# Arithmétique – Cryptographie

Gaetan Bisson

https://gaati.org/bisson/

# Introduction

> *« Choisissez un entier $y$ et communiquez-le moi ; je vous renverrai, après un rapide calcul, un entier $x$ vérifiant $x^{111} = y \bmod 501$. Sauriez-vous en faire autant ? Si personne d'autre ne le peut alors, en retenant les chiffres* 111 *et* 501*, vous me permettez de vous prouver mon identité. »*

Ce cours vous permettra de comprendre, résoudre et construire de tels « énigmes » en exploitant la structure que confèrent aux nombres entiers et rationnels les opérations d'addition et de multiplication. Cette structure est non seulement fondamentale en algèbre, mais aussi critique pour de nombreuses technologies du monde numérique, notamment la cryptographie (science des codes secrets).

L'étude de cette structure nous amènera à :

— construire et analyser des cryptosystèmes à clef publique ;
— entrevoir les structures abstraites sous-jacentes : groupes, anneaux et corps.

# Table des matières

# Chapitre 1

# Primitives symétriques

La cryptographie est l'étude des techniques visant à protéger les communications. Ce n'est qu'entre 1918 (Enigma) et 1976 (Diffie–Hellman) qu'elle s'établit comme science à part entière. Auparavant et depuis l'antiquité, sa pratique restait amateur avec quelques systèmes cryptographiques inventés puis abandonnés dès leurs faiblesses identifiées.

Ce chapitre présente les principales primitives cryptographiques classiques. Celles, plus modernes, qui exploitent des structures algébriques, seront décrites au chapitre suivant. Toutes visent à assurer que des messages numériques puissent être transmis par un canal non sécurisé (pensez à la poste) tout en garantissant leur :

— **intégrité :** le message n'a pas été modifié ;
— **authenticité :** le destinataire sait de qui le message provient ;
— **confidentialité :** seul le destinataire et l'expéditeur connaissent le message.

## 1.1 Contexte et terminologie

Jules César avait pour usage, afin de rendre un message privé inintelligible d'éventuels espions, de l'écrire comme suite de lettres de l'alphabet latin $\mathbb{A} = \{A, \dots, Z\}$ puis de remplacer chacune de ces lettres par celle se trouvant trois crans plus loin dans l'alphabet.

**Exemple.** *Le message BONJOUR devenait ainsi ERQMRXU.*

L'expéditeur du message devait au préalable s'accorder avec son destinataire sur l'utilisation de cette méthode ; il ne lui restait alors plus qu'à espérer que le message ainsi transformé soit inintelligible à tout observateur passif. C'est ce que formalise la définition suivante.

**Définition.** *Soit $M = \mathbb{A}^{(\mathbb{N})}$ l'ensemble des messages. On appelle **méthode de chiffrement** tout couple $(E, D)$ de fonctions de $M$ dans lui-même vérifiant $D \circ E = \mathrm{id}_M$ ; visuellement, on a :*

$$\underset{\textit{message}}{m \in M} \xrightarrow[E]{\textit{chiffrement}} \underset{\textit{chiffré}}{E(m)} \xrightarrow[\mathrm{id}]{\textit{transmission}} \underset{\textit{chiffré}}{E(m)} \xrightarrow[D]{\textit{déchiffrement}} \underset{\textit{message}}{D(E(m)) = m}$$

*Un espion ne verrait circuler sur le canal de transmission que des chiffrés $E(m)$ ; on qualifie la méthode de chiffrement de **sûre** si ces observations ne lui permettent de rien inférer sur les messages $m$. En outre, on dit qu'elle est **symétrique** lorsque, connaissant $E$, on peut facilement calculer $D$.*

Le chiffrement de César est symétrique : si l'on sait que chiffrer revient à décaler chaque lettre de trois crans vers la droite, il est évident que pour déchiffrer on opère ce même décalage mais vers la gauche. Toutefois, il est loin d'être sûr : les chiffrés paraissent certes méconnaissables, mais deviner à leur vue la méthode de chiffrement utilisée est un jeu d'enfant pour n'importe quel initié :

1. On se rend assez rapidement compte qu'il s'agit d'un chiffrement par décalage, par exemple en effectuant des statistiques sur la fréquence d'apparition des lettres.
2. Si ces statistiques ne donnent pas directement la valeur du décalage, on peut facilement tester les 26 possibilités en un temps relativement court.

Comme enseignements empiriques, nous retiendrons de cette anecdote historique que pour croire en la sûreté d'une méthode de chiffrement les deux propriétés ci-dessous sont fortement désirables :

— les chiffrés ne doivent pas pouvoir être distingués de messages aléatoires ;
— tester toutes les possibilités de chiffrement doit être infaisable.

## 1.2 Chiffrement par flot

Commençons par décomposer les messages numériques en symboles élémentaires.

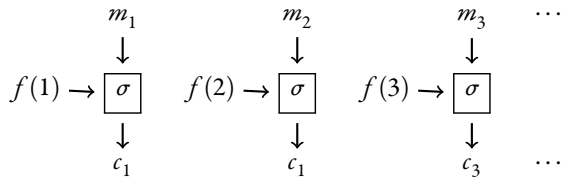
**Définition.** *On appelle alphabet $\mathbb{A}$ tout ensemble qui n'est pas un singleton. Un alphabet étant fixé, on appelle lettre tout élément $a \in \mathbb{A}$ et message toute suite finie de lettres $m = m_1 m_2 \cdots m_n$ avec $m_i \in \mathbb{A}$. L'ensemble de tous les messages se note donc $\mathbb{A}^{(\mathbb{N})}$.*

En pratique, on pourra considérer :
— l'alphabet booléen, $\{0, 1\}$ ;
— l'alphabet latin $\{A, \ldots, Z\}$ ;
— l'ensemble des caractères ASCII.

On peut facilement convertir des messages d'un alphabet vers un autre par des correspondances arbitraires, par exemple $A = 01000001$ ; ces conversions sont aisément calculables et l'alphabet considéré n'a donc aucune pertinence particulière en cryptographie.

**Définition.** *Un chiffrement par flot consiste en la donnée de :*
— *une fonction pseudo aléatoire $f : \mathbb{N} \to \mathbb{A}$ ;*
— *une fonction inversible $\sigma : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$.*

*Le chiffrement du message $m_1 m_2 \cdots m_n$ est alors $c_1 c_2 \cdots c_n$ avec $c_i = \sigma(m_i, f(i))$ ; visuellement :*




**Exemple.** *On retrouve le chiffrement de César en prenant comme alphabet $\mathbb{A} = \{A, \ldots, Z\}$, comme constante $f(i) = 3$ et comme opération $\sigma(x, y) = x + y \mod 26$.*

Si la fonction $f$ est réellement aléatoire, nous obtenons un chiffrement dont la sûreté peut être prouvée rigoureusement et inconditionnellement, au sens où les chiffrés ne transportent strictement aucune information sur les messages. C'est en fait la seule méthode de chiffrement garantissant cela [15]. Faut de mieux, pendant la guerre froide, des diplomates voyageaient

ainsi avec des mallettes remplies de valeurs (réellement aléatoires) pour $f(i)$ de sorte que leurs supérieurs puissent ensuite échanger des messages en parfaite confidentialité.

Depuis, ce n'est plus l'existence même d'une information sur les messages qui importe aux cryptographes, mais la faisabilité de l'extraire des chiffrés. Cela explique la définition de sûreté donnée plus haut et pourquoi elle a pu paraître malcommode. Ce « compromis » est nécessaire pour concevoir des méthodes cryptographiques efficaces en pratique. Par exemple, dans le cas des chiffrements par flot, il consiste à accepter des fonctions $f$ pseudo aléatoires, dont en particulier certaines dont la description tient en quelques octets, éliminant ainsi le lourd transport de mallettes diplomatiques.

De nos jours, on prend typiquement $\mathbb{A} = \{0,1\}$ et $\sigma = \otimes$. Comme fonction pseudo aléatoire, on peut notamment envisager la famille suivante, même si la cryptographie moderne sait mieux faire.

**Définition.** *Un registre à rétroaction linéaire (LFSR en anglais) consiste en la donnée de :*
- *un état initial $s_1 s_2 \dots s_r \in \{0,1\}^r$ ;*
- *une application linéaire $r : \{0,1\}^r \to \{0,1\}^r$.*

*En posant $s_{i+r} = r(s_i, s_{i+1}, \dots, s_{i+r-1})$ on obtient la fonction pseudo aléatoire $f(i) = s_{i+r}$.*

**Exercice.** *Prenons* 001 *pour état initial et $(x,y,z) \mapsto x \otimes z$ comme application linéaire ; calculer les vingt premiers bits donnés par $f$.*

**Attention !** La notion de « faisabilité » est omniprésente en cryptographie mais il est très délicat de lui donner un sens mathématique rigoureux. Dans ce cours, nous nous contenterons de l'assimiler à une expérience pratique : résoudre le problème demandé doit être impossible en temps raisonnable (dix ans) et coût raisonnable (cent milliards de francs). Tous les coups sont permis : construire un supercalculateur, investir dans la recherche, etc.

En pratique, les cryptographes *supposent* qu'un problème est infaisable lorsqu'il a été étudié depuis au moins dix ans et que la meilleure méthode connue pour le résoudre nécessite au moins $2^{128}$ opérations élémentaires ; la technologie actuelle ne permettant pas d'effectuer plus de $2^{64}$ opérations par seconde, même avec tous les ordinateurs du monde, le résoudre prendrait donc des millénaires.

## 1.3 Chiffrement par bloc

Chiffrer un message lettre par lettre possède des avantages (facilité d'implantation) mais aussi des inconvénients (grande malléabilité). De nos jours, on considère comme plus robustes les méthodes de chiffrement qui traitent les lettres « bloc par bloc ». Dans ce chapitre nous noterons $r$ le nombre de lettres dans un bloc. Pour fixer les idées, dans le cas binaire $\mathbb{A} = \{0,1\}$, on utilise généralement $r = 128$.

