| = |\lambda| b$. Mais $0 \leq |u' - u| < b$ puisque $0 < u < b$ et $0 < u' < b$. D'où $0 \leq |\lambda| b < b$, donc $\lambda = 0$, et donc $(u', v') = (u, v)$. □

Leçon 3

$\mathbb{Z}$ comme anneau factoriel

Prérequis: L'arithmétique dans $\mathbb{Z}$ développée dans les deux précédentes leçons, plus quelques rudiments sur les congruences pour les applications de la section 3.

1. Notion de nombre premier.

1.1 Définition.

On appelle nombre premier tout entier p supérieur ou égal à 2 tel que les seuls entiers naturels divisant p soient 1 et p.

Exemples. 2 est le seul nombre premier pair; 3,5,7,11,13 sont premiers.
Attention: 0 et 1 ne sont pas premiers.

Remarque terminologique. Un entier n est dit premier s'il possède dans $\mathbb{Z}$ exactement quatre diviseurs: $1, -1, n, -n$, deux à deux distincts. Le terme de nombre premier signifie donc entier naturel premier, et il est clair qu'un entier est premier si et seulement si sa valeur absolue est un nombre premier.

1.2 Premières propriétés.

Proposition.

(i) *Tout entier différent de 1 et de -1 admet au moins un diviseur premier.*

(ii) *Tout entier n supérieur ou égal à 2 qui n'est pas un nombre premier admet au moins un diviseur premier p tel que $p^2 \leq n$.*

Preuve. Il est clair qu'il suffit de prouver (i) pour un entier naturel n supérieur ou égal à 2. Notons $D(n)$ l'ensemble des diviseurs de n supérieurs ou égaux à 2. Il est non-vide car il contient n. Comme $\mathbb{N}$ est bien ordonné, $D(n)$ admet un plus petit élément p. C'est un diviseur de n, supérieur à 2; montrons qu'il est premier. Pour cela, considérons un entier naturel a divisant p. Par transitivité de la divisibilité, a divise n. Si $a \geq 2$, alors $a \in D(n)$, donc $p \leq a$ par minimalité de p; ainsi a divise p et $p \leq a$, donc $a = p$. Sinon, $a = 1$. Ceci prouve (i).

De plus, il existe $k \in \mathbb{N}$ tel que $n = kp$. Supposons que n n'est pas premier. Donc $k \neq 1$, c'est-à-dire $k \geq 2$. Ainsi $k \in D(n)$, ce qui implique $p \leq k$. On obtient $n = kp \geq p^2$, ce qui prouve (ii). □

1.3 Ensemble des nombres premiers.

Théorème. *Le sous-ensemble de $\mathbb{N}$ formé des nombres premiers est infini.*

Preuve. Par l'absurde, supposons que l'ensemble des nombres premiers soit fini. Notons alors N le produit de tous les nombres premiers. C'est un entier supérieur à 2. L'entier $N + 1$ est un entier supérieur à 3; d'après la proposition 1.2 ci-dessus, il admet un diviseur premier p. Celui-ci apparaissant comme un des facteurs du produit N, on a à la fois p qui divise $N+1$ et p qui divise N, ce qui implique de façon simple que p divise 1. Ce qui contredit le fait que p est premier. □

Notations. On note $\mathcal{P}$ l'ensemble des nombres premiers. Comme c'est un ensemble infini dénombrable (sous-ensemble infini de $\mathbb{N}$), on peut aussi noter ses éléments sous forme d'une suite $(p_n)_{n\geq 1}$, où p_n désigne le n-ième nombre premier, avec donc $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11 \ldots$.

Remarque. La proposition ci-dessous donne une autre preuve du fait que l'ensemble des nombres premiers est infini. Elle est constituée de deux cas très particuliers et faciles d'un théorème profond de Dirichlet selon lequel il existe une infinité de nombres premiers de la forme $an + b$ dès lors que a et b sont premiers entre eux.

Proposition. *Il existe une infinité de nombres premiers de la forme $4n + 3$ avec $n \in \mathbb{N}$, et une infinité de nombre premiers de la forme $6m + 5$, avec $m \in \mathbb{N}$.*

Preuve. On ne démontre que le premier point, la preuve du second étant analogue et laissée au lecteur. Notons E l'ensemble des nombres premiers de la forme $4n + 3$ avec $n \in \mathbb{N}$. Il est non-vide, car par exemple 3 ou 7 sont dans E. Par l'absurde, supposons que E soit fini. Appelons N le produit de tous les éléments de E et posons $a = 4N - 1$. Soit p un diviseur premier de a. Il est de la forme $4n$ ou $4n + 1$ ou $4n + 2$ ou $4n + 3$, avec $n \in \mathbb{N}$.

Mais p étant premier, les cas $4n$ ou $4n+2$ sont impossibles (notons qu'on ne peut pas avoir $p=2$ puisque a est impair). Si p était du type $4n+3$, il appartiendrait à E, donc diviserait N, donc diviserait $4N$, et comme p divise $a=4N-1$, on obtiendrait que p divise 1, ce qui est impossible. En résumé, tout diviseur premier de a est de la forme $4n+1$. Il en résulte que tout diviseur de a est de cette forme. En particulier il existe $q\in\mathbb{N}$ tel que $a=4q+1$. Mais l'égalité $4q+1=4N-1$ est absurde. C'est donc que E est infini. □

1.4 Un algorithme pour déterminer si un entier naturel est ou non premier.

Soit $n\geq 3$ un entier. Pour tout entier $i\geq 1$, considérons la division euclidienne de n par le i-ème nombre premier p_i:

$$n=p_iq_i+r_i,\quad q_i\in\mathbb{N},\ 0\leq r_i<p_i.$$

Comme $n\geq p_iq_i$ pour tout $i\geq 1$ et comme la suite des p_i est strictement croissante, il existe un plus petit entier $k\geq 1$ tel que $p_j>q_j$ pour tout $j\geq k$.

• S'il existe un entier $i\leq k-1$ tel que $r_i=0$, alors n n'est pas premier (en effet, on a alors $n=p_iq_i$ et $q_i\neq 1$ puisque $q_i\geq p_i$ du fait que $i\leq k-1$).

• Sinon, n n'est divisible par aucun des nombres premiers $p_1,\ldots,p_{k-1}$. Si n n'était pas premier, il existerait d'après la proposition 4 de 1.2 un nombre premier p divisant n et tel que $p^2\leq n$. L'entier q tel que $n=pq$ vérifierait $p\leq q$, donc p serait l'un des p_i pour $1\leq i\leq k-1$; contradiction. C'est donc que n est premier.

Concrètement: on effectue les divisions euclidiennes de n par les p_i jusqu'à ce que $p_i>q_i$; si l'un des restes s'annule, n n'est pas premier. Sinon, n est premier.

EXEMPLE: considérons $n=127$. On effectue les divisions euclidiennes successives: $127=2\times 63+1$, $127=3\times 42+1$, $127=5\times 25+1$, $127=7\times 18+1$, $127=11\times 11+6$, $127=13\times 9+10$. Comme $p_6=13>q_6=9$, on s'arrête. Aucun reste n'étant nul, on conclut que 127 est premier.

1.5 Un algorithme pour déterminer les nombres premiers inférieurs à un entier naturel donné.

PROPOSITION. *Pour tout $k\in\mathbb{N}^*$, le $(k+1)$-ième nombre premier p_k est:*

$$p_{k+1}=\mathrm{Min}\Big(\mathbb{N}\setminus(\{0,1\}\cup p_1\mathbb{N}\cup p_2\mathbb{N}\cup\ldots\cup p_k\mathbb{N})\Big).$$

Preuve. Notons $A_k=\mathbb{N}\setminus(\{0,1\}\cup p_1\mathbb{N}\cup p_2\mathbb{N}\cup\ldots\cup p_k\mathbb{N})$. Il est clair que $p_{k+1}\in A_k$. Comme $A_k\neq\emptyset$, il admet un plus petit élément a_k. D'après la proposition 3 de 1.2, il existe un nombre premier p qui divise a_k. Comme $a_k\in A_k$, on a $p\notin\{p_1,p_2,\ldots,p_k\}$. On en déduit que $p_{k+1}\leq p\leq a_k$. Mais par ailleurs $a_k\leq p_{k+1}$ puisque $p_{k+1}\in A_k$. On conclut que $a_k=p=p_{k+1}$. □

Algorithme (dit "crible d'Eratosthène").

Soit n un entier, $n\geq 2$. Notons p_j le plus grand des nombres premiers vérifiant $p_j^2\leq n$. On dresse la liste des entiers de $[\![2,n]\!]$.

• étape 1: on barre tous les éléments de $[\![2,n]\!]$ qui sont des multiples stricts de $p_1=2$ (ie. des multiples de p_1 strictement supérieurs à p_1). D'après la proposition, le premier élément non barré après p_1 est $p_2=3$.

• étape 2: on barre ensuite tous les éléments de $[\![2,n]\!]$ qui sont des multiples stricts de p_2. D'après la proposition, le premier élément non barré après p_2 est $p_3=5$.

...

• étape j: on barre enfin tous les éléments de $[\![2,n]\!]$ qui sont des multiples stricts de p_j.

Affirmation: les entiers de $[\![2,n]\!]$ qui restent non-barrés sont les nombres premiers inférieurs à n.

En effet. Soit $m\in[\![2,n]\!]$ non premier. Il existe un nombre premier p_i et un entier $q\geq 2$ tels que $m=p_iq$. Ou bien $i\leq j$, c'est-à-dire $p_i\leq p_j$, de sorte que m a été barré à l'étape i. Ou bien $i>j$, c'est-à-dire $p_i>p_j$; on a alors $q<p_j$ (car sinon $q\geq p_j$ impliquerait $m=p_iq\geq p_ip_j>p_j^2\geq n$) de sorte que tout diviseur premier de q est de la forme p_k pour $k<j$ et donc $m=p_iq$ est un multiple strict de p_k, qui a été barré à l'étape k. □

Exemple. On détermine les nombres premiers inférieurs ou égaux à $n=60$, en barrant successivement les multiples stricts et inférieurs à 60 de $p_1=2$, $p_2=3$, $p_3=5$ et $p_4=7$ (plus grand nombre premier de carré inférieur à 60); les entiers restant non barrés sont ceux qui sont encadrés ci-dessous:

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

2. Décomposition en produit de facteurs premiers.

Le but de cette partie est de démontrer l'existence et l'unicité de la décomposition d'un entier en produit de facteurs premiers, et d'en indiquer quelques applications. La preuve de l'existence d'une telle décomposition est à peu près évidente à partir de la proposition 1.2. La preuve de l'unicité est un peu plus délicate, et utilise le résultat de la proposition 2.1 suivante.

2.1 Résultats préliminaires.

Lemme. *Un nombre premier est premier avec tout entier qu'il ne divise pas.*

Preuve. Soit p un nombre premier. Soient a un entier non divisible par p et d le pgcd de a et p. Comme d divise p, on ne peut avoir que $d = p$ ou $d = 1$. Comme d divise a et que p ne divise pas a par hypothèse, d ne peut pas valoir p . C'est donc que $d = 1$. □

Conséquences. Deux nombres premiers distincts sont premiers entre eux. Tout nombre premier est premier avec tout entier naturel non-nul qui lui est strictement inférieur.

Proposition.

(i) *Si un nombre premier divise un produit d'entiers, alors il divise l'un des facteurs de ce produit.*

(ii) *Si un nombre premier divise un produit de nombres premiers, alors il est égal à l'un d'entres eux.*

Preuve. Soit p un nombre premier. Supposons que p divise le produit bc de deux entiers b et c. Supposons que p ne divise pas b. Alors, d'après le lemme, p est premier avec b. Ce qui, d'après le théorème de Gauss, implique que p divise c. Ceci prouve (i). Le point (ii) s'en déduit immédiatement. □

2.2 Le résultat fondamental.

Théorème. *Soit n un entier supérieur ou égal à 2. Il existe, et ceci de façon unique, un entier $s \geq 1$, des nombres premiers $p_1, p_2, \ldots, p_s$ vérifiant que $p_1 < p_2 < \cdots < p_s$, et des entiers naturels non-nuls $\alpha_1, \alpha_2, \ldots, \alpha_s$ tels que:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}.$$

Preuve. Montrons l'existence d'une telle décomposition par récurrence sur n. C'est clair si $n = 2$. Supposons-la vraie pour tout entier strictement inférieur à n. Soit p un diviseur premier de n. Si $n = p$, il n'y a rien à démontrer. Sinon, il existe $2 \leq n_0 \leq n-1$ tel que que $n = pn_0$. En appliquant l'hypothèse de récurrence à n_0, on a $n = pp_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$. S'il existe $1 \leq j \leq s$ tel que $p = p_j$, alors $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_j^{\alpha_j+1} \ldots p_s^{\alpha_s}$, d'où le résultat. Sinon, on obtient une décomposition du type voulu (en ordonnant p relativement aux p_i), avec $s+1$ facteurs, et un exposant 1 pour le facteur p.

Montrons l'unicité. Supposons pour cela que $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$, avec $s \in \mathbb{N}^*$, $p_1 < p_2 < \cdots < p_s$ premiers, $\alpha_i \in \mathbb{N}^*$ pour tout $1 \leq i \leq s$, et $t \in \mathbb{N}^*$, $q_1 < q_2 < \cdots < q_t$ premiers, $\beta_j \in \mathbb{N}^*$ pour tout $1 \leq j \leq t$. D'après le point (ii) de la proposition 2.1, chaque p_i $(1 \leq i \leq s)$ est égal à un des q_j $(1 \leq j \leq t)$, et chaque q_j est égal à l'un des p_i. Comme les p_i sont à deux distincts, ainsi que les q_j, on a nécessairement $s = t$. De plus la condition de croissance sur les p_i et les q_j implique que l'on a précisément $p_1 = q_1, p_2 = q_2, \ldots, p_s = q_s$. Donc finalement: $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$. Si $\beta_1 < \alpha_1$, on en déduit l'égalité $p_2^{\alpha_2} \ldots p_s^{\alpha_s} = p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$; celle-ci implique que p_1 divise le produit $p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, ce qui est impossible d'après le point (ii) de la proposition 2.1. De même $\beta_1 > \alpha_1$ conduit à une contradiction. C'est donc que $\alpha_1 = \beta_1$. On prouve de façon analogue que $\alpha_i = \beta_i$ pour tout $1 \leq i \leq s$. □

Définitions. L'écriture de n sous la forme $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ s'appelle la décomposition de n en produit de facteurs premiers, ou encore la décomposition primaire de n. Chaque p_i $(1 \leq i \leq s)$ s'appelle un facteur premier de la décomposition. Chaque $p_i^{\alpha_i}$ s'appelle un facteur primaire.

Attention à la notation. La notation p_i pour désigner les différents facteurs premiers dans la décomposition du théorème ci-dessus est traditionnelle, mais ne doit pas être confondue avec la même notation p_i pour désigner le i-ème nombre premier (voir fin du 1.3 ci-dessus).

Remarques. Il découle évidemment du théorème fondamental ci-dessus (dont on reprend les notations) que tout entier n non-nul et non-inversible dans $\mathbb{Z}$ se décompose de façon unique sous la forme $n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, où ε est un élément inversible de l'anneau $\mathbb{Z}$, c'est-à-dire $\varepsilon = \pm 1$. Ceci montre que $\mathbb{Z}$ est un anneau factoriel.

A noter aussi que l'unicité de la décomposition primaire exige de considérer, comme on l'a fait (et comme on le fait toujours), que 1 n'est pas premier.

