

Année universitaire 2004-2005

UNIVERSITÉ D'ORLÉANS

Olivier GARET

Structures Mathématiques
(Licence 1ère année semestre 2)

Table des matières

Table des matières	i
1 Construction de \mathbb{N}	1
1.1 Lois de composition interne	1
1.2 Groupes, sous-groupes	2
1.3 Axiomes de Peano	3
1.4 \mathbb{N} , ce monoïde	3
1.4.1 Définition de l'addition	3
1.4.2 Propriétés de l'addition	4
1.4.3 Relation d'ordre sur \mathbb{N}	5
1.5 Multiplication des entiers	8
1.5.1 Définition et propriétés	8
1.5.2 Division euclidienne	8
1.5.3 Bases de numération	9
1.6 Exercices	11
2 \mathbb{Z}	13
2.1 Relations d'équivalentes	13
2.1.1 Relations d'équivalences et partitions	13
2.1.2 Ensemble quotient	14
2.2 Construire \mathbb{Z}	16
2.3 La structure d'anneau	17
2.3.1 vocabulaire	17
2.3.2 Propriétés de \mathbb{Z}	17
2.3.3 Règles de calcul	17
2.4 Exercices	19
3 Divisibilité	23
3.1 Sous-groupes de \mathbb{Z}	23
3.2 PGCD	24
3.2.1 Compléments sur les groupes	24

3.2.2	PGCD de deux entiers	24
3.2.3	Propriétés de base	24
3.2.4	Algorithme d'Euclide	26
3.2.5	Lemme de Gauss – Application à la résolution de l'équation de l'équation $au + bv = n$	27
3.2.6	PGCD de plusieurs entiers	29
3.3	PPCM de deux ou plusieurs entiers	30
3.4	Congruence	31
3.5	Exercices	32
4	Nombres premiers	35
4.1	Définition et premières propriétés	35
4.2	Décomposition d'un nombre en produit de facteurs premiers	36
4.2.1	Existence et unicité de la décomposition	36
4.2.2	Application au calcul du PGCD et du PPCM	37
4.3	Exercices	39
5	$\mathbb{Z}/n\mathbb{Z}$	41
5.1	Construction de l'anneau $\mathbb{Z}/n\mathbb{Z}$	41
5.2	Inversibles de $\mathbb{Z}/n\mathbb{Z}$	41
5.2.1	Caractérisation des inversibles	41
5.2.2	Groupe des éléments inversibles – indicatrice d'Euler	42
5.3	Théorème chinois	43
5.4	Calcul de l'indicatrice d'Euler	44
5.5	Codage RSA	45
5.6	Exercices	47

Chapitre 1

Construction de \mathbb{N}

1.1 Lois de composition interne

Définition: Soit X un ensemble. On appelle loi de composition interne sur X toute application \star de $X \times X$ dans X :

$$\begin{aligned} X \times X &\rightarrow X \\ (x, y) &\mapsto x \star y := \star(x, y) \end{aligned}$$

Ici, on choisira d'utiliser la $x \star y$ plutôt que $\star(x, y)$. Voici pourquoi :

Définition: Soit X un ensemble et \star une loi de composition interne sur X . On dit que \star est associative si on a

$$\forall (x, y, z) \in X \times X \times X \quad (x \star y) \star z = x \star (y \star z)$$

Ainsi, pour une loi de composition interne associative, on peut écrire $x \star y \star z$ sans que cela soit source d'ambiguïté.

Exemples: $+$ et \times sont des lois de composition internes sur \mathbb{R} . $/$ est une loi de composition interne sur $]0, +\infty[$.

De plus, $+$ et \times sont des lois de composition internes associatives sur \mathbb{R} . Cependant, $/$ n'est pas une loi de composition interne associative sur $]0, +\infty[$ car $1/(1/2) = 2$ n'est pas égal à $(1/1)/2 = 1/2$.

Définition: On dit qu'un élément e est neutre pour la loi de composition interne \star sur X si

$$\forall x \in X \quad e \star x = x \star e = x.$$

Il y a toujours au plus un élément neutre, car si e et e' sont deux éléments neutre $e = e \star e' = e'$.

Définition: Le couple (X, \star) formé par un ensemble X et une loi de composition interne associative sur X possédant un élément neutre est appelé un monoïde.

Exemples: Si \mathcal{G} est une famille d'applications d'un ensemble E dans lui-même telle que

- $\text{Id}_E \in \mathcal{G}$.
- $\forall (f, g) \in \mathcal{G} \times \mathcal{G} \quad f \circ g \in \mathcal{G}$,

alors (\mathcal{G}, \circ) est un monoïde

Par exemple, l'ensemble des applications affines sur \mathbb{R} forme un monoïde.

Définition: On dit qu'un élément x d'un monoïde (X, \star) dont l'élément neutre est noté e est inversible s'il existe un $y \in X$ tel que

$$x \star y = y \star x = e.$$

S'il existe, un tel élément est nécessairement unique : en effet si $x \star y = y \star x = e$ et $x \star y' = y' \star x = e$, alors

$$y' = y' \star e = y' \star (x \star y) = (y' \star x) \star y = e \star y = y.$$

Usuellement, on note x^{-1} l'inverse de x lorsqu'il existe. (On trouvera plus rarement $x^{\star-1}$) : cette notation n'est employée que si plusieurs structures de groupe sont mises sur l'ensemble considéré et qu'une ambiguïté est possible.)

1

1.2 Groupes, sous-groupes

Définition: Un monoïde (G, \star) dont tous les éléments sont inversibles est appelé un groupe.

Exemples: Si \mathcal{G} est une famille de bijections d'un ensemble E dans lui-même telle que

- $\text{Id}_E \in \mathcal{G}$.
- $\forall (f, g) \in \mathcal{G} \times \mathcal{G} \quad f \circ g \in \mathcal{G}$,

alors (\mathcal{G}, \circ) est un groupe.

Lorsque X est un ensemble fini, on note $\mathcal{S}(X)$ le groupe formé par l'ensemble des bijections de X dans lui-même muni de la composition

Traditionnellement, on appelle "permutations" les éléments de $\mathcal{S}(X)$, et, fort logiquement, on appelle ce groupe le groupe des permutations.

Définition: Soit (G, \star) un groupe, H une partie de G . On dit que H est un sous-groupe de G si (H, \star) un groupe.

On montre (le faire!) que H est un sous-groupe de G si et seulement si pour tous x, y de H , $x \star y^{-1} \in H$.

On dit souvent d'un sous-groupe de $\mathcal{S}(X)$ qu'il est un "groupe de permutations". Historiquement, c'est l'étude de groupes de permutations qui ont amené à l'invention de la notion de groupes

1.3 Axiomes de Peano

Les axiomes de Peano postulent l'existence d'un ensemble \mathbb{N} contenant un élément 0 et d'une application injective

$$\begin{aligned} s : \mathbb{N} &\rightarrow \mathbb{N} \setminus \{0\} \\ x &\mapsto s(x) \end{aligned}$$

et vérifiant la propriété suivante : si $A \subset \mathbb{N}$, $0 \in A$ et $s(A) \subset A$, alors $A = \mathbb{N}$. Cette propriété est appelée principe de récurrence.

Notation : on note couramment $1 = s(0)$, $2 = s(1)$, $3 = s(2)$, $4 = s(3)$, $5 = s(4)$, $6 = s(5)$, $7 = s(6)$, $8 = s(7)$, $9 = s(8)$.

Dans la suite, on verra que $s(n)$ est ce que nous avons l'habitude $n + 1$, où plus précisément que l'on peut définir une addition "+" (en fait une loi de composition interne) de telle manière que $n + 1 = s(n)$.

On connaît plus souvent la propriété de récurrence sous la forme suivante : si $\mathcal{P}(n) \rightarrow \mathcal{P}(n + 1)$ et que $\mathcal{P}(0)$, alors $\mathcal{P}(n)$ est vraie pour tout n . Pour démontrer cela, il suffit d'appliquer le principe de récurrence à l'ensemble $A = \{n \in \mathbb{N}; \mathcal{P}(n) \text{ est vrai}\}$.

Une autre conséquence simple du principe de récurrence est que pour tout $n \neq 0$, existe $k \in \mathbb{N}; n = s(k)$. En effet notons $A = \{0\} \cup \{s(k); k \in \mathbb{N}\}$: il est facile de voir que $0 \in A$ et que $s(A) \subset A$. On en déduit que $A = \mathbb{N}$, ce qui signifie que tout entier naturel est soit 0, soit l'image d'un entier naturel par s .

1.4 \mathbb{N} , ce monoïde

1.4.1 Définition de l'addition

Il est possible de définir une loi de composition interne $+$ sur \mathbb{N} caractérisée par les identités

$$\begin{cases} n + 1 = s(n) \\ n + s(p) = s(n + p) \end{cases}$$

Il n'est pas évident d'écrire une preuve rigoureuse de l'existence d'une telle loi de composition interne. Donnons juste quelques idées. Si on met ensemble les deux propriétés ci-dessus et que l'on fait $p = 0$, on a $s(n) = n + 1 = n + s(0) = s(n + 0)$. Comme s est injective, on doit nécessairement définir $n + 0 = n$. On sait donc comment définir $n + 0$ et $n + 1$. Voyons comment définir $n + 2$: comme $2 = s(1)$, il faut définir $n + 2 = n + s(1) = s(n + 1)$,

ce qui est bien une définition correcte puisque $s + 1$ est définie. De même on définit $n + 3$ par $n + 3 = s(n + 2)$, etc. Toute la difficulté consiste à donner un sens rigoureux à ce “etc.” Nous préférons renvoyer le lecteur à un ouvrage de référence pour cette preuve assez technique.

1.4.2 Propriétés de l’addition

Nous allons montrer que la loi de composition interne définie ci-dessus est une loi associative et commutative pour laquelle 0 est l’élément neutre.

Montrons d’abord que pour tout n , $0 + n = n$ (rappelons qu’on sait déjà que $n + 0 = n$ car on l’a défini comme cela). Soit $A_0 = \{n \in \mathbb{N}; 0 + n = n\}$. On a clairement $0 \in A_0$ car $0 + 0 = 0$. Maintenant montrons que $n \in A_0 \longrightarrow s(n) \in A_0$: on a pour tout $n \in \mathbb{N}$ $0 + s(n) = s(0 + n)$. Mais si $n \in A_0$, alors $0 + n = n$, d’où $0 + s(n) = s(n)$, ce qui montre que $s(n) \in A_0$. D’après le principe de récurrence $A_0 = \mathbb{N}$.

On va maintenant montrer l’associativité : soit $B = \{n \in \mathbb{N} ; \forall(p, q) \in \mathbb{N}^2 (p+q)+n = p+(q+n)\}$. Comme 0 est neutre pour +, $0 \in B$. Maintenant montrons que $n \in B \longrightarrow s(n) \in B$: on a

$$\begin{aligned} (p + q) + s(n) &= s((p + q) + n) \textit{définition de l'addition} \\ &= s(p + (q + n)) \textit{hypothèse de récurrence} \\ &= p + s(q + n) \textit{définition de l'addition} \\ &= p + (q + s(n)) \textit{définition de l'addition} \end{aligned}$$

Montrons maintenant la commutativité. On va commencer par montrer que $\forall n \in \mathbb{N} \quad 1 + n = n + 1$. Notons $C = \{n \in \mathbb{N}; n + 1 = 1 + n\}$. $0 \in C$ car 0 est neutre pour +. Ensuite, notons $C = \{n \in \mathbb{N}; n + 1 = 1 + n\}$. Montrons que $n \in C \longrightarrow s(n) \in C$: on a

$$\begin{aligned} 1 + s(n) &= 1 + (n + 1) \\ &= (1 + n) + 1 \textit{ par associativité} \\ &= (n + 1) + 1 \textit{ hypothèse de récurrence} \\ &= s(n) + 1 \end{aligned}$$

Maintenant, notons $D = \{p \in \mathbb{N}; \forall n \in \mathbb{N} \quad n + p = p + n\}$. Comme 0 est

neutre pour $+$, on sait que $0 \in B$. Montrons que $p \in D \longrightarrow s(p) \in D$.

$$\begin{aligned}
 n + s(p) &= s(n + p) && \text{définition de l'addition} \\
 &= s(p + n) && \text{hypothèse de récurrence} \\
 &= (p + n) + 1 && \text{par définition} \\
 &= p + (n + 1) && \text{associativité} \\
 &= p + (1 + n) && \text{d'après la propriété montrée au dessus} \\
 &= (p + 1) + n && \text{hypothèse de récurrence} \\
 &= s(p) + n && \text{par définition}
 \end{aligned}$$

1.4.3 Relation d'ordre sur \mathbb{N}

On définit une relation \leq binaire sur N par

$$\forall a, b \in \mathbb{N}^2 \quad a \leq b \iff \exists n \in \mathbb{N} \quad a + n = b.$$

\leq est bien une relation d'ordre car on a

- Réflexivité : pour tout entier naturel a , $a \leq a$ car $a = a + 0$.
- Transitivité : pour tous entier naturel a, b, c , si $a \leq b$ et $b \leq c$, alors $a \leq c$. En effet si, $a \leq b$, on peut écrire $b = a + n_1$ pour un certain entier n_1 , et si $b \leq c$, on peut écrire $c = b + n_2$ pour un certain entier n_2 , d'où finalement $c = b + n_2 = (a + n_1) + n_2 = a + (n_1 + n_2)$, donc $a \leq c$.
- Antisymétrie Il s'agit de montrer que si $a \leq b$ et $b \leq a$, alors $a = b$. Dans ce cas, on peut écrire $b = a + n_1$, $a = b + n_2$, d'où $a = a + (n_1 + n_2)$. On va d'abord montrer que $n_1 + n_2 = 0$. Pour celà, on va montrer que pour tout $b, a, b \in \mathbb{N}$ ($n + a = n + b$) \implies ($a = b$). Pour celà, il suffit de montrer que pour tout n , l'application

$$\begin{aligned}
 s_n : \mathbb{N} &\rightarrow \mathbb{N} \\
 x &\mapsto x + n
 \end{aligned}$$

est injective. Mais par définition de l'addition, on a la formule de récurrence $s_{n+1} = s \circ s_n$. Comme s est injective et s_0 aussi (c'est l'identité), il est facile de montrer par récurrence que s_n est injective pour tout n .