**Définition.** *On appelle chiffrement par bloc toute fonction inversible $f : \{0,1\}^r \to \{0,1\}^r$.*

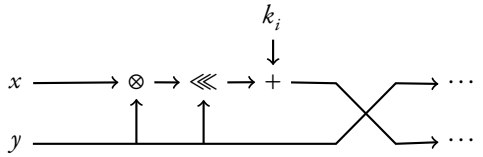
Évidemment, cette définition fait abstraction des deux objectifs premiers en cryptographie : efficacité et sécurité. Par soucis d'efficacité, les méthodes standards de chiffrement par bloc sont construites à partir des opérations élémentaires des processeurs, à savoir :
- l'addition modulo $2^{64}$
- le ou exclusif bit-à-bit
- le décalage circulaire

Par soucis de sécurité, ces méthodes utilisent **toutes** ces opérations de manière croisée.

**Définition.** *Décomposons un message en blocs $b_1 b_2 \cdots b_n$ avec $b_i \in \{0,1\}^r$. La méthode de chiffrement par bloc RC5 [11] consiste à calculer $(c_{2i}, c_{2i+1}) = f_0 \circ f_1 \circ \cdots \circ f_{39}(b_{2i}, b_{2i+1})$ avec*

$$f_i(x,y) = (y, ((x \otimes y) \lll y) + k_i)$$

*où $k = k_0 k_1 \cdots k_{39}$ désigne une suite arbitraire de blocs aléatoires. Visuellement, il s'agit de répéter quarante fois le circuit suivant :*




Remarquons que la description complète de cette méthode est publique, à l'exception de la suite $k$ appelée **clef de chiffrement**. Cette clef doit être choisie aléatoirement par l'expéditeur, partagée avec le destinataire (qui peut alors déchiffrer en effectuant les opérations ci-dessus en sens inverse) mais gardée secrète de toute autre personne ; elle permet aux interlocuteurs de paramétrer le chiffrement de manière unique. On remplace ainsi des mallettes de plusieurs millions d'octets en une seule « clef » de quelques octets.

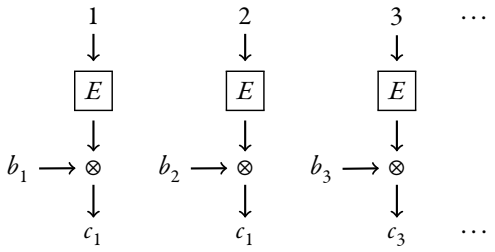
La sécurité du système repose sur le fait que, sans a priori connaître la clef $k$, la méthode la plus efficace pour retrouver des messages $m_i$ à partir de chiffrés $c_i$ consiste à essayer toutes les clefs de (dé)chiffrement possibles. Le nombre de possibilités pour $k$ étant supérieur à $2^{128}$, ceci est infaisable.

## 1.4 Modes d'opération

En pratique, les données à chiffrer possèdent souvent une redondance assez forte. Il est par exemple fréquent qu'un message comporte deux blocs identiques. Si les blocs de ce message sont chiffrés de manière indépendante, comme vu jusqu'ici, cette propriété se retrouvera sur le chiffré.

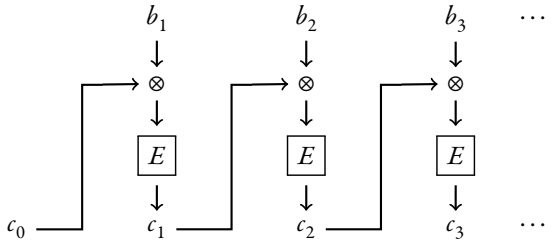
Afin d'éviter de telles fuites d'information, aussi minimes semblent-elles, différentes manières robustes d'appliquer un chiffrement aux blocs d'un message ont été mises au point ; elles sont connues sous le nom de « modes d'opération ».

**Définition.** *Soit $E : \{0,1\}^r \to \{0,1\}^r$ un chiffrement par bloc. Décomposons un message en blocs $b_1 b_2 \cdots b_n$ avec $b_i \in \{0,1\}^r$. Le chiffrement compteur (CTR en anglais) est $c_1 c_2 \cdots c_n$ avec $c_i = b_i \otimes E(i)$ ; visuellement :*




Très brièvement, l'avantage de cette méthode est évidemment sa simplicité ; sa faiblesse majeure est cependant que le $i^{\text{e}}$ bloc est toujours chiffré de la même façon, par un bête ou exclusif.

**Définition.** *Soit $E : \{0,1\}^r \to \{0,1\}^r$ un chiffrement par bloc et $c_0 \in \{0,1\}^r$ un vecteur arbitraire (IV en anglais). Décomposons un message en blocs $b_1 b_2 \cdots b_n$ avec $b_i \in \{0,1\}^r$. Le chiffrement chaîné (CBC en anglais) est $c_1 c_2 \cdots c_n$ avec $c_i = b_i \otimes E(i)$; visuellement on a :*




Cette approche a pour grand avantage qu'elle « diffuse » le chiffrement ; toutefois c'est aussi là son inconvénient : afin de chiffrer le $i^{\text{e}}$ bloc, il faut chiffrer tous les précédents.

## 1.5 Fonctions de hachage

Pour finir notre brève présentation des primitives cryptographiques classiques, il nous reste à introduire la notion de « fonction de hachage ».

**Définition.** *On appelle fonction de hachage toute application $h : \mathbb{A}^{(\mathbb{N})} \to \mathbb{A}^r$ calculable efficacement. Elle est dite sûre si elle vérifie :*

— *Étant donné $c \in \mathbb{A}^r$ il est infaisable de trouver $m \in \mathbb{A}^{(\mathbb{N})}$ tel que $h(m) = c$.* (préimage)

— *Il est infaisable de trouver $m \neq m' \in \mathbb{A}^{(\mathbb{N})}$ tel que $h(m) = h(m')$.* (collision)

**Exercice.** *Considérer des applications naturelles et voir qu'elles ne satisfont pas cette définition.*

Les fonctions de hachage ont d'innombrables applications en cryptographie mais aussi bien au delà en informatique. On s'en sert notamment pour :

— vérifier l'intégrité des fichiers ;

— identifier des utilisateurs sans stocker leurs mots de passe ;

— concevoir des devises électroniques décentralisés telles Bitcoin [8].

Bien que la conception de fonctions de hachage soit un exercice très difficile, on pourrait, à titre d'exemple, considérer la construction suivante (avec $r \geqslant 128$) :

1. Décomposer le message $m$ en blocs $b_1 \cdots b_n$ avec $b_i \in \{0,1\}^r$.
2. Chiffrer $b_1 \cdots b_n$ avec RC5 (prendre $k = 0$) en mode CBC (prendre $c_0 = 0$) ; on obtient $c_1 \cdots c_n$.
3. Chiffrer $c_1 \cdots c_n$ avec RC5 (prendre $k = c_n$) en mode CBC (prendre $c_0 = 0$) ; on obtient $d_1 \cdots d_n$.
4. Renvoyer $d_n$.

**Exercice.** *Essayer de simplifier la procédure ci-dessus et voir qu'elle perd en sécurité.*

# Chapitre 2

# Primitives asymétriques

Les primitives cryptographiques vues au chapitre précédent, certaines remontant à l'antiquité, sont dites **symétriques**, c'est-à-dire que toute personne sachant chiffrer sait aussi déchiffrer. Autrement dit, la même clef sert à la fois au chiffrement et au déchiffrement ; cette clef ne doit donc être communiquée qu'aux interlocuteurs et on dit ainsi que ces méthodes sont **à clef secrète**.

Depuis les années 1980 [2] des méthodes de chiffrement **asymétriques** ont vu le jour, c'est-à-dire que l'on peut connaître la méthode de chiffrement $E$ sans pour autant savoir calculer son inverse $D$. En d'autre termes, la clef de déchiffrement (paramétrant $D$) est distincte de la clef de chiffrement (paramétrant $E$). Cette dernière peut ainsi être rendue publique et on dit que ces méthodes sont **à clef publique**.

Ces méthodes, plus avancées, exploitent les propriétés mathématiques d'objets issus de l'arithmétique. Ce chapitre présente succinctement les plus élémentaires de ces méthodes. Les suivants auront pour objectif d'étudier les aspects mathématiques sous-jacents.

## 2.1 Chiffrement à clef publique

Au chapitre précédent, la dépendance de $E$ et $D$ en la clef $k$ était implicite. Maintenant que nous comprenons mieux l'intérêt des clefs, rendons la explicite dans le cas asymétrique grâce à la définition suivante.

**Définition.** *On appelle méthode de chiffrement à clef publique tout triplet $(G, E, D)$ de fonctions :*

- $G : \mathbb{A}^r \to \mathbb{A}^r \times \mathbb{A}^r$ (construction des clefs)
- $E : \mathbb{A}^r \times \mathbb{A}^{(\mathbb{N})} \to \mathbb{A}^{(\mathbb{N})}$ (chiffrement)
- $D : \mathbb{A}^r \times \mathbb{A}^{(\mathbb{N})} \to \mathbb{A}^{(\mathbb{N})}$ (déchiffrement)

*vérifiant, pour tout couple $(e, d)$ dans l'image de $G$ et pour tout message $m$,*

$$D(d, E(e, m)) = m.$$

*Elle est dite sûre si, étant donnés $G$, $E$, $D$, $e$ et $c$, il est infaisable de trouver $m$ tel que $c = E(e, m)$.*

Concrètement, une telle méthode étant fixée, chaque utilisateur choisi une valeur aléatoire $z \in \mathbb{A}^r$, calcule $(e, d) = G(z)$ et publie $e$ comme étant la clef à utiliser pour chiffrer des messages à son intention. Chacun peut alors chiffrer un messages $m$ en $c = E(e, m)$ de sorte que seul lui puisse le déchiffrer en calculant $D(d, c)$.

**Remarque.** *L'aléa $z$ sert uniquement à garantir l'unicité du couple $(e, d)$ construit par chaque utilisateur ; il est implicite dans la plupart des descriptions de fonctions $G$ et, une fois les clefs construites, il peut être oublié.*

Avec les méthodes symétriques, chaque couple d'interlocuteurs doit secrètement se mettre d'accord sur une clef privée avant d'utiliser le cryptosystème. Ici, en revanche, seule une clef par utilisateur suffit et nul besoin d'échange secret préalable.