2.3 Application: ensemble des diviseurs d'un entier.

PROPOSITION. *Un entier naturel m divise un entier naturel n si et seulement si tous les facteurs premiers dans la décomposition primaire de m apparaissent comme des facteurs premiers dans la décomposition primaire de n, avec un exposant supérieur à celui qu'ils admettent dans la décomposition primaire de m.*

En d'autres termes: si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ est la décomposition primaire d'un entier $n \geq 2$, alors les diviseurs de n dans $\mathbb{N}$ sont tous les entiers de la forme:

$$m = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}, \quad \text{avec } 0 \leq \beta_i \leq \alpha_i \text{ pour tout } 1 \leq i \leq s.$$

Preuve. Soit m un diviseur de n. Si $m = 1$, on a le résultat voulu avec $\beta_1 = \dots = \beta_s = 0$. Si $m \neq 1$, tout diviseur premier de m divise $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, donc est égal à l'un des p_i d'après 2.1. Ceci prouve qu'il existe des entiers naturels $\beta_1, \dots, \beta_s$ tels que $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$. L'entier $p_1^{\beta_1}$ divise m, qui divise n, donc est un diviseur de $n = p_1^{\alpha_1} q$, où l'on a posé $q = p_2^{\alpha_2} \dots p_s^{\alpha_s}$. Puisque $p_1^{\beta_1}$ est premier avec q, il résulte du théorème de Gauss que $p_1^{\beta_1}$ divise $p_1^{\alpha_1}$, et donc $\beta_1 \leq \alpha_1$. On montre de même que $\beta_i \leq \alpha_i$ pour tout $1 \leq i \leq s$. On a ainsi montré que tout diviseur de n est de la forme voulue; la réciproque est évidente. □

Attention ! Dans l'énoncé de la proposition ci-dessus, le produit $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ n'est pas la décomposition primaire de m car les exposants β_i peuvent valoir 0 (de sorte que certains p_i peuvent ne pas diviser pas m).

COROLLAIRE. *Soit n un entier supérieur ou égal à 2. Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ sa décomposition primaire. Alors le nombre $\sigma_0(n)$ des diviseurs de n dans $\mathbb{N}$ est égal à:*

$$\sigma_0(n) = (1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_s).$$

Preuve. Résulte immédiatement de la proposition précédente. □

Exemple élémentaire. Soit $n = 756 = 2^2 \times 3^3 \times 7$. Il admet $\sigma_0(756) = (2+1) \times (3+1) \times (1+1) = 24$ diviseurs, qui sont tous les entiers $m = 2^i \times 3^j \times 7^k$ pour $0 \leq i \leq 2$, $0 \leq j \leq 3$ et $0 \leq k \leq 1$. Donc:

$$D_{756} = \{1, 2, 3, 4, 6, 7, 9, 12, 14, 18, 21, 27, 28, 36, 42, 54, 63, 84, 108, 126, 189, 252, 378, 756\}$$

2.4 Application: calcul du pgcd et du ppcm de deux entiers.

PROPOSITION. *Soient a et b deux entiers naturels supérieurs ou égaux à 2.*

(i) *Il existe un entier $r \geq 1$, des nombres premiers deux à deux distincts $p_1, p_2, \dots, p_r$, et deux r-uplets $(\alpha_1, \alpha_2, \dots, \alpha_r) \in \mathbb{N}^r$ et $(\beta_1, \beta_2, \dots, \beta_r) \in \mathbb{N}^r$ tels que:*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}.$$

(ii) *En posant $\gamma_i = \min(\alpha_i, \beta_i)$ et $\delta_i = \max(\alpha_i, \beta_i)$ pour tout $1 \leq i \leq r$, on a alors:*

$$\text{pgcd}(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} \quad \text{et} \quad \text{ppcm}(a, b) = p_1^{\delta_1} p_2^{\delta_2} \dots p_r^{\delta_r}.$$

Preuve. Notons $\{p_1, \dots, p_r\}$ la réunion de l'ensemble des diviseurs premiers de a et de l'ensemble des diviseurs premiers de b. Pour tout $1 \leq i \leq r$, notons α_i l'exposant de p_i dans la décomposition primaire de a si p_i divise a, et posons $\alpha_i = 0$ si p_i ne divise pas a. Notons β_i l'exposant de p_i dans la décomposition primaire de b si p_i divise b, et posons $\beta_i = 0$ si p_i ne divise pas b. Le point (i) est alors clair. Le point (ii) résulte de la proposition 2.3. □

Attention ! Dans l'énoncé de la proposition ci-dessus, les produits $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ ne sont pas les décompositions primaires de a et b car les exposants α_i et β_i peuvent être nuls.

Exemple élémentaire. Soient $a = 756 = 2^2 \times 3^3 \times 7$ et $b = 240 = 2^4 \times 3 \times 5$.
On écrit $a = 2^2 \times 3^3 \times 5^0 \times 7^1$ et $b = 2^4 \times 3^1 \times 5^1 \times 7^0$
D'où $\text{pgcd}(a, b) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$ et $\text{ppcm}(a, b) = 2^4 \times 3^3 \times 5^1 \times 7^1 = 15120$.

Attention ! La proposition ci-dessus ne doit pas être considérée comme une méthode systématique pour calculer le pgcd de deux entiers. Dans la plupart des calculs numériques, l'algorithme d'Euclide reste beaucoup plus rapide et efficace sur le plan pratique.

2.5 Application: exemples de fonctions arithmétiques multiplicatives.

Définition. On appelle fonction arithmétique multiplicative sur $\mathbb{N}^*$ toute application $f : \mathbb{N}^* \to \mathbb{N}$ telle que, quels que soient des éléments a et b de $\mathbb{N}^*$ premiers entre eux, on a $f(ab) = f(a)f(b)$.

PROPOSITION. *Une fonction arithmétique multiplicative f sur $\mathbb{N}^*$ est entièrement déterminée par ses valeurs sur les puissances des nombres premiers.*

Preuve. Pour tout entier naturel $n \geq 2$, donné par sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, on a $f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2} \dots p_s^{\alpha_s})$, car $p_1^{\alpha_1}$ est premier avec $p_2^{\alpha_2} \dots p_s^{\alpha_s}$. D'où en réitérant: $f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_s^{\alpha_s})$. □

EXEMPLE 1. L'application $\sigma_0 : \mathbb{N}^* \to \mathbb{N}$ qui, à tout entier $n \geq 1$, associe le nombre de diviseurs de n, est une fonction arithmétique multiplicative. Il est clair que, pour toute puissance p^α d'un nombre premier p, on a $\sigma_0(p^\alpha) = \text{card}\{1, p, p^2, \dots, p^\alpha\} = \alpha + 1$. On retrouve le résultat du corollaire de 2.3.

EXEMPLE 2. L'application $\sigma_1 : \mathbb{N}^* \to \mathbb{N}$ qui, à tout entier $n \geq 1$, associe la somme des diviseurs de n, est une fonction arithmétique multiplicative.

En effet. Pour toute puissance p^α d'un nombre premier p, on a $\sigma_1(p^\alpha) = 1 + p + p^2 + \dots + p^\alpha = (p^{\alpha+1} - 1)(p-1)^{-1}$. Pour tout entier naturel $n \geq 2$, donné par sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, on a d'après la proposition 2.3, l'égalité: $\sigma_1(n) = (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots (1 + p_s + p_s^2 + \dots + p_s^{\alpha_s})$. □

EXEMPLE 3. On verra au paragraphe 3.2 du le chapitre 4 que l'indicatrice d'Euler est une fonction arithmétique multiplicative.

EXERCICE. Montrer que la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{N}$ définie par: $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par un carré distinct de 1, et $\mu(n) = (-1)^k$ si $n = p_1 p_2 \dots p_k$ avec $p_1, \dots, p_k$ premiers deux à deux distincts, est une fonction arithmétique multiplicative.

3. QUELQUES CARACTÉRISATIONS DES NOMBRES PREMIERS, ET APPLICATIONS.

3.1 Caractérisation des idéaux maximaux de $\mathbb{Z}$.

Rappel. Tous les idéaux de l'anneau $\mathbb{Z}$ sont principaux, c'est-à-dire de la forme $n\mathbb{Z}$ avec $n \in \mathbb{Z}$. Pour un tel idéal, les éléments de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ sont les classes d'équivalence de la relation d'équivalence associée à l'idéal $n\mathbb{Z}$, c'est-à-dire définie par: $\overline{x} = \overline{y} \Leftrightarrow x - y \in n\mathbb{Z}$. Cette relation d'équivalence est aussi appelée congruence modulo n, et l'on note $x \equiv y\,[n]$ pour signifier que $x - y \in n\mathbb{Z}$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $x - y = nk$.

PROPOSITION: *Pour tout entier $p \geq 2$, les conditions suivantes sont équivalentes:*

(i) *p est premier;*

(ii) *l'idéal $p\mathbb{Z}$ est un idéal premier de l'anneau $\mathbb{Z}$;*

(iii) *l'idéal $p\mathbb{Z}$ est un idéal maximal de l'anneau $\mathbb{Z}$;*

(iv) *l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps;*

(v) *l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est intègre.*

Preuve. Dire que l'idéal $p\mathbb{Z}$ (qui est non-nul et distinct de $\mathbb{Z}$) est premier signifie par définition que, pour tout $(x, y) \in \mathbb{Z}^2$ vérifiant $xy \in p\mathbb{Z}$, on a $x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$. L'équivalence de (i) et (ii) est alors claire.

Montrons que (i) ⇒ (iii). On suppose (i). Soit I un idéal de $\mathbb{Z}$ tel que $p\mathbb{Z} \subseteq I$. Il existe $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$, et l'inclusion $p\mathbb{Z} \subseteq n\mathbb{Z}$ traduit alors que n divise p. Comme p est premier, ceci implique que $n = 1$ ou $n = p$, c'est-à-dire $I = \mathbb{Z}$ ou $I = p\mathbb{Z}$, ce qui prouve que $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$.

Montrons que (iii) ⇒ (iv). On suppose l'idéal $p\mathbb{Z}$ maximal. Soit $\overline{n}$ un élément quelconque non-nul de $\mathbb{Z}/p\mathbb{Z}$, avec $n \in \mathbb{Z}$, $n \notin p\mathbb{Z}$. Formons l'idéal $I = n\mathbb{Z} + p\mathbb{Z}$. On a $p\mathbb{Z} \subseteq I$ (par définition de I), et $p\mathbb{Z} \neq I$, (car sinon l'élément n de I appartiendrait à $p\mathbb{Z}$, ce qui est exclu). La maximalité de $p\mathbb{Z}$ implique alors que $I = \mathbb{Z}$. En particulier $1 \in I$, donc il existe $a, b \in \mathbb{Z}$ tels que $an + bp = 1$. Dans $\mathbb{Z}/p\mathbb{Z}$, cette égalité devient $\overline{a}\,\overline{n} = \overline{1}$, ce qui prouve que $\overline{n}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. On conclut que $\mathbb{Z}/p\mathbb{Z}$ est un corps.

L'implication (iv) ⇒ (v) est évidente. Montrons enfin que (v) ⇒ (i). Supposons $\mathbb{Z}/p\mathbb{Z}$ intègre et considérons un diviseur $k \in \mathbb{N}$ de p. Il existe donc $s \in \mathbb{N}$ tel que $p = ks$. On a alors $\overline{k}\,\overline{s} = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Par hypothèse d'intégrité, il en résulte que $\overline{k} = \overline{0}$ ou $\overline{s} = \overline{0}$. Si $\overline{k} = \overline{0}$, on déduit que p divise k, d'où $p = k$ puisque k divise p et que les deux sont positifs. Si $\overline{s} = \overline{0}$, il existe $h \in \mathbb{N}$ tel que $s = hp$, d'où $p = ks = khp$, ce qui implique $kh = 1$, donc $k = h = 1$. On a ainsi vérifié que les seuls diviseurs positifs de p sont p et 1. On conclut que p st premier. □

3.2 Petit théorème de Fermat et nombres pseudo-premiers

LEMME PRÉLIMINAIRE. *Si p est un nombre premier, alors p divise C_p^k pour tout $k \in [\![1, p-1]\!]$.*

Preuve. D'une part p divise le produit $k!C_p^k$ puisque $k!C_p^k = p(p-1)\cdots(p-k+1)$. D'autre part p est premier avec $k!$ puisque p est premier et $k < p$. D'après le lemme de Gauss, on conclut que p divise C_p^k. □

THÉORÈME. *Soit $p \geq 2$ un entier.*

(i) *Si p est premier, alors, pour tout $n \in \mathbb{Z}$, on a: $n^p \equiv n \bmod p$.*

(ii) *p est premier si et seulement si, pour tout $n \in \mathbb{Z}$ tel que $n \notin p\mathbb{Z}$, on a: $n^{p-1} \equiv 1 \bmod p$.*

Preuve. Supposons p premier. Il résulte du lemme précédent et de la formule du binôme que $(a+b)^p \equiv a^p + b^p \bmod p$ pour tous $a, b \in \mathbb{Z}$. On en déduit que, si $n \geq 2$ est un entier fixé, et $a_1, a_2, \ldots, a_n$ des entiers quelconques, on a $(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \bmod p$. En particulier pour $a_1 = a_2 = \cdots = a_n = 1$, il vient $n^p \equiv n \bmod p$. Le résultat pour tout $n \in \mathbb{Z}$ s'en déduit immédatement. Si de plus on suppose que p ne divise pas n, le fait que p divise $n(n^{p-1}-1)$ implique avec le lemme de Gauss que p divise $n^{p-1}-1$, d'où $n^{p-1} \equiv 1 \bmod p$. Ceci prouve le point (i) et le sens direct du point (ii).

Pour la réciproque du (ii), supposons que p vérifie $n^{p-1} \equiv 1 \bmod p$ pour tout $n \in \mathbb{Z}$ tel que $n \notin p\mathbb{Z}$. Cela signifie que $\overline{n}^{p-1} = \overline{1}$ pour tout $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\overline{n} \neq \overline{0}$. En d'autre terme, tout élément non-nul $\overline{n}$ de $\mathbb{Z}/p\mathbb{Z}$ admet $\overline{n}^{p-2}$ pour inverse dans $\mathbb{Z}/p\mathbb{Z}$. Il en résulte que $\mathbb{Z}/p\mathbb{Z}$ est un corps, et donc p est premier. □

ATTENTION ! La seconde assertion du théorème est une caractérisation des nombres premiers. Ce n'est pas le cas de la première assertion (qui est connue sous le nom de petit théorème de Fermat), qui donne seulement une condition nécessaire pour qu'un nombre soit premier.

Et cette condition n'est pas suffisante ! Il existe des entiers $p \geq 2$ qui vérifient $n^p \equiv n \bmod p$ pour tout $n \in \mathbb{Z}$ et qui ne sont pas premiers. On les appelle parfois nombres pseudo-premiers, ou nombres absolument pseudo-premiers, ou nombres de Carmichaël. Par exemple 561, 1105, 1729, 2465, 2821,... Il a été prouvé (relativement récemment) que leur ensemble est infini.

EXERCICE. Montrons que 561 est un nombre de Carmichaël.

Il n'est pas premier car $561 = 3 \times 11 \times 17$. Fixons $n \in \mathbb{Z}$ quelconque et posons $N = n^{561} - n$.

$N = n(n^{560}-1) = n((n^2)^{280}-1)$. Or $((n^2)^{280}-1)$ est divisible par (n^2-1). Il existe donc $k_1 \in \mathbb{Z}$ tel que $((n^2)^{280}-1) = (n^2-1)k_1$. Donc $N = (n^3-n)k_1$. Mais, d'après le petit théorème de Fermat, le nombre premier 3 divise (n^3-n). On conclut que 3 divise N.

De même, $N = n(n^{560}-1) = n((n^{10})^{56}-1)$. Or $((n^{10})^{56}-1)$ est divisible par $(n^{10}-1)$. Il existe donc $k_2 \in \mathbb{Z}$ tel que $((n^{10})^{56}-1) = (n^{10}-1)k_2$. Donc $N = (n^{11}-n)k_2$. Mais, d'après le petit théorème de Fermat, le nombre premier 11 divise $(n^{11}-n)$. On conclut que 11 divise N.

De même, $N = n(n^{560}-1) = n((n^{16})^{35}-1)$. Or $((n^{16})^{35}-1)$ est divisible par $(n^{16}-1)$. Il existe donc $k_3 \in \mathbb{Z}$ tel que $((n^{16})^{535}-1) = (n^{16}-1)k_3$. Donc $N = (n^{17}-n)k_3$. Mais, d'après le petit théorème de Fermat, le nombre premier 17 divise $(n^{17}-n)$. On conclut que 17 divise N.

En résumé, 3, 11 et 17 divisent $N = n^{561} - n$, donc 561 divise $n^{561} - n$, et ceci quel que soit $n \in \mathbb{Z}$.

La même méthode permet de montrer que 1105 est un nombre de Carmichaël, en observant que $1105 = 5 \times 13 \times 17$ avec $1105 = 4 \times 276 + 1 = 12 \times 92 + 1 = 16 \times 69 + 1$.