Ainsi, de $a + 0 = a = a + (n_1 + n_2)$, on déduit que $n_1 + n_2 = 0$ n_1 est nécessairement nul, car s'il existe k_1 entier avec $n_1 = s(k_1) = k_1 + 1$. Dès lors, on pourrait écrire $0 = n_1 + n_2 = k_1 + 1 + n_2 = (k_1 + n_2) + 1 + s(k_1 + n_2)$, ce qui contredirait un axiome de base de \mathbb{N} . On en déduit que $b = a + n_1 = a + 0 = a$, ce qu'il fallait démontrer.

Bien évidemment, on définit la relation \geq binaire sur N par

$$\forall a, b \in \mathbb{N}^2 \quad (a \geq b) \iff (b \leq a).$$

Il est facile de déduire de ce qui précède que \geq est une relation d'ordre.

Théorème 1. (\mathbb{N}, \leq) est un ensemble totalement ordonné, c'est à dire que pour tout $(a, b) \in \mathbb{N}^2$ on a $a \leq b$ ou $b \leq a$.

Démonstration. On va prouver cela par récurrence : soit

$$C = \{a \in \mathbb{N}; \forall b \in \mathbb{N}; a \leq b \text{ ou } b \leq a\}$$

Il est clair que $0 \in C$, car $b = 0 + b$, soit $0 \leq b$ pour tout entier naturel b . Supposons $a \in C$ et montrons que $a + 1 \in C$. Soit $n \in \mathbb{N}$. Si $b = 0$, on a évidemment $b \leq a + 1$. Sinon, il existe b' entier tel que $b = b' + 1$. L'hypothèse de récurrence nous dit que $b' \leq a$ ou $b' \geq a$. Il y a deux cas possibles

- si $b' \leq a$, alors $b = b' + 1 \leq a + 1$.
- si $a \leq b'$ et $a \neq b'$, alors on peut écrire $b' = a + c$ avec $c \neq 0$, donc on peut écrire $c = c' + 1$, d'où $b' = a + c' + 1 = (a + 1) + c'$, d'où $a + 1 \leq c'$. \square

On note

$$(a < b) = (a \leq b) \text{ et } a \neq b$$

ainsi que

$$(a > b) = (a \geq b) \text{ et } a \neq b$$

En utilisant le fait que l'ordre est total, il est facile de voir que le contraire de $a < b$ (resp. $a > b$) est $a \geq b$ (resp. $a \leq b$).

Le lemme qui suit est utilisé très fréquemment dans les raisonnements qui mettent en oeuvre des entiers :

Lemme 1. Pour tous entiers n et p , on a

$$(n < p) \iff (n + 1 \leq p)$$

$$(n \geq p) \iff (n + 1 > p)$$

Démonstration. On va seulement prouver la première équivalence, car la deuxième n'est que la contraposée de la première.

Sens direct. Supposons $n < p$: on a donc $n \leq p$: il existe un entier naturel k avec $p = n + k$. $k \neq 0$, sinon on aurait $n = p$: il existe donc un entier m tel que $k = m + 1$: on a donc $p = n + k = (n + 1) + m$, d'où $n + 1 \leq p$.

- Réciproque. Supposons $n + 1 \leq p$: il existe un entier k tel que $p = (n + 1) + k = n + (k + 1)$. On a donc $n \leq p$. Montrons que $n \neq p$. Si on avait $n = p$, on aurait $n + 0 = n = n + (k + 1)$, d'où $k + 1 = s(k)0$, ce qui est impossible.

□

Corollaire 1. *Pour tout $n \in \mathbb{N}$, l'unique élément x qui satisfasse simultanément aux inéquations*

$$n \leq x \text{ et } x < n + 1$$

est $x = n$.

Démonstration. Montrons que $x = n$ est la seule solution possible : si $x < n + 1$, on a $x \leq n$, d'après la deuxième équivalence du lemme précédent : ainsi $n \leq x < n + 1$ implique $n \leq x \leq n$ d'où $x = n$.

Vérifions maintenant que $x = n$ est bien une solution. On doit vérifier $n \leq n$ et $n < n + 1$: la première inégalité est évidente, quant à la deuxième, c'est une conséquence du sens (2) \implies (1) dans la première équivalence du lemme précédent. □

Théorème 2. *L'ensemble ordonné (\mathbb{N}, \leq) est bien ordonné : toute partie non vide de \mathbb{N} admet un plus petit élément.*

Démonstration. Soit A une partie non vide de \mathbb{N} . Notons M l'ensemble des minorants de A . M est non-vidé car $0 \in M$. Il est clair que M n'est pas \mathbb{N} tout entier, car si $a \in A$, $a + 1 > a$, donc $a + 1 \notin M$. Il n'est pas possible que l'implication $(a \in M) \implies (a + 1 \in M)$, car comme $0 \in M$, le principe de récurrence impliquerait que $M = \mathbb{N}$, ce qui, on l'a vu, est faux. Il existe donc $a_0 \in M$ tel que $a_0 + 1 \notin M$. Si $a_0 + 1 \notin M$, c'est qu'il existe $x \in A$, avec $x < a_0 + 1$. Mais comme a_0 minore a , on a $a_0 \leq x$, d'où $a_0 \leq x < a_0 + 1$, ce qui implique $x = a_0$, donc $a_0 \in A$. Ainsi a_0 est dans A et est mineur tous les éléments de A : c'est son plus petit élément. □

Théorème 3. *Toute partie majorée de \mathbb{N} admet un plus grand élément.*

Démonstration. La preuve est laissée en exercice. □

1.5 Multiplication des entiers

1.5.1 Définition et propriétés

Théorème 4 (Admis). *Il existe une unique loi de composition interne notée \times sur \mathbb{N} vérifiant :*

$$\begin{aligned} \forall n \in \mathbb{N} \quad n \times 0 &= 0 \\ \forall (n, p) \in \mathbb{N} \times \mathbb{N} \quad p \times (n + 1) &= (p \times n) + p \end{aligned}$$

On l'appelle multiplication

Proposition 1 (Propriétés de la multiplication). – Associativité : $\forall (p, q, r) \in \mathbb{N}^3 \quad (p \times q) \times r = p \times (q \times r)$.

- Distributivité par rapport à l'addition : $\forall (p, q, r) \in \mathbb{N}^3 \quad (p + q) \times r = p \times r + q \times r$. et $\forall (p, q, r) \in \mathbb{N}^3 \quad r \times (p + q) = r \times p + r \times q$.
- Commutativité $\forall (p, q) \in \mathbb{N}^2 \quad p \times q = q \times p$.
- Régularité de la multiplication par un entier non nul :

$$\forall (p, q, r) \in \mathbb{N}^2 \times \mathbb{N}_* \quad pr = qr \implies p = q.$$

Remarque :

$$(p \times 1) = p \times (0 + 1) = p \times 0 + p = 0 + p = p.$$

1.5.2 Division euclidienne

Lemme 2 (Propriété d'Archimède). *Si $(a, b) \in \mathbb{N} \times \mathbb{N}_*$, il existe $n \in \mathbb{N}$ tel que $nb > a$.*

Démonstration. Comme $b \geq 1$, et on peut prendre par exemple $n = a + 1$: $(a + 1)b \geq a + 1 > a$. □

Théorème 5. *Si $(a, b) \in \mathbb{N} \times \mathbb{N}_*$. Il existe un unique couple (q, r) d'entiers naturels vérifiant $a = nq + r$.*

Démonstration. – Montrons d'abord l'existence d'un tel couple. On va montrer par récurrence sur p la propriété :

$$(H_p) : (n < bp) \implies \exists (q, r) \in \mathbb{N} \times \mathbb{N} \quad a = bq + r \text{ et } 0 \leq r < b.$$

Pour $p = 0$ c'est vrai car le faux implique le vrai. Pour $p = 1$, c'est vrai car si $n < p$, on écrit $n = 0.b + n$. Montrons que la propriété est héréditaire : Soit $n < b(p + 1)$. Si $n < b$ la preuve est terminée.

Sinon $n \geq b$, donc il existe un entier n_1 tel que $n = n_1 + b$. Comme $n < b(p+1)$, on a nécessairement $n_1 < bp$. Donc d'après l'hypothèse de récurrence, on peut écrire, $n_1 = bq + r$ avec $q \in \mathbb{N}$ et $0 \leq r < b$. On en déduit l'écriture $n = (b+1)q + r$. Ainsi (H_p) est réalisée pour tout p . Soit maintenant n entier : d'après la propriété d'Archimède, il existe p tel que $n < bp$: comme H_p est vraie, il existe $(q, r) \in \mathbb{N} \times \mathbb{N}$ avec $a = bq + r$ et $0 \leq r < b$.

- Montrons maintenant l'unicité : supposons que l'on ait $a = bq_1 + r_1 = bq_2 + r_2$. Quitte à échanger les rôles, on peut supposer que $q_1 \leq q_2$, ainsi on peut écrire $q_2 = q_1 + d$, avec $d \in \mathbb{N}$, d'où il ressort $bq_1 + r_1 = bq_1 + bd + r_2$, d'où $r_1 = bd + r_2$. On a $bd \leq bd + r_2 = r_1 < b$. Cela implique que $d = 0$. On en déduit $r_1 = r_2$ et $q_1 = q_2$. □

1.5.3 Bases de numération

Théorème 6. *Soit b un entier naturel non nul. Pour tout entier naturel n , on peut trouver un entier naturel p et une suite d'entiers $(a_n)_{0 \leq k \leq p}$ tel que*

$$n = \sum_{k=0}^p a_k b^k$$

avec

$$\forall k \in \{0, \dots, p\} \quad 0 \leq a_k < b \text{ et } (a_p > 0 \text{ ou } p = 0).$$

On dit alors que la suite $a_p a_{p-1} \dots a_0$ forme l'écriture de n en base b . Cette écriture est unique.

Démonstration. – D'abord, l'existence de l'écriture en base b d'un entier inférieur n strictement à b est évidente car chaque nombre inférieur strictement à b est sa propre écriture en base b : $p = 0$ et $a_0 = n$. De même b s'écrit en base b : "10" : $p = 1, a_0 = 0, a_1 = 1$.

On va montrer maintenant l'existence par l'absurde. Soit A l'ensemble des entiers qui n'admettent pas d'écriture en base b .

On suppose par l'absurde que A est non vide. Soit donc n son plus petit élément. D'après ce qui précède $n > b$. Effectuons maintenant la division euclidienne de n par b : on écrit $n = bq + r$, avec q entier et $0 \leq r < b$. On a forcément $q \neq 0$, sinon on aurait $n < b$, ce qui n'est pas possible. On ne peut pas non plus avoir $q = 1$, car alors on aurait $n = b + r$, ce qui constituerait une écriture de n en base b : "1r" : $p = 1, a_0 = r, a_1 = 1$. Comme $q > 1$, on a clairement $n \geq 2b > b$.

Comme b est strictement plus petit que le plus petit des entiers qui n'admettent pas d'écriture en base b , b admet une écriture en base b :

on peut écrire

$$q = \sum_{k=0}^p a_k b^k$$

avec

$$\forall k \in \{0, \dots, p\} \quad 0 \leq a_k < b \text{ et } (a_p > 0 \text{ ou } p = 0).$$

Maintenant

$$n = r + bq = r + \sum_{k=0}^p a_k b^{k+1}$$

Ainsi $a_p a_{p-1} \dots a_0 r$ constitue une écriture en base b de n , d'où la contradiction.

- Montrons d'abord que si un entier admet deux écritures, elles admettent nécessairement le même nombre de chiffres : si on a

$$n = \sum_{k=0}^p a_k b^k$$

avec

$$\forall k \in \{0, \dots, p\} \quad 0 \leq a_k < b \text{ et } (a_p > 0 \text{ ou } p = 0).$$

Si $p = 0$, on a $0 \leq n < b$. Sinon, on a

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

Ainsi, si un entier naturel non nul n admet une écriture à $p+1$ chiffres, on a $b^p \leq n \leq b^{p+1} - 1$. Donc si n admet une écriture à $p+1$ chiffres et une écriture à $q+1$ chiffres, on a $b^p \leq n \leq b^{p+1} - 1$ et $b^q \leq n \leq b^{q+1} - 1$. D'où $b^p \leq b^{q+1} - 1$ et $b^q \leq b^{p+1} - 1$, ce qui implique $p \leq q$ et $q \leq p$, d'où $p = q$. Définissons la suite d'entiers naturels $(q_k)_{0 \leq k \leq p}$ par la récurrence

$$\begin{cases} q_0 = n \\ q_{k+1} = \text{quotient de la division de } q_k \text{ par } b \end{cases}$$

et définissons $(r_k)_{0 \leq k \leq p}$ par la formule

$$r_k = \text{reste de la division de } q_k \text{ par } b.$$

De la sorte, on a $q_k = b q_{k+1} + r_k$, avec $0 \leq r_k < b$. Considérons maintenant une écriture de n en base b .

$$n = \sum_{k=0}^p a_k b^k$$

avec $\forall k \in \{0, \dots, p\}$ $0 \leq a_k < b$. On va montrer que pour tout $i \in \{0, \dots, p\}$, on a $r_i = a_i$, ce qui montrera l'unicité Posons, pour $0 \leq i \leq p$:

$$Q_i = \sum_{k=i}^p a_k b^{k-i}.$$

Il est aisé de voir que l'on a $Q_i = bQ_{i+1} + a_i$, de telle sorte que Q_{i+1} est quotient de la division de Q_i par b , et a_i le reste de la division de Q_i par b . D'autre part, il est clair que $Q_0 = n$. Ainsi, on a

$$\left\{ \begin{array}{l} q_0 = n \\ Q_0 = n \\ q_{k+1} = \text{quotient de la division de } q_k \text{ par } b \\ Q_{k+1} = \text{quotient de la division de } Q_k \text{ par } b \end{array} \right.$$

Ainsi, il est aisé de montrer par récurrence que $q_k = Q_k$ pour tout $i \in \{0, \dots, p\}$.