**Définition.** *La méthode de chiffrement à clef publique RSA [12] fonctionne* ***essentiellement*** *comme il suit :*

1. *Pour construire un couple de clefs, choisir deux nombres premiers $p$ et $q$ aléatoirement. Calculer alors deux entiers $a$ et $b$ vérifiant $ab = 1 \bmod (p-1)(q-1)$. Calculer $n = pq$. Renvoyer comme clef publique $e = (n, a)$ et comme clef privée $d = (n, b)$.*
2. *On chiffre des messages $m \in \{1, \dots, n\}$ par $E : (e, m) \mapsto m^a \bmod n$.*
3. *On déchiffre grâce à $D : (d, m) \mapsto m^b \bmod n$.*

L'égalité $D(d, E(e, m)) = m$ est-elle toujours satisfaite ? Calculer $d$ à partir de la clef publique est-il difficile ? Pour répondre de manière satisfaisante à ces questions, nous allons devoir étudier l'arithmétique des entiers.

**Exercice.** *Soit la clef publique $(n = 26, a = 5)$. Essayer de déchiffrer le message* `TKXJY` *où l'on a codé $A = 0$, $B = 1$, $C = 2$, etc.*

## 2.2 Signature électronique

**Définition.** *On appelle méthode de signature électronique tout triplet $(G, S, V)$ de fonctions :*

— $G : \mathbb{A}^r \to \mathbb{A}^r \times \mathbb{A}^r$ (construction des clefs)
— $S : \mathbb{A}^r \times \mathbb{A}^{(\mathbb{N})} \to \mathbb{A}^{(\mathbb{N})}$ (signature)
— $V : \mathbb{A}^r \times \mathbb{A}^{(\mathbb{N})} \times \mathbb{A}^{(\mathbb{N})} \to \{\texttt{vrai}, \texttt{faux}\}$ (vérification)

*vérifiant, pour tout couple $(s, v)$ dans l'image de $G$ et pour tout message $m$,*

$$V(v, m, S(s, m)) = \texttt{vrai}.$$

*Elle est dite sûre si, étant donnés $G$, $S$, $V$, $v$ et $m$, il est infaisable de trouver $c$ satisfaisant $V(v, m, c) = \texttt{vrai}$.*

La forte similarité de cette définition avec la précédente n'est pas un hasard. Toute méthode $(G, E, D)$ de chiffrement à clef publique devient une méthode de signature électronique « en échangeant les clefs », c'est-à-dire pour $S = E$, $s = e$, $v = d$ et $V : (v, m, c) \mapsto (m = D(v, c))$.

Dans le cas de RSA il se trouve que la condition de sûreté est vérifiée ; c'est ce que nous utilisons dans l'introduction avec $n = 501$ et $d = 111$. Mon exposant $e$ secret était 3. De nouveau, cela s'expliquera par l'arithmétique des entiers.

## 2.3 Mise en garde

Ce chapitre et le précédent n'ont fait que présenter des notions et constructions cryptographiques relativement naïves et élémentaires. Bien d'autres subtilités doivent être surmontés afin de concevoir des cryptosystèmes robustes et les analyser rigoureusement. Cela requiert notamment des connaissances en informatique théorique et en théorie des probabilités. Exposer ces fondements de la cryptographique moderne fait l'objet d'ouvrages à part entière, tels [4, 5].

Nous n'aborderons pas non plus ici les principes de sécurité nécessaires à la bonne utilisation de la cryptographie logicielle en pratique. Les utilisateurs (notamment leur mauvaise gestion des clefs privés) sont souvent le maillon le plus faible d'un système cryptographique. Si vous êtes amenés à utiliser vous-même un tel système, **par pitié, renseignez vous au préalable !**

En conclusion, cette partie du cours n'avait la prétention que d'introduire la cryptographie comme motivation pour l'étude des objets mathématiques sous-jacents à ses avancées modernes. Alors que nous abordons cette étude, gardons toutefois à l'esprit la dimension concrète (notamment la notion d'efficacité) que donne la cryptographie à ces notions théoriques.

# Chapitre 3

# Arithmétique des entiers

## 3.1 Propriétés élémentaires

On note $\mathbb{N} = \{0, 1, 2, \dots\}$ l'ensemble des entiers naturels muni des opérations usuelles d'addition et de multiplication. En rajoutant les nombres négatifs, on obtient l'ensemble $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Cela devrait pour vous être une évidence qu'il vérifie :

- pour l'addition :
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, x + (y + z) = (x + y) + z$ *(associativité)*
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x + y = y + x$ *(commutativité)*
  - $\exists 0 \in \mathbb{Z}, \forall x \in \mathbb{Z}, x + 0 = x$ *(élément neutre)*
  - $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x + y = 0$ *(inverse)*
- pour la multiplication :
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(associativité)*
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \cdot y = y \cdot x$ *(commutativité)*
  - $\exists 1 \in \mathbb{Z}, \forall x \in \mathbb{Z}^*, x \cdot 1 = x$ *(élément neutre)*
- pour la compatibilité :
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, x \cdot (y + z) = x \cdot y + x \cdot z$ *(distributivité)*

On dit ainsi que $\mathbb{Z}$ est un anneau. Vous étudierez cette classe d'objet en plus grande généralité dans les cours *Groupes et Anneaux* (S5) et *Anneaux et Corps* (S6).

L'anneau $\mathbb{Z}$ est de surcroit ordonné, ce qui signifie qu'il est muni d'une relation que l'on notera $\leqslant$ (celle que vous connaissez) qui vérifie :

- pour l'ordre :
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$ *(transitivité)*
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \leqslant y \wedge y \leqslant x \Rightarrow x = y$ *(antisymétrie)*
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \leqslant y \vee y \leqslant x$ *(totalité)*
- pour la compatibilité :
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, x \leqslant y \Rightarrow x + z \leqslant y + z$ *(addition)*
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, 0 \leqslant x \wedge 0 \leqslant y \Rightarrow 0 \leqslant xy$ *(multiplication)*

En combinant ces propriétés élémentaires, on peut justifier la grande majorité des calculs directs ou évidents que l'on peut effectuer avec les entiers. Ce cours va quant à lui se concentrer sur l'étude la structure de $\mathbb{Z}$ au delà de ces postulats de base.

## 3.2 Divisibilité

S'il est évident qu'on peut ajouter, soustraire ou multiplier deux entiers entre eux, cela n'est pas aussi clair pour la division. Dans certains contextes, notamment en sciences physiques, où les entiers sont des nombres réels parmi d'autres, il est parfaitement pertinent d'écrire $2/3 = 0,666\ldots$ et pour cela de sortir du cadre strict des entiers. Toutefois, il est aussi intéressant de considérer le cas restreint à $\mathbb{Z}$ et, nous le verrons plus tard, cela trouve de nombreuses applications, notamment en cryptographie.

**Définition.** *Soient $a$ et $b$ deux entiers. S'il existe $q \in \mathbb{Z}$ tel que $a = qb$ on dit que :*
- *$a$ est un multiple de $b$ ;*
- *$b$ est un diviseur de $a$ ;*
- *$b$ divise $a$, ce qu'on note « $b \mid a$ ».*

Vous savez bien que les entiers pairs (resp. impairs) sont ceux qui sont divisible par deux (resp. ne le sont pas) ; prenez de surcroit l'habitude, lorsqu'un entier $n$ est supposé pair (resp. impair) d'écrire immédiatement $n = 2k$ (resp. $n = 2k + 1$) pour un certain $k \in \mathbb{Z}$.

**Remarque.** *Si $b$ divise $a$, soit $a = qb$, on a aussi $a = (-q)(-b)$ donc $-b$ divise $a$. Les problèmes de divisibilité restent donc inchangés par multiplication par $\pm 1$. Par la suite, pour simplifier les énoncés, nous serons donc souvent amener à nous restreindre aux diviseurs positifs, ce qui revient à regarder la divisibilité dans $\mathbb{N}$ plutôt que $\mathbb{Z}$.* ***N'oubliez pas pour autant les diviseurs négatifs.***

Évidemment, chaque entier $a$ est divisible par lui-même (prendre $q = 1$), est divisible par 1 (prendre $q = a$) et divise zéro (prendre $q = 0$). En outre :

**Proposition.** *Quels que soient $a, b, c, d, e \in \mathbb{Z}$ on a :*
- *Si $a \mid b$ et $b \mid c$, alors $a \mid c$.*
- *Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$.*
- *Si $a \mid b$ et $a \mid c$, alors $a \mid bd + ce$.*
- *Si $a \mid b$ et $b > 0$, alors $a \leqslant b$.*

**Exemple.** *L'entier 6 divise 42 mais pas 45. En effet, on a $42 = 6 \cdot 7$. En revanche, si $q \leqslant 7$, on a $6q \leqslant 42$ alors que, si $q \geqslant 8$, on a $6q \geqslant 48$ ; aucun $q \in \mathbb{Z}$ ne satisfait donc $6q = 45$.*

**Exercice.** *Énumérer tous les diviseurs de 60 puis ceux de 61.*

**Exercice.** *Montrer que, pour tout $n \in \mathbb{Z}$, l'entier $n^2 - n$ est pair. Montrer alors que $3 \mid n^3 - n$ quel que soit $n \in \mathbb{Z}$.*

Lorsqu'un entier n'est pas divisible par un autre, on sait exactement pourquoi :

**Théorème** (division euclidienne). *Soient $a$ et $b > 0$ deux entiers. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ vérifiant $a = bq + r$ et $0 \leqslant r < b$. On appelle $q$ et $r$ respectivement le quotient et le reste de la division euclidienne de $a$ par $b$.*

Remarquons que $b$ divise $a$ si et seulement si $r$ est nul. Rappelons par ailleurs qu'en CE1 nous avons vu une méthode très efficace pour calculer le couple $(q, r)$ :

| | |
|---|---|
| 12345 | 67 |
| $-100 \times 67$ | 184 |
| 5645 | |
| $-80 \times 67$ | |
| 285 | |
| $-4 \times 67$ | |
| 17 | |

**Exercice.** *Calculer la division euclidienne de 1234567 par 89.*

## 3.3 Diviseurs communs

Rappelons d'abord deux résultats essentiels normalement vus au S2.