3.3 Théorème de Wilson

THÉORÈME: *Un entier $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1 \bmod p$.*

Preuve. Supposons d'abord qu'il existe $k \in \mathbb{N}$ tel que $(p-1)! + 1 = kp$. Soit r un diviseur de p distinct de p. On a $r \in \{1, 2, \ldots, p-1\}$, donc r divise $(p-1)!$. Ainsi r divise à la fois p et $(p-1)!$, donc divise $(p-1)! - kp = 1$. On conclut que $r = 1$; ce qui prouve que p est premier.

Réciproquement, supposons p premier. Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps; notons-le $\mathbb{F}_p$. Dans $\mathbb{F}_p[X]$, considérons le polynôme $P(X) = X^{p-1} - \overline{1}$. D'après le point (ii) du théorème 3.2, tout $a \in \mathbb{Z}$ tel que $a \notin p\mathbb{Z}$ vérifie $a^{p-1} \equiv 1 \bmod p$. Ce qui se traduit par: tout $\overline{a} \in \mathbb{F}_p$ tel que $\overline{a} \neq \overline{0}$ vérifie $P(\overline{a}) = \overline{0}$. Les zéros de $P(X)$ dans $\mathbb{F}_p$ sont donc tous les éléments non-nuls de $\mathbb{F}_p$. Le produit de ces $p-1$ zéros simples doit valoir au signe près le terme constant de $P(X)$. Plus précisément, $(-1)^{p-1}\overline{1} \times \overline{2} \times \cdots \times \overline{p-1} = -\overline{1}$. D'où le résultat puisque $(-1)^{p-1} = 1$ lorsque $p \geq 3$ et $-\overline{1} = \overline{1}$ lorsque $p = 2$. □

Remarque finale. Les compléments possibles sur ce chapitre sont innombrables (résultats sur la répartition des nombres premiers, divers algorithmes et leurs implantations, propriétés des nombres de Fermat et de Mersenne, des nombres parfaits, des nombres d'Euclide,...) tant les nombres premiers sont omniprésents en arithmétique en particulier, et en mathématiques en général.

Leçon 4

Quotients de l'anneau $\mathbb{Z}$

Prérequis: L'arithmétique dans $\mathbb{Z}$ développée dans les trois précédentes leçons.

1. Congruences dans $\mathbb{Z}$.

1.1 Notion de congruence et premières propriétés

Définition. Soit n un entier naturel. Deux entiers x et y sont dits congrus modulo n lorsque $x-y$ est divisible par n dans $\mathbb{Z}$. On note alors $x \equiv y\,[n]$.

$$x \equiv y\,[n] \quad \Leftrightarrow \quad x-y \in n\mathbb{Z} \quad \Leftrightarrow \quad \exists\, k \in \mathbb{Z},\ x-y = nk.$$

Lemme. Soit n un entier naturel non-nul.

(i) *Tout entier x est congru modulo n au reste de la division euclidienne de x par n.*

(ii) *Deux entiers x et y sont congrus modulo n si et seulement s'ils ont le même reste dans la division euclidienne par n.*

Preuve. Soit $x = pn + r$ avec $(p,r) \in \mathbb{Z}^2$ tel que $0 \leq r < n$. On a $x - r = pn \in n\mathbb{Z}$, donc $x \equiv r\,[n]$, ce qui montre (i). Considérons de plus $y = p'n + r'$ avec $(p,r) \in \mathbb{Z}^2$ tel que $(p',r') \in \mathbb{Z}^2$ tel que $0 \leq r' < n$. On a $x - y = (p-p')n + (r-r')$. Si $r = r'$, alors $x - y = (p-p') \in n\mathbb{Z}$, donc $x \equiv y\,[n]$. Si $x \equiv y\,[n]$, alors $x - y \in n\mathbb{Z}$, donc $r - r' = x - y - (p-p')n \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un sous-groupe additif; mais il résulte de $0 \leq r < n$ et $0 \leq r' < n$ que $-n < r - r' < n$, et donc $r - r'$ divisible par n implique $r - r' = 0$, ce qui achève la preuve. □

Proposition et définition. *Pour tout entier naturel n, la relation "est congru modulo n à" est une relation d'équivalence sur $\mathbb{Z}$, que l'on appelle la congruence modulo n.*

Preuve. Simple vérification, laissée au lecteur. □

Notations. Soit n un entier naturel fixé. Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n.

$$\overline{x} = \{y \in \mathbb{Z}\,;\, x \equiv y\,[n]\} = \{x + kn\,;\, k \in \mathbb{Z}\}, \text{ que l'on note parfois: } \overline{x} = x + n\mathbb{Z}.$$

Rappelons que tout élément d'une classe $\overline{x}$ s'appelle un représentant de la classe $\overline{x}$. Dire qu'un entier y est un représentant de la classe $\overline{x}$ signifie donc que $x \equiv y\,[n]$, ou encore que $\overline{x} = \overline{y}$.
On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n, c'est-à-dire l'ensemble des classes de congruences de tous les entiers.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{x}\,;\, x \in \mathbb{Z}\}.$$

Remarques

(i) Si $n = 0$, la relation de congruence modulo 0 est l'égalité dans $\mathbb{Z}$. Dans ce cas, on a $\overline{x} = \{x\}$ pour tout $x \in \mathbb{Z}$, et $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

(ii) Si $n = 1$, la relation de congruence modulo 1 est la relation triviale dans $\mathbb{Z}$, c'est-à-dire $x \equiv y\,[1]$ quels que soient les entiers x et y. Donc $\overline{x} = \mathbb{Z}$ pour tout $x \in \mathbb{Z}$, et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.

On ne considérera plus dans la suite que le cas où $n \geq 2$.

Théorème. *Soit n un entier naturel supérieur ou égal à 2.*

(i) *Pour tout $x \in \mathbb{Z}$, il existe un unique représentant de $\overline{x}$ qui appartient à $[\![0, n-1]\!]$.*

(ii) *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n, et l'on a: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.*

Preuve. D'après le lemme vu au début de ce paragraphe, le reste de la division euclidienne de x par n est l'unique représentant de $\overline{x}$ qui appartient à $[\![0, n-1]\!]$, d'où (i). Le point (ii) découle directement de (i). □

1.2 Compatibilité de la congruence avec les lois de l'anneau $\mathbb{Z}$

Proposition. *Pour tout entier naturel n, la relation de congruence modulo n est compatible avec l'addition et avec la multiplication dans $\mathbb{Z}$, ce qui signifie que, quels que soient des entiers x, x', y, y':*

$$\textit{si}\ \ x \equiv x'\,[n]\ \ \textit{et}\ \ y \equiv y'\,[n], \quad \textit{alors}\quad x + y \equiv x' + y'\,[n]\ \ \textit{et}\ \ xy \equiv x'y'\,[n].$$

Preuve. On a $x - x' \in n\mathbb{Z}$ et $y - y' \in n\mathbb{Z}$. D'une part $(x+y) - (x'+y') = (x-x') + (y-y') \in n\mathbb{Z}$ comme somme de deux éléments de $n\mathbb{Z}$, ce qui prouve que $x + y \equiv x' + y'$ $[n]$. D'autre part $xy - x'y' = x(y-y') + (x-x')y'$. Comme $n\mathbb{Z}$ est un idéal, le fait que $y - y' \in n\mathbb{Z}$ implique que $x(y-y') \in n\mathbb{Z}$. De même $(x-x')y \in n\mathbb{Z}$, et donc la somme $x(y-y') + (x-x')y'$ appartient à $n\mathbb{Z}$, ce qui prouve que $xy \equiv x'y'$ $[n]$. □

Remarque. La principale application de cette proposition est la possibilité de munir l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'opérations $+$ et $\times$ définies à partir des opérations correspondantes dans $\mathbb{Z}$, comme on va le développer dans la partie suivante. Donnons d'abord deux autres exemples élémentaires.

1.3 Une application de la compatibilité: critères de divisibilité

THÉORÈME (dit de Pascal). *Soit m un entier naturel non-nul; soit (r_i) la suite d'entiers de $\{0, 1, \ldots, m-1\}$ définie par: $r_0 = 1$ et $r_{i+1} =$ le reste de la division euclidienne de $10r_i$ par m.*

Alors, pour tout entier naturel $a = \overline{a_n \ldots a_0}$ en numération décimale, on a: $a \equiv \sum_{i=0}^{n} a_i r_i$ $[m]$.

Preuve. Il suffit de montrer que: pour tout $i \in \mathbb{N}$, on a $r_i \equiv 10^i$ $[m]$, car cela implique, par compatibilité de la congruence avec la multiplication et l'addition, que $a_i r_i \equiv a_i 10^i$ $[m]$, et donc $a = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i r_i$ $[m]$.

Pour montrer la congruence voulue, on raisonne par récurrence. Pour $i = 0$, on a $r_0 = 1$ donc $r_0 \equiv 10^0$ $[m]$. Supposons que, pour un entier $i \geq 0$, on a $r_i \equiv 10^i$ $[m]$. Alors $10r_i \equiv 10^{i+1}$ $[m]$. Mais d'après le point (i) de la proposition, $10r_i$ est congru modulo m au reste de la division euclidienne de $10r_i$ par m, qui n'est autre par définition que r_{i+1}. Donc $r_{i+1} \equiv 10^{i+1}$ $[m]$, ce qui est la propriété voulue à l'ordre $i+1$. □

Exemples: soit a un entier naturel, et $a = \overline{a_n \ldots a_0}$ son écriture décimale. En appliquant le théorème avec diverses valeurs de m, on obtient les critères suivants de divisibilité:

- Pour $m = 3$, on a $r_0 = 1$, $r_1 = 1$ car $10 = 3 \times 3 + 1$, et $r_i = 1$ pour tout $i \in \mathbb{N}$. Ainsi $a \equiv \sum_{i=0}^{n} a_i$ $[3]$, d'où:
$$[a = \overline{a_n \ldots a_0} \text{ divisible par } 3] \Leftrightarrow [\sum_{i=0}^{n} a_i \text{ divisible par } 3]$$
- Pour $m = 9$, on a aussi $r_i = 1$ pour tout $i \in \mathbb{N}$, car $10 = 1 \times 9 + 1$. Donc comme ci-dessus:
$$[a = \overline{a_n \ldots a_0} \text{ divisible par } 9] \Leftrightarrow [\sum_{i=0}^{n} a_i \text{ divisible par } 9]$$
- Pour $m = 5$, on a $r_0 = 1$, $r_1 = 0$ car $10 = 2 \times 5 + 0$, et $r_i = 0$ pour tout $i \in \mathbb{N}^*$. Ainsi $a \equiv a_0$ $[5]$, d'où:
$$[a = \overline{a_n \ldots a_0} \text{ divisible par } 5] \Leftrightarrow [a_0 \text{ divisible par } 5] \Leftrightarrow [a_0 = 0 \text{ ou } a_0 = 5]$$
- Pour $m = 6$, on a $r_0 = 1$, $r_1 = 4$ car $10 = 1 \times 6 + 4$, $r_2 = 4$ car $10 \times 4 = 6 \times 6 + 4$, puis $r_i = 4$ pour tout $i \in \mathbb{N}^*$. Ainsi: $a \equiv a_0 + \sum_{i=1}^{n} 4a_i$ $[6]$. Il en résulte que: $[x = \overline{a_n \ldots a_0} \text{ divisible par } 6] \Leftrightarrow [a_0 + \sum_{i=1}^{n} 4a_i \text{ divisible par } 6]$
- Pour $m = 11$, on a $r_0 = 1$, $r_1 = 10$ car $10 = 0 \times 11 + 10$, puis $r_2 = 1$ car $10 \times 10 = 9 \times 11 + 1$, et ensuite $r_i = 1$ pour tout i pair et $r_i = 10$ pour tout i impair. Comme de plus $10 \equiv -1$ $[11]$, on a $a \equiv \sum_{i=0}^{n} (-1)^i a_i$ $[11]$, d'où:
$$[x = \overline{a_n \ldots a_0} \text{ divisible par } 11] \Leftrightarrow [a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n \text{ divisible par } 11]$$

1.4 Un exemple d'application dans l'enseignement élémentaire: la preuve par neuf.

PROPOSITION. (i) *Tout entier naturel est congru modulo 9 à la somme des chiffres de son écriture décimale.*

(ii) *Soient x, y, z trois entiers naturels, et $x = \overline{a_n \ldots a_0}$, $y = \overline{b_m \ldots b_0}$, $z = \overline{c_p \ldots c_0}$ leurs écritures décimales.*

$$\textit{Si } xy = z, \textit{ alors: } (\sum_{i=0}^{n} a_i)(\sum_{i=0}^{m} b_i) \equiv (\sum_{i=0}^{p} c_i) \ [9].$$

Preuve. Soit $x = \overline{a_n \ldots a_0}$. Donc $x = \sum_{i=0}^{n} a_i 10^i$. Or $10 \equiv 1$ $[9]$ implique par compatibilité de la congruence avec le produit que $10^i \equiv 1^i$ $[9]$, et donc $a_i 10^i \equiv a_i$ $[9]$. D'où l'on déduit par compatibilité de la congruence avec la somme que $(\sum_{i=0}^{n} a_i 10^i) \equiv (\sum_{i=0}^{n} a_i)$ $[9]$. Ce qui prouve (i). Pour (ii), il suffit de remarquer que (toujours par compatibilité) $x \equiv (\sum_{i=0}^{n} a_i)$ $[9]$ et $y \equiv (\sum_{i=0}^{m} b_i)$ $[9]$ impliquent $xy \equiv (\sum_{i=0}^{n} a_i)(\sum_{i=0}^{m} b_i)$ $[9]$, puis d'appliquer la transitivité de la congruence.

Remarque. Cette proposition donne une condition nécessaire pour l'égalité $xy = z$ (qui permet par contraposée de repérer certaines erreurs éventuelles dans le calcul du produit xy), mais elle n'est pas suffisante. Il est clair par exemple qu'une permutation des chiffres n'est pas détectée par ce test.

2. L'anneau $\mathbb{Z}/n\mathbb{Z}$.

Dans toute cette partie, on fixe un entier $n \geq 2$.

2.1 Lois quotients.

Lemme. Les lois de composition internes + et × construites sur $\mathbb{Z}/n\mathbb{Z}$ en posant:

$$\textit{pour tout } (\overline{x},\overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2, \quad \overline{x}+\overline{y} = \overline{x+y} \quad \textit{et} \quad \overline{x}\times\overline{y} = \overline{x\times y},$$

sont bien définies, indépendamment des représentants choisis, et la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, qui à tout $x \in \mathbb{Z}$ associe $\pi(x) = \overline{x}$, vérifie:

$$\textit{pour tout } (x,y) \in \mathbb{Z}^2, \quad \pi(x+y) = \pi(x)+\pi(y) \quad \textit{et} \quad \pi(x\times y) = \pi(x)\times\pi(y). \qquad (*)$$

Preuve. Fixons $\overline{x}$ et $\overline{y}$ deux éléments quelconques de $\mathbb{Z}/n\mathbb{Z}$. On pose $\overline{x}+\overline{y} = \overline{x+y}$. Prenons un autre représentant x' de la classe $\overline{x}$, et un autre représentant y' de la classe $\overline{y}$. Cela signife que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, ou encore $x \equiv x'\,[n]$ et $y \equiv y'\,[n]$. D'après la proposition de 1.2, on a alors $x+y \equiv x'+y'\,[n]$, donc $\overline{x'+y'} = \overline{x+y}$, c'est-à-dire $\overline{x}+\overline{y} = \overline{x'}+\overline{y'}$. Ceci prouve le résultat pour l'addition; on raisonne de même pour la multiplication. □

Remarque. Le produit de deux éléments $\overline{x}$ et $\overline{y}$ de $\mathbb{Z}/n\mathbb{Z}$ sera noté indifféremment $\overline{x}\times\overline{y}$, ou $\overline{x}.\overline{y}$, ou $\overline{x}\,\overline{y}$.