Comme a_i le reste de la division de Q_i par b et r_i le reste de la division de q_i par b , il s'ensuit que $a_i = r_i$ pour tout $i \in \{0, \dots, p\}$.

□

1.6 Exercices

1. Pour chacun des couples suivants $(X, \text{application})$, dites si l'application est une loi de composition interne ou une loi de composition interne associative sur X .

Dans tous les cas, on donnera une preuve du résultat annoncé.

- \times sur \mathbb{R}_+ .
 - \times sur \mathbb{R}_- .
 - $-$ sur \mathbb{R}_- .
 - $(x, y) \mapsto x \wedge y = \max(x, y)$ sur \mathbb{R} .
 - $(x, y) \mapsto x \star y = |x - y|$ sur \mathbb{R} .
 - $(x, y) \mapsto x \star y = |x - y|$ sur $\{0, 1\}$.
2. Dans un monoïde quelconque, montrez que si $a \star x = e$ et $x \star b = e$, alors nécessairement $a = b$.
 3. Si A et B sont deux parties d'un ensemble E , on définit la différence symétrique de A et B :

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Étudier les propriétés de la loi Δ sur $\mathcal{P}(E)$.

4. Soient x et y deux éléments inversibles d'un monoïde. Montrer que $x \star y$ est inversible. Réciproquement, si $x \star y$ est inversible, peut-on affirmer que x et y sont inversibles ?
5. Si u et v sont éléments de $] - 1, 1[$, on définit : $u * v = \frac{u+v}{1+uv}$. $*$ est-elle une loi de groupe sur $] - 1, 1[$?
6. Soient a, b deux éléments d'un group (G, \star) d'élément neutre *cp/vidée*, n un entier naturel. On suppose que $(a \star b)^n = e$. Montrer que $(b \star a)^n = e$.
7. Montrer qu'il n'existe pas de suite infinie $(u_n)_{n \geq 0}$ strictement décroissante à valeurs dans \mathbb{N} .
8. Écrire 12,57,128 en base 3.
9. Comment s'écrit en base 7 la somme du nombre qui s'écrit 1286 en base 7 et du nombre qui s'écrit 3126 en base 7.
10. Un entier naturel n est dit pratique si chaque entier naturel inférieur ou égal à n peut s'écrire comme somme de diviseurs distincts de n . Par exemple 6 est pratique, car $1 = 1, 2 = 2, 3 = 3, 4 = 1 + 3, 5 = 2 + 3, 6 = 6$.
Montrer qu'il existe une infinité de nombres pratiques.
11. Dans le système à base 10, un nombre s'écrit 20800. Quelle est la base du système de numération dans lequel il s'écrit 50500 ? *Baccalauréat série Math. Elem. , session 1967, sud Viet-Nam*
12. Déterminer la base d'un système de numération dans lequel les nombres 123, 140, 156 sont en progression arithmétique.

Chapitre 2

\mathbb{Z}

2.1 Relations d'équivalentes

Définition: On appelle relation d'équivalence sur un ensemble X toute relation binaire \mathcal{R} possédant les propriétés suivantes

- Symétrie : $\forall (x, y) \in X^2 \quad x\mathcal{R}y \iff y\mathcal{R}x$.
- Réflexivité : $\forall x \in X \quad x\mathcal{R}x$.
- Transitivité $\forall (x, y, z) \in X^3 \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies x\mathcal{R}z$.

Exemple: Soit X et E deux ensembles et f une fonction de X dans E . Alors, la relation binaire \mathcal{R} sur X définie par

$$x\mathcal{R}y \iff f(x) = f(y)$$

est une relation d'équivalence.

Par exemple, si $X = \{-2, -1, 0, 1, 2, 3\}$, $E = \{0, 1, 2, 3\}$ et $f(x) = |x|$, alors $2\mathcal{R}(-2)$ mais pas $1\mathcal{R}0$.

Définition: On appelle système de représentants d'une relation d'équivalence \mathcal{R} sur un ensemble X une partie R de X telle que

$$\forall x \in X \quad \exists ! r \in R \quad x\mathcal{R}r.$$

Dans notre exemple $\{0, 1, 2, 3\}$ est un système de représentants. $\{-2, 0, 1, 3\}$ aussi. En revanche $\{0, 1, 2\}$ et $\{-2, 0, 1, 2, 3\}$ n'en sont pas.

2.1.1 Relations d'équivalences et partitions

Définition: On appelle partition d'un ensemble X toute famille $(A_i)_{i \in I}$ de parties de X deux à deux disjointes dont la réunion fait X . En d'autres termes, une partition de X est une famille $(A_i)_{i \in I}$ de parties de X telle que chaque élément de X appartienne à exactement une de ces parties.

Exemples:

- Les ensembles $\{1, 3, 6\}$, $\{2, 5\}$, $\{4\}$ forment une partition de l'ensemble $\{1, 2, 3, 4, 5, 6\}$.
- Soit X et E deux ensembles et f une fonction de X dans E . Pour tout $e \in E$, on pose $A_e = f^{-1}(\{e\}) = \{x \in X; f(x) = e\}$. Alors, les ensembles $(A_e)_{e \in E}$ forment une partition de X .
Par exemple, si $X = \{-2, -1, 0, 1, 2, 3\}$, $E = \{0, 1, 2, 3\}$ et $f(x) = |x|$, on a $A_0 = \{0\}$, $A_1 = \{-1, 1\}$, $A_2 = \{-2, 2\}$, $A_3 = \{3\}$.

Soit \mathcal{R} une relation d'équivalence sur X . On considère l'application de X dans $\mathcal{P}(X)$ (l'ensemble des parties, ou si l'on préfère, des sous-ensembles de X)

$$\begin{aligned} X &\rightarrow \mathcal{P}(X) \\ x &\mapsto \{y \in X; x\mathcal{R}y\} \end{aligned}$$

$C(x)$ est appelée classe d'équivalence de x . Remarquons que $C(x) = C(y)$ si et seulement si $x\mathcal{R}y$. Il est facile de voir que l'ensemble des valeurs prises par l'application C forme une partition de X .

Exemple: Reprenons la relation d'équivalence sur $X = \{-2, -1, 0, 1, 2, 3\}$ définie par $x\mathcal{R}y \iff (|x| = |y|)$. On a

$$\begin{aligned} C(-2) &= \{-2; 2\} \\ C(-1) &= \{-1; 1\} \\ C(0) &= \{0\} \\ C(1) &= \{-1; 1\} \\ C(2) &= \{-2; 2\} \\ C(3) &= \{3\} \end{aligned}$$

Afin d'alléger les notations, lorsque aucune ambiguïté n'est possible, on note $\bar{x} = C(x)$.

Ainsi, les classes d'équivalences sont $\{-2; 2\}$, $\{-1; 1\}$, $\{0\}$, $\{3\}$: il est aisé de vérifier qu'elles forment bien un partition de X .

Inversement, si on se donne une partition $(A_e)_{e \in E}$ forment une partition de X , il est possible de définir une relation d'équivalence correspondante : il suffit de définir \mathcal{R} par

$$x\mathcal{R}y \iff \exists e; x \in A_e \text{ et } y \in A_e.$$

2.1.2 Ensemble quotient

Définition: Soit \mathcal{R} une relation d'équivalence sur X . On appelle quotient de X par \mathcal{R} et on note X/\mathcal{R} l'ensemble des classes d'équivalences de X pour

la relation \mathcal{R} .

Exemple: Pour la relation d'équivalence sur $X = \{-2, -1, 0, 1, 2, 3\}$ définie par $x\mathcal{R}y \iff (|x| = |y|)$, on a $X/\mathcal{R} = \{\{-2; 2\}, \{-1; 1\}, \{0\}, \{3\}\}$.

Remarque : sur un ensemble X quelconque, l'égalité est toujours une relation d'équivalence. Dans ce cas, chaque classe d'équivalence est constitué d'un unique élément. Et on a $X/\mathcal{R} = \{\{x\}; x \in X\}$, que l'on peut évidemment identifier à X .

Théorème 7. Soit \mathcal{R} une relation d'équivalence sur un ensemble X , \mathcal{R}' une relation d'équivalence sur un ensemble X' et f une application de X dans X' .

On suppose que

$$\forall(x, y) \in X^2 \quad x\mathcal{R}y \implies f(x)\mathcal{R}'f(y).$$

Alors, il existe une application \bar{f} de X/\mathcal{R} dans X'/\mathcal{R}' telle que

$$\forall x \in X \quad \overline{f(x)} = \bar{f}(\bar{x}).$$

On dit alors que l'application f passe au quotient.

Démonstration. Soit $C \in X/\mathcal{R}$. C est une partie non vide de X . Notons $A = f(C)$. A est non vide car C non vide. Soient y_1 et y_2 deux éléments de A . Par définition de A , il existe x_1 et x_2 dans $C \subset X$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. Par définition d'une classe d'équivalence, on a $x_1\mathcal{R}x_2$, ce qui, par hypothèse, entraîne $y_1\mathcal{R}'y_2$, soit $\bar{y}_1 = \bar{y}_2$. Ainsi \bar{A} est un singleton, ce qui signifie que pour tout $C \in X/\mathcal{R}$, il existe un unique $D \in X'/\mathcal{R}'$ tel que $f(C) \subset D$. On va donc définir $\bar{f}(C)$ par $\bar{f}(C) = D$.

Vérifions maintenant que l'application définie satisfait bien à la condition voulue. Soit $x \in X$; notons $C = \bar{x}$ et $D = \bar{f}(C) : f(C) \subset D$. En particulier $x \in C$, donc $f(x) \in \bar{f}(C)$, d'où $\overline{f(x)} = \bar{f}(\bar{x})$. \square

Exemple: On considère la relation d'équivalence sur $X = \{-2, -1, 0, 1, 2, 3\}$ définie par $x\mathcal{R}y \iff (|x| = |y|)$, on a $X/\mathcal{R} = \{\{-2; 2\}, \{-1; 1\}, \{0\}, \{3\}\}$. Considérons l'application

$$\begin{aligned} X &\rightarrow Y = \mathbb{N} \\ x &\mapsto x^2 \end{aligned}$$

On voit que f passe au quotient.

Corollaire 2. Soit X un ensemble, et \star une loi de composition interne sur X . On suppose que \sim est une relation d'équivalence sur X telle que

$$\forall(x, x', y, y') \in X^4 \quad x \sim x' \text{ et } y \sim y' \implies x \star y \sim x' \star y',$$

alors il existe une loi de composition interne $\bar{\star}$ sur X/\sim telle que

$$\forall (x, y) \in X^2 \quad \overline{x \star y} = \bar{x} \star \bar{y}$$

Démonstration. On définit une relation d'équivalence \mathcal{R} sur $X \times X$ par

$$\forall ((x, y), (x', y')) \in X^2 \times X^2 \quad (x, y)\mathcal{R}(x', y') \iff x \sim x' \text{ et } y \sim y'.$$

On définit alors f sur X^2 par $f((x, y)) = x \star y$ est on applique le théorème précédent. \square

2.2 Construire \mathbb{Z}

La construction de \mathbb{Z} ne va pas de soi. L'idée même de considérer nombres négatifs a longtemps été considérée, au mieux comme une astuce d'écriture, au pis comme une diablerie.

Sans un cours de mathématique de collège, on introduit souvent les nombres relatifs comme représentants d'un déplacement, par exemple le déplacement d'un ascenseur. Ainsi "+2" est ce que l'on fait pour fasser du premier au troisième étage, et "-2" ce que l'on fait pour passer du troisième au premier. Le problème étant qu'il ne suffit pas, pour définir -2 efficacement, de définir "-2" comme étant ce que l'on fait pour passer du 4e étage au second, car ce faisant, on néglige, ce qui est tout aussi vrai, que "-2" ce que l'on fait pour passer du 4e étage au second. Pour permettre d'identifier ces deux déplacements comme deux avatars d'un même objet, on va utiliser la notion d'ensemble quotient.

Définition: Soit \sim la relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$ définie par

$$(a, b) \sim (c, d) \iff a + d = b + c$$

On pose $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$. Si l'on note $+$ la loi de composition interne sur $\mathbb{N} \times \mathbb{N}$ définie par

$$(x, y) + (z, t) = (x + z, y + t).$$

Il est clair que que

$$(x, y) \sim (x', y') \text{ et } (z, t) \sim (z', t') \implies (x, y) + (z, t) \sim (x', y') + (z', t')$$

Ceci permet ainsi de définir une addition sur \mathbb{Z} grâce au corollaire 2.