**Théorème.** *Tout sous-ensemble non-vide et majoré de $\mathbb{Z}$ admet un plus grand élément.*
*Tout sous-ensemble non-vide et minoré de $\mathbb{Z}$ admet un plus petit élément.*

**Définition.** *Soient $a$ et $b$ deux entiers.*
*Le plus grand commun diviseur (PGCD) est le plus grand entier positif divisant $a$ et $b$.*
*Le plus petit commun multiple (PPCM) est le plus petit entier positif divisible par $a$ et par $b$.*
*On note :*

$$\operatorname{pgcd}(a,b) = \inf\{n \in \mathbb{N}^* : n \mid a \wedge n \mid b\}$$
$$\operatorname{ppcm}(a,b) = \sup\{n \in \mathbb{N}^* : a \mid n \wedge b \mid n\}$$

**Exemple.** *On peut naïvement calculer un plus grand commun diviseur, par exemple* $\operatorname{pgcd}(42,60)$*, en énumérant les diviseurs des deux nombres : on a* $\operatorname{div}(42) = \{1,2,3,6,7,14,21,42\}$ *et* $\operatorname{div}(60) = \{1,2,3,4,5,6,10,12,15,20,30,60\}$*, d'où* $\operatorname{div}(42) \cap \operatorname{div}(60) = \{1,2,3,6\}$ *ce qui donne* $\operatorname{pgcd}(42,60) = 6$*. Ce n'est heureusement pas la méthode la plus efficace.*

**Algorithme** (Euclide).
*Entrée :* *Deux entiers positifs $a$ et $b$.*
*Sortie :* *Leur* pgcd.

1. *Calculer le reste $r$ de la division euclidienne de $a$ par $b$.*
2. *Si $r = 0$, renvoyer $b$.*
3. *Sinon, assigner $a \leftarrow b$ et $b \leftarrow r$ puis retourner en 1.*

**Exemple.** *Pour calculer* $\operatorname{pgcd}(42,60)$ *on aurait pu donc écrire :*

$$\begin{aligned} 42 &= 0 \times 60 + 42 \\ 60 &= 1 \times 42 + 18 \\ 42 &= 2 \times 18 + 6 \\ 18 &= 3 \times 6 + 0 \end{aligned}$$

Pour prouver qu'après un nombre fini d'étapes cet algorithme renvoi un résultat et que celui-ci est correct, nous allons d'abord énoncer un lemme que l'on pourra facilement démontrer en exercice.

**Lemme.** *Pour tout triplet $(a,b,k) \in \mathbb{Z}^3$, on a* $\operatorname{pgcd}(a + kb, b) = \operatorname{pgcd}(a,b)$.

*Preuve de l'algorithme.* L'algorithme est correct car la valeur $\operatorname{pgcd}(a,b)$ y est invariante. Il termine car les valeurs prises par $r$ sont positives et strictement décroissantes. Par ailleurs, deux itérations donnent $r \leftarrow r \bmod (b \bmod r)$ et en distinguant les cas $(b \bmod r) \in \{0,\dots,\frac{r}{2}\} \cup \{\frac{r}{2},\dots,r\}$ on montre que le nombre d'itérations est au plus logarithmique en les arguments, soit linéaire en leur taille. □

**Exercice.** *Calculer la valeur de* $\operatorname{pgcd}(123, \operatorname{pgcd}(456,789))$.

**Exercice.** *Considérons la suite de Fibonacci définie par $\phi_0 = 0$, $\phi_1 = 1$ et $\phi_{n+1} = \phi_n + \phi_{n-1}$ avec $\phi_0 = 0$ et $\phi_1 = 1$. Montrer que* $\operatorname{pgcd}(\phi_n, \phi_{n+1}) = 1$*. On souhaite généraliser ce résultat.*
*Démontrer par récurrence sur $m$ l'égalité $\phi_{n+m} = \phi_m \phi_{n+1} + \phi_{m-1}\phi_n$. En déduire que* $\operatorname{pgcd}(\phi_n, \phi_{kn+r}) = \operatorname{pgcd}(\phi_n, \phi_r)$*. Conclure enfin que* $\operatorname{pgcd}(\phi_n, \phi_m) = \phi_{\operatorname{pgcd}(n,m)}$.

## 3.4 Relations de Bézout

Si $d$ est un diviseur commun de $a$ et $b$ alors, quels que soient les entiers $u$ et $v$, on a toujours $d \mid au + bv$. Le cas d'égalité est exactement celui du pgcd :

**Théorème** (Bézout). *Le* pgcd *de deux entiers $a$ et $b$ est le plus petit entier strictement positif $d$ pour lequel il existe des entiers $u$ et $v$ vérifiant $d = au + bv$. Une telle équation s'appelle une relation de Bézout.*

**Exemple.** *Pour* $\text{pgcd}(42, 60) = 6$ *on a effectivement* $6 = 3 \cdot 42 - 2 \cdot 60$.

*Démonstration.* Dans l'algorithme d'Euclide chaque valeur de $r$ est, par récurrence, de la forme $au + bv$ ; c'est donc le cas du pgcd. Tout autre combinaison linéaire à coefficients entiers $au + bv > 0$ est un multiple du pgcd (puisqu'il divise $a$ et $b$) et ne peut donc être plus petite. □

On peut calculer ces coefficients $u$ et $v$ en combinant les divisions euclidiennes utilisées par l'algorithme ci-dessus.

**Exemple.** *Concernant* $\text{pgcd}(42, 60)$ *on a :*

$$\begin{aligned} 0 &= 1 \times 18 - 3 \times \ \ 6 \\ 6 &= 1 \times 42 - 2 \times 18 \\ 18 &= 1 \times 60 - 1 \times 42 \\ 42 &= 1 \times 42 - 0 \times 60 \end{aligned}$$

*d'où l'on tire* $6 = 42 - 2(60 - 42) = 3 \cdot 42 - 2 \cdot 60$.

Plus systématiquement, cela donne :

**Algorithme** (Euclide étendu).
*Entrée :* *Deux entiers positifs $a$ et $b$.*
*Sortie :* *Un triplet $(d, u, v)$ avec $d = \text{pgcd}(a, b) = au + bv$.*

1. *Assigner $(u, s) = (1, 0)$ et $(v, t) = (0, 1)$.*
2. *Tant que $b > 0$ :*
3. *Calculer le quotient $q$ de la division euclidienne de $a$ par $b$.*
4. *Assigner $(a, b) \leftarrow (b, a - qb)$.*
5. *Assigner $(u, s) \leftarrow (s, u - qs)$.*
6. *Assigner $(v, t) \leftarrow (t, v - qt)$.*
7. *Renvoyer $(a, u, v)$.*

*Démonstration.* Vérifier les invariants $a = a_0 u + b_0 v$ et $b = a_0 s + b_0 t$. □

**Exercice.** *Trouver une relation de Bézout entre* 123 *et* 456.

## 3.5 Structure multiplicative

Nous sommes à présent en mesure de montrer le résultat fondamental suivant.

**Théorème.** *Les diviseurs communs de deux entiers sont exactement ceux de leur* pgcd.
*Les multiples communs de deux entiers sont exactement ceux de leur* ppcm.

*Démonstration.* Tout diviseur commun divise les combinaisons linéaires donc le pgcd.

Soit maintenant $m = \text{ppcm}\, q + r$ la division euclidienne d'un multiple commun par le ppcm ; le reste $r$ est un multiple commun strictement inférieur au ppcm donc il est nécessairement nul. □

Le schéma de la figure 3.1 interprète ce résultat visuellement en représentant verticalement les notions de divisibilité et multiplicité.

On en déduit notamment les propriétés fondamentales ci-dessous.

**Proposition.** *Soient $a$, $b$ et $c$ des entiers positifs. On a :*
- $\text{ppcm}(ca, cb) = c\,\text{ppcm}(a, b)$
- $\text{pgcd}(ca, cb) = c\,\text{pgcd}(a, b)$
- $\text{pgcd}(a, b)\,\text{ppcm}(a, b) = ab$

*Démonstration.* Pour la dernière égalité, se ramener au cas où $\text{pgcd}(a, b) = 1$. □

C'est un cas important auquel il est souvent avantageux de se ramener.

**Définition.** *On dit que deux entiers $a$ et $b$ sont premiers entre eux lorsque* $\text{pgcd}(a, b) = 1$.

Le fait qu'ils soient premiers entre eux signifie essentiellement que les structures multiplications induites par deux entiers sont orthogonales. Plus précisément :

**Lemme** (Gauss). *Si $a$ et $b$ sont premiers entre eux et si $a \mid bc$, alors $a \mid c$.*

*Démonstration.* Multiplions par $c$ une relation de Bézout $1 = au + bv$ ; on obtient $c = acu + bcv$ et le résultat est clair. □

**Exercice.** *Combien y a-t-il d'entiers positifs premiers à* 210 *et plus petit que lui ?*

**Exercice.** *Montrer que* $\text{pgcd}(a, c) = 1$ *implique* $\text{pgcd}(ab, c) = \text{pgcd}(b, c)$.
*Plus généralement, que dire de l'égalité* $\text{pgcd}(ab, c) = \text{pgcd}(a, c)\,\text{pgcd}(b, c)$ *?*

**Exercice.** *On note $F_n = 2^{2^n} + 1$ le $n^e$ nombre de Fermat ; montrer que $F_m = (F_n - 1)^{2^{m-n}} + 1$ puis en déduire que* $\text{pgcd}(F_m, F_n) = 1$ *lorsque $m \neq n$.*

## 3.6 Primalité

**Définition.** *On dit qu'un entier $p > 1$ est premier s'il n'admet comme diviseurs positifs que* 1 *et $p$.*

**Exercice.** *Déterminer les treize plus petits nombres premiers.*

On entend souvent dire que les nombres premiers sont les briques de base de la structure multiplicative des entiers ; c'est essentiellement pour la raison suivante.

**Proposition.** *Tout entier $n > 0$ peut se décomposer comme produit de nombres premiers.*

*Démonstration.* C'est clairement le cas de 1. Supposons ce résultat vérifié pour $\{1, \dots, n-1\}$. Si $n$ n'est pas premier, il admet un diviseur strict $d \in \{2, \dots, n-1\}$ et on applique l'hypothèse de récurrence à $d$ et $\frac{n}{d}$ avant d'en faire le produit. □

**Exemple.** *On a* $42 = 2 \cdot 3 \cdot 7$ *et* $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

Plus tard, on montrera que cette décomposition est unique à l'ordre des facteurs près. C'est pour cela qu'on adopte la convention que le nombre 1 n'est pas premier : on devrait sinon considérer des décompositions « idiotes » comme $42 = 2 \cdot 13 \cdot 7 \cdot 1 \cdot 1 \cdot 1$.