Théorème. *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des deux lois de composition internes définies au lemme précédent est un anneau commutatif unitaire; l'élément neutre pour l'addition est $\overline{0}$ et l'élément neutre pour la multiplication est $\overline{1}$. De plus, la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, est un morphisme d'anneaux unitaires.*

Preuve. La propriété (∗) de π permet de vérifier tous les axiomes de la structure d'anneau pour $\mathbb{Z}/n\mathbb{Z}$ à partir de la propriété correspondante pour l'anneau $\mathbb{Z}$ (c'est ce qu'on l'on appelle un transport de structure).
A titre d'exemple, montrons la commutativité de l'addition. Soit $(\overline{x},\overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2$. On a: $\overline{x}+\overline{y} = \pi(x)+\pi(y) = \pi(x+y)$; mais $x+y = y+x$ dans $\mathbb{Z}$, donc $\pi(x+y) = \pi(y+x) = \pi(y)+\pi(x) = \overline{y}+\overline{x}$. On a ainsi vérifié que $\overline{x}+\overline{y} = \overline{y}+\overline{x}$, ce qui prouve que l'addition dans $\mathbb{Z}/n\mathbb{Z}$ est commutative. On procède de même pour les autres propriétés de la structure d'anneau. La propriété (∗) traduit alors que π est un morphisme d'anneaux. □

Remarques. Il résulte de ce théorème que l'on peut calculer dans $\mathbb{Z}/n\mathbb{Z}$ avec les règles de calcul usuelles dans un anneau commutatif. Attention cependant à une différence fondamentale avec le calcul dans $\mathbb{Z}$: il peut y avoir dans $\mathbb{Z}/n\mathbb{Z}$ des diviseurs de zéro ! C'est-à-dire qu'un produit peut être nul sans qu'aucun des facteurs ne le soit; par exemple, dans $\mathbb{Z}/6\mathbb{Z}$, on a $\overline{2}\times\overline{3} = \overline{0}$ bien que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$. (Pour plus de détails sur cette question, voir le paragraphe suivant).

Conséquence. Contrairement à ce qui se passe dans $\mathbb{Z}$, une équation linéaire de degré 1 dans $\mathbb{Z}/n\mathbb{Z}$ peut avoir plusieurs solutions; par exemple, dans $\mathbb{Z}/16\mathbb{Z}$, l'équation $\overline{4}x = \overline{0}$ a quatre solutions, qui sont $\overline{0}$, $\overline{4}$, $\overline{8}$, $\overline{12}$. Elle peut aussi en avoir aucune; par exemple, dans $\mathbb{Z}/16\mathbb{Z}$, l'équation $\overline{4}x = \overline{6}$ n'a pas de solutions (car on aurait sinon $4x \equiv 6\,[16]$, donc $2x-3 \equiv 0\,[8]$, ce qui est impossible puisque $2x-3$ est toujours impair dans $\mathbb{Z}$.

2.2 Elements inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Théorème. *Pour tout entier x, l'élément $\overline{x}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si les entiers x et n sont premiers entre eux.*

Preuve. $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe un élément $\overline{y}$ de $\mathbb{Z}/n\mathbb{Z}$ tel que $\overline{xy} = \overline{1}$, ce qui équivaut à l'existence d'un entier y tel que $xy \equiv 1\,[n]$, ou encore à l'existence d'un entier y et d'un entier k tel que $xy-kn = 1$. D'après le théorème de Bézout, cette dernière condition est satisfaite si et seulement si x et n sont premiers entre eux. □

Corollaire fondamental. *Les conditions suivantes sont équivalentes:*

(i) *l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps;*
(ii) *l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre;*
(iii) *l'entier n est un nombre premier.*

Preuve. (i) implique (ii) puisque tout corps est un anneau intègre. Pour montrer que (ii) implique (iii), raisonnons par contraposée en supposant que n n'est pas premier. Il existe alors deux entiers non-nuls p et q distincts de 1 et de -1 tels que $n = pq$. On a donc $\overline{pq} = \overline{n} = \overline{0}$. Et pourtant $\overline{p} \neq \overline{0}$ (car sinon, il existerait un entier k tel que $p = kn$, d'où $n = knq$, ce qui contredirait $q \neq \pm 1$), et de même $\overline{q} \neq \overline{0}$. On a ainsi vérifié que n non premier implique que $\mathbb{Z}$ n'est pas intègre, ce qui prouve que (ii) implique (iii). Montrons enfin que (iii) implique (i). Supposons n premier. Il en résulte que tout entier appartenant à $[\![1, n-1]\!]$ est premier avec n. En appliquant le théorème précédent, on déduit que les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont $\overline{1}, \overline{2}, \ldots, \overline{n-1}$. En d'autres termes tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sauf $\overline{0}$ sont inversibles, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Remarques et exemples. On sait que, d'une façon générale, pour tout annau commutatif unitaire A, l'ensemble des éléments inversibles de l'anneau A est un groupe pour la multiplication, que l'on note $U(A)$, et que l'on appelle le groupe des unités de A. D'après le théorème ci-dessus, l'ordre du groupe $U(\mathbb{Z}/n\mathbb{Z})$ (ie. le nombre de ses éléments) est exactement le nombre d'entiers compris entre 1 et $n-1$ et premiers avec n. Ce nombre $\varphi(n)$ définit la fonction indicatrice d'Euler sur laquelle on donnera des précisions dans la partie 3 de cette leçon. Contentons-nous ici de quelques exemples.

- $U(\mathbb{Z}/10\mathbb{Z}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$; de plus $\overline{3}^2 = \overline{9}$ et $\overline{3}^3 = \overline{7}$, ce qui montre que $U(\mathbb{Z}/10\mathbb{Z})$ est cyclique d'ordre 4.
- $U(\mathbb{Z}/12\mathbb{Z}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$; de plus $\overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1}$, ce qui montre que $U(\mathbb{Z}/12\mathbb{Z})$ n'est pas cyclique, mais isomorphe au groupe de Klein.
- Lorsque p est premier, on a d'après le corollaire ci-dessus $U(\mathbb{Z}/p\mathbb{Z}) = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$. On peut démontrer que c'est un groupe cyclique.

2.3 Le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

PROPOSITION. *Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique.*

Preuve. Considérons $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ muni de sa structure de groupe pour l'addition. On a: $\overline{2} = \overline{1} + \overline{1}$, $\overline{3} = \overline{1} + \overline{1} + \overline{1}$, et d'une façon générale $\overline{x} = \overline{1} + \cdots + \overline{1}$ (somme de x termes) pour tout $x \in [\![1, n]\!]$, jusqu'à $\overline{n} = \overline{0}$. Ceci prouve que $\mathbb{Z}/n\mathbb{Z}$ est engendré, en tant que groupe additif, par le seul élément $\overline{1}$; c'est donc un groupe monogène, et comme il est fini, il est cyclique. □

Exemple et remarque. Considérons $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. En tant que groupe additif, on a vu que $\mathbb{Z}/6\mathbb{Z}$ est engendré par $\overline{1}$. Mais il est aussi engendré par $\overline{5}$ car:

$$\overline{5} + \overline{5} = \overline{4}, \quad \overline{5} + \overline{5} + \overline{5} = \overline{3}, \quad \overline{5} + \overline{5} + \overline{5} + \overline{5} = \overline{2}, \quad \overline{5} + \overline{5} + \overline{5} + \overline{5} + \overline{5} = \overline{1}, \quad \overline{5} + \overline{5} + \overline{5} + \overline{5} + \overline{5} + \overline{5} = \overline{0}.$$

En revanche, il n'est pas engendré par $\overline{3}$ car $\overline{3} + \overline{3} = \overline{0}$, et donc une somme de termes tous égaux à $\overline{3}$ ne donnera toujours que $\overline{3}$ ou $\overline{0}$, et non tous les éléments de $Z/6\mathbb{Z}$.

La question naturelle qui se dégage est donc, pour un n donné, de déterminer, parmi tous les éléments de $\mathbb{Z}/n\mathbb{Z}$, ceux qui l'engendrent en tant que groupe additif. La proposition suivante y répond.

PROPOSITION. *Pour tout entier x, l'élément $\overline{x}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ si et seulement si les entiers x et n sont premiers entre eux.*

Preuve. Si $\overline{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$, il existe un entier m vérifiant $1 \leq m \leq n-1$ tel que l'élément $\overline{1}$ soit la somme de m termes $\overline{1} = \overline{x} + \cdots + \overline{x}$. Ceci implique que l'on a dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ l'égalité $\overline{mx} = \overline{1}$. D'où $\overline{x}$ inversible, et le résultat voulu d'après le théorème 2.2. Réciproquement, supposons $\overline{x}$ et $\overline{m}$ premiers entre eux. D'après le théorème 2.2, il existe un entier m vérifiant $1 \leq m \leq n-1$ tel que $\overline{1} = \overline{mx} = \overline{x} + \cdots + \overline{x}$. Mais comme $\overline{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$, tout élément de $\mathbb{Z}/n\mathbb{Z}$ s'exprime comme une somme de termes tous égaux à $\overline{1}$, et donc comme une somme de termes tous égaux à $\overline{x}$. On conclut que $\overline{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$. □

Une application algébrique de ces résultats est la description suivante de tout groupe cyclique.

COROLLAIRE. *Tout groupe cyclique est isomorphe à un groupe additif $\mathbb{Z}/n\mathbb{Z}$.*

Plus précisément, si $G = \{e, a, a^2, \ldots, a^{n-1}\}$ est un groupe cyclique d'ordre n (noté multiplicativement), alors l'application $f : G \to \mathbb{Z}/n\mathbb{Z}$ qui, à tout élément a^x (avec $0 \leq x \leq n-1$), associe $\overline{x}$, est un isomorphisme de groupes de $(G, .)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$. En outre, un élément a^x de G est un générateur de G si et seulement si x et n sont premiers entre eux.

Preuve. Simple, laissée au lecteur. □

3. Applications et résultats complémentaires.

3.1 Systèmes de congruences et théorème chinois.

Données et notations. On fixe deux entiers $a \geq 1, b \geq 1$.

1. On considère l'anneau $\mathbb{Z}/a\mathbb{Z}$; on note $\overline{x}$ la classe modulo a d'un entier x.
2. On considère l'anneau $\mathbb{Z}/b\mathbb{Z}$; on note $\widetilde{x}$ la classe modulo b d'un entier x.
3. On considère l'anneau produit $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Ses éléments sont les couples $(\overline{x}, \widetilde{y})$, avec $x, y \in \mathbb{Z}$. Il est fini, formé de ab éléments. Rappelons que les lois + et . dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont définies par:
$$(\overline{x_1}, \widetilde{y_1}) + (\overline{x_2}, \widetilde{y_2}) = (\overline{x_1} + \overline{x_2}\,,\ \widetilde{y_1} + \widetilde{y_2}) = (\overline{x_1 + x_2}\,,\ \widetilde{y_1 + y_2}),$$
$$(\overline{x_1}, \widetilde{y_1}).(\overline{x_2}, \widetilde{y_2}) = (\overline{x_1}.\overline{x_2}\,,\ \widetilde{y_1}.\widetilde{y_2}) = (\overline{x_1 x_2}\,,\ \widetilde{y_1 y_2}).$$
4. On considère par ailleurs l'anneau $\mathbb{Z}/ab\mathbb{Z}$; il est fini, formé de ab éléments. On note $\widehat{x}$ la classe modulo ab d'un entier x.

Théorème (dit Chinois). *Avec les données et notations ci-dessus, on considère l'application:*
$$\begin{array}{rccc} f: & \mathbb{Z}/ab\mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & \widehat{x} & \mapsto & (\overline{x}, \widetilde{x}). \end{array}$$

(i) *L'application f est bien définie, et est un morphisme d'anneaux.*

(ii) *Si les entiers a et b sont premiers entre eux, alors f est un isomorphisme.*

Preuve. Pour montrer (i), considérons deux entiers x et y vérifient $\widehat{x} = \widehat{y}$. Alors $x - y$ est un multiple de ab, donc $x - y$ est multiple de a (d'où $\overline{x} = \overline{y}$) et $x - y$ est multiple de b (d'où $\widetilde{x} = \widetilde{y}$), d'où finalement $f(\widehat{x}) = f(\widehat{y})$. Ceci prouve que f est bien définie. Le fait que f soit un morphisme d'anneaux se vérifie de façon évidente. Pour (ii), considérons un élément $\widehat{x}$ du noyau de f. On a $f(\widehat{x}) = (\overline{0}, \widetilde{0})$, donc $\overline{x} = \overline{0}$ et $\widetilde{x} = \widetilde{0}$, c'est-à-dire $x \in a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$, où μ désigne le ppcm de a et b. Or, puisque a et b sont ici supposés premiers entre eux, on a $\mu = ab$. Donc $x \in ab\mathbb{Z}$, ou encore $\widehat{x} = \widehat{0}$. Ceci prouve que f est injective. Il en résulte que f est bijective car les ensembles de départ et d'arrivée sont finis de même nombre d'éléments ab. □

Corollaire 1. *Avec les données et notations ci-dessus, les conditions suivantes sont équivalentes:*

(i) *les entiers a et b sont premiers entre eux;*

(ii) *les anneaux $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$ sont isomorphes;*

(iii) *les groupes additifs $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$ sont isomorphes;*

(iv) *le groupe additif $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique.*

Preuve. On a montré au théorème précédent que (i)⇒(ii). Les implications (ii)⇒(iii) et (iii)⇒(iv) sont évidentes. Pour montrer (iv)⇒(i), raisonnons par contraposée en supposant que a et b ne sont pas premiers entre eux. Le ppcm μ de a et b est donc strictement inférieur au produit ab. Soit $(\overline{x}, \widetilde{y})$ un élément quelconque de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Comme a divise μ, on a $\mu x \in a\mathbb{Z}$, donc la somme $\overline{x} + \overline{x} + \cdots \overline{x}$ (avec μ termes) est $\mu\overline{x} = \overline{\mu x} = \overline{0}$. De même $\mu\widetilde{y} = \widetilde{0}$. Ainsi tout élément $(\overline{x}, \widetilde{y})$ de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ vérifie $\mu(\overline{x}, \widetilde{y}) = (\overline{0}, \widetilde{0})$ avec $\mu < ab$. En d'autres termes, tout élément de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est d'ordre strictement inférieur à ab. Et donc le groupe additif $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ n'est pas cyclique. Ce qui achève la preuve. □

Corollaire 2 (Systèmes de congruences). *Soient α et β deux entiers quelconques. Soient a et b deux entiers naturels non-nuls premiers entre eux. Alors le système de congruences* (S) *suivant:*
$$x \equiv \alpha\,[a] \quad \text{et} \quad x \equiv \beta\,[b].$$
admet des solutions dans $\mathbb{Z}$.

Preuve. Comme a et b sont premiers entre eux, l'application f du théorème précédent est surjective. Donc il existe $x \in \mathbb{Z}$ tel que $f(\widehat{x}) = (\overline{\alpha}, \widetilde{\beta})$, c'est-à-dire $\overline{x} = \overline{\alpha}$ et $\widetilde{x} = \widetilde{\beta}$, ce qui prouve que x est solution de (S). □

La question naturelle est alors de trouver explicitement toutes les solutions de (S), ce que l'on peut faire par la preuve directe suivante.

Proposition *Avec les données et notations du corollaire 2, l'ensemble des solutions dans $\mathbb{Z}$ de* (S) *est :*
$$S = \{au\beta + bv\alpha + \lambda ab\,;\, \lambda \in \mathbb{Z}\},$$
où (u, v) désigne un couple d'entiers tels que $au + bv = 1$.

Preuve. D'après le théorème de Bézout, il existe deux entiers u, v tels que $au + bv = 1$. Posons $x_0 = au\beta + bv\alpha$. D'une part $x_0 \equiv au\beta\,[b]$, et d'autre part $au\beta \equiv \beta\,[b]$ puisque $au \equiv 1\,[b]$. D'où par transitivité $x_0 \equiv \beta\,[b]$. De même $x_0 \equiv \alpha\,[a]$. Ainsi $x_0 \in S$. Un entier quelconque x appartient alors à S si et seulement si $x - x_0 \equiv 0\,[a]$ et $x - x_0 \equiv 0\,[b]$, ce qui équivaut à $x - x_0 \in a\mathbb{Z} \cap b\mathbb{Z}$. Or le ppcm de a et b est le produit ab puisque a et b sont premiers entre eux; donc $x \in S$ si et seulement si $x - x_0 \in ab\mathbb{Z}$, ce qui achève la preuve. □

3.2 Indicatrice d'Euler.

Définition. Pour tout entier $n \geq 2$, on note $\varphi(n)$ le nombre d'entiers compris entre 1 et $n-1$ qui sont premiers avec n. Donc:

$$\varphi(n) = \text{Card}\{k \in [\![1, n-1]\!] \ ; \ \text{pgcd}(k, n) = 1\}.$$

En convenant de plus de poser $\varphi(1) = 1$, on définit ainsi une application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, appelée *fonction indicatrice d'Euler.*

Remarque: il résulte de l'étude faite de $\mathbb{Z}/n\mathbb{Z}$ que, pour tout $n \geq 2$,

1. $\varphi(n)$ est le nombre de générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$;
2. $\varphi(n)$ est le nombre d'éléments du groupe multiplicatif $U(\mathbb{Z}/n\mathbb{Z})$ des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

La détermination d'une formule explicite pour le calcul de $\varphi(n)$ procède alors en plusieurs étapes.