Quelques propriétés simples (à démontrer en exercice)

1. $\forall z \in \mathbb{Z} \exists ! n \in \mathbb{N} \quad z = \overline{(n, 0)}$ ou $z = \overline{(0, n)}$.
2. Les applications $n \mapsto \overline{(n, 0)}$ et $n \mapsto \overline{(0, n)}$ sont injectives.

3. $\forall (a, b) \in \mathbb{N} \times \mathbb{N} \quad \overline{(a, b)} + \overline{(b, a)} = \overline{(0, 0)}$ item $\forall (a, b) \in \mathbb{N} \times \mathbb{N} \quad \overline{(a, 0)} + \overline{(b, 0)} = \overline{(a + b, 0)}$
4. $\forall z \in \mathbb{Z} \quad z + \overline{(0, 0)} = \overline{(0, 0)} + z = z$

Ainsi, on voit aisément que $(\mathbb{Z}, +)$ est un groupe et que l'on peut identifier \mathbb{N} à l'ensemble des éléments de \mathbb{Z} de la forme $\overline{(0, n)}$, tout en préservant les propriétés de l'addition. Ainsi on écrira par exemple simple $5 \in \mathbb{Z}$, au lieu de $\overline{(5, 0)} \in \mathbb{Z}$.

Définition: Pour $z \in \mathbb{Z}$, on note $-z$ l'opposé de z

2.3 La structure d'anneau

2.3.1 vocabulaire

Définition: Soit A un ensemble, $+$ et \times deux loi de composition interne sur A . On dit que le triplet $(A, +, \times)$ est un anneau si

- $(A, +)$ est un groupe commutatif; l'élément neutre pour la loi $+$ est noté 0 .
- (A, \times) est un monoïde
- La loi de composition interne \times est distributive par rapport à $+$:
 $\forall (p, q, r) \in A^3 \quad (p + q) \times r = p \times r + q \times r$. et $\forall (p, q, r) \in A^3 \quad r \times (p + q) = r \times p + r \times q$.

Définition: On dit qu'un anneau commutative si la multiplication de cet anneau est commutative.

2.3.2 Propriétés de \mathbb{Z}

On admettra qu'il est possible de définir une multiplication \times sur \mathbb{Z} telle que

$$\forall (a, b) \times (c, d) \in (\mathbb{N}^2)^2 \quad \overline{(a, b)} \times \overline{(c, d)} = \overline{(ac + bd, bc + ad)}$$

et telle que $(\mathbb{Z}, +, \times)$ soit un anneau commutatif.

(La preuve n'est pas particulièrement difficile, tous les ingrédients ont été donnés ici, mais ce n'est pas franchement passionnant, donc on pourra s'en passer.)

2.3.3 Règles de calcul

Définition: Soit $(A, +, \times)$ un anneau. On note 1_A (ou 1) l'élément neutre pour la multiplication dans A . On définit les puissances de a par $a^0 = 1$ et

la récurrence $a^{n+1} = a^n \times a$. On montre sans difficulté

$$\forall (n, p) \in \mathbb{N}^2 a^{n+p} = a^n \times a^p$$

Si a est inversible, on définit, pour $n > 0$ a^{-n} par la récurrence $a^{-(n+1)} = a^{-n} \times a^{-1}$. On montre alors de même

$$\forall (n, p) \in \mathbb{Z}^2 a^{n+p} = a^n \times a^p.$$

Il n'est pas difficile de montrer que si a et b commutent (c'est à dire si $ab = ba$), alors $\forall n \in \mathbb{N} \quad (ab)^n = a^n b^n$.

Théorème 8 (Binôme de Newton). *Soit $(A, +, \times)$ un anneau. Pour tous éléments a et b de A tels que $ab = ba$, on a*

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Démonstration. On va montrer cela par récurrence. Pour $n = 0$, l'identité se résume à $1 = 1$ tandis que pour $n = 1$, c'est simplement $a + b = a + b$. Supposons donc l'identité vérifiée au rang n , et montrons qu'elle est alors vérifiée au rang $n + 1$.

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n \\ &= (a + b) \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{(n+1)-(k+1)} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{(n+1)-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\ &= a^{n+1} + \sum_{k=1}^n \binom{n}{k-1} a^k b^{(n+1)-k} + \sum_{k=1}^n \binom{n}{k} a^k b^{n-k+1} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^n \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{(n+1)-k} + b^{n+1} \\ &= a^{n+1} b + \sum_{k=1}^n \binom{n+1}{k} a^k b^{(n+1)-k} + b^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k} \end{aligned}$$

□

2.4 Exercices

1. Dans l'ensemble des élèves d'une classe, la relation binaire "être de sexe opposé" est-elle une relation d'équivalence ?
2. On note

$$\mathbb{Z}[i] = \{a + ib; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}.$$

- (a) Montrer que $\mathbb{Z}[i]$ est un anneau commutatif (on admettra que \mathbb{C} est un anneau commutatif).
- (b) Pour $z = a + ib \in \mathbb{Z}[i]$, on pose $\mathcal{N}(z) = a^2 + b^2$. Montrer que $\mathcal{N}(zz') = \mathcal{N}(z)\mathcal{N}(z')$.
- (c) Montrer dans \mathbb{Z} l'identité de Lagrange :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

- (d) L'identité de Lagrange est-elle vraie dans tout anneau commutatif ?
 - (e) Soit A un anneau commutatif. On note M l'ensemble des éléments de A qui peuvent s'écrire comme somme de deux carrés. Montrer que (M, \times) est un monoïde.
3. Soit $j = \exp(\frac{2i\pi}{3})$. Montrer $1 + j + j^2 = 0$. On note

$$\mathbb{Z}[j] = \{a + jb; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}.$$

Montrer que $\mathbb{Z}[j]$ est un anneau commutatif (on admettra que \mathbb{C} est un anneau commutatif).

4. On dit qu'un élément x d'un anneau A est nilpotent si il existe $n \geq 0$ tel que $x^n = 0$. Dans ce cas, on appelle indice de nilpotence de x le plus petit n tel que $x^n = 0$. Montrer que l'ensemble des éléments nilpotents d'un anneau commutatif forme un anneau.
5. Soit A un anneau, e son élément unité pour la multiplication.
 - (a) Montrer que si deux éléments a et b de A vérifient $ab = ba$, alors pour $n \geq 1$, on a

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

- (b) Montrer que si x est nilpotent, alors $e - x$ est inversible.
- (c) Montrer que si x est nilpotent et que x' est l'inverse de $e - x$, alors $e - x$ est nilpotent.

6. Soit A un anneau, e son élément unité. Pour x , élément nilpotent d'indice p , on pose

$$\exp(x) = \sum_{k=0}^p \frac{x^k}{k!}$$

Soient a et b deux éléments nilpotents de A . Pourquoi a-t'on le droit de parler de $\exp(a+b)$? Montrer que $\exp(a+b) = \exp(a)\exp(b)$. Montrer que pour tout nilpotent x $\exp(x)$ est inversible.

7. *Théorème de Lagrange* Soit G un groupe fini. et H un sous-groupe de G . On définit une relation binaire \mathcal{R}_H sur G par

$$(g\mathcal{R}_H g') \iff \exists h \in H \quad g' = gh.$$

- Montrer que \mathcal{R}_H est une relation d'équivalence.
- Montrer qu'il y a exactement $|H|$ classes d'équivalences pour \mathcal{R}_H et qu'elles ont toutes le même cardinal.
- En déduire que $|H|$ divise $|G|$.
- Soit $x \in G$. Montrer qu'il existe n entier naturel non nul tel que $x^n = e$. Indication : Considérer la suite e, x, x^2, x^3, \dots . On appelle ordre de x le plus petit entier naturel non nul tel que $x^n = e$. Montrer que l'ordre de x divise $|G|$.

8. *Théorème de Cauchy*

(G, \star) désigne un groupe fini, d'ordre n , d'élément neutre e . p est un diviseur premier de n . On désigne par σ la bijection de $\{1, \dots, p\}$ dans lui-même définie de la manière suivante : $\sigma(p) = 1$ et

$$\forall i \in \{1, \dots, p-1\} \quad \sigma(i) = i+1.$$

On définit, par récurrence, σ^k pour tout entier naturel k par : $\sigma^0 = \text{Id}$ et $\sigma^{k+1} = \sigma \circ \sigma^k$.

- Vérifier que, si r désigne le reste de la division euclidienne de k par p , on a $\sigma^k = \sigma^r$.
- On définit une partie G^p de E par

$$E = \{(x_1, \dots, x_p) \in G^p \mid x_1 \star \dots \star x_p = e\}.$$

- On définit une relation binaire \mathcal{R} sur E par

$$((x_1, \dots, x_p)\mathcal{R}(x'_1, \dots, x'_p)) \iff (\exists k \in \mathbb{N} \quad \forall i \in \{1, \dots, p\} x'_i = x_{\sigma^k(i)}).$$

- Vérifier que \mathcal{R} est une relation d'équivalence sur E .

- ii. Vérifier que les classes d'équivalences pour la relation \mathcal{R} ont chacune 1 ou p éléments.
- (d) On note α le nombre de classes pour \mathcal{R} ayant 1 élément, β le nombre de classes pour \mathcal{R} ayant p éléments. Montrer que

$$\alpha + \beta p = n^{p-1}.$$

- (e) En déduire qu'il existe un élément x de G distinct de e tel que $x^{*p} = e$.

9. On considère l'ensemble

$$G = \{x + y\sqrt{2}; x^2 - 2y^2 = 1\}.$$

- (a) Montrer que G est un groupe.
- (b) Soient z et z' dans G , avec $z = x + y\sqrt{2}$ et $z' = x' + y'\sqrt{2}$, avec $x > x' > 1$, $y > 0$ et $y' > 0$. On pose $t = z(z')^{-1}$. Soient α et β entiers tels que $t = \alpha + \beta\sqrt{2}$. Montrer que $1 < \alpha < x$ et $\beta > 0$.
- (c) Quel est le plus petit entier x tel qu'il existe $y > 0$ avec $x + y\sqrt{2} \in G$?
- (d) Montrer que $G = \{(3 + 2\sqrt{2})^n; n \in \mathbb{Z}\}$.
- (e) Décrire l'ensemble des points à coordonnées entières de l'hyperbole d'équation

$$x^2 - 2y^2 = 1.$$

10. Soit u un endomorphisme de \mathbb{R}^2 . On suppose que u est un projecteur, c'est à dire que $u \circ u = u$. On note

$$V = \{a\text{Id} + bu; (a, b) \in \mathbb{R} \times \mathbb{R}\}.$$

Montrer que V , muni de l'addition des endomorphismes et de la composition comme loi mutliplicative, est un anneau.

Chapitre 3

Divisibilité

3.1 Sous-groupes de \mathbb{Z}

Pour tout entier naturel nul n , on note $n\mathbb{Z}$ l'ensemble des multiples de n :

$$n\mathbb{Z} = \{kn; k \in \mathbb{Z}\}.$$

Théorème 9. *Les ensembles A tel que $(A, +)$ soit un sous-groupe de $(\mathbb{Z}, +)$ sont exactement les ensembles de la forme $n\mathbb{Z}$, où n décrit l'ensemble des entiers naturels.*

Démonstration. – Sens direct : tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$.

Soit A un sous-groupe de \mathbb{Z} . Si A est réduit à $\{0\}$, on a terminé car $\{0\} = 0\mathbb{Z}$. Sinon, A contient au moins un élément non nul (mettons x). Lorsque x est dans A , $-x$ y est aussi. Mais de x et de $-x$, l'un des deux est strictement positif. On en déduit que l'ensemble $A \cap \mathbb{N}_*$ est non-vidé. Soit donc n_0 le plus petit élément de $A \cap \mathbb{N}_*$. On va montrer que $A = n_0\mathbb{Z}$.

On montre par récurrence sur k que pour tout $k \in \mathbb{N}$, $kn_0 \in A$ (utiliser l'identité $(k+1)n_0 = kn_0 + n_0$). On en déduit que pour tout $k \in \mathbb{N}$, $-kn_0 \in A$. Finalement $n_0\mathbb{Z} \subset A$.

Soit n un élément de $A \cap \mathbb{N}_*$. On effectue la division euclidienne de n par n_0 : $n = n_0q + r$ avec $0 \leq r < n_0$. On a nécessairement $q > 0$, sinon le caractère minimal de n_0 serait contredit. Il s'ensuit que $0 \leq r < n_0$. On a $r = n + (-n_0q)$. n et $-n_0q$ sont dans A , or A est un groupe donc r est dans A . r est positif, il est dans A et est strictement plus petit que n_0 : il ne peut être strictement positif, sinon cela contredirait le caractère minimal de n_0 : on a donc $r = 0$, soit $n = n_0q$, ce qui signifie que $n \in n_0\mathbb{Z}$. Reste avoir les éléments négatifs : soit n un élément négatif

de A ; $-n$ est un élément positif de A , donc $-n \in n_0\mathbb{Z}$, donc $n \in n_0\mathbb{Z}$.
Ainsi $A \subset n_0\mathbb{Z}$, ce qui achève la preuve.

- Réciproque : tout ensemble de la forme $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} .
La preuve est laissée en exercice.

□

3.2 PGCD

3.2.1 Compléments sur les groupes

Lemme 3. Soit (G, \times) un groupe. Soit \mathcal{H} une famille de parties de G telle que pour tout $H \in \mathcal{H}$, (H, \times) est un sous-groupe de G . Alors $(\bigcap_{H \in \mathcal{H}} H, \times)$ est un sous-groupe de (G, \times) .

Démonstration. La preuve est laissée en exercice. □

Définition: Soit (G, \times) un groupe, X une partie de G . On appelle sous-groupe engendré par X l'intersection de tous les sous-groupes de G qui contiennent X (il existe au moins un tel sous-groupe, car G en est un). D'après le lemme précédent, c'est bien un sous-groupe de (G, \times) . Par construction, c'est le plus petit sous-groupe de G qui contient X . On le note $\langle X \rangle$.