Pour énumérer les nombres premiers, on a la méthode suivante.

**Algorithme** (crible d'Ératosthène)**.**

*Entrée :* *Un entier $n$.*
*Sortie :* *Les nombres premiers inférieurs à $n$.*

1. *Construire l'ensemble $E = \{2, \dots, n\}$.*
2. *Tant que $E$ est non vide :*
3. *Soit $p$ le plus élément de $E$.*
4. *Enlever de $E$ tous les multiples de $p$.*
5. *Afficher $p$.*

Il est fastidieux d'énumérer tous ces multiples. On peut en réalité s'arrêter bien avant $n$ car, on un entier $d$ ne divise jamais $n$ tout seul : son cofacteur $\frac{n}{d}$ le divise tout autant. Comme le montre la proposition ci-dessous, l'un de ces deux facteurs est nécessairement « petit ».

**Proposition.** *Si un $n \in \mathbb{N}$ n'admet aucun diviseur dans l'ensemble $\left\{2, 3, \dots, \lfloor \sqrt{n} \rfloor\right\}$ alors il est premier.*

*Démonstration.* Montrons la contraposée. Soit donc $n$ un nombre admettant un diviseur non trivial $d$. Si $d \leqslant \sqrt{n}$ alors le résultat est clair. Si $\sqrt{n} < d < n$ alors on a encore

$$\sqrt{n} = \frac{n}{\sqrt{n}} < d < \frac{n}{n} = 1$$

donc $\frac{n}{d}$ est un diviseur de $n$ plus petit que $\sqrt{n}$. □

Cette proposition permet d'effectuer le crible d'Ératosthène de manière plus efficace : lorsque $p > \sqrt{n}$ on peut directement afficher tous les éléments de $E$ comme étant premiers. Mais le crible s'arrête-t-il ?

**Théorème.** *Il existe une infinité de nombres premiers.*

*Démonstration.* Supposons qu'il n'y en ait que $n$ et notons les $p_1, \dots, p_n$ ; alors l'entier $1 + p_1 \cdots p_n$ n'est divisible par aucun de ces nombres. □

L'ensemble des nombres premiers, que l'on note $\mathscr{P}$, est donc infini.

**Exercice.** *Montrer que si $n^k - 1$ est premier avec $k > 1$, alors $n = 2$ et $k$ est premier.*

## 3.7 Factorisation

Toute la puissance des nombres premiers réside en essence dans le fait que, multiplicativement, ils agissent dans des directions parfaitement orthogonales : ils forment une base orthonormée de la structure multiplicative des entiers !

**Lemme.** *Si un premier $p$ divise un produit d'entiers $ab$, alors $p \mid a$ ou $p \mid b$.*

*Démonstration.* Si $p \nmid a$ alors ils n'ont que l'unité comme diviseur commun ; on a donc une relation de Bézout $1 = pu + av$. En la multipliant par $b$ on obtient $b = pbu + abv$ d'où il est clair que $p$ divise $b$. □

**Théorème.** *La décomposition d'un entier non nul comme produit de facteurs premiers est unique à l'ordre de ces facteurs près.*

*Démonstration.* Soient $p_1 \cdots p_n = q_1 \cdots q_m$ deux tels décompositions où l'on suppose que les facteurs premiers sont ordonnés par ordre croissant. Si $p_1 = q_1$ on peut diviser chaque membre par ce même facteur afin de se ramener au cas où $p_1 \neq q_1$. Comme $p_1$ divise le membre de gauche, il divise nécessairement au moins un des facteurs du membre de droite ; c'est cependant impossible car ces facteurs sont tous des nombres premiers distincts de $p_1$. □

**Exercice.** *Factoriser l'entier* 1122. *Que dire de* 1123 *?*

Factoriser un nombre permet de rendre sa structure multiplicative parfaitement transparente. Afin de le montrer, considérons d'abord le cas des puissances de nombres premiers.

**Proposition.** *Si $p$ est premier, l'ensemble des diviseurs de $p^\alpha$ est exactement $\{1, p, p^2, p^3, \ldots, p^{\alpha-1}, p^\alpha\}$.*

*Si $a$ et $b$ sont premiers entre eux, l'ensemble des diviseurs de $ab$ est en bijection avec le produit cartésien de celui des diviseurs de $a$ et de celui des diviseurs de $b$.*

*Démonstration.* Tout diviseur du produit $ab$ se décompose en $d = \mathrm{pgcd}(a, d)\frac{d}{\mathrm{pgcd}(a,d)}$ où le premier facteur divise $a$ et le second divise $b$, par le lemme de Gauss.

En prenant $a = p$ et $b = p^\alpha$ on obtient un preuve par récurrence du premier résultat.

En supposant $\mathrm{pgcd}(a, b) = 1$ on a de surcroit l'unicité de cette décomposition. □

En combinant ces deux résultats, on obtient une caractérisation complète de la divisibilité en termes de la décomposition en facteurs premiers.

**Corollaire.** *Soient $p_1, \ldots, p_n$ des nombres premiers distincts ; pour tout vecteur $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, l'ensemble des diviseurs de l'entier $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ est*

$$\left\{ p_1^{\beta_1} \cdots p_n^{\beta_n} : (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n, \beta_1 \leqslant \alpha_1, \ldots, \beta_n \leqslant \alpha_n \right\}$$

On en déduit notamment les propriétés suivants sur le pgcd et le ppcm.

**Corollaire.** *Avec les mêmes notations, on a :*

$$\mathrm{pgcd}\left(p_1^{\alpha_1} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n}\right) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_n,\beta_n)},$$
$$\mathrm{ppcm}\left(p_1^{\alpha_1} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n}\right) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_n^{\max(\alpha_n,\beta_n)}.$$

**Exemple.** *On retrouve* $\mathrm{pgcd}(42, 60) = \mathrm{pgcd}(2^1 3^1 5^0 7^1, 2^2 3^1 5^1 7^0) = 2^1 3^1 5^0 7^0 = 2 \cdot 3 = 6$.

Adoptons dès à présent une notation pour ces exposants.

**Définition.** *La valuation d'un entier $n$ en un nombre premier $p$ est le plus grand entier $v$ tel que $p^v$ divise $n$. On le note* $\mathrm{val}_p(n)$.

Avec cette notation, on a, quel que soit $n \in \mathbb{N}^*$,

$$n = \prod_{p \in \mathscr{P}} p^{\mathrm{val}_p(n)}.$$

**Exercice.** *On note $\sigma$ la fonction associant à chaque entier la somme de ses diviseurs ; par exemple, $\sigma(4) = 1 + 2 + 4 = 7$. Montrer que si $n$ et $m$ sont premiers entre eux alors $\sigma(mn) = \sigma(m)\sigma(n)$.*

*En déduire que les entiers pairs $n$ vérifiant $\sigma(n) = 2n$ sont exactement ceux de la forme $2^{k-1}(2^k - 1)$ où $2^k - 1$ est premier. Montrer ensuite que, dans ce cas, $k$ est premier.*

**Exercice.** *Supposons que la série* $\sum_{p\in\mathscr{P}} \frac{1}{p}$ *converge. Montrer que c'est alors le cas de* $\prod_{p\in\mathscr{P}} \left(1+\frac{1}{p}\right)$ *puis encore de* $\prod_{p\in\mathscr{P}} \frac{1}{1-\frac{1}{p}}$. *Développer ce produit et aboutir à une contradiction.*

**Exercice.** *On note* $p_i$ *le* $i^e$ *nombre premier. Tracer le nuage de point* $(i, p_{i+1}-p_i) \in \mathbb{R}^2$ *pour* $i \in \{1, 100\}$.

**Exercice.** *Soit* $p$ *un nombre premier et* $m > n$ *deux entiers. Montrer que* $\text{pgcd}(p^m-1, p^n-1) = p^{\text{pgcd}(m,n)} - 1$. *On pourra commencer par calculer une division euclidienne.*

## 3.8 Congruence

**Définition.** *On dit que* $a$ *est congru à* $b$ *modulo* $c$ *(tous trois entiers, avec* $c \neq 0$*) lorsque* $a-b$ *est divisible par* $c$ *; on note cela* $a \equiv b \mod c$.

**Exercice.** *Caractériser les entiers* $x$ *vérifiant* $2x+3 \equiv 1 \mod 7$.

La notion de congruence est certainement bien plus explicite sous la forme que donne lui résultat suivant.

**Lemme.** *Le reste de la division euclidienne de* $a$ *par* $b$ *est le plus petit entier positif congru à* $a$ *modulo* $b$. *Deux entiers sont congrus modulo* $b$ *si et seulement si leurs divisions euclidiennes par* $b$ *donnent le même reste.*

**Exemple.** 42 *et* 127 *sont congrus modulo* 17 *car* $42-127 = -85 = -5\cdot 17$. *On a par ailleurs* $42 = 2\cdot 17+8$ *et* $127 = 7\cdot 17+8$.

Soit $n$ un entier non-nul fixé. La relation de congruence modulo $n$ possède de nombreux points communs avec celle d'égalité, notamment les assertions suivantes :

— $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall c \in \mathbb{Z}, a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$ *(transitivité)*
— $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, a \equiv b \Rightarrow b \equiv a$ *(symétrie)*
— $\forall a \in \mathbb{Z}, a \equiv a$ *(réflexivité)*

On dit ainsi que la congruence est relation d'équivalence. Elle est de surcroit compatible avec les opérations d'addition et de multiplication :

— $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall c \in \mathbb{Z}, \forall d \in \mathbb{Z}, a \equiv b \wedge c \equiv d \Rightarrow a+c \equiv b+d$ *(addition)*
— $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall c \in \mathbb{Z}, \forall d \in \mathbb{Z}, a \equiv b \wedge c \equiv d \Rightarrow a\cdot c \equiv b\cdot d$ *(multiplication)*

On peut donc calculer *modulo* $n$, c'est-à-dire sans se préoccuper de savoir de quels entiers les restes qu'on manipule proviennent exactement.

**Exercice.** *Que vaut* $42^{777} \mod 6$ *? Et* $43^{888} \mod 6$ *? Et* $41^{999} \mod 6$ *?*

**Remarque.** *La relation de congruence est une approximation de la relation d'égalité. Par abus de notation, il est parfaitement légitime de substituer le symbole d'égalité « = » au symbole de congruence « ≡ ». Par la suite, nous noterons tout simplement* $a = b \mod c$.