Lemme. Si p est un nombre premier, alors $\varphi(p) = p - 1$.

Preuve. Tout entier de $[\![1, p-1]\!]$ est alors premier avec p. □

Lemme. Si p est un nombre premier et si α est un entier strictement positif, alors $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Preuve. Il y a $p^\alpha - 1$ entiers compris (au sens large) entre 1 et $p^\alpha - 1$. Parmi eux, ceux qui ne sont pas premiers avec p^α sont exactement ceux qui sont divisibles par p (car p est premier), c'est-à-dire ceux qui sont de la forme mp avec $m \in \mathbb{N}^*$ tel que $mp < p^\alpha$. Il y en a autant que de valeurs de m telles que $1 \leq m < p^{\alpha-1}$, à savoir $p^{\alpha-1} - 1$. On conclut que $\varphi(p^\alpha) = (p^\alpha - 1) - (p^{\alpha-1} - 1) = p^\alpha - p^{\alpha-1}$. □

PROPOSITION. *La fonction φ est une fonction arithmétique multiplicative, ce qui signifie que, pour tout couple $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que a et b soient premiers entre eux, on a: $\varphi(ab) = \varphi(a)\varphi(b)$.*

Preuve. Fixons deux entiers $a, b \geq 1$ premiers entre eux. D'après le théorème chinois, l'anneau $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à l'anneau produit $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. En particulier, $\varphi(ab)$ est égal au nombre d'éléments de $U(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$. Or on vérifie aisément qu'un élément $(\overline{x}, \overline{y})$ de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est inversible si et seulement si $\overline{x}$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$ et $\overline{y}$ est inversible dans $\mathbb{Z}/b\mathbb{Z}$. Il en résulte que $U(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) = U(\mathbb{Z}/a\mathbb{Z}) \times U(\mathbb{Z}/b\mathbb{Z})$ est formé de $\varphi(a)\varphi(b)$ éléments. D'où l'égalité. □

On arrive alors au résultat général suivant (où $\mathcal{P}$ désigne l'ensemble des nombres premiers):

THÉORÈME. *Pour tout entier $n \geq 2$, on a:* $\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p|n}} (1 - \frac{1}{p})$.

Preuve. Considérons la décomposition de n en produit de facteurs premiers: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ avec $p_1, p_2, \ldots, p_s$ premiers deux à deux distincts, et les $\alpha_i \geq 1$. D'après la proposition, on a: $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s})$. En appliquant le second lemme, il vient: $\varphi(n) = p_1^{\alpha_1}(1 - \frac{1}{p_1}) p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_s^{\alpha_s}(1 - \frac{1}{p_s})$, d'où le résultat. □

3.3 Applications à certains résultats classiques d'arithmétique.

THÉORÈME D'EULER. *Soient a et n deux entiers ≥ 2. Si a et n sont premiers entre eux, alors* $a^{\varphi(n)} \equiv 1\,[n]$.

Preuve. Comme a est premier avec n, on sait que $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$. On peut donc considérer l'application $t : U(\mathbb{Z}/n\mathbb{Z}) \to U(\mathbb{Z}/n\mathbb{Z})$ définie par $t(\overline{x}) = \overline{ax}$ pour tout $\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})$. Parce que $\overline{a}$ est inversible dans $U(\mathbb{Z}/n\mathbb{Z})$, l'application t est clairement une bijection. Donc:

$$\prod_{\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})} \overline{x} \ = \ \prod_{\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})} \overline{ax} \ = \ \overline{a}^{\,|U(\mathbb{Z}/n\mathbb{Z})|} \times \prod_{\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})} \overline{x},$$

où $|U(\mathbb{Z}/n\mathbb{Z})|$ désigne le nombre d'éléments du groupe $U(\mathbb{Z}/n\mathbb{Z})$, qui n'est autre que $\varphi(n)$. D'où $\overline{a}^{\varphi(n)} = \overline{1}$, ce qui achève la preuve. □

COROLLAIRE (PETIT THÉORÈME DE FERMAT). *Soit p un nombre premier. Alors:*

(i) *pour tout $a \in \mathbb{Z}$ tel que $a \notin p\mathbb{Z}$, on a:* $a^{p-1} \equiv 1\,[p]$,

(ii) *pour tout $a \in \mathbb{Z}$ on a:* $a^p \equiv a\,[p]$.

Preuve. Le point (i) est la traduction immédiate du théorème précédent puisque $\varphi(p) = p - 1$ lorsque p est premier. Le point (ii) s'obtient en multipliant les deux membres de (i) par a. □

Remarque. Le point (ii) est appelé le petit théorème de Fermat; nous l'avons déjà rencontré dans la leçon 3, avec une preuve différente et directe, n'utilisant pas l'indicatrice d'Euler). Rappelons que réciproquement (i) implique que p est premier, ce qui n'est pas le cas de (ii); (voir, dans la leçon 3, le paragraphe sur les nombres pseudo-premiers).

THÉORÈME DE WILSON. Un entier $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1\,[p]$.

Preuve. Supposons p premier. Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps, que l'on notera $\mathcal{F}_p$. Tous les éléments de $\mathcal{F}_p$ distincts de $\overline{0}$ sont inversibles. Il est clair que $\overline{1}$ a pour inverse lui-même, ainsi que $-\overline{1} = \overline{p-1}$. Réciproquement, soit $\overline{x}$ un élément non-nul de $\mathcal{F}_p$ tel que $\overline{x} = \overline{x}^{-1}$. On a alors $\overline{x}^2 = \overline{1}$, donc $(\overline{x}-\overline{1})(\overline{x}+\overline{1}) = \overline{0}$, ce qui, parce que $\mathcal{F}_p$ est ici un corps donc un anneau intègre, implique $\overline{x} = \pm\overline{1}$. En résumé, $\overline{1}$ et $-\overline{1} = \overline{p-1}$ sont les seuls éléments de $\mathcal{F}_p$ égaux à leur propre inverse. On calcule:

$$\overline{(p-1)!} = \overline{1} \times \underbrace{\overline{2} \times \cdots \times \overline{p-2}}_{\overline{1}} \times \overline{(p-1)} = \overline{1} \times \overline{(p-1)} = -\overline{1},$$

en remarquant que le produit des facteurs situés au centre vaut $\overline{1}$ puisque les facteurs qui y interviennent sont deux à deux inverses l'un de l'autre. On conclut que $(p-1)! \equiv -1\,[p]$.

Réciproquement, supposons $(p-1)! \equiv -1\,[p]$. Pour tout $x \in [\![1, p-1]\!]$, on peut écrire $\overline{(p-1)!} = \overline{x} \times \overline{y}$, où $\overline{y}$ désigne le produit de tous les éléments non-nuls de $\mathbb{Z}/p\mathbb{Z}$ distincts de $\overline{x}$. Or, par hypothèse, $\overline{(p-1)!} = -\overline{1}$. Donc $\overline{x} \times \overline{y} = -\overline{1}$, d'où $\overline{x}$ inversible dans $\mathbb{Z}/p\mathbb{Z}$, d'inverse $-\overline{y}$. Ceci étant vrai pour tout élément $\overline{x}$ non-nul de $\mathbb{Z}/p\mathbb{Z}$, on conclut que $\mathbb{Z}/p\mathbb{Z}$ est un corps, et donc p est premier. □

Leçon 5

Corps des fractions de l'anneau $\mathbb{Z}$

1. L'ensemble $\mathbb{Q}$ des nombres rationnels.

1.1 Fractions équivalentes

Notations et définition. On appelle fraction tout couple (a,b) où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. On note $\mathcal{F} = \mathbb{Z} \times \mathbb{Z}^*$ l'ensemble des fractions. Si $(a,b) \in \mathcal{F}$, a est appelé le numérateur et b le dénominateur de la fraction (a,b).

Définition. Deux fractions (a,b) et (c,d) sont dites équivalentes lorsque $ad = bc$ dans $\mathbb{Z}$. On note alors $(a,b) \sim (c,d)$.

Proposition. *La relation $\sim$ est une relation d'équivalence dans $\mathcal{F}$.*

Preuve. La réflexivité et la symétrie sont évidentes. Pour la transitivité, considérons trois fractions (a,b), (c,d) et (e,f). Supposons que $(a,b) \sim (c,d)$ et $(c,d) \sim (e,f)$. On a donc: $ad = bc$ et $cf = de$. Il vient $adf = bcf = bde$, et comme $d \neq 0$, l'intégrité de $\mathbb{Z}$ implique $af = be$, d'où $(a,b) \sim (e,f)$. □

Notation. Pour toute fraction (a,b), on note $\frac{a}{b}$ la classe d'équivalence de (a,b) pour la relation $\sim$. Donc:

$$\tfrac{a}{b} = \{(c,d) \in \mathcal{F}\,;\, (c,d) \sim (a,b)\} = \{(c,d) \in \mathcal{F}\,;\, ad = bc\}.$$

Toute fraction (c,d) appartenant à $\frac{a}{b}$ s'appelle un représentant de la classe $\frac{a}{b}$.

1.2 Nombres rationnels

Définition. On appelle nombre rationnel toute classe d'équivalence pour la relation $\sim$ dans $\mathcal{F}$.

Notation. On note $\mathbb{Q}$ l'ensemble des nombres rationnels, c'est-à-dire l'ensemble quotient de l'ensemble des fractions par la relation d'équivalence $\sim$, ce que l'on note: $\mathbb{Q} = \mathcal{F}/\sim$.

Proposition (égalité de deux rationnels). *Deux nombres rationnels sont égaux si et seulement si tout représentant de l'un est équivalent à tout représentant de l'autre:*

$$(\tfrac{a}{b} = \tfrac{c}{d} \text{ dans } \mathbb{Q}) \;\Leftrightarrow\; ((a,b) \sim (c,d) \text{ dans } \mathcal{F}) \;\Leftrightarrow\; (ad = bc \text{ dans } \mathbb{Z}).$$

Preuve. Evidente. □

Proposition (simplification). *Pour toute fraction (a,b) et tout entier d non-nul, on a: $\frac{ad}{bd} = \frac{a}{b}$.*

Preuve. On a $(ad)b = (bd)a$, d'où $(ad, bd) \sim (a,b)$, et donc $\frac{ad}{bd} = \frac{a}{b}$. □

Théorème et définition. *Pour tout nombre rationnel x, il existe une unique fraction (a,b) vérifiant $x = \frac{a}{b}$ telle que $b \in \mathbb{N}^*$ et telle que les entiers a et b soient premiers entre eux. On l'appelle le représentant irréductible du nombre rationnel x.*

Preuve. Soit $x \in \mathbb{Q}$. Il existe $(c,e) \in \mathcal{F}$ telle que $x = \frac{c}{e}$. Notons $d = \mathrm{pgcd}(c,e)$. Il existe deux entiers α et β premiers entre eux tels que $c = \alpha d$ et $e = \beta d$. Comme $e \neq 0$, on a $\beta \neq 0$. Si $\beta > 0$, on pose $a = \alpha$ et $b = \beta$. On a alors, en utilisant la proposition précédente: $x = \frac{c}{e} = \frac{\alpha d}{\beta d} = \frac{\alpha}{\beta} = \frac{a}{b}$.
Si $\beta < 0$, on pose $a = -\alpha$ et $b = -\beta$. □

1.3 Injection canonique de $\mathbb{Z}$ dans $\mathbb{Q}$.

Lemme. L'application $\phi : \mathbb{Z} \to \mathbb{Q}$ qui, à un entier a associe le rationel $\phi(a) = \frac{a}{1}$, est injective.

Preuve. Soient a et c deux entiers tels que $\phi(a) = \phi(c)$. On a alors: $\frac{a}{1} = \frac{c}{1}$. D'où $a \times 1 = 1 \times c$, donc $a = c$. □

Conséquence fondamentale. Il résulte du lemme que l'application $\widehat{\phi} : \mathbb{Z} \to \phi(\mathbb{Z})$ définie par $\widehat{\phi}(a) = \phi(a)$ pour tout $a \in \mathbb{Z}$ est une bijection de $\mathbb{Z}$ sur le sous-ensemble $\phi(\mathbb{Z})$, image directe de l'ensemble par $\mathbb{Z}$ par ϕ.

Convention: on convient d'identifier $\mathbb{Z}$ avec le sous-ensemble $\phi(\mathbb{Z})$ de $\mathbb{Q}$, qui lui est équipotent.
Via cette identification, $\mathbb{Z}$ est un sous-ensemble de $\mathbb{Q}$, et on pose $a = \frac{a}{1}$, pour tout $a \in \mathbb{Z}$.
En d'autres termes: quel que soit $a \in \mathbb{Z}$, on a: $a = \frac{a}{1} = \{(c,d) \in \mathcal{F}\,;\, c = ad\} = \frac{ad}{d}$ pour tout $d \in \mathbb{Z}^*$.

En particulier: $0 = \frac{0}{1}$ (et aussi $0 = \frac{0}{b}$ pour tout $b \in \mathbb{Z}^*$) et $1 = \frac{1}{1}$ (et aussi $1 = \frac{a}{a}$ pour tout $a \in \mathbb{Z}^*$).

1.4 Dénombrabilité de l'ensemble $\mathbb{Q}$.

PROPOSITION. *L'ensemble $\mathbb{Q}$ est infini dénombrable.*

Preuve. Puisqu'il existe d'après 1.3 une injection de $\mathbb{Z}$ dans $\mathbb{Q}$, et puisque $\mathbb{Z}$ est infini, l'ensemble $\mathbb{Q}$ est infini. De plus, on peut d'après le théorème de 1.2 considérer l'application $\mathbb{Q} \to \mathbb{Z} \times \mathbb{N}^*$ qui, à tout nombre rationnel, associe son unique représentant irréductible; c'est clairement une injection de $\mathbb{Q}$ dans $\mathbb{Z} \times \mathbb{N}^*$. On sait que $\mathbb{Z}$ et $\mathbb{N}^*$ sont infinis dénombrables, et que le produit cartésien de deux ensembles infinis dénombrables est infini dénombrable. D'où le résultat. □

2. Opérations et relation d'ordre dans $\mathbb{Q}$.

2.1 Addition dans $\mathbb{Q}$.

Lemme. Soient $\frac{a}{b}$ et $\frac{c}{d}$ deux nombres rationnels. Le rationnel $\frac{a}{b} + \frac{c}{d}$ défini par:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

est indépendant des représentants choisis, ce qui signifie que, si $\frac{a}{b} = \frac{a'}{b'}$ et si $\frac{c}{d} = \frac{c'}{d'}$, alors $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$.

Preuve. Un calcul évident montre que l'on a $(ad+bc)b'd' = (a'd' + b'c')bd$ dès lors que $ab' = a'b$ et $cd' = c'd$. □

Définition. Le rationnel $\frac{a}{b} + \frac{c}{d}$ ainsi défini est appelé la somme du rationnel $\frac{a}{b}$ et du rationnel $\frac{c}{d}$. La loi de composition interne $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ qui, à un couple de rationnels (x, y), associe la somme $x + y$, est appelée l'addition dans $\mathbb{Q}$.

PROPOSITION.