Définition: Si x est un élément d'un groupe G , on appelle sous-groupe engendré par x et on note simplement $\langle x \rangle$ le sous-groupe de G engendré par le singleton $\{x\}$.

Exemple: Pour $n \in \mathbb{Z}$ $\langle n \rangle = n\mathbb{Z}$.

Définition: On dit qu'un groupe G est monogène si il existe $x \in G$ tel que $G = \langle x \rangle$.

Exemple: On a montré que les sous-groupes de \mathbb{Z} sont tous monogènes.

3.2.2 PGCD de deux entiers

Définition: Soit a et b deux entiers relatifs. L'entier positif n tel que $\langle n \rangle = \langle \{a, b\} \rangle$ est appelé plus grand commun diviseur (PGCD) des entiers a et b . On note $a \wedge b$ le PGCD de a et de b .

Définition: On dit que deux entiers sont premiers entre eux si leur PGCD est égal à 1.

3.2.3 Propriétés de base

Si n est un diviseur de a et de b , alors a et b appartiennent à $\langle n \rangle$, donc $\langle a \wedge b \rangle$ est un sous-groupe de $\langle n \rangle$, ce qui implique que n divise

$\langle a \wedge b \rangle$. Comme un diviseur de $a \wedge b$ divise évidemment à la fois a et b , on peut dire que l'ensemble des diviseurs de a et b est exactement l'exemple des diviseurs de $a \wedge b$.

Théorème 10. *Soient a et b deux entiers relatifs. On a*

$$(a \wedge b)\mathbb{Z} = \{au + bv; (u, v) \in \mathbb{Z} \times \mathbb{Z}\}.$$

En particulier, il existe des entiers relatifs u et v tels que

$$au + bv = a \wedge b.$$

Démonstration. Considérons $G = \{au + bv; (u, v) \in \mathbb{Z} \times \mathbb{Z}\}$. Il est facile de voir que G est un sous-groupe de \mathbb{Z} et qu'il contient à la fois a et b . Par définition $\langle a, b \rangle$ est l'intersection de tous les sous-groupes de \mathbb{Z} qui contiennent a et b . Donc $\langle a, b \rangle \subset G$, soit $(a \wedge b)\mathbb{Z} = \langle a \wedge b \rangle \subset G$. Réciproquement, comme $\langle a, b \rangle$ contient a et b , il est évident qu'il en contient les combinaisons : $G \subset \langle a, b \rangle = (a \wedge b)\mathbb{Z}$. \square

Corollaire 3 (Identité de Bezout). *Soit a et b deux entiers relatifs. a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au + bv = 1$.*

Démonstration. Supposons qu'il existe des entiers relatifs u et v tels que $au + bv = 1$. $a \wedge b$ divise a et b , donc divise $au + bv = 1$. Comme il est positif, c'est donc 1. La réciproque est une conséquence immédiate du théorème précédent. \square

Quels que soient les entiers relatifs a, b, c , on a

1. $a \wedge b = b \wedge a$.
2. $ca \wedge cb = |c|(a \wedge b)$.

Démonstration. 1. Évident.

2. Soient u et v deux entiers tels que $au + bv = a \wedge b$. On a $(ac)u + (bc)v = c(a \wedge b)$, ce qui signifie que $c(a \wedge b) \in \langle ac, bc \rangle = \langle ac \wedge bc \rangle$, ce qui signifie que $ac \wedge bc$ divise $c(a \wedge b)$. D'autre part $a \wedge b$ divise a et b , donc $c(a \wedge b)$ divise ac et bc , donc $c(a \wedge b)$ divise $ac \wedge bc$. $c(a \wedge b)$ et $ac \wedge bc$ se divisent l'un l'autre et sont positifs : ils sont donc égaux. \square

3.2.4 Algorithme d'Euclide

Lemme 4 (Lemme d'Euclide). *Quels que soient les entiers relatifs a, b, q , on a $a \wedge b = b \wedge (a - qb)$. En particulier si r est le reste de la division euclidienne de a par b , on a $a \wedge b = b \wedge r$.*

Démonstration. A l'évidence $a \wedge b$ divise à la fois a et b , donc à la fois b et $a - qb$: $a \wedge b$ est donc un diviseur de $b \wedge (a - qb)$. Maintenant, on a $a = (a - bq) + bq$: $b \wedge (a - qb)$ divise $a - bq$ et bq , donc a . Il divise donc a et b , donc $a \wedge b$. $a \wedge b$ et $b \wedge (a - bq)$ se divisent l'un l'autre et sont positifs : ils sont donc égaux. \square

Théorème 11. *Pour calculer le PGCD de deux nombres entiers positifs, on peut utiliser l'Algorithme d'Euclide : on définit par récurrence une suite $(a_n), (b_n)$*

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} a_0 = a \\ b_0 = b \end{array} \right. \\ \left\{ \begin{array}{l} a_{n+1} = b_n \\ b_{n+1} = \text{reste de la division de } a_n \text{ par } b_n \end{array} \right. \end{array} \right.$$

On s'arrête dès que $b_n = 0$. Alors $a \wedge b$ vaut a_n .

Démonstration. D'après le lemme d'Euclide, on a $a_{n+1} \wedge b_{n+1} = a_n \wedge b_n$. Comme $a \wedge b$, on a pour tout n : $a_n \wedge b_n = a \wedge b$. Si $b_n = 0$, on a alors $a_n \wedge b_n = a_n \wedge 0 = a_n$.

Il reste à prouver qu'un tel n existe bien. Raisonnons par l'absurde : si il n'y avait pas de tel n on pourrait à l'aide de la formule de récurrence définir des suite infinies $(a_n), (b_n)$. Mais b_{n+1} est le reste de la division euclidienne de a_n par b_n , donc $b_{n+1} < b_n$. On aurait donc une suite infinie strictement décroissante d'entiers naturels, ce qui est impossible. \square

Exemple: Calcul de $1980 \wedge 632$.

n	a_n	b_n	$a = b \times q + r$
0	1980	632	$1980 = 3 \times 632 + 84$
1	632	84	$632 = 7 \times 84 + 44$
2	84	44	$84 = 1 \times 44 + 40$
3	44	40	$44 = 1 \times 40 + 4$
4	40	4	$40 = 10 \times 4 + 0$
5	4	0	PGCD=4

A partir de l'algorithme d'Euclide, on peut trouver une solution pour l'équation $au + bv = a \wedge b$. En effet si on a

$$\left\{ \begin{array}{l} a = bq + r \\ bu + rv = d \end{array} \right. ,$$

on a $(a - bq)v = rv = d - bu$, soit $av + b(u - qv) = d$. Autrement dit, une solution (u, v) pour l'équation de Bezout associée au couple (b, r) induit une solution $(v, u - qv)$ pour l'équation de Bezout associée au couple (a, b) .

Dans l'algorithme d'Euclide, le dernier couple considéré est toujours de la forme $(a, 0)$, dans ce cas il y a une solution évidente : le couple $(1, 0)$, car $4 = 4 \times 1 + 0 \times 0$.

Ainsi, si n_0 est le premier entier n tel que $b_n = 0$, on peut construire une suite $(u_n, v_n)_{0 \leq n \leq n_0}$ par récurrence descendante :

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} u_{n_0} = 1 \\ v_{n_0} = 0 \end{array} \right. \\ \left\{ \begin{array}{l} u_n = v_{n+1} \\ v_n = u_{n+1} - q_n v_{n+1} \end{array} \right. \end{array} \right. ,$$

où q_n est le quotient de la division de a_n par b_n .

Exemple: Détermination d'une solution de l'équation $1980u + 632v = 4$.

n	a_n	b_n	q_n	$a = b \times q + r$	u_n	$v_n = u_{n+1} - q_n \times v_{n+1}$
0	1980	632	3	$1980 = 632 \times 3 + 84$	-15	$47 = 2 - 3 \times (-15)$
1	632	84	7	$632 = 84 \times 7 + 44$	2	$-15 = (-1) - 7 \times 2$
2	84	44	1	$84 = 44 \times 1 + 40$	-1	$2 = 1 - 1 \times (-1)$
3	44	40	1	$44 = 40 \times 1 + 4$	1	$-1 = 0 - 1 \times 1$
4	40	4	10	$40 = 4 \times 10 + 0$	0	$1 = 1 - 10 \times 0$
5	4	0	PGCD = 4		1	0

Vérification : $1980 \times (-15) + 632 \times 47 = 4$

3.2.5 Lemme de Gauss – Application à la résolution de l'équation de l'équation $au + bv = n$

Lemme 5 (Lemme de Gauss). *Quels que soient les entiers relatifs non nuls a, b, d , on a*

$$d|ab \text{ et } a \wedge d = 1 \implies d|b.$$

Démonstration. Si a et d sont premiers entre eux, alors il existe u et v tels que $au + dv = 1$. En multipliant par b , on obtient $(ab)u + d(bv) = b$. d divise ab et d , donc il divise b . \square

Corollaire 4. *Si $a \wedge n = 1$ et $b \wedge n = 1$, alors $(ab)|n$.*

Démonstration. $(ab) \wedge n$ est un diviseur de n . Il est donc premier avec a puisque a est premier avec n . Mais $(ab) \wedge n$ est aussi un diviseur de ab . C'est donc un diviseur de b , d'après de lemme de Gauss. C'est un diviseur b et de n , donc c'est un diviseur de $b \wedge n = 1$: c'est donc 1. \square

Remarque : cette proposition peut s'étendre par récurrence au produit d'un nombre quelconque de termes.

Résolution de l'équation de l'équation $au + bv = n$

Soient a, b, n entiers relatifs fixés On veut trouver tous les couples $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = n$. Tout d'abord, on a vu au théorème 10 que les entiers de la forme $au + bv$ étaient exactement les multiples de $a \wedge b$. Donc si $a \wedge b$ ne divise pas n , il n'y a pas de solution.

Sinon, considérons une solution particulière (u_0, v_0) (une telle solution peut être trouvée en appliquant la méthode d'Euclide, puis en multipliant par $\frac{n}{a \wedge b}$ la solution trouvée.) Soit donc (u_0, v_0) tel que $au_0 + bv_0 = n$. Soit (u, v) un autre couple tel que $au + bv = n$: on a, en faisant la différence :

$$a(u - u_0) + b(v - v_0) = 0$$

Posons $a' = a/(a \wedge b)$ et $b' = b/(a \wedge b)$: on a

$$a'(u - u_0) + b'(v - v_0) = 0$$

Il s'ensuit que b' divise $a'(v - v_0)$. Mais b' et a' sont premiers entre eux, donc b' divise $v - v_0$: il existe un entier relatif k tel que $v - v_0 = kb'$. On conclut alors que $u - u_0 = -ka'$. Ainsi, toute solution s'écrit sous la forme

$$(u, v) = (u_0, v_0) + k(b', -a'),$$

où (u_0, v_0) est une solution particulière. On vérifie facilement que tout couple qui s'écrit ainsi est une solution de l'équation $au + bv = n$.

Exemple: Résolution de l'équation $30u + 12v = 24$.

On applique l'Algorithme d'Euclide

n	a_n	b_n	q_n	$a = b \times q + r$	u_n	$v_n = u_{n+1} - q_n \times v_{n+1}$
0	30	12	2	$30 = 12 \times 2 + 6$	1	$-2 = 0 - 2 \times 1$
1	12	6	2	$12 = 6 \times 2 + 0$	0	$1 = 1 - 2 \times 0$
2	6	0	PGCD = 6		1	0

Le PGCD 6 divise bien 24, donc il y a une solution. Grâce à l'algorithme d'Euclide, on obtient la solution de l'équation de Bezout associée $30 \times 1 +$

$12 \times (-2) = 6$ En multipliant par 4, cela nous donne bien une solution particulière : $(u_0, v_0) = (4, -8)$:

$$30 \times 4 + 12 \times (-8) = 24.$$

On a $30/(30 \wedge 12) = 30/6 = 5$ tandis que $12/(30 \wedge 12) = 12/6 = 2$.

On obtient finalement

$$\{(u, v) \in \mathbb{Z} \times \mathbb{Z} \mid 30u + 12v = 24\} = (4, -8) + \mathbb{Z}(2, -5).$$

Remarque : si on remarque tout de suite que 30 et 12 sont divisibles par 6, on transforme l'équation en $5u + 2v = 4$, ce qui simplifie les calculs ultérieurs.

3.2.6 PGCD de plusieurs entiers

Définition: Soient a_1, \dots, a_k des entiers relatifs. L'ensemble

$$G = \{a_1 n_1 + a_2 n_2 + \dots + a_k n_k; (n_1, \dots, n_k) \in \mathbb{Z}^k\}.$$

est le sous-groupe de \mathbb{Z} engendré par a_1, \dots, a_k : $\langle a_1, \dots, a_k \rangle$. L'unique entier naturel d tel que $G = \langle d \rangle = d\mathbb{Z}$ est appelé PGCD des entiers a_1, \dots, a_k .

Comme dans le cas de deux entiers, on montre qu'un diviseur de a_1, \dots, a_k est nécessairement un diviseur de leur PGCD.

Définition: Soient a_1, \dots, a_k des entiers relatifs. On dit que les entiers a_1, \dots, a_k sont premiers dans leur ensemble si leur PGCD est 1.

Théorème 12 (Associativité du PGCD). Soient $a_1, \dots, a_k, b_1, \dots, b_n$ des entiers relatifs. On note A le PGCD de a_1, \dots, a_k , B le PGCD de b_1, \dots, b_n et C le PGCD de $a_1, \dots, a_k, b_1, \dots, b_n$. Alors $C = A \wedge B$.