Modulo $n$, nous pouvons donc ajouter et multiplier des entiers comme nous le faisions dans $\mathbb{Z}$. Mais, parfois, on peut aussi diviser !

**Proposition.** *Soient* $a$ *et* $b$ *deux entiers strictement positifs. L'équation* $xa = 1 \mod b$ *admet une solution* $x \in \mathbb{Z}$ *si et seulement si* $\text{pgcd}(a, b) = 1$. *Cette solution est alors le coefficient d'une relation de Bézout* $xa + by = 1$.

*Démonstration.* En exercice. □

**Exercice.** *Trouver tous les entiers* $x$ *vérifiant* $53x - 37 = 42 \mod 15$.
*En existe-t-il vérifiant* $54x - 37 = 42 \mod 15$ *?*
*Et* $54x - 37 = 41 \mod 15$ *?*

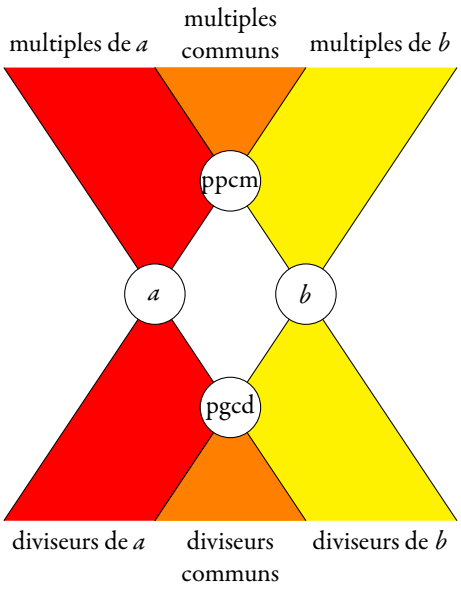



FIGURE 3.1 – Le pgcd et le ppcm parmi les diviseurs et les multiples.

# Chapitre 4

# Décompositions et applications

## 4.1 Systèmes d'écriture

Avant d'exploiter plus avant les propriétés arithmétiques des entiers et tout particulièrement la notion de congruence, nous allons brièvement discuter des systèmes d'écriture possibles pour ces nombres.

Nous écrivons couramment les entiers *en base dix*, c'est-à-dire que nous les décomposons en une suite de chiffres dont chacun peut prendre dix valeurs, à savoir $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ; autant que les doigts de la main. Peut-être savez-vous aussi que pour les ordinateurs il est plus commode de manipuler des entiers écrits *en base deux* c'est à dire formés uniquement de zéros et de uns. Généralisons maintenant ce concept.

**Définition.** *Soit $b \geqslant 2$ un entier. Tout entier $n \in \mathbb{N}$ s'écrit de manière unique en base $b$, c'est-à-dire sous la forme*

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots c_1 b + c_0$$

*pour $k \in \mathbb{N}$ et $(c_k, c_{k-1}, \ldots, c_1, c_0) \in \{0, 1, \ldots, b-1\}^k$ avec $c_k \neq 0$. Les coefficients $c_i$ sont appelés les chiffres de l'écriture de $n$ en base $b$ et on note*

$$n = \overline{c_k c_{k-1} \cdots c_1 c_0}^{(b)}$$

*Démonstration.* Soit $n = b q_0 + c_0$ la division euclidienne de $n$ par $b$. Soit alors $q_0 = b q_1 + c_1$ celle de $q_0$ par $b$, puis encore $q_1 = b q_2 + c_2$ celle de $q_1$ par $b$, etc. La suite $q_i$ est strictement décroissante jusqu'à son annulation ; on note $k$ le plus petit indice pour lequel $q_{k+1} = 0$ et on peut alors vérifier les conditions de la définition.

L'unicité pourra être démontrée en exercice. □

Évidemment, la longueur $k + 1$ de l'écriture en base $b$ est prévisible.

**Proposition.** *L'écriture d'un entier $n$ en base $b$ admet $k + 1$ chiffres pour $k = \left\lfloor \frac{\log(n)}{\log(b)} \right\rfloor$.*

**Exercice.** *Écrire en base* 10 *l'entier* $\overline{101010}^{(2)}$. *Écrire l'entier* 421 *en base* 2 *puis* 3 *puis* 5.

**Exercice.** *Combien de chiffres l'écriture décimale d'un entier de* 1024 *bits comporte-t-elle ?*

Les opérations d'addition et de multiplication peuvent s'effectuer directement sur l'écriture en base $b$ comme on le fait depuis l'école primaire en base dix : en propageant les retenues. Énoncer cela formellement serait assez lourd ; faisons plutôt des exemples.

**Exercice.** *Calculer la somme puis le produit de* $\overline{101010}^{(2)}$ *et* $\overline{10010}^{(2)}$.
*Faire de même pour* $\overline{421}^{(6)}$ *et* $\overline{505}^{(6)}$.

**Proposition.** *L'entier* $\overline{c_k \dots c_0}^{(10)}$ *est :*
— *divisible par* 2 *si et seulement si* $c_0$ *l'est ;*
— *divisible par* 5 *si et seulement si* $c_0$ *l'est ;*
— *divisible par* 3 *si et seulement si* $\sum_{i=0}^{k} c_i$ *l'est ;*
— *divisible par* 11 *si et seulement si* $\sum_{i=0}^{k}(-1)^i c_i$ *l'est ;*
— *divisible par* 7 *si et seulement si*

$$\sum_{i=0}^{\lfloor \frac{k}{3} \rfloor}(-1)^i \overline{c_{3i+2}c_{3i+1}c_{3i}}^{(10)}$$

*l'est.*

*Démonstration.* Les deux premières assertions sont évidentes en écrivant

$$n = \sum_{i=0}^{k} c_i 10^i = c_0 + 2 \cdot 5 \cdot \sum_{i=1}^{k} c_i 10^{i-1}.$$

Pour la troisième, on regarde le résidu modulo 3 : comme $10 = 1 \bmod 3$, on a

$$n = \sum_{i=0}^{k} c_i 10^i = \sum_{i=0}^{k} c_i \bmod 3.$$

□

**Exercice.** *Factoriser l'entier* 1566180.

L'écriture en base deux est mathématiquement la plus simple. Elle apparait naturellement dans de nombreux domaines des mathématiques et de l'informatique. Voyons maintenant l'une des applications où elle joue un rôle important.

**Algorithme** (exponentiation lente).
*Entrée :* *Deux entiers positifs* $x$ *et* $n$.
*Sortie :* *L'entier* $x^n$.

1. *Poser* $y = 1$.
2. *Pour* $i \in \{1, \dots, n\}$ *:*
3. *Assigner* $y \leftarrow xy$.
4. *Renvoyer* $y$.

Cet algorithme calcule $x^n$ en exactement $n$ multiplications. Certaines sont redondantes : par exemple, pour calculer $x^4$, il est plus rapide de calculer $x^2$ puis de le multiplier par lui même. C'est l'idée de base de l'algorithme ci-dessous.

**Algorithme** (exponentiation rapide).
*Entrée :* *Deux entiers positifs* $x$ *et* $n$.
*Sortie :* *L'entier* $x^n$.

1. *Poser* $y = 1$.
2. *Tant que* $n \neq 0$ *:*
3. *Si* $n \bmod 2 = 1$, *assigner* $y \leftarrow xy$.
4. *Assigner* $n = \lfloor n/2 \rfloor$.
5. *Assigner* $x \leftarrow xx$.
6. *Renvoyer* $y$.

Dans le cas où seul le résultat modulo un certain entier $m$ nous intéresse, il sera bien évidemment opportun de réduire les valeurs de $x$ et $y$ modulo $m$ à chaque itération afin qu'elle restent les plus petites possibles, ce qui facilitera les multiplications.

## 4.2 Factorisation ludique

Le problème de la factorisation est récurrent lorsque l'on calcule toute sorte d'objets mathématiques. Plus tard, nous verrons notamment qu'il est au cœur du cryptosystème RSA. Nous présenterons alors des méthodes efficaces pour factoriser un entier donné. Ici nous nous contenterons de remarques ludiques.

Supposons qu'un entier $n$ soit presque premier dans le sens où $n = pq$ avec $p$ et $q$ premiers ; c'est en quelque sorte le type d'entiers le plus difficile à factoriser. La probabilité de trouver un facteur non trivial de $n$ en tirant des entiers de $\{0, \dots, n-1\}$ au hasard est évidemment $\frac{2}{n}$. En revanche, nous allons voir que la probabilité qu'un sous-ensemble de $\{0, \dots, n-1\}$ contienne deux entiers dont la différence donne un facteur non trivial de $n$ est infiniment plus élevée !

**Proposition.** *Le nombre de fonctions injectives de* $\{1, \dots, x\}$ *dans* $\{1, \dots, y\}$ *est* $\prod_{i=0}^{x-1}(y-i)$*, pour un total de* $y^x$ *fonctions.*

**Corollaire.** *Si, dans un ensemble de cardinal* $y$*, on choisit* $\sqrt{y}$ *éléments au hasard avec répétition, la probabilité qu'un même élément ait été choisi deux fois converge vers* $e^{-1/2} \approx 0,6$ *lorsque* $y$ *tend vers l'infini.*

*Démonstration.* Poser $x = \sqrt{y}$ dans la proposition et utiliser la formule de Stirling. □

**Exemple** (paradoxe des anniversaires)**.** *Les années comptent* 365 *jours. Dans une classe de* 20 *élèves, il y a environ* 40% *de chance que deux aient le même anniversaire.*

Pour trouver des facteurs non triviaux d'un entier $n$, on peut exploiter ce « paradoxe » en cherchant des entiers dont la différence donne un facteur non trivial de $n$. Par analogie avec l'exemple ci-dessus, les élèves sont des entiers modulo $n$ et leurs anniversaires leurs résidus modulo les facteurs de $n$. Lorsque $n$ n'est pas premier, son plus petit facteur est inférieur à $y = \sqrt{n}$. En considérant $x = \sqrt{y} = n^{1/4}$ entiers, la probabilité que la différence de deux d'entre eux donne un facteur non trivial de $n$ est donc de 40%.