(i) *Pour l'addition définie ci-dessus, $\mathbb{Q}$ est un groupe abélien.*

(ii) *$\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Q}$ (ou encore, l'addition dans $\mathbb{Q}$ prolonge l'addition dans $\mathbb{Z}$).*

Preuve. Pour (i), on vérifie directement par des calculs simples que l'addition est commutative et associative, qu'elle admet $0 = \frac{0}{1}$ comme élément neutre, et que tout rationnel $\frac{a}{b}$ admet $\frac{-a}{b}$ comme opposé. Pour (ii), il suffit de remarquer que l'injection $i : \mathbb{Z} \to \mathbb{Q}$ considérée en 1.3 vérifie $i(a + c) = i(a) + i(c)$ pour tout $(a, c) \in \mathbb{Z}$, ce qui est clair puisque $\frac{a}{1} + \frac{c}{1} = \frac{a+c}{1}$. □

2.2 Multiplication dans $\mathbb{Q}$.

Lemme. Soient $\frac{a}{b}$ et $\frac{c}{d}$ deux nombres rationnels. Le rationnel $\frac{a}{b} \times \frac{c}{d}$ défini par:

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

est indépendant des représentants choisis, ce qui signifie que, si $\frac{a}{b} = \frac{a'}{b'}$ et si $\frac{c}{d} = \frac{c'}{d'}$, alors $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Preuve. Un calcul évident montre que l'on a $(ac)(b'd') = (a'c')(bd)$ dès lors que $ab' = a'b$ et $cd' = c'd$. □

Définition. Le rationnel $\frac{a}{b} \times \frac{c}{d}$ ainsi défini est appelé le produit du rationnel $\frac{a}{b}$ par le rationnel $\frac{c}{d}$. On le note aussi $\frac{a}{b}.\frac{c}{d}$, ou simplement $\frac{a}{b}\frac{c}{d}$. La loi de composition interne $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ qui, à un couple de rationnels (x, y), associe le produit xy, est appelée la multiplication dans $\mathbb{Q}$.

PROPOSITION.

(i) *La multiplication dans $\mathbb{Q}$ est commutative, associative, admet 1 pour élément neutre, et tout rationnel non-nul $\frac{a}{b}$ admet $\frac{b}{a}$ pour inverse dans $\mathbb{Q}$.*

(ii) *La multiplication dans $\mathbb{Q}$ prolonge la multiplication dans $\mathbb{Z}$.*

Preuve. Pour (i), on vérifie directement par des calculs simples la commutativité et l'associativité. Pour tout $x = \frac{a}{b}$ dans $\mathbb{Q}$, on a $1.x = \frac{1}{1}.\frac{a}{b} = \frac{1a}{1b} = \frac{a}{b} = x$, donc 1 est neutre. Enfin tout rationnel non-nul est de la forme $\frac{a}{b}$ avec $a \neq 0$, et l'on a alors $\frac{a}{b}.\frac{b}{a} = \frac{ab}{ba} = 1$. Pour (ii), il suffit de remarquer que l'injection $i : \mathbb{Z} \to \mathbb{Q}$ considérée en 1.3 vérifie $i(ac) = i(a)i(c)$ pour tout $(a, c) \in \mathbb{Z}$, ce qui est clair puisque $\frac{a}{1}.\frac{c}{1} = \frac{ac}{1}$. □

2.3 Structure de corps de $\mathbb{Q}$.

THÉORÈME. *$(\mathbb{Q}, +, \times)$ est un corps commutatif.*

Preuve. Résulte des points (i) des propositions 2.1 et 2.2, et de la distributivité de $\times$ sur $+$ dans $\mathbb{Q}$, que l'on vérifie par un calcul direct élémentaire. □

PROPOSITION.

(i) $\mathbb{Z}$ *est un sous-anneau de* $\mathbb{Q}$*;*

(ii) *tout sous-anneau de* $\mathbb{Q}$ *contient* $\mathbb{Z}$*;*

(iii) *le seul sous-corps de* $\mathbb{Q}$ *est* $\mathbb{Q}$*.*

Preuve. (i) résulte des points (ii) des propositions 2.1 et 2.2. Pour (ii), considérons un sous-anneau A de $\mathbb{Q}$. Il contient nécessairement 0 et 1. Comme A est stable par addition, il contient aussi $1+1=2, 1+1+1=3, \ldots$ et donc tous les entiers naturels. Comme A est stable par passage à l'opposé, on conclut que A contient $\mathbb{Z}$. Pour (iii), considérons un sous-corps K de $\mathbb{Q}$. Comme K est un sous-anneau, on déduit de (ii) que K contient $\mathbb{Z}$. Comme de plus l'inverse de tout élément non-nul de K doit appartenir à K, il en résulte que K contient les inverses des entiers non-nuls. Dès lors, étant stable par multiplication, K contient tous les produits d'entiers par des inverses d'entiers non-nuls, d'où $K = \mathbb{Q}$. □

2.4 Relation d'ordre sur $\mathbb{Q}$.

Lemme. Soit x un rationnel tel que $x \neq 0$. Deux cas seulement peuvent se présenter: ou bien, pour tout représentant (a,b) de x, le produit ab appartient à $\mathbb{N}^*$, ou bien, pour tout représentant (a,b) de x, le produit ab est strictement négatif dans $\mathbb{Z}$.

Preuve. Soient (a,b) et (c,d) deux représentants de x. On a $ad = bc$, donc $(ab)(cd) = a^2d^2$ est strictement positif dans $\mathbb{Z}$. Il en résulte que les entiers ab et cd sont de même signe, ce qui achève la preuve. □

Notations et terminologie.

1. On note $\mathbb{Q}^*$ l'ensemble des nombres rationnel distincts de 0.
2. Les rationnels non-nuls satisfaisant la première condition du lemme ci-dessus sont dits strictement positifs; on note $\mathbb{Q}_+^*$ leur ensemble. On pose $\mathbb{Q}_+ = \mathbb{Q}_+^* \cup \{0\}$ et on appelle rationnels positifs les éléments de $\mathbb{Q}_+$.
3. Les rationnels non-nuls satisfaisant la seconde condition du lemme ci-dessus sont dits strictement négatifs; on note $\mathbb{Q}_-^*$ leur ensemble. On pose $\mathbb{Q}_- = \mathbb{Q}_-^* \cup \{0\}$ et on appelle rationnels négatifs les éléments de $\mathbb{Q}_-$.

On déduit ainsi du lemme les partitions suivantes de $\mathbb{Q}$:

Corollaire. $\mathbb{Q} = \mathbb{Q}_-^* \cup \mathbb{Q}_+ = \mathbb{Q}_- \cup \mathbb{Q}_+^* = \mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^*$.

Définitions. Soient x et y deux nombres rationnels. On dit que x est inférieur ou égal à y, ce que l'on note $x \leq y$, lorsque le nombre rationnel $y - x$ est positif.

$$x \leq y \quad \Leftrightarrow \quad y - x \in \mathbb{Q}_+$$

On dit que x est strictement inférieur à y, ce que l'on note $x < y$, lorsque le nombre rationnel $y - x$ est strictement positif, ce qui équivaut à $x \leq y$ et $x \neq y$.

PROPOSITION. *La relation $\leq$ est une relation d'ordre total dans $\mathbb{Q}$, qui prolonge la relation d'ordre usuelle dans $\mathbb{Z}$ (ce qui signifie que l'injection $i : \mathbb{Z} \to \mathbb{Q}$ est croissante).*

Preuve. Le fait que la relation $\leq$ soit réflexive, antisymétrique et transitive se vérifie facilement. Il résulte du corollaire précédent que, quels que soient x et y dans $\mathbb{Q}$, on a $y - x \in \mathbb{Q}_+$ ou $y - x \in \mathbb{Q}_-$; donc $x \leq y$ ou $y \leq x$. La relation $\leq$ est donc une relation d'ordre total dans $\mathbb{Q}$. Pour le second point, considérons deux entiers m et n tels que $m \leq n$ dans $\mathbb{Z}$. Si $m = n$ dans $\mathbb{Z}$, alors $\frac{m}{1} = \frac{n}{1}$ c'est-à-dire $m = n$ dans $\mathbb{Q}$. Sinon, $n - m \in \mathbb{N}^*$, alors $(n-m) \times 1$ est strictement positif dans $\mathbb{Z}$, et il résulte donc de la définition même de $\mathbb{Q}_+^*$ que $n - m = \frac{n}{1} - \frac{m}{1}$ est strictement positif dans $\mathbb{Q}$. D'où $\frac{m}{1} \leq \frac{n}{1}$ c'est-à-dire $m \leq n$ dans $\mathbb{Q}$. □

THÉORÈME. $(\mathbb{Q}, +, \times, \leq)$ *est un corps totalement ordonné, ce qui signifie que la relation d'ordre total $\leq$ définie sur le corps $\mathbb{Q}$ vérifie de plus:*

(i) *la relation $\leq$ est compatible avec l'addition dans $\mathbb{Q}$,*

(ii) *le produit de deux rationnels positifs est positif.*

Preuve. Evident d'après les définitions précédentes. □

Conséquences pratiques.

Rappelons que le point (i) ci-dessus signife que: $\forall\ (x,y,z) \in \mathbb{Q}^3,\ (\ x \leq y\ \Rightarrow\ x+z \leq y+z\ )$.

Il résulte immédiatement du point (ii) ci-dessus que: $\forall\ (x,y) \in \mathbb{Q}^3,\ \forall\ z \in \mathbb{Q}^+,\ (\ x \leq y\ \Rightarrow\ xz \leq yz\ )$.

Terminons par deux autres propriétés importantes de l'ordre dans $\mathbb{Q}$.

PROPOSITION. *Le corps $\mathbb{Q}$ est archimédien, ce qui signifie que:* $\forall\ x \in \mathbb{Q}_+,\ \forall\ y \in \mathbb{Q}_+^*,\ \exists\ n \in \mathbb{N},\ x \leq ny$

Preuve. Si $x = \frac{a}{b}$ avec $(a,b) \in \mathbb{N} \times \mathbb{N}^*$ et $y = \frac{c}{d}$ avec $(c,d) \in \mathbb{N} \times \mathbb{N}^*$, prendre $n = ad$. □

PROPOSITION. *La relation d'ordre dans $\mathbb{Q}$ vérifie:* $\forall\ x \in \mathbb{Q},\ \forall\ y \in \mathbb{Q},\ (\ x < y\ \Rightarrow\ \exists\ z \in \mathbb{Q},\ x < z < y\ )$.

Preuve. Il suffit de prendre $z = \frac{x+y}{2}$. □

Cette dernière proposition permet de vérifier par une récurrence simple que, entre deux rationnels distincts, il existe une infinité de rationnels (l'analogue de cette propriété pour les entiers est évidemment fausse).

2.5 Valeur absolue d'un nombre rationnel.

Définition. Pour tout nombre rationnel x, on appelle valeur absolue de x, et l'on note $|x|$, le rationnel positif égal à x lorsque x est positif, et égal à $-x$ lorsque x est négatif.

PROPOSITION. *Pour tous rationnels x et y, on a:* $|xy| = |x|.|y|$ *et* $|x+y| \leq |x| + |y|$.

Preuve. Evident. □

3. Compléments et prolongements

3.1 Sur le plan algébrique.

Remarque 1. Puisque $\mathbb{Q}$ est un corps, il est clair que l'on sait résoudre dans $\mathbb{Q}$ toute équation algébrique de degré 1, c'est-à-dire de la forme $ax + b = 0$ avec $(a,b) \in \mathbb{Q}^2$. L'ensemble des solutions est $\{-\frac{b}{a}\}$ si $a \neq 0$, est $\mathbb{Q}^2$ si $(a,b) = (0,0)$, et est vide si $a = 0$ et $b \neq 0$. C'est une propriété évidemment fausse dans l'anneau $\mathbb{Z}$.

Remarque 2. Certaines équations algébriques à coefficients dans $\mathbb{Q}$ de degré strictement plus grand que 1 admettent évidemment des solutions dans $\mathbb{Q}$ (par exemple $4x^2 = 9$), mais d'autres non.

Exemple. L'équation $x^2 = p$ avec p nombre premier n'admet pas de solution dans $\mathbb{Q}$.

En effet, supposons qu'il existe $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ tel que $x^2 = p$. D'après le théorème de 1.2, on peut sans restriction supposer a et b premiers entre eux. L'égalité $(\frac{a}{b})^2 = p$ implique $a^2 = pb^2$ dans $\mathbb{Z}$. Ainsi p divise a^2 ce qui, comme p est premier, implique que p divise a. Il existe alors $c \in \mathbb{Z}$ tel que $a = cp$. L'égalité $a^2 = pb^2$ devient donc $c^2p^2 = pb^2$, d'où $c^2p = b^2$. Ainsi p divise b^2 ce qui, comme p est premier, implique que p divise b. On conclut que p est un diviseur premier commun à a et b, ce qui contredit l'hypothèse que a et b sont premiers entre eux. □

Remarque 3. Le passage au corps des nombres réels ne suffit pas à assurer l'existence de solution pour toute équation algébrique. Si certaines équations algébriques à coefficients dans $\mathbb{Q}$ admettent des solutions réelles alors qu'elles n'en admettent pas dans $\mathbb{Q}$ (par exemple $x^2 = p$ avec p nombre premier), d'autres n'en ont pas (par exemple $x^2 + 1 = 0$), ce qui justifie la construction du corps des nombres complexes.

3.2 Sur le plan topologique.

1. *Le corps ordonné $\mathbb{Q}$ ne vérifie pas l'axiome de la borne supérieure.*

Preuve. On considère dans $\mathbb{Q}$ la partie: $A = \{x \in \mathbb{Q}_+\ ;\ x^2 < 2\}$. Elle est non vide (car contient 1). Elle est majorée (par 2). On se propose de montrer qu'elle n'admet pas de borne supérieure dans $\mathbb{Q}$.

On introduit pour cela le sous-ensemble $B = \{x \in \mathbb{Q}_+\ ;\ x^2 > 2\}$. Puisque l'équation $x^2 = 2$ n'a pas de solution dans $\mathbb{Q}$, on a $\mathbb{Q}_+ = A \cup B$. On raisonne en plusieurs étapes:

(i) Pour tout $x \in A$, il existe $y \in A$ tel que $y > x$.

En effet, posons $y = \frac{2x+2}{x+2}$. On a alors $x - y = \frac{x^2-2}{x+2}$ et $y^2 - 2 = 2\frac{x^2-2}{(x+2)^2}$. L'hypothèse $x^2 < 2$ implique alors $y^2 < 2$ et $x < y$.

(ii) Pour tout $x \in B$, il existe $y \in B$ tel que $y < x$.

En effet, toujours avec $y = \frac{2x+2}{x+2}$, les égalités $x - y = \frac{x^2-2}{x+2}$ et $y^2 - 2 = 2\frac{x^2-2}{(x+2)^2}$ avec l'hypothèse $x^2 > 2$ implique $y^2 > 2$ et $x > y$.

(iii) B est l'ensemble des majorants de A dans $\mathbb{Q}$.

En effet, il est clair que tout élément de B majore A. Réciproquement, soit M un majorant de A dans $\mathbb{Q}$. D'une part $M \in \mathbb{Q}_+$ puisque $A \subset \mathbb{Q}_+$, d'autre part il résulte de (i) que $M \notin A$. Donc, puique $\mathbb{Q} = A \cup B$, on a forcément $M \in B$.

Bilan: la partie A de $\mathbb{Q}$ est non-vide, majorée, et elle n'admet pas de plus petit majorant dans $\mathbb{Q}$ (d'après les points (ii) et (iii) ci-dessus). □

Les conséquences de cette propriété sont évidemment très importantes pour toute considération de topologie ou d'analyse dans $\mathbb{Q}$.

En effet, les propriétés de la valeur absolue dans $\mathbb{Q}$ vues en 2.5 permettent de considérer dans $\mathbb{Q}$ par exemple les notions de suites convergentes ou de suite de Cauchy, mais, du fait de la défaillance de l'axiome de la borne supérieure, les propriétés obtenues vont être très différentes de celles connues sur les réels (suites croissantes et majorées de rationnels ne convergeant pas dans $\mathbb{Q}$, suites de Cauchy ne convergeant pas dans $\mathbb{Q}$,...)

2. $\mathbb{Q}$ *comme sous-corps ordonné de* $\mathbb{R}$. Supposons maintenant connu le corps ordonné $\mathbb{R}$ des nombres réels. Il contient $\mathbb{Q}$ comme sous-corps ordonné, strictement. On peut caractériser les rationnels parmi les réels par la périodicité de leur développement décimal (voir la leçon sur les nombres décimaux).

(i) $\mathbb{Q}$ *est dense dans* $\mathbb{R}$.