Démonstration. Il suffit de remarquer que

$$\langle a_1, \dots, a_k, b_1, \dots, b_n \rangle = \langle a_1, \dots, a_k \rangle + \langle b_1, \dots, b_n \rangle.$$

□

Cela nous autorise à noter $a_1 \wedge a_2 \wedge \dots \wedge a_n$ le PGCD des entiers a_1, \dots, a_n pris dans leur ensemble.

Exemple: Calcul du PGCD de 322, 126 et 21

On commence par calculer $322 \wedge 126$:

n	a_n	b_n	q_n	$a = b \times q + r$
0	322	126	2	$322 = 126 \times 2 + 70$
1	126	70	1	$126 = 70 \times 1 + 56$
2	70	56	1	$70 = 56 \times 1 + 14$
3	56	14	4	$56 = 14 \times 4 + 0$
4	14	0	PGCD = 14	

Et ensuite $21 \wedge 14$.

n	a_n	b_n	q_n	$a = b \times q + r$
0	21	14	1	$21 = 14 \times 1 + 7$
1	14	7	2	$14 = 7 \times 2 + 0$
2	7	0	PGCD = 7	

Ainsi $322 \wedge 126 \wedge 21 = 7$.

3.3 PPCM de deux ou plusieurs entiers

Définition: Soient a_1, \dots, a_k des entiers relatifs. L'intersection des groupes $a_1\mathbb{Z}, a_2\mathbb{Z}, \dots, a_k\mathbb{Z}$:

$$G = \bigcap_{i=1}^k (a_i\mathbb{Z})$$

est un sous-groupe de \mathbb{Z} . On appelle plus petit commun multiple de a_1, \dots, a_k l'unique entier naturel m tel que $m\mathbb{Z} = G$.

Par construction, si un nombre n est multiple de a_1, \dots, a_k , c'est un multiple de leur PPCM.

Comme l'intersection est associative, le PPCM l'est aussi : on note donc $a_1 \vee a_2 \vee \dots \vee a_n$ le PPCM des entiers a_1, \dots, a_k pris dans leur ensemble.

Théorème 13. Soient a, b des entiers relatifs quelconques. On a

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

Démonstration. Le nombre $\frac{ab}{a \wedge b}$ est un multiple de a , car $\frac{ab}{a \wedge b} = \frac{b}{a \wedge b} \times a$. C'est aussi un multiple de b , car $\frac{ab}{a \wedge b} = \frac{a}{a \wedge b} \times b$. C'est donc un multiple de $a \vee b$. Ainsi $(a \vee b)(a \wedge b)$ divise ab . Soient u et v deux entiers relatifs tels que $au + bv = a \wedge b$. En multipliant l'identité par $a \vee b$, on obtient

$$a(a \vee b)u + (a \vee b)bv = (a \wedge b)(a \vee b).$$

Comme $a \vee b$ est un multiple de b , $a(a \vee b)$ est un multiple de ab . De même $(a \vee b)b$ est un multiple de ab . Finalement $(a \wedge b)(a \vee b)$ est un multiple de ab . Les entiers positifs ab et $(a \wedge b)(a \vee b)$ se divisent l'un l'autre : ils sont donc égaux. \square

Exemple: Calcul de $120 \vee 55$.

On calcule d'abord $120 \wedge 55$:

n	a_n	b_n	q_n	$a = b \times q + r$
0	120	55	2	$120 = 55 \times 2 + 10$
1	55	10	5	$55 = 10 \times 5 + 5$
2	10	5	2	$10 = 5 \times 2 + 0$
3	5	0	PGCD = 5	

On a alors $120 \vee 55 = \frac{120 \times 55}{120 \wedge 55} = \frac{120 \times 55}{5} = 120 \times 11 = 1320$.

3.4 Congruence

Définition: Soit n un entier non nul. On définit une relation binaire sur \mathbb{Z} appelée congruence modulo n et notée $\equiv [n]$ définie par

$$(a \equiv b [n]) \iff (a - b \in n\mathbb{Z}).$$

Il est facile de voir que la congruence modulo n est une relation d'équivalence. Quelques propriétés :

1. $a \equiv b [n]$ et $c \equiv d [n]$ impliquent $a + c \equiv b + d [n]$
2. $a \equiv b [n]$ et $c \equiv d [n]$ impliquent $ac \equiv bd [n]$
3. $a \equiv b [n]$ implique $\forall k \in \mathbb{N} \quad a^k \equiv b^k [n]$.
4. $a \equiv b [n]$ implique $ac \equiv bc [nc]$
5. Si d divise n , alors $a \equiv b [n]$ implique $a \equiv b [d]$
6. Si $a \equiv b [n]$ et $a \equiv b [m]$, alors $a \equiv b [n \vee m]$

Exemple: Calcul du chiffre des unités de l'écriture décimale de 3^{402} . On a

$$\begin{aligned} 3^2 &\equiv -1 [10] \\ 3^4 &\equiv 1 [10] \\ 3^{400} &\equiv 1 [10] \\ 3^{402} &\equiv 3^{400} \cdot 3^2 \equiv -1 [10] \\ 3^{402} &\equiv 9 [10] \end{aligned}$$

Donc le chiffre des unités de l'écriture décimale de 3^{402} est 9.

Exemple: En utilisant les congruences modulo 5, on montre que l'équation $x^3 - 13x + 6 = 0$ n'a pas de solution entière.

On remarque d'abord que $x^3 - 13x + 6 \equiv x^3 + 2x + 1 [5]$ (La nouvelle expression est plus facile à calculer). Ensuite on teste pour toutes les congruences modulo 5 possibles

$$\begin{aligned}
 x \equiv 0 [5] &\implies x^3 + 2x + 1 \equiv 1 [5] \\
 x \equiv 1 [5] &\implies x^3 + 2x + 1 \equiv 3 [5] \\
 x \equiv 2 [5] &\implies x^3 + 2x + 1 \equiv 3 [5] \\
 x \equiv 3 [5] &\implies x^3 + 2x + 1 \equiv 4 [5] \\
 x \equiv 4 [5] &\implies x^3 + 2x + 1 \equiv 3 [5]
 \end{aligned}$$

Ainsi, pour tout x entier, $x^3 - 13x + 6$ n'est jamais congru à 0 modulo 5. Il ne peut donc jamais être nul.

3.5 Exercices

- Montrer qu'un entier naturel est congrus à la somme des chiffres de son écriture dans la base b modulo $b - 1$.
- (a) Étudier, suivant les valeurs de l'entier naturel n , le reste de la division par 7 du nombre $A = n^2 - n + 1$.
 (b) En déduire les entiers n tels que le nombre A soit divisible par 7.
 (c) Déterminer le reste de la division par 7 du nombre $B = 2753^2 - 2753 + 1$.

Baccalauréat série C 1968, Cambodge et Laos

- (a) Déterminer, dans l'ensemble \mathbb{N} des entiers naturels, toutes les solutions de l'équation

$$2x - 3y = 0.$$

- (b) Déterminer, dans l'ensemble \mathbb{N} des entiers naturels, une solution de l'équation

$$2x - 3y = 3.$$

En déduire toutes les autres solutions.

Baccalauréat série C, septembre 1968, Montréal et New York

- Trouver le reste dans la division par 7 du nombre 65^{346} . *Baccalauréat série Mathématiques élémentaires, 1967, Antilles*
- Construire tous les couples d'entiers positifs vérifiant la relation $3x + 13y = 166$.
- Quels sont les entiers positifs n pour lesquels $15 \times 3^n - 3$ est divisible par 7? *Baccalauréat série math. elem., session octobre-novembre 1967, Mexico*

7. Quel peut être, suivant les valeurs du nombre entier naturel n , le reste de la division par 7 du nombre 2^n ? En déduire le reste de la division par 7 du nombre $N = 247^{349}$.
8. (a) Sans effectuer la division de 761945 par 11, trouver le reste de cette opération.
(b) Montrer qu'en changeant un seul chiffre du dividende, on peut le rendre divisible par 11. Indiquer tous les nombres divisibles par 11 que l'on peut obtenir de cette façon. Quels sont, parmi eux, ceux qui sont également divisibles par 15 ?
9. Déterminer les chiffres x et y de façon que le nombre qui dans le système décimal s'écrit $28x75y$ soit divisible à la fois par 3 et par 11.
10. Soit q et r le quotient et le reste de la division d'un nombre entier a par un nombre entier b . Sachant que $a + b + r = 3025$ et $q = 50$, rétablir la division.
11. (a) Comment faut-il choisir l'entier naturel n pour que le nombre $A = 2^n - 1$ soit divisible par 9 ?
(b) Montrer que si cette condition est réalisée, le nombre A est divisible par 7. Quel est le reste de la division de A par 21 ?
12. En utilisant la théorie des congruences, déterminer la forme générale des entiers naturels n tels que $n^3 - n + 1$ soit divisible par 7.

Chapitre 4

Nombres premiers

4.1 Définition et premières propriétés

Définition: On dit qu'un entier naturel est un nombre premier lorsqu'il est différent de 1 et qu'il n'est pas possible de l'écrire comme produit de deux entiers naturels différents de 1.

Lemme 6. *Soit n un entier naturel et p un nombre premier. Si p ne divise pas n , alors p et n sont premiers entre eux.*

Démonstration. $p \wedge n$ est un diviseur de p . C'est donc p ou 1. Dans le premier cas, $p|n$, dans le deuxième cas p et n sont premiers entre eux. \square

Lemme 7. *Soit a, b deux entiers naturels et p un nombre premier. Si p divise ab , alors $p|a$ ou $p|b$.*

Démonstration. Supposons donc que p divise ab . Si p ne divise pas a , alors d'après le lemme précédent, il est premier avec a . Donc, d'après le lemme de Gauss, p divise b . \square

Lemme 8. *Soit $n > 1$. Le plus petit diviseur de n strictement supérieur à 1 est un nombre premier.*

Démonstration. Tout d'abord, l'ensemble des diviseurs de n strictement supérieurs à 1 est non vide, puisqu'il contient n : il a donc bien un plus petit élément. Soit d cet élément. Si d n'était pas premier, il existerait des entiers a et b strictement supérieurs à 1 tels que $d = ab$. Mais alors on aurait $1 < a < d$ et $a|n$, ce qui contredirait le caractère minimal de d . \square

Corollaire 5. *Si un entier $n > 1$ n'est pas premier, il admet au moins un diviseur premier inférieur ou égal à \sqrt{n} .*

Démonstration. Soit p le plus petit diviseur de n strictement supérieur à 1. C'est un nombre premier. Soit q l'unique entier tel que $n = pq$. $q > 1$ car sinon n serait premier. q est donc un diviseur de n strictement supérieur à 1, donc $q \geq p$. Cela entraîne $n = pq \geq p^2$. \square

Exemple: Supposons acquis que les nombres 2, 3, 5, 7 sont les nombres premiers inférieurs à 10. 97 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7. Il n'y a pas d'autre nombre premier p tel que $p^2 \leq 97$. Donc 97 est un nombre premier.

Liste des nombres premiers entre 1 et 100 :

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97.

Pour résoudre des problèmes d'arithmétique, il est bon de savoir retrouver facilement les plus petits des nombres premiers. Remarquer que, excepté $91 = 7 \times 13$, la primalité de tous les nombres plus petit que 100 peut être testée à l'aide des critères de divisibilité par 2, 3, 5, 11.

Théorème 14. *L'ensemble des nombres premiers est infini.*

Démonstration. On raisonne par l'absurde. Supposons qu'il n'existe qu'un nombre fini de nombres premiers. Notons alors M leur produit. Aucun nombre premier ne divise $M + 1$, sinon il diviserait 1 (car tout nombre premier divise M). Pourtant on sait que tout nombre entier admet un diviseur premier. Il y a donc une contradiction. \square

4.2 Décomposition d'un nombre en produit de facteurs premiers

Définition: Soit n en entier naturel et p un nombre premier. On appelle valuation p -adique de n et on note $\nu_p(n)$ le plus grand entier i tel que p^i divise n .

4.2.1 Existence et unicité de la décomposition

Théorème 15. *Soit n un entier strictement supérieur à 1. On note P_n l'ensemble des diviseurs premiers de n . Il existe une unique suite d'entiers $(\nu_p(n))_{p \in P_n}$ telle que*

$$n = \prod_{p \in P_n} p^{\nu_p(n)}$$

De plus, on a

$$\forall p \in P_n \quad \nu_p(n) = v_p(n).$$

4.2. DÉCOMPOSITION D'UN NOMBRE EN PRODUIT DE FACTEURS PREMIERS 37

Démonstration. – Existence

Considérons l'ensemble des entiers k tels qu'il existe une suite $(u_i)_{1 \leq i \leq k}$ d'entiers strictement supérieurs à 1 avec

$$\prod_{i=1}^k u_i = n.$$

Cet ensemble est non vide car 1 est dedans (considérer la suite d'un unique terme n) et bornée car

$$2^k \geq \prod_{i=1}^k u_i = n.$$

Soit k_0 son plus grand élément et considérons une suite $\prod_{i=1}^{k_0} u_i = n$. Chaque terme du produit est nécessairement un nombre premier car sinon, on pourrait en l'écrivant sous forme d'un produit de deux termes différents de 1 obtenir une suite de longueur $n_0 + 1$ dont le produit fait n , ce qui contredirait la maximalité de n_0 . Par définition, chacun de ces nombres premiers est un diviseur de n . En regroupant les nombres égaux, on obtient la factorisation annoncée.