Pour que cet approche soit efficace, toute la difficulté est d'identifier des couples $(\alpha, \beta)$ d'entiers dont la différence donne un facteur non trivial de $n$ sans avoir à les énumérer et calculer $\operatorname{pgcd}(\alpha - \beta, n)$ pour chacun. La méthode de Pollard [9] construit pour cela ces entiers comme valeurs d'une fonction pseudo-aléatoire $f : \{1, \dots, n\} \to \{1, \dots, n\}$ qui préserve les résidus ; pour chercher ces couples efficacement, elle exploite l'observation :

$$\text{Si } f^a(1) = f^b(1) \text{ et } a \geqslant 2b, \text{ alors } f^{2(a-b)}(1) = f^{(a-b)}(1).$$

On peut donc se contenter de tester les couples $(\alpha = f^k(1), \beta = f^{2k}(1))$, ce qui donne l'algorithme ci-dessous.

**Algorithme** (Pollard [9])**.**

*Entrée :* *Un entier $n$.*
*Sortie :* *Un facteur de $n$.*

1. *Poser $\alpha = \beta = 1$ et $f : x \mapsto x^2 + c \bmod n$ avec $c$ aléatoire.*
2. *Répéter $99n^{1/4}$ fois :*
3. *Calculer $\alpha \leftarrow f(\alpha)$ et $\beta \leftarrow f(f(\beta))$.*
4. *Si $\operatorname{pgcd}(\alpha - \beta, n) \notin \{1, n\}$ : renvoyer $\operatorname{pgcd}(\alpha - \beta, n)$.*
5. *Retourner en 1.*

Le cours de *Calcul Formel* (S6) en discutera en davantage de détails.

## 4.3 Problème du sac à dos

Finissons ce chapitre en discutant d'un problème classique qui exploite la structure additive des entiers. Il a été le support de nombreux cryptosystèmes pionniers.

**Définition.** *Le problème du sac à dos consiste, étant donnés un entier $x$ et une suite finie $S \in \mathbb{Z}^n$, d'identifier une sous-suite de $S$ de somme $x$.*

**Exemple.** *Si $S = (2, 3, 5, 7, 11, 13, 17, 19)$ et $x = 25$ alors la sous-suite $(3, 5, 17)$ est une solution du problème. En revanche, le problème équivalent pour $x = 4$ n'admet pas de solution.*

En toute généralité, ce problème est NP-complet, c'est-à-dire qu'il n'est pas plus facile à résoudre que n'importe quel problème pour lequel on sait rapidement vérifier les solutions (ici, il suffit de calculer la somme). Le résoudre devrait donc être infaisable pour des suites $S$ bien choisies de longueur $n = 1024$ ou plus. On peut cependant en construire des instances faciles.

**Définition.** *On dit qu'une suite d'entiers est supercroissante si chaque terme est strictement supérieur à la somme de tous ceux qui le précèdent.*

**Algorithme.**

*Entrée :* *Un entier $x$ et une suite supercroissante $(s_i)_{i\in\{1,\dots,n\}} \in \mathbb{Z}^n$.*
*Sortie :* *Sa sous-suite de somme $x$, si elle existe.*

1. *Tant que $n > 0$ :*
2. *Si $x > s_n$ :*
3. *Ajouter $s_n$ à la sous-suite $T$.*
4. *Assigner $x \leftarrow x - s_n$.*
5. *Assigner $n \leftarrow n - 1$.*
6. *Si $x = 0$, renvoyer $T$.*

C'est ainsi que l'un des premiers cryptosystèmes à clef publique inventé fonctionnait ; il a très mal vieilli (on sait depuis l'attaquer efficacement [13]) mais reste un excellent objet d'étude. L'idée y est de dissimuler une instance facile du problème du sac à dos par des multiplications modulaires.

**Définition.** *La méthode de chiffrement à clef publique de Merkle–Hellman [6] fonctionne comme il suit :*

1. *La clef secrète consiste en une suite supercroissante $(s_i)_{i\in\{1,\dots,n\}}$ ainsi qu'un entier $u$ premier à $v = \sum_i s_i$. La clef publique correspondante est la suite $(t_i = u s_i \bmod v)_{i\in\{1,\dots,n\}}$.*
2. *On chiffre un message $m \in \{0,1\}^n$ en $c = \sum_i m_i t_i$.*
3. *On déchiffre $c$ en identifiant la sous-suite de $(s_i)$ de somme $u^{-1}c \bmod v$.*

# Chapitre 5

# Arithmétique modulaire

L'objectif de ce chapitre est de pouvoir calculer avec des entiers en ne se préoccupant que de leurs restes modulo un nombre fixé $n$.

## 5.1 Anneaux résiduels

Identifions d'abord tous les entiers desquels un reste donné modulo $n$ peut provenir.

**Définition.** *Soit $n$ un entier. On appelle classe de congruence modulo $n$ tout sous-ensemble maximal $S$ de $\mathbb{Z}$ dont les éléments sont deux-à-deux congrus modulo $n$.*

**Exemple.** *Décrire l'unique classe de congruence contenant 2 modulo 6.*

**Remarque.** *Soit $x$ un élément d'une classe de congruence $S$ modulo $n$. Elle contient nécessairement aussi $x + kn$ pour tout $k \in \mathbb{Z}$. Or ce sont là les seuls entiers congrus à $x$ modulo $n$. On a donc exactement $S = \{x + kn : k \in \mathbb{Z}\} = x + n\mathbb{Z}$.*

Lorsque le module $n$ est implicite, on notera $\overline{x}$ la classe de l'entier $x$ ; on dira aussi que $x$ est un représentant de cette classe.

Nous avons vu que la relation de congruence était compatible avec les opérations d'addition et de multiplication. On peut donc effectuer des opérations sur les classes : si $S$ et $T$ sont des classes modulo $n$, il en va de même pour leurs sommes et produits ensemblistes :

$$S + T = \{s + t : s \in S, t \in T\}, \qquad S \cdot T = \{s \cdot t : s \in S, t \in T\}.$$

Il est donc légitime de munir l'ensemble des classes de ces opérations.

**Définition.** *On appelle anneau résiduel des entiers modulo $n$, noté $\mathbb{Z}/n\mathbb{Z}$, l'ensemble des classes de congruence modulo $n$ muni des opérations qu'y induisent l'addition et la multiplication usuelle.*

Ne soyons pas effrayé par le fait que $\mathbb{Z}/n\mathbb{Z}$ est un ensemble d'ensemble : en pratique, pour calculer avec des classes, il suffira d'en prendre des représentants et de leur appliquer les opérations voulues.

**Exemple.** *Dans le cas $n = 6$, on a $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, notamment $\overline{2} \cdot \overline{5} = \overline{2 \cdot 5} = \overline{10} = \overline{4}$.*

*On peut d'ailleurs écrire ses tables complètes :*

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| × | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

*La table d'addition semble parfaitement raisonnable, mais la table de multiplication présente quant à elle plusieurs curiosités ; nous y reviendrons.*

Calculer dans $\mathbb{Z}/n\mathbb{Z}$ revient ainsi à calculer « normalement » tout en réduisant modulo $n$ lorsque c'est opportun. Cela muni $\mathbb{Z}/n\mathbb{Z}$ d'une structure qui vérifie elle aussi les propriétés élémentaires de la section 3.1, exceptés évidemment celle portant sur l'ordre. Cet anneau mérite donc une étude propre.

## 5.2 Restes chinois

**Théorème** (restes chinois)**.** *Deux entiers $n$ et $m$ sont premiers entre eux si et seulement si l'application*

$$\begin{cases} \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \qquad x \longmapsto (x \bmod n, x \bmod m) \end{cases}$$

*est une bijection.*

*Démonstration.* Si $nu + mv = 1$ est une relation de Bézout, alors $(a, b) \mapsto amv + bnu$ est l'application inverse. Si $d > 1$ est un diviseur commun, les résidus modulo $n$ et $m$ étant identiques modulo $d$, le couple $(0, 1)$ n'a pas d'antécédent. □

**Remarque.** *Cette bijection respecte par ailleurs les opérations d'addition et de multiplication des deux anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ; c'est ce que l'on appelle un isomorphisme d'anneau. Son existence signifie que les structures de ces deux anneaux sont identiques.*

En tout premier lieu, cela signifie que l'on peut résoudre des systèmes de congruences lorsque les modules sont premiers entre eux.

**Exercice.** *Trouver un $x \in \mathbb{Z}$ vérifiant* $\begin{cases} x = 3 \bmod 5 \\ x = 7 \bmod 11 \end{cases}$ *. Pareil pour* $\begin{cases} x = 2 \bmod 3 \\ x = 5 \bmod 7 \\ x = 11 \bmod 13 \end{cases}$ .

On peut, en toute généralité, étendre le théorème des restes chinois à $k$ facteurs.

**Théorème** (restes chinois)**.** *Soit $m = n_1 \cdots n_k$ un produit de $k$ facteurs premiers deux à deux. L'application*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ \qquad x \longmapsto (x \bmod n_1, \ldots, x \bmod n_k) \end{cases}$$

*admet pour inverse $(x_1, \ldots, x_k) \mapsto u_1 \frac{m}{n_1} x_1 + \cdots + u_k \frac{m}{n_k}$ où les coefficients $u_i$ satisfont la relation de Bézout généralisée $1 = u_1 \frac{m}{n_1} + \cdots + u_k \frac{m}{n_k}$.*

## 5.3 Éléments inversibles

**Définition.** *Posons $R = \mathbb{Z}/n\mathbb{Z}$. On dit que $x \in R$ est inversible s'il existe $y \in R$ tel que $xy = 1$. On appelle groupe multiplicatif de $R$ l'ensemble de ses éléments inversibles ; on le note $R^\times$.*

Remarquons que $R^\times$ est stable par multiplication ; en effet, on a $(xy)^{-1} = y^{-1}x^{-1}$.

**Exemple.** *On a $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$.*

Évidemment, 0 n'est jamais inversible quel que soit le module $n$, alors que 1 et $-1$ le sont toujours. On a donc

$$\{\pm 1\} \subset (\mathbb{Z}/n\mathbb{Z})^\times \subset \mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}.$$

**Attention !** L'habitude de « simplifier » l'équation $ab = ac$ en multipliant ses membres par $a^{-1}$ est certainement ancrée au plus profond de vous. Mais lorsque $a$ n'a pas d'inverse, résistez-y ! Si $2x = 4 \bmod 6$ il est faux de déduire $x = 2 \bmod 6$ ; on a seulement $x = 2 \bmod 3$.