Preuve. Soient x et y deux réels tels que $x < y$. Posons $\varepsilon = y - x \in \mathbb{R}_+^*$. Parce que $\mathbb{R}$ est archimédien, il existe $n \in \mathbb{N}^*$ tel que $n\varepsilon > 1$, donc $\frac{1}{n} < \varepsilon$. En notant $m = [nx] + 1$, on a $m - 1 = [nx] \leq nx < m$, d'où $x < \frac{m}{n} \leq x + \frac{1}{n} < x + \varepsilon = y$. Ainsi $\mathbb{Q} \cap]x, y[\neq \emptyset$, ce qui prouve le résultat voulu. □

(ii) $\mathbb{Q}$ *n'est pas complet.*

Preuve. Considérons les deux suites de rationnels $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ définies par:

$$u_n = 1 + 1 + \tfrac{1}{2} + \tfrac{1}{6} + \tfrac{1}{24} + \cdots + \tfrac{1}{n!} = \sum_{k=0}^{n} \tfrac{1}{k!} \quad \text{et} \quad v_n = u_n + \tfrac{1}{(n+1)!}.$$

On vérifie aisément que ces deux suites sont adjacentes. Par suite, elles convergent dans $\mathbb{R}$, vers une limite commune e qui vérifie $u_n < e < v_n$ pour tout $n \in \mathbb{N}$. Montrons que e est irrationnel. Par l'absurde, supposons que $e = \frac{p}{q}$ avec $p, q \in \mathbb{N}^*$. En réduisant tous les termes de la somme u_q au même dénominateur $q!$, on peut écrire $u_q = \frac{a}{q!}$ avec $a \in \mathbb{N}^*$. L'encadrement $u_q < e < v_q$ conduit alors à: $\frac{a}{q!} < \frac{p}{q} < \frac{a}{q!} + \frac{1}{q \times q!}$ Donc: $a < p \times (q-1)! < a + \frac{1}{q}$. On en tire en particulier: $a < p \times (q-1)! < a + 1$, ce qui est impossible puisque $p \times (q-1)!$ est entier.

On conclut que la suite de rationnels (u_n) ne converge pas dans $\mathbb{Q}$ (puisque sa limite dans $\mathbb{R}$ n'appartient pas à $\mathbb{Q}$), bien qu'elle soit évidemment de Cauchy (puisque convergeant dans $\mathbb{R}$). □

Leçon 6

Anneau des nombres décimaux

I. Notion de nombre décimal.

1.1 Ensemble des nombres décimaux.

1.1.a. Définition.

On appelle nombre décimal tout nombre rationnel x pour lequel il existe $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ tels que $x = \frac{a}{10^n}$.
En d'autres termes, un rationnel x est un nombre décimal lorsqu'il existe $n \in \mathbb{N}$ tel que $x.10^n$ soit entier.

1.1.b. Notations et remarques.

(i) On note $\mathbb{D}$ le sous-ensemble de $\mathbb{Q}$ formé des nombres décimaux. Il est clair que: $\mathbb{Z} \subseteq \mathbb{D} \subseteq \mathbb{Q}$.

(ii) Pour tout $n \in \mathbb{N}$, on note $\mathbb{D}_n$ le sous-ensemble de $\mathbb{D}$ formé des nombres décimaux de la forme $\frac{a}{10^n}$ avec $a \in \mathbb{Z}$. Il est clair que $\mathbb{D}_n \subset \mathbb{D}_{n+1}$ et que $\mathbb{D} = \bigcup_{n\in\mathbb{N}} \mathbb{D}_n$.

(iii) L'inclusion $\mathbb{Z} \subseteq \mathbb{D}$ est stricte. Il est immédiat qu'un nombre décimal $x = \frac{a}{10^n}$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ est un entier si et seulement si 10^n divise a dans $\mathbb{Z}$. Par exemple $\frac{3}{10} \in \mathbb{D}$ et $\frac{3}{10} \notin \mathbb{Z}$.

(iv) L'inclusion $\mathbb{D} \subseteq \mathbb{Q}$ est également stricte.

Ainsi $\frac{2}{3} \in \mathbb{Q}$ et $\frac{2}{3} \notin \mathbb{D}$. En effet, si $\frac{2}{3}$ était un nombre décimal, il existerait $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ tels que $\frac{2}{3} = \frac{a}{10^n}$, d'où $3a = 2.10^n$; l'entier 3 diviserait 2.10^n, ce qui est faux.

La proposition suivante caractérise ceux des éléments de $\mathbb{Q}$ qui sont dans $\mathbb{D}$.

1.1.c. Proposition. Soit $x = \frac{a}{b} \in \mathbb{Q}$ sous forme irréductible, avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, et $\text{pgcd}(a, b) = 1$. Alors:

$$[\, x \in \mathbb{D} \,] \Leftrightarrow [\, b = 1 \text{ ou les seuls diviseurs premiers de } b \text{ sont 2 et 5} \,].$$

Preuve. Si $\frac{a}{b} \in \mathbb{D}$, il existe $c \in \mathbb{Z}$ et $n \in \mathbb{N}$ tels que $\frac{a}{b} = \frac{c}{10^n}$, donc $a.10^n = cb$. Ainsi b divise $a.10^n$. Comme b est premier avec a, on déduit du lemme de Gauss que b divise 10^n, d'où le résultat voulu. Réciproquement si $b = 2^p 5^q$ avec $p, q \in \mathbb{N}$, on a $x = \frac{a}{b} = \frac{a}{2^p 5^q} = \frac{a 2^q 5^p}{10^{p+q}}$, et donc $x \in \mathbb{D}$. □

1.2 Anneau des nombres décimaux.

1.2.a Proposition. L'ensemble $\mathbb{D}$ des nombres décimaux est un sous-anneau du corps $\mathbb{Q}$.

Preuve. Evidente, laissée au lecteur. □

1.2.b Remarque. Le sous-anneau $\mathbb{D}$ n'est pas un sous-corps de $\mathbb{Q}$. Il existe des éléments non-nuls de $\mathbb{D}$ qui ne sont pas inversibles dans $\mathbb{D}$, c'est-à-dire plus précisément dont l'inverse dans $\mathbb{Q}$ n'appartient pas au sous-anneau $\mathbb{D}$. C'est le cas par exemple de $x = \frac{3}{2} = \frac{15}{10}$, dont l'inverse $\frac{2}{3}$ n'est pas dans $\mathbb{D}$ comme on l'a vu ci-dessus. Il est donc naturel de chercher à déterminer le groupe des unités de l'anneau $\mathbb{D}$, c'est-à-dire le groupe multiplicatif des éléments de $\mathbb{D}$ qui sont inversibles dans $\mathbb{D}$. C'est l'objet de la proposition suivante.

1.2.c Proposition. Soit $x = \frac{a}{10^n} \in \mathbb{D}$ avec $a \in \mathbb{Z}^*$. Alors:

$$[\, x \text{ inversible dans } \mathbb{D} \,] \Leftrightarrow [\, a = \pm 1 \text{ ou les seuls diviseurs premiers de } a \text{ sont 2 et 5} \,].$$

Preuve. Supposons $x = \frac{a}{10^n}$ inversible dans $\mathbb{D}$. Donc $x^{-1} = \frac{10^n}{a} \in \mathbb{D}$. En notant $a = a'.2^p 5^q$ avec $p, q \in \mathbb{N}$ et $a' \in \mathbb{Z}^*$ non divisible par 2 ni par 5, on a $x^{-1} = \frac{2^n 5^n}{a'.2^p 5^q} \in \mathbb{D}$, ce qui implique d'après la proposition 1.1.c que $a' = \pm 1$, et prouve le résultat voulu. La réciproque est claire, toujours d'après la proposition 1.1.c. □

1.2.d. Remarque. On vérifie aisément que les sous-ensembles $\mathbb{D}_n$ sont des sous-groupes additifs de $\mathbb{D}$, mais ne sont pas stables par multiplication si $n \geq 1$ (le produit d'un élément de $\mathbb{D}_n$ par un élément de $\mathbb{D}_m$ appartient $\mathbb{D}_{n+m}$).

1.3 Ecriture décimale des nombres décimaux.

1.3.a Proposition. Soit $x = \frac{a}{10^n}$ un nombre décimal, avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$. Il existe, et ceci de façon unique, un entier $\alpha_0 \in \mathbb{Z}$ et des entiers naturels $\alpha_1, \dots, \alpha_n \in [\![0, 9]\!]$ tels que:

$$x = \alpha_0 + \alpha_1 10^{-1} + \alpha_2 10^{-2} \cdots + \alpha_{n-1} 10^{n-1} + \alpha_n 10^{-n}.$$

Preuve. En effectuant des divisions euclidiennes successives par 10, on obtient:

$a = 10q_1 + \alpha_n$ avec $0 \leq \alpha_n < 10$,
$= 10(10q_2 + \alpha_{n-1}) + \alpha_n = 10^2 q_2 + 10\alpha_{n-1} + \alpha_n$ avec $0 \leq \alpha_{n-1}, \alpha_n < 10$,
$= 10^2(10q_3 + \alpha_{n-2}) + 10\alpha_{n-1} + \alpha_n = 10^3 q_3 + 10^2\alpha_{n-2} + 10\alpha_{n-1} + \alpha_n$ avec $0 \leq \alpha_{n-2}, \alpha_{n-1}, \alpha_n < 10$,
.....

En itérant, on détermine ainsi (et ceci de façon unique par unicité du quotient et du reste dans la division euclidienne) un entier $\alpha_0 \in \mathbb{Z}$ et des entiers $\alpha_1, \dots, \alpha_n \in [\![0, 9]\!]$ tels que: $a = 10^n\alpha_0 + 10^{n-1}\alpha_1 + \cdots + 10\alpha_{n-1} + \alpha_n$. Le résultat voulu s'en déduit en divisant les deux membres par 10^n. □

1.3.b Notation. Lorsque l'on suppose de plus que x est positif dans la proposition ci-dessus, on note:

$$x = \alpha_0, \alpha_1\alpha_2 \dots \alpha_n.$$

L'entier α_0 est la partie entière de x. Le chiffre α_1 est le chiffre des dixièmes, α_2 celui des centièmes,... D'une manière générale, α_k est appelée la k-ième décimale de a (pour $1 \leq k \leq n$).

1.3.c Exemples.
$x = \frac{28}{10^2} = (0.10^2 + 2.10 + 8).10^{-2} = 0 + 2.10^{-1} + 8.10^{-2}$; on note $x = 0, 28$.
$x = \frac{35147}{10^3} = (35.10^3 + 1.10^2 + 4.10 + 7).10^{-3} = 35 + 1.10^{-1} + 4.10^{-2} + 7.10^{-3}$; on note $x = 35, 147$.

1.3.d Cas des nombres décimaux négatifs. Si $y \in \mathbb{D}$ est négatif, on pose $x = -y$. On utilise la notation 1.3.b pour x, et l'on note $y = -\alpha_0, \alpha_1\alpha_2 \dots \alpha_n$.
Prenons par exemple $y = -\frac{321}{10^2} = (-4.10^2 + 7.10 + 9).10^{-2} = -4 + 7.10^{-1} + 9.10^{-2}$. Usuellement, on n'utilise pas l'écriture $y = (-4), 79$. On pose $x = -y = 3 + 2.10^{-1} + 1.10^{-2} = 3, 21$ et on écrit $y = -x = -3, 21$.

1.3.e Remarque. L'unicité dans la proposition 1.3.a s'entend pour un choix de n fixé. En effet, il est clair que $x = \frac{a}{10^n} = \frac{10a}{10^{n+1}} = \frac{100a}{10^{n+2}} = \cdots$, de sorte que l'on peut toujours rajouter des chiffres α_{n+i} nuls.
Par exemple $x = \frac{321}{10^2} = \frac{3210}{10^3} = \frac{32100}{10^4} = \cdots$, de sorte que $x = 3, 21 = 3, 210 = 3, 2100 = \cdots$

1.3.f Remarque de transition. Le but de ce qui suit est de définir une écriture décimale pour tout nombre réel, ce qui ne peut se faire qu'en passant d'une suite finie de chiffres (suffisante pour écrire tout nombre décimal) à une suite éventuellement infinie (nécessaire pour étendre à tout réel).

II. Approximations décimales et développement décimal d'un nombre réel.

2.1 Valeurs décimales approchées d'un réel.

2.1.a Définition. Soit $x \in \mathbb{R}$. Pour tout $n \in \mathbb{N}$, on appelle *valeur décimale approchée* de x à 10^{-n} près par défaut ou par excès les nombres décimaux définis respectivement par:

$$u_n = 10^{-n}[10^n x] \qquad \text{et} \qquad v_n = 10^{-n}([10^n x] + 1) = u_n + 10^{-n}. \tag{1}$$

Par définition de la partie entière, on a: $10^n u_n = [10^n x] \leq 10^n x < [10^n x] + 1 = 10^n v_n$. Et donc:

$$u_n \leq x < v_n \quad \text{et} \quad v_n - u_n = 10^{-n}. \tag{2}$$

On a $u_n \in \mathbb{D}_n$ et $v_n \in \mathbb{D}_n$, et on vérifie aisément que, pour tout $n \in \mathbb{N}$, le couple (u_n, v_n) défini par (1) est le seul couple d'éléments de $\mathbb{D}_n$ vérifiant la propriété (2).

2.1.b Remarques.

- Pour tout $x \in \mathbb{R}$, on a $u_0 = [x] \leq x < v_0 = [x] + 1$.
- Pour tout $x \in \mathbb{Z}$ et tout $n \in \mathbb{N}$, on a $[10^n x] = 10^n x$, donc $u_n = x < v_n = x + 10^{-n}$.
- Pour tout $x \in \mathbb{D}$, la suite (u_n) est stationnaire.
  En effet: soit $x = 10^{-n}a$ avec $n \in \mathbb{N}$ et $a \in \mathbb{Z}$; soit $m \geq n$, de sorte que $10^m x = 10^{m-n}a$ qui est entier; donc $u_m = 10^{-m}[10^m x] = 10^m 10^{m-n}a = 10^{-n}a$; ainsi $u_m = x$ dès lors que $m \geq n$.
  Par exemple: soit $x = 1976.10^{-2} = 19, 76$. On a: $u_0 = 19$ et $v_0 = 20$; $u_1 = 19, 7$ et $v_1 = 19, 8$; $u_2 = 19, 76 = x$ et $v_2 = 19, 77$; puis $u_m = x$ et $v_m = x + 10^{-m}$ pour $m \geq 2$.

2.1.c Exemple. Pour le réel (rationnel) $x = \frac{9}{7}$, les cinq premiers termes des suites (u_n) et (v_n) sont:

$u_0 = E(\frac{9}{7}) = 1$, et donc $v_0 = 2$,
$u_1 = 10^{-1}E(\frac{90}{7}) = 10^{-1}.12 = 1,2$ et donc $v_1 = 1,3$,
$u_2 = 10^{-2}E(\frac{900}{7}) = 10^{-2}.128 = 1,28$ et donc $v_2 = 1,29$,
$u_3 = 10^{-3}E(\frac{9000}{7}) = 10^{-3}.1285 = 1,285$ et donc $v_3 = 1,286$,
$u_4 = 10^{-4}E(\frac{90000}{7}) = 10^{-4}.12857 = 1,2857$ et donc $v_4 = 1,2858$.

2.1.d Théorème. Pour tout réel x, les suites (u_n) et (v_n) ci-dessus sont adjacentes et convergent vers x.

Preuve. Pour tout entier naturel n, posons $a_n = [10^n x]$. On a: $a_n \leq 10^n x < a_n + 1$ et donc, en multipliant par 10, il vient: $10a_n \leq 10^{n+1}x < 10a_n + 10$. Or par définition de a_{n+1}, on a: $10^{n+1}x < a_{n+1} + 1$. Par suite, $10a_n < a_{n+1} + 1$ et donc $10a_n \leq a_{n+1}$, ce qui conduit, en multipliant par 10^{-n-1}, à $u_n \leq u_{n+1}$. Ainsi (u_n) est croissante. On montre de façon analogue que (v_n) est décroissante. Comme de plus $(v_n - u_n) = 10^{-n}$ converge vers 0, on conclut que les deux suites sont adjacentes. On sait qu'elles convergent alors vers une même limite l; puisque $u_n \leq x < v_n$ pour tout $n \in \mathbb{N}$, on a nécessairement $l = x$. □

2.1.e Corollaire. $\mathbb{D}$ est dense dans $\mathbb{R}$.

Preuve. Claire puisque, d'après ce qui précède, tout réel est limite d'une suite de décimaux. □

2.2 Développement décimal d'un réel.

2.2.a Théorème fondamental.