– Unicité

Considérons une écriture

$$n = \prod_{p \in P_n} p^{\nu_p(n)}.$$

Pour tout $p \in P_n$ $p^{\nu_p(n)} | n$, donc $v_p(n) \geq \nu_p(n)$. Raisonnons par l'absurde et supposons qu'il existe p_0 tel que $v_{p_0}(n) > \nu_{p_0}(n)$: il existerait k entier tel que $n = kp_0^{v_{p_0}(n)}$, soit

$$kp_0^{v_{p_0}(n) - \nu_{p_0}(n)} = \prod_{p \in P_n \setminus \{p_0\}} p^{\nu_p(n)}$$

Il s'ensuit que p_0 divise $\prod_{p \in P_n \setminus \{p_0\}} p^{\nu_p(n)}$, donc p_0 n'est pas premier avec $\prod_{p \in P_n \setminus \{p_0\}} p^{\nu_p(n)}$, ce qui est évidemment faux puisqu'il est premier avec tous les termes du produit. □

4.2.2 Application au calcul du PGCD et du PPCM

Théorème 16. *Soit a et b deux entiers naturels. On a pour tout p premier*

$$- v_p(a \wedge b) = \min(v_p(a), v_p(b)).$$

$$- v_p(a \vee b) = \max(v_p(a), v_p(b))$$

Démonstration.

$p^{\min(v_p(a), v_p(b))}$ divise $p^{v_p(a)}$, qui lui-même divise a , donc $p^{\min(v_p(a), v_p(b))}$ divise a . De même $p^{\min(v_p(a), v_p(b))}$ divise b . Donc $p^{\min(v_p(a), v_p(b))}$ divise $a \wedge b$. Donc $v_p(a \wedge b) \geq \min(v_p(a), v_p(b))$. Maintenant soit i tel que p^i divise $a \wedge b$. On a $p^i | a$. Donc $i \leq v_p(a)$. De même $i \leq v_p(b)$, d'où $i \leq \min(v_p(a), v_p(b))$. En particulier $v_p(a \wedge b) \leq \min(v_p(a), v_p(b))$. Finalement $v_p(a \wedge b) = \min(v_p(a), v_p(b))$

Considérons l'entier

$$M = \prod_{p: v_p(a)+v_p(b)>0} p^{\max(v_p(a), v_p(b))}$$

A l'évidence M est multiple de a tout comme de b . M est donc un multiple de $a \vee b$. Il s'ensuit que pour tout p , on a $v_p(a \vee b) \leq v_p(M) = \max(v_p(a), v_p(b))$. Pour tout multiple m de a , on a $v_p(m) \geq v_p(a)$. De même pour tout multiple m de b , on a $v_p(m) \geq v_p(b)$. Appliqué à $m = a \vee b$, cela donne $v_p(a \vee b) \geq \max(v_p(a), v_p(b))$. \square

Corollaire 6. Soient a et b deux entiers naturels. On a

$$a \wedge b = \prod_{p: v_p(a)+v_p(b)>0} p^{\min(v_p(a), v_p(b))}$$

$$a \vee b = \prod_{p: v_p(a)+v_p(b)>0} p^{\max(v_p(a), v_p(b))}$$

Exemple: Calcul du PPCM et du PGCD de 1248 et 2600

On a

$$1248 = 2^5 \times 3 \times 13$$

et

$$2600 = 2^3 \times 5^2 \times 13$$

D'où

$$1248 \wedge 2600 = 2^3 \times 13 = 104$$

et

$$1248 \vee 2600 = 2^5 \times 3 \times 5^2 \times 13 = 31200$$

Vérification :

$$104 \times 31200 = 3244800 = 1248 \times 2600.$$

4.3 Exercices

1. Déterminer l'ensemble des diviseurs positifs de 120 ?
2. Combien y a-t'il de diviseurs positifs de 1000 ?
3. Montrer qu'un nombre est le carré d'un entier si et seulement si il a un nombre impair de diviseurs positifs .
4. Déterminer le plus petit entier ayant 15 diviseurs positifs.
5. (a) Montrer que
 - si deux nombres ne sont pas premiers entre eux, l'un au moins de leurs diviseurs communs est premier ;
 - si deux nombres sont premiers entre eux, tout nombre premier qui divise leur produit divise l'un et est premier avec l'autre ;
 - si deux nombres sont premiers entre eux, leur somme et leur produit sont aussi deux nombres premiers entre eux.
- (b) Calculer deux nombres, connaissant leur somme, 135, et leur plus petit multiple commun, 504.

Baccalauréat série C, session de septembre 1968, groupe I

6. Soit, en numération en base a ($a > 3$) le nombre $N = 1320$.
 - (a) Montrer que ce nombre est divisible par a , $a + 1$, $a + 2$ et se met sous la forme $a(a + 1)(a + 2)$.
 - (b) Pour quelles valeurs de a est-il divisible par $a - 1$?
 - (c) En prenant pour valeur de a la plus petite de celles trouvées à la question précédente, décomposer N en produit de facteurs premiers.

Baccalauréat série math. élem., sujet de remplacement 1967, Antilles

7. (a) Soit p un nombre premier. Montrer que

$$v_p(n!) = \sum_{k=0}^{+\infty} \text{Ent}\left(\frac{n}{p^k}\right).$$

- (b) En déduire l'inégalité

$$\frac{n}{p} - 1 < v_p(n!) \leq \frac{n}{p} + \frac{n}{p(p-1)}.$$

En considérant l'expression $(1 + 1)^{2m+1}$, montrer $\binom{2m+1}{m} \leq 4^m$. En déduire la majoration

$$\prod_{m+1 < p \leq 2m+1} p \leq 4^m.$$

- (c) Montrer par récurrence sur n l'inégalité $\prod_{p \leq n} p \leq 4^n$.
 (d) On admet l'estimation

$$\ln n! = n \ln n - n + O(\ln n).$$

Montrer qu'on a

$$\sum_{p \leq x} \frac{\ln p}{p} = \ln x + O(1).$$

8. Exprimer $v_p(n)$ à l'aide de l'écriture de n en base p .
 9. Par combien de zéros se termine l'écriture $100!$ en base 10 ?
 10. Quel est le dernier chiffre non nul de l'écriture décimale de $20!$?
 11. (a) Soit $d(n)$ le nombre de diviseurs de n . Montrer que pour tout entier naturel non nul n , on a $d(n) \leq 2\sqrt{n}$.
 (b) Soient a_1, \dots, a_n des entiers distincts. Montrer que

$$\sum_{k=1}^n \frac{1}{\text{PPCM}(a_1, \dots, a_k)} \leq \frac{7}{2}.$$

Indication : on pourra montrer que

$$\frac{1}{\text{PPCM}(a_1, \dots, a_k)} \leq \frac{4}{k^2} \leq \frac{4}{k(k-1)} = 4\left(\frac{1}{k-1} - \frac{1}{k}\right).$$

12. Montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4.
 13. Déterminer tous les couples (a, b) d'entiers naturels tels que $m + 11\Delta = 203$, m étant le PPCM et Δ le PGCD de a et de b .
Baccalauréat série C, Clermont 1970
 14. Résoudre l'équation

$$3^{x+2} + 9^{x-1} = 1458,$$

où x est l'inconnue (réelle).

Baccalauréat série C, Dijon 1970

Chapitre 5

$\mathbb{Z}/n\mathbb{Z}$

5.1 Construction de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition: Soit n un entier naturel non nul. On appelle $\mathbb{Z}/n\mathbb{Z}$ le quotient de l'ensemble \mathbb{Z} par la relation d'équivalence "congruence modulo n "

$\mathbb{Z}/n\mathbb{Z}$ est un ensemble à n éléments :

$$\mathbb{Z}/n\mathbb{Z} = \{\overset{\circ}{0}, \overset{\circ}{1}, \dots, \overset{\circ}{n-1}\},$$

où

$$\overset{\circ}{k} = k + n\mathbb{Z}.$$

D'après les propriétés de la congruence relatives à l'addition et à la multiplication dans \mathbb{Z} , l'addition et la multiplication "passent au quotient" : en appliquant le corollaire 2 à l'addition et à la multiplication, on peut définir une addition et une multiplication sur $\mathbb{Z}/n\mathbb{Z}$ telle que pour tous entiers a et b , on ait $a + b = \overset{\circ}{a} + \overset{\circ}{b}$ et $ab = \overset{\circ}{a}\overset{\circ}{b}$. Ces deux opérations héritent des propriétés de l'addition et de la multiplication sur \mathbb{Z} , au sens qu'une identité dans \mathbb{Z} entraîne une identité dans $\mathbb{Z}/n\mathbb{Z}$: il s'ensuit que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif. L'élément neutre pour l'addition est $\overset{\circ}{0}$ et l'élément neutre pour la multiplication est $\overset{\circ}{1}$.

5.2 Inversibles de $\mathbb{Z}/n\mathbb{Z}$

5.2.1 Caractérisation des inversibles

Théorème 17. Soit n un entier naturel non nul et $k \in \mathbb{Z}$. $\overset{\circ}{k}$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Démonstration. – Si $\overset{\circ}{k}$ est inversible, il existe $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $x\overset{\circ}{k} = \overset{\circ}{1}$. Soit $u \in \mathbb{Z}$ tel que $x = \overset{\circ}{u}$: on a $\overset{\circ}{u}\overset{\circ}{k} = \overset{\circ}{1}$, soit $1 - uk \in n\mathbb{Z}$: il existe un entier relatif v tel que $1 - uk = vn$. On a donc

$$vn + uk = 1,$$

ce qui implique, d'après Bezout, que k et n sont premiers entre eux.

– Si $k \wedge n = 1$, alors, d'après Bezout, il existe des entiers relatifs u et v tels que

$$vn + uk = 1.$$

On a donc $\overset{\circ}{v}\overset{\circ}{n} + \overset{\circ}{u}\overset{\circ}{k} = \overset{\circ}{1}$, soit, puisque $\overset{\circ}{n} = \overset{\circ}{0}$: $\overset{\circ}{u}\overset{\circ}{k} = \overset{\circ}{1}$, ce qui montre que $\overset{\circ}{k}$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. □

5.2.2 Groupe des éléments inversibles – indicatrice d'Euler

Définition: On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Rappel : $k \wedge n = 1 \iff \overset{\circ}{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Définition: Pour tout entier naturel n , on note $\varphi(n)$ le cardinal de l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$. La fonction $n \mapsto \varphi(n)$ est appelée fonction indicatrice d'Euler.

Lemme 9. $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un groupe.

Démonstration. Laissée en exercice. □

Théorème 18 (Théorème d'Euler). Soit $n \geq 2$ et a un entier premier avec n . On a

$$a^{\varphi(n)} \equiv 1 [n].$$

Démonstration. Il est équivalent de montrer que $\overset{\circ}{a}^{\varphi(n)} = \overset{\circ}{1}$. Considérons l'application $M_{\overset{\circ}{a}}$ du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ dans lui-même définie par $M_{\overset{\circ}{a}}(x) = \overset{\circ}{a}x$. M est clairement une bijection : l'application $M_{\overset{\circ}{a}^{-1}}(x) = \overset{\circ}{a}^{-1}x$ en est évidemment la réciproque. Comparons les nombres $K = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} x$ et $K = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} M(x)$: ils sont égaux car c'est le produit des mêmes nombres (à l'ordre près). Mais

$$K = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} M(x) = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} \overset{\circ}{a}x = \overset{\circ}{a}^{\varphi(n)} \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} x = \overset{\circ}{a}^{\varphi(n)} L.$$

On a donc $L = \overset{\circ}{a}^{\varphi(n)} L$. Mais L est inversible car L est dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, donc $\overset{\circ}{a}^{\varphi(n)} = \overset{\circ}{1}$. □

Corollaire 7. Soit p un nombre premier, a un entier quelconque. On a

$$\forall k \in \mathbb{N} \quad a^{1+(p-1)k} \equiv a \pmod{p}.$$

En particulier

$$a^p \equiv a \pmod{p}.$$

Ce dernier résultat est appelé petit théorème de Fermat.

Démonstration. Si $a \equiv 0 \pmod{p}$, l'égalité est évidente, sinon a est premier avec p . On écrit alors $a^{1+(p-1)k} = a \times (a^{p-1})^k = a \times a^{\varphi(p)}$ et il suffit alors d'appliquer le lemme précédent. \square

Définition: On appelle corps un anneau dont tous les éléments non nuls sont inversibles.

Exemple: D'après ce qui précède, $\mathbb{Z}/p\mathbb{Z}$ est un corps.