Pour tout $x \in \mathbb{R}$, il existe une unique suite $(\alpha_k)_{k\geq 0}$ d'entiers telle que:

(i) *pour tout $k \geq 1$, $\alpha_k \in [\![0, 9]\!]$;*

(ii) $x = \alpha_0 + \sum_{k=1}^{+\infty} \frac{\alpha_k}{10^k}$;

(iii) *pour tout $N \geq 0$, il existe un entier $k > N$ tel que $\alpha_k \neq 9$.*

Preuve. 1. Existence. Montrons que, en posant comme ci-dessus $a_n = [10^n x]$ pour tout $n \in \mathbb{N}$, la suite (α_k) définie par: $\alpha_0 = a_0$ et $\alpha_k = a_k - 10a_{k-1}$ pour tout $k \geq 1$, répond à la question.

• Point (i). Soit $k \geq 1$. Par définition des a_k, on a: $10^k x - 1 < a_k \leq 10^k x$ et $10^{k-1}x - 1 < a_{k-1} \leq 10^{k-1}x$. On en déduit: $10^k x - 1 - 10^k x < \alpha_k < 10^k x - 10(10^{k-1}x - 1)$. Donc: $-1 < \alpha_k < 10$, et finalement $\alpha_k \in [\![0, 9]\!]$ puisque α_k est entier.

• Point (ii). Pour tout $n \geq 1$, on a: $\sum_{k=0}^{n} \frac{\alpha_k}{10^k} = a_0 + \sum_{k=1}^{n} \left[\frac{a_k}{10^k} - \frac{a_{k-1}}{10^{k-1}}\right] = \frac{a_n}{10^n}$, et donc, en reprenant les notations (1) de 2.1.a: $\sum_{k=0}^{n} \frac{\alpha_k}{10^k} = u_n$. D'où le résultat puisque d'aprs 2.1.d la suite (u_n) converge vers x.

• Point (iii). Par l'absurde, supposons qu'il existe $N \in \mathbb{N}$ tel que $\alpha_k = 9$ pour tout $k > N$. On aurait alors d'après (ii) l'égalité: $x = \sum_{k=0}^{N} \frac{\alpha_k}{10^k} + \frac{9}{10^{N+1}} \sum_{p=0}^{+\infty} \frac{1}{10^p}$, c'est-à-dire $x = u_N + \frac{9}{10^{N+1}} \times \frac{1}{1-\frac{1}{10}} = u_N + \frac{1}{10^N}$. Avec les notations (1) de 2.1.a, on obtiendrait $x = v_N$, ce qui contredirait l'inégalité (2) de 2.1.a.

2. Unicité. Supposons qu'il existe une autre suite (β_k) vérifiant les conditions (i), (ii) et (iii). Pour tout $n \in \mathbb{N}$, posons $x_n = \sum_{k=0}^{n} \frac{\beta_k}{10^k}$. On se propose de vérifier que x_n est, pour tout n, la valeur décimale approchée de x à 10^{-n} près par défaut, ce qui impliquera $x_n = u_n$ pour tout $n \in \mathbb{N}$, et donc $\alpha_k = \beta_k$ pour tout $k \in \mathbb{N}$. Les conditions (i) et (ii) impliquent d'abord que, pour tout $n \in \mathbb{N}$, on a: $x_n \leq x = x_n + \sum_{k=n+1}^{+\infty} \frac{\beta_k}{10^k} \leq x_n + \frac{1}{10^n}$. Si la seconde inégalité n'était pas toujours stricte, il existerait $N \in \mathbb{N}$ tel que $x = x_N + \frac{1}{10^N}$. Comme la suite (y_n) définie par $y_n = x_n + \frac{1}{10^n}$ est décroissante, on aurait alors $x = x_n + \frac{1}{10^n}$ pour tout $n \geq N$, et donc en particulier $x_{n+1} + \frac{1}{10^{n+1}} = x_n + \frac{1}{10^n}$ pour tout $n \geq N$. Ainsi, pour tout $n \geq N$, on obtiendrait $x_{n+1} - x_n = \frac{9}{10^{n+1}}$, d'où $\beta_{n+1} = 9$, ce qui contredirait la propriété (iii). C'est donc que $x_n \leq x < x_n + \frac{1}{10^n}$ pour tout $n \in \mathbb{N}$. Comme $x_n \in \mathbb{D}_n$, l'unicité observée à la fin de 2.1.a montre que $x_n = u_n$, ce qui achève la preuve. □

2.2.b Définition. Avec les données et notations du théorème ci-dessus, l'expression du point (ii) s'appelle **le** développement décimal propre du réel x.

2.2.c Remarques, terminologie, notations.

- Dans l'expression *développement décimal propre* du réel x pour désigner l'écriture de (ii), l'adjectif "propre" est relatif à la propriété (iii), qui assure l'unicité, [voir la fin de la preuve ci-dessus et plus loin en 2.2.c].

- On a observé dans la preuve du théorème, et il est important de retenir que, avec les notations du théorème, les valeurs décimales approchées à 10^{-n} près de x sont données par:

$$u_n = \alpha_0 + \sum_{k=1}^{n} \frac{\alpha_k}{10^k} \ \leq \ x \ < \ v_n = u_n + 10^{-n}.$$

- En rappelant la troisième remarque de 2.1.b, il en résulte que le développement décimal propre d'un nombre décimal est fini, au sens où tous les α_k sont nuls à partir d'un certain rang.

- Lorsque x est un réel positif positif, on note $x = \alpha_0, \alpha_1\alpha_2\alpha_3\ldots$ son développement décimal propre, les points de suspension exprimant le fait qu'il ne s'agit pas forcément d'une suite finie.

  Pour tout $k \geq 1$, α_k s'appelle la k-ième décimale de x.

  Par exemple: $\frac{12}{25} = 0,48 = 0,4800000\ldots$; $\frac{12}{11} = 1,09090909\ldots$; $\pi = 3,141592654\ldots$

  le nombre de Mahler $= 0,123456789101112131415\ldots$

  Lorsque x est négatif, on procède comme en 1.3.d en considérant pour $y = -x$ l'écriture ci-dessus, et en plaçant un signe $-$ devant.

2.2.d Remarque. Si l'on ne suppose plus la condition (iii) du théorème 2.2.a, on peut ne plus avoir unicité du développement décimal. Montrons par exemple que: $7,25 = 7,25000000\ldots = 7,24999999\ldots$

Posons pour cela: $x = 7 + \frac{2}{10} + \frac{5}{100} + \sum_{k=3}^{+\infty} \frac{0}{10^k}$ et $x' = 7 + \frac{2}{10} + \frac{4}{100} + \sum_{k=3}^{+\infty} \frac{9}{10^k}$.

Donc: $x' - x = -\frac{1}{100} + 9\sum_{k=3}^{+\infty} \frac{1}{10^k} = -\frac{1}{100} + 9\big(\frac{1}{1-\frac{1}{10}} - 1 - \frac{1}{10} - \frac{1}{100}\big) = -\frac{1}{100} + 9\big(\frac{10}{9} - \frac{111}{100}\big) = 0$

On montre de même que tout nombre décimal admet deux développements décimaux distincts, l'un propre (formé de 0 à partir d'un certain rang) et un impropre (formé de 9 à partir d'un certain rang). Dans la pratique, on ne considèrera toujours que des développements décimaux propres.

III. Exemples d'applications.

3.1 Comparaison de deux réels par leur développement décimal

Proposition. Soient x et y deux réels donnés par leur développement décimal (propre):

$$x = \alpha_0 + \sum_{k=1}^{+\infty} \frac{\alpha_k}{10^k} \quad et \quad y = \beta_0 + \sum_{k=1}^{+\infty} \frac{\beta_k}{10^k}.$$

Alors : $(x < y) \Leftrightarrow (\exists\ N \in \mathbb{N},\ \alpha_N < \beta_N$ *et* $\alpha_k = \beta_k$ *pour tout* $0 \leq k < N)$.

Preuve. Supposons $x < y$. En particulier $x \neq y$, et par unicité du développement décimal, on peut considérer le plus petit entier $N \geq 0$ tel que $\alpha_N \neq \beta_N$. En reprenant la seconde remarque de 2.2.b, on a:

$u_N = \alpha_0 + \sum_{k=1}^{N} \alpha_k 10^{-k} \leq x < v_N = u_N + 10^{-N}$ et $u'_N = \beta_0 + \sum_{k=1}^{N} \beta_k 10^{-k} \leq y < v'_N = u'_N + 10^{-N}$.

On en déduit: $x \geq \alpha_0 + \alpha_1 10^{-1} + \alpha_2 10^{-2} \cdots + \alpha_{N-1} 10^{N-1} + \alpha_N 10^{-N}$,

et $\qquad y < \beta_0 + \beta_1 10^{-1} + \beta_2 10^{-2} \cdots + \beta_{N-1} 10^{N-1} + (\beta_N + 1) 10^{-N}$.

Puisque $\alpha_k = \beta_k$ si $0 \leq k \leq N-1$, il vient $0 < y - x < (\beta_N + 1 - \alpha_N) 10^{-N}$, donc $\alpha_N \leq \beta_N$, et finalement $\alpha_N < \beta_N$. La réciproque repose sur le même type de calcul et est laissée au lecteur. □

3.2 Caractérisation des rationnels par la périodicité de leur développement décimal propre.

3.2.a Définition Soit x un réel. On dit que son développement décimal propre $x = \alpha_0 + \sum_{k=1}^{+\infty} \frac{\alpha_k}{10^k}$ est périodique lorsqu'il existe deux entiers naturels N et p tels que, pour tout $n \geq N$, on ait $\alpha_n = \alpha_{n+p}$.
En clair cela signifie que, à partir d'un certain rang, un même groupe de chiffres se répète.
Par exemple:

→ $\frac{377}{300} = 1.25666666\ldots$, $\frac{1}{11} = 0,909090909\ldots$, $\frac{5}{7} = 0,714285714285714285\ldots$ sont périodiques,

→ tout développement décimal fini (représentant donc un nombre décimal) est périodique,

→ les développements $0,1234567891011121314\ldots$ ou $0,01001000100001\ldots$ ne sont pas périodiques.

3.2.b Théorème. Un réel est rationnel si et seulement si son développement décimal propre est périodique.

Preuve. Supposons $x \in \mathbb{Q}$; notons $x = \frac{p}{q}$ avec $p \in \mathbb{Z}, q \in \mathbb{N}^*$ premiers entre eux. On définit par récurrence deux suites (α_n) et (r_n) par divisions euclidiennes successives:

$p = \alpha_0 q + r_0$, $10r_0 = \alpha_1 q + r_1$, $10r_1 = \alpha_2 q + r_2$, ... avec $0 \leq r_0, r_1, r_2, \ldots < q$;

et plus généralement: $10r_{n-1} = \alpha_n q + r_n$ avec $0 \leq r_n < q$,

ce qui détermine α_n et r_n de façon unique à partir des précédents.
Il est clair que $\alpha_n \in [\![0, 9]\!]$ pour tout $n \geq 1$, (en effet, pour tout $n \geq 1$, on a $0 \leq \alpha_n q = 10r_{n-1} - r_n \leq 10r_{n-1} < 10q$ d'où $0 \leq \alpha_n < 10$).
De plus, on a:

$p = \alpha_0 q + r_0$ donc $\frac{p}{q} = \alpha_0 + \frac{r_0}{q}$;
$10r_0 = \alpha_1 q + r_1$ donc $\frac{r_0}{q} = \frac{\alpha_1}{10} + \frac{r_1}{10q}$, d'où $\frac{p}{q} = \alpha_0 + \frac{\alpha_1}{10} + \frac{r_1}{10q}$;
$10r_1 = \alpha_2 q + r_2$ donc $\frac{r_1}{10q} = \frac{\alpha_2}{10^2} + \frac{r_2}{10^2 q}$, d'où $\frac{p}{q} = \alpha_0 + \frac{\alpha_1}{10} + \frac{\alpha_2}{10^2} + \frac{r_2}{10^2 q}$;
et par récurrence évidente: $x = \frac{p}{q} = \alpha_0 + \sum_{k=1}^{n} \frac{\alpha_k}{10^k} + \frac{r_n}{10^n q}$.

Il en résulte que, en posant $a_n = [10^n x]$ pour tout $n \in \mathbb{N}$, on a: $\alpha_0 = a_0$ et $\alpha_k = a_k - 10a_{k-1}$ pour tout $k \geq 1$. Donc, d'après le début de la preuve du théorème 2.2.a, la suite (α_n) ainsi construite est exactement la suite des coefficients du développement décimal propre de x.

Ce développement est périodique. En effet, comme tout reste r_n vérifie $0 \leq r_n < q$, on retrouve nécessairement dans la suite des divisions euclidiennes effectuées le même reste après au plus q opérations. Plus précisément, il existe des entiers k, l tels que $0 \leq k < l \leq q$ et $r_k = r_l$. On a donc: $\alpha_{k+1} q + r_{k+1} = 10r_k = 10r_l = \alpha_{l+1} q + r_{l+1}$ d'où $\alpha_{l+1} = \alpha_{k+1}$ et $r_{l+1} = r_{k+1}$ (par unicité du quotient et du reste dans la division euclidienne). En itérant, on obtient $r_{l+m} = r_{k+m}$ et $\alpha_{l+m} = \alpha_{k+m}$ pour tout $m \geq 1$. Ceci implique, en notant $p = l - k$, que l'on a $\alpha_{n+p} = \alpha_n$ pour tout $n \geq k + 1$.

• Réciproquement, soit $x = \alpha_0 + \sum_{k=1}^{+\infty} \frac{\alpha_k}{10^k}$ un réel donné par son développement décimal propre, que l'on suppose périodique: il existe donc $p \geq 1$ tel que $\alpha_{n+p} = \alpha_n$ pour n supérieur à un certain rang N, que l'on suppose choisi minimum. On sait que la valeur décimale approchée par défaut à 10^{-n} près de x est donnée par: $u_n = \alpha_0 + \sum_{k=1}^{n} \frac{\alpha_k}{10^k}$ pour tout $n \geq 0$. Définissons une nouvelle suite (β_k) par $\beta_k = u_{N+kp}$ pour tout $k \geq 0$. C'est une suite extraite de (u_n), donc elle converge vers la même limite que (u_n), c'est-à-dire x (théorème 2.1.d). On calcule, en utilisant la périodicité:

$$\beta_{k+1} - \beta_k = \sum_{i=N+kp+1}^{N+kp+p} \frac{\alpha_i}{10^i} = \sum_{j=N+1}^{N+p} \frac{\alpha_{j+kp}}{10^{j+kp}} = 10^{-kp} \sum_{j=N+1}^{N+p} \frac{\alpha_j}{10^j} = 10^{-kp}(u_{N+p} - u_N),$$

si bien que:

$$\beta_{k+1} = \beta_0 + (u_{N+p} - u_N)(1 + 10^{-p} + 10^{-2p} + \cdots + 10^{-kp}).$$

Il en résulte que: $x = \lim_{k \to +\infty} \beta_k = \beta_0 + (u_{N+p} - u_N)(1 - 10^{-p})^{-1}$, qui est bien un rationnel puisque la suite (u_n) est à termes rationnels. □

3.3 Non-dénombrabilité de $\mathbb{R}$.

Proposition. L'ensemble $\mathbb{R}$ n'est pas dénombrable.

Preuve. Raisonnons par l'absurde en supposant qu'il existe une bijection f de $\mathbb{N}$ sur $\mathbb{R}$. Considérons pour tout $n \in \mathbb{N}$ le développement décimal propre de $f(n)$, noté:

$$f(n) = \alpha_{n,0} + \sum_{k=1}^{+\infty} \frac{\alpha_{n,k}}{10^k}.$$

Soit y le réel dont le développement décimal propre $y = \beta_0 + \sum_{k=1}^{+\infty} \frac{\beta_k}{10^k}$ est défini de la façon suivante:

β_0 = n'importe quel entier sauf $\alpha_{0,0}$, de sorte que $y \neq f(0)$ puisque leurs parties entières diffèrent,
β_1 = n'importe quel entier de $[\![0, 9]\!]$ sauf $\alpha_{1,1}$, de sorte que $y \neq f(1)$ puisque leurs chiffres des dixièmes diffèrent,

et plus généralement, pour tout $k \geq 1$,

β_k = n'importe quel entier de $[\![0, 9]\!]$ sauf $\alpha_{k,k}$, de sorte que $y \neq f(k)$ puisque leurs k-ièmes décimales diffèrent.

Par construction, $y \neq f(k)$ pour tout $k \in \mathbb{N}$, ce qui contredit la surjectivité de f. □