5.3 Théorème chinois

Théorème 19. Soient p et q deux entiers premiers entre eux. Pour tous $a, b \in \mathbb{Z}$, il existe $x_0 \in \mathbb{Z}$ tel que pour $x \in \mathbb{Z}$ on ait

$$(x \equiv a \pmod{p} \text{ et } x \equiv b \pmod{q}) \iff x \equiv x_0 \pmod{pq}.$$

Démonstration. On va chercher x_0 sous la forme $x_0 = bkp + alq$, avec $k, l \in \mathbb{Z}$. Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\overset{\circ}{x}_0 = \overset{\circ}{b} \overset{\circ}{k} \overset{\circ}{p}$, tandis que dans $\mathbb{Z}/q\mathbb{Z}$, on a $\overset{\circ}{x}_0 = \overset{\circ}{a} \overset{\circ}{l} \overset{\circ}{q}$. Ainsi, si on a dans $\mathbb{Z}/q\mathbb{Z}$ $\overset{\circ}{k} \overset{\circ}{p} = \overset{\circ}{1}$, et que dans le même temps on a dans $\mathbb{Z}/p\mathbb{Z}$ $\overset{\circ}{l} \overset{\circ}{q} = \overset{\circ}{1}$, on aura dans $\mathbb{Z}/q\mathbb{Z}$: $\overset{\circ}{x}_0 = \overset{\circ}{b}$ et dans $\mathbb{Z}/p\mathbb{Z}$: $\overset{\circ}{x}_0 = \overset{\circ}{a}$, ce qui signifie que

$$x_0 \equiv a \pmod{p} \text{ et } x_0 \equiv b \pmod{q}. \quad (5.1)$$

Comme p et q sont premiers entre eux, p est inversible dans $\mathbb{Z}/q\mathbb{Z}$ de même que q est inversible dans $\mathbb{Z}/p\mathbb{Z}$. On peut donc trouver de tels k et l , ce qui permet de trouver un x_0 vérifiant (5.1). Comme la congruence modulo pq implique la congruence modulo p et modulo q , il est clair que $x \equiv a \pmod{p}$ et $x \equiv b \pmod{q}$ dès que $x \equiv x_0 \pmod{pq}$. Réciproquement, si $x \equiv a \pmod{p}$ et $x \equiv b \pmod{q}$, on a $x \equiv x_0 \pmod{p}$ et $x \equiv x_0 \pmod{q}$, donc p et q divisent tous deux $x - x_0$. Comme ils sont premiers entre eux pq divise $x - x_0$, donc $x \equiv x_0 \pmod{pq}$. \square

Exemple: Déterminons le plus petit entier dont le reste de la division par 5 soit 1 et le reste de la division par 7 soit 2. On le cherche sous la forme $x_0 = 1.7.k + 2.5.l$. On doit, d'une part, trouver un inverse à 7 dans $\mathbb{Z}/5\mathbb{Z}$, et d'autre part trouver inverse à 5 dans $\mathbb{Z}/7\mathbb{Z}$.

Dans $\mathbb{Z}/5\mathbb{Z}$, on a $\overset{\circ}{7} = \overset{\circ}{2}$. On remarque que $2 \times 3 = 6 = 5 + 1$. Donc dans $\mathbb{Z}/5\mathbb{Z}$, on a $\overset{\circ}{2}\overset{\circ}{3} = \overset{\circ}{1} : \overset{\circ}{3}$ est donc l'inverse de $\overset{\circ}{2} = \overset{\circ}{7}$. On peut donc prendre $k = 3$.

Je remarque que $5 \times 3 = 15 = 14 + 1$: donc on a dans $\mathbb{Z}/7\mathbb{Z} : \overset{\circ}{5}\overset{\circ}{3} = \overset{\circ}{1}$. On peut donc prendre $l = \overset{\circ}{3}$. Cela nous mène à $x_0 = 51$. Ainsi, d'après le théorème chinois, les entiers dont le reste de la division par 5 est 1 et le reste de la division par 7 est 2 sont les entiers congrus à 51 modulo $7 \times 5 = 35$. Le plus petit d'entre eux est le reste de la division de 51 par 35, c'est à dire 16.

Corollaire 8. *Soient p et q deux entiers premiers entre eux. On pose $n = pq$. Alors, l'application*

$$\begin{aligned} \Psi_n : \{0, \dots, n-1\} &\rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ k &\mapsto (k + p\mathbb{Z}, k + q\mathbb{Z}) \end{aligned}$$

est une bijection.

Démonstration. C'est juste une reformulation du théorème chinois. □

5.4 Calcul de l'indicatrice d'Euler

Lemme 10. *Soient p et q deux entiers premiers entre eux. On a*

$$\varphi(pq) = \varphi(p)\varphi(q),$$

où φ est l'indicatrice d'Euler.

Démonstration. Posons $n = pq$. On reprend les notations du corollaire précédent. Soit $A_n = \{k \in \{0, \dots, n-1\}; k \wedge n = 1\}$. Comme $k \wedge n = 1 \iff \overset{\circ}{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$, on a $\varphi(n) = |A_n|$. Nous allons montrer que

$$\Psi_n(A_n) = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times.$$

Soit k tel que $k \wedge n = 1$. Soit a entier tel que $ak \equiv 1 [n]$. Comme p divise n , on a $ak \equiv 1 [p]$. Ce qui montre que dans $\mathbb{Z}/p\mathbb{Z}$, la classe de a est l'inverse de la classe de k . De même, dans $\mathbb{Z}/q\mathbb{Z}$, la classe de a est l'inverse de la classe de k . Ainsi, $\Psi_n(A_n)$ est bien dans $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Reste à voir la surjectivité. Soit $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Notons x' l'inverse de x , y' l'inverse de y , $a = \Psi_n^{-1}(x, y)$ et $b = \Psi_n^{-1}(x', y')$. On a $ab - 1 \equiv 0 [p]$ car dans $\mathbb{Z}/p\mathbb{Z}$, on a $\overset{\circ}{a}\overset{\circ}{b} = \overset{\circ}{x}\overset{\circ}{x}' = \overset{\circ}{1}$. De même $ab - 1 \equiv 0 [q]$. Comme p et q sont premiers entre eux, on a alors $ab - 1 \equiv 0 [n]$, ce qui montre que $a \wedge n = 1$, ce qui montre que

(x, y) a bien son antécédent dans A_n . A_n et $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ sont donc en bijection, donc ils ont même cardinal, soit

$$\varphi(pq) = \varphi(p)\varphi(q)$$

□

Lemme 11. *Soit p un nombre premier et α un entier strictement positif. On a*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

Démonstration. Rappelons que $\varphi(n)$ est le nombre d'entiers entre 0 et $n - 1$ qui sont premiers avec n . En l'occurrence $\varphi(p^\alpha)$ est le nombre d'entiers entre 0 et $p^\alpha - 1$ qui sont premiers avec p^α . Mais être premier avec p^α , c'est équivalent à être premier avec p : c'est ne pas être multiple de p . Il y a exactement $p^\alpha/p = p^{\alpha-1}$ multiples de p entre 0 et p^α . On a donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$. □

Théorème 20. *Soit n un entier naturel. Sa décomposition en produit de facteurs premiers s'écrit*

$$n = \prod_{p|n} p^{v_p(n)}.$$

Alors, son indicatrice d'Euler est donnée par la formule

$$\varphi(n) = \prod_{p|n} (p^{v_p(n)} - p^{v_p(n)-1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Démonstration. Par récurrence sur le nombre de diviseurs premiers de n . □

5.5 Codage RSA

On suppose qu'Alice veut envoyer un message secret à Bob, mais qu'elle sait que sa communication peut être espionnée.

Génération des clefs

Voilà ce que doit faire Alice pour générer les clefs

1. Choisir aléatoirement et de manière indépendante deux grands nombres premiers p et q . On pose $N = pq$.
2. Choisir aléatoirement un entier e avec $1 < e < N$ qui est premier avec $(p - 1)(q - 1)$.
3. Déterminer un entier d tel que $ed \equiv 1 \pmod{(p - 1)(q - 1)}$

4. Détruire toute trace de p et q .

Le couple (N, e) constitue la clef publique, qu'Alice doit donner à quiconque souhaite pouvoir lui envoyer des messages cryptés. Alice garde pour elle seule le couple (N, d) , qui constitue la clef privée. C'est à l'aide de cette clef qu'elle pourra décoder les messages reçus.

Cryptage des messages

Supposons que Bob veuille envoyer un message secret à Alice. Il le transforme en une suite de nombres entre 0 et $N - 1$. Le procédé de transcription doit être bijectif et très simple. Alice doit évidemment connaître ce procédé, qu'il n'y a pas lieu d'essayer de tenir secret. Si m_i est le i -ème nombre de cette suite, Bob transmettra le nombre c_i de $\{0, \dots, N - 1\}$ défini par

$$c_i \equiv m_i^e [N].$$

Le calcul de m_i^e peut être fait à l'aide de la méthode d'exponentiation rapide basée sur l'écriture de e en base 2.

Cryptage des messages

Alice peut alors décoder le message à l'aide de sa clef secrète grâce la formule

$$m_i \equiv c_i^d [N].$$

Démonstration. Dans $\mathbb{Z}/N\mathbb{Z}$, on a $\hat{m}_i^e = (\hat{c}_i^d)^e = \hat{c}_i^{ed}$. On sait que $ed \equiv 1 [(p-1)(q-1)]$: il existe un entier k tel que $ed = 1 + k(p-1)(q-1)$. On a donc

$$\begin{aligned} c_i^d &= m_i^{ed} \\ &= m_i^{1+k(p-1)(q-1)} \end{aligned}$$

En appliquant deux fois le corollaire 7, on obtient $c_i^d \equiv m_i [p]$ et $c_i^d \equiv m_i [q]$. Comme p et q sont premiers entre eux, cela implique $c_i^d \equiv m_i [pq]$, ce qui achève la preuve. \square

Signature de messages

Il est très facile sur Internet d'envoyer un message en y accolant l'adresse e-mail d'un autre. Il est donc très important d'avoir des techniques permettant d'authentifier l'auteur d'un message. L'algorithme RSA peut être utilisé à celà. Supposons que les correspondants se sont mis d'accord sur une fonction h , dite fonction de hachage, qui à un message (pas nécessairement crypté) M associe un nombre $h(M) \in \{0, \dots, N - 1\}$. La fonction de hachage est une donnée publique.

Supposons que Alice veuille envoyer un message M à Bob, de manière à ce que Bob puisse l'authentifier. Elle calculera $s = h(M)^d$ modulo N , faisant ainsi usage de sa clef privée. Elle enverra à Bob le couple (M, s) . Bob, qui connaît la clef publique d'Alice et la clef de hachage va calculer $h(M)$ et s^e modulo N . Si les deux coïncident, on peut conclure qu'Alice est bien l'auteur du message.

Sécurité de l'algorithme

Pour trouver/décoder les messages envoyés à Alice ou se faire passer pour elle, il faut connaître e : il semble ainsi que l'on ait besoin de connaître $(p-1)(q-1)$. Jusqu'à preuve du contraire, la seule méthode générale qu'on connaisse est de factoriser N pour trouver p et q . Lorsque N est grand, ce calcul demande de puissants ordinateurs.

5.6 Exercices

1. Soient a, b, c trois entiers naturels. Montrer que abc est divisible par 7 si $a^3 + b^3 + c^3$ l'est.
2. Quels sont les entiers x tels que $x^x - 3$ soit divisible par 7 ?
3. On dit qu'un nombre entier supérieur à un est mauvais si il n'est pas premier et ne s'écrit pas comme somme de deux nombres premiers. Quel est le plus petit nombre mauvais ? Montrer qu'il existe une infinité de nombres mauvais.
4. *Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ – application à l'indicatrice d'Euler*
Avant de faire cet exercice, on aura intérêt à revoir le théorème de Lagrange.
 - (a) Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
 - (b) Soit n entier naturel non nul et d un diviseur positif de n . Montrer que $H = \{x \in \mathbb{Z}/n\mathbb{Z}; dx = 0\}$ contient tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d . À l'aide de la première question, montrer alors que H est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .
 - (c) En déduire que

$$n = \sum_{d|n} \varphi(d).$$

5. *Algorithme d'exponentiation rapide*

Soit n un entier naturel non nul et $x \in \mathbb{Z}/n\mathbb{Z}$. On veut calculer rapidement x^n . On suppose que m s'écrit en base 2 :

$$n = \sum_{k=0}^m a_k 2^k.$$

On pose $u_0 = 1$, et pour $0 \leq i \leq m$:

$$u_{i+1} = \begin{cases} (u_i)^2 & \text{si } a_i = 0 \\ (u_i)^2 \times x & \text{si } a_i = 1 \end{cases}$$

- (a) Montrer que $u_{m+1} = x^n$. Indication : construire une suite $(c_i)_{0 \leq i \leq m+1}$ telle que pour tout $i \in \{0, \dots, m+1\}$, on ait $u_i = x^{c_i}$.
- (b) Montrer que 9 divise $2^{33} + 2$.
6. (a) Écrire 1800 en base 2.
 (b) En déduire que 30967 s'écrit en base 2 : $\overline{111101011}$.
 (c) Montrer que 30967 n'est pas un nombre premier.
 Indication : on pourra utiliser le petit théorème de Fermat...et une calculatrice.
7. Déterminer tous les entiers n tels que $\varphi(n)$ est impair.
8. Soit A l'ensemble des entiers strictement supérieurs à 1. On définit, pour $x \in A$: $\Psi(x) = 2\varphi(x)$, où φ est la fonction indicatrice d'Euler.
- (a) Montrer que pour tout x dans A , $\Psi(x) \in A$.
 (b) Déterminer l'ensemble des points fixes de A .
 (c) Soit $x \in A$. On définit une suite $(u_n)_{n \geq 0}$ par la donnée de $u_0 = x$ et de la récurrence $u_{n+1} = \Psi(u_n)$. Montrer que quel que soit $x \in A$, la suite $(u_n)_{n \geq 0}$ converge.
 (d) Montrer que si $x = 10^k$, avec $k \geq 1$, alors

$$\lim_{n \rightarrow +\infty} u_n = 8^k.$$

9. (a) Déterminer des entiers naturels a et k tels que $a^2 = 5 + 139k$.
 (b) Résoudre dans $\mathbb{Z}/139\mathbb{Z}$ l'équation $x^2 - 3x + 4 = 0$.
10. Déterminer les couples $(a, b) \in (\mathbb{Z}/13\mathbb{Z})^2$ tels que $a^2 + b^2 = 0$.
11. Calculer

$$\sum_{x \in (\mathbb{Z}/1973\mathbb{Z})^\times} x^{-1}.$$

12. Combien y a-t-il de nombres complexes tels qu'il existe un entier $k \in \{0, \dots, 10\}$, avec $z^k = 1$?