**Proposition.** *La classe modulo $n$ d'un entier $a$ est inversible, soit $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, si et seulement si* $\operatorname{pgcd}(a, n) = 1$.

*Démonstration.* C'est évidente en traduisant le pgcd par une relation de Bézout. □

**Exercice.** *Énumérer les éléments inversibles modulo* 20. *Pareil modulo $p^2$ si $p$ est premier.*

## 5.4 Indicatrice d'Euler

Afin de comprendre la structure du groupe multiplicatif, il est en premier lieu nécessaire de comprendre son cardinal ou, comme on l'appelle dans le cas des groupes, son ordre.

**Définition.** *La fonction indicatrice d'Euler, notée $\varphi$, associe à tout entier $n$ l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ de son anneau résiduel.*

**Exemple.** *On a $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, etc.*

**Proposition.** *Si $p$ est un nombre premier, pour tout $\alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.*
*Si $n$ et $m$ sont premiers entre eux, on a $\varphi(nm) = \varphi(n)\varphi(m)$.*

**Exemple.** *On a $\varphi(637) = \varphi(7^2 \cdot 13) = \varphi(7^2) \cdot \varphi(13) = (7-1)7 \cdot 12 = 504$.*

*Démonstration.* Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont les classes des entiers de $\{1, \dots, n\}$ premiers à $n$. Caractériser alors explicitement, dans les deux cas ci-dessus, les entiers inférieurs mais non premiers au module considéré. □

On peut ainsi efficacement calculer l'indicatrice d'Euler de tout entier dont on connaît la factorisation. C'est notamment le cas des petits entiers qu'illustre la figure 5.1.

**Exercice.** *La figure 5.1 semble indiquer que $\varphi(n)$ est majorée par $n$ et minorée par une fonction sous linéaire ; montrer que c'est effectivement le cas en étudiant les valeurs extrémales de $\frac{\varphi(n)}{n}$.*

Pour information, on a plus précisément le résultat (admis) suivant :

**Théorème** (Mertens). *La fonction indicatrice d'Euler vérifie*

$$\liminf_{n\to\infty} \frac{\log(\log(n))}{n} \varphi(n) = e^{-\gamma}.$$

**Corollaire.** *Un entier $p$ est premier si et seulement si tout les éléments de l'anneau résiduel associé $\mathbb{Z}/p\mathbb{Z}$ sont inversibles à l'exception de* 0.

C'est la situation que nous connaissions dans $\mathbb{Q}$ ou dans $\mathbb{R}$. Ce type d'anneau s'appelle un corps. Lorsque l'inversibilité des éléments non nuls joue un rôle, on pourra donc appeler $\mathbb{Z}/p\mathbb{Z}$ le corps premier d'ordre $p$ et le noter $\mathbb{F}_p$.

**Exercice.** *Soit $p$ un nombre premier et $k$ un entier. Que vaut la somme $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} x^k$ ?*

## 5.5 Groupe multiplicatif

**Théorème.** *Pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ on a $x^{\varphi(n)} = 1$.*

*Démonstration.* Le groupe étant fini, on a des exposants $k \neq \ell$ vérifiant $x^k = x^\ell$ ; comme $x$ est inversible cela implique $x^{k-\ell} = 1$. Or $\varphi(n)$ est un multiple de $k-\ell$ car on peut partitionner le groupe en sous-ensembles à $k-\ell$ éléments :
- Chaque partie $S_y = \{yx^1, yx^2, \dots, yx^{k-\ell}\}$ est de cardinal $k-\ell$ ;
- Si $S_y \neq S_z$ alors $S_y \cap S_z = \emptyset$.

□

**Exemple.** *Pour $2 \in (\mathbb{Z}/15\mathbb{Z})^\times$ on a bien $2^{\varphi(15)} = 2^8 = 256 = 1$.*
*Attention, cependant, de ne pas appliquer ce théorème avec de mauvais exposants...*

$$2^{15} = 32768 = 3 \neq 1, \qquad 2^{15-1} = 16384 = 4 \neq 1.$$

**Corollaire** (petit théorème de Fermat)**.** *Si $p$ est premier alors :*
- *Pour tout $x$ non divisible par $p$, on a $x^{p-1} = 1 \bmod p$.*
- *Pour tout $x$, on a $x^p = x \bmod p$.*

L'application la plus directe du petit théorème de Fermat au calcul modulaire est qu'il « autorise » de réduire modulo $(p-1)$ les exposants d'une équation modulo $p$ : si $k = (p-1)q + r$ est la division euclidienne de $k$ par $p-1$, on a, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$),

$$x^k = x^{(p-1)q+r} = x^{(p-1)q} x^r = \left(x^{p-1}\right)^q x^r = x^r.$$

On peut aussi l'utiliser pour résoudre directement des équations du type $x^k = y$ dans $\mathbb{Z}/p\mathbb{Z}$ lorsque $k$ est premier avec $(p-1)$ : soit une relation de Bézout du type $ku + (p-1)v = 1$ ; en mettant l'équation à la puissance $u$ on obtient $y^u = x^{ku} = x^{1-(p-1)v} = x$. Dans le cadre plus général de $\mathbb{Z}/n\mathbb{Z}$ cela donne le résultat ci-dessous.

**Proposition.** *L'application $x \in \mathbb{Z}/n\mathbb{Z} \mapsto x^k \in \mathbb{Z}/n\mathbb{Z}$ est bijective si et seulement si $k$ est premier avec $\varphi(n)$.*

Le cas où $\operatorname{pgcd}(k, \varphi(n)) > 1$, par exemple lorsque $k = 2$, est nettement plus complexe et le traiter dans toute sa généralité nous amènerait à dépasser le modeste cadre de ce cours. Considérons toutefois deux exemples typiques :
- Dans $\mathbb{Z}/7\mathbb{Z}$, l'équation $x^2 = 2$ a pour solutions $x = 3$ et $x = 4$.
- Dans $\mathbb{Z}/7\mathbb{Z}$, l'équation $x^2 = 3$ n'admet aucune solution.

Le nombre de racines $k^{\text{e}}$ fluctue donc visiblement ; il reste toutefois borné comme le montre le résultat très classique suivant.

**Théorème.** *Tout polynôme $P(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ admet au plus* $\deg(P)$ *racines.*

*Démonstration.* Si $\alpha$ est une racine de $P$ alors la division euclidienne $P(X) = (X-\alpha)Q(X)$ montre que les racines de $P$ sont celles de $Q$ et $\alpha$ ; le résultat s'obtient par récurrence sur le degré de $P$. □

Attention toutefois à ce que ce résultat repose de manière fondamentale sur le fait que $p$ est premier. En témoigne l'équation $x^2 = 1 \bmod 15$ et ses quatre solutions 1, 4, 11 et 14.

**Exercice** (théorème de Wilson). *Montrer que l'égalité* $(p-1)! = p-1 \bmod p$ *est vérifiée si et seulement si* $p$ *est premier. Est-ce un moyen efficace de déterminer si un nombre est premier ?*

## 5.6 Primalité effective

Afin de déterminer si un nombre $n$ est premier, on peut évidemment lui appliquer la définition à la lettre, c'est-à-dire vérifier explicitement qu'aucun entier compris entre 2 et $n-1$ ne le divise. On peut en réalité s'arrêter à $\sqrt{n}$ :

**Lemme.** *Un entier n est premier si et seulement s'il n'a aucun diviseur compris entre* 2 *et* $\sqrt{n}$.

*Démonstration.* Si $n$ admet un diviseur $d$ supérieur à $\sqrt{n}$, alors l'entier $\frac{n}{d}$ est un autre diviseur qui, lui, est inférieur à $\sqrt{n}$. □

Pour établir la liste complète des nombres premiers plus petit qu'un entier donné $n$, on peut mutualiser ces « tests ». C'est-à-dire que, pour chaque diviseur potentiel $d$, on élimine les nombres qui en sont des multiples. Cela donne l'algorithme ci-dessous.

**Algorithme** (crible d'Ératosthène).

*Entrée :* *Un entier $n$.*
*Sortie :* *L'ensemble $\mathscr{P} \cap \{2, \dots, n\}$.*

1. *Former les ensembles $L = \{2, \dots, n\}$ et $P = \emptyset$.*
2. *Tant que $L \neq \emptyset$ :*
3. *Soit $p$ le plus petit élément de $L$.*
4. *Enlever de $L$ tous les multiples de $p$.*
5. *Rajouter $p$ à $P$.*
6. *Renvoyer $P$.*

Cette méthode donne efficacement l'ensemble $\mathscr{P} \cap \{2, \dots, n\}$ mais, pour tester la seule primalité d'un entier donné $n$, on sait faire bien mieux. Le petit théorème de Fermat, par exemple, donne un critère vérifiable efficacement que satisfont les nombres premiers. Malheureusement sa réciproque est fausse : il existe de (rares) entiers composés $n$ (dits de Carmichael) tels que pour tout $x$ on ait $x^n = x \bmod n$, par exemple $n = 561$. Un léger raffinement suffit toutefois à les éliminer.

**Théorème** (Miller [7]). *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si tous ses éléments non nuls sont des racines de l'unité.*

Lorsque $n$ est composé, la densité des non racines de l'unité n'est cependant pas suffisamment élevée pour permettre de vérifier ce critère rapidement. Une légère généralisation des conditions donne le critère suivant :

**Théorème** (Rabin [10]). *Pour $n > 4$, l'ensemble des éléments non nuls $x \in \mathbb{Z}/n\mathbb{Z}$ vérifiant $x^{n-1} \neq 1$ ou $\operatorname{pgcd}(x^{(n-1)/2^j} - 1, n) \neq 1$, $n$ pour un certain $j \in \mathbb{N}$ est vide lorsque $n$ est premier et de cardinal au moins $\frac{3}{4}(n-1)$ lorsque $n$ est composé.*

Cela donne le test de primalité suivant.

**Algorithme** (Miller–Rabin).
*Entrée :* *Un entier $n$.*
*Sortie :* *S'il est premier.*

1. *Si $n < 5$ : renvoyer* `vrai` *si $n = 2$ ou $n = 3$ et* `faux` *sinon.*
2. *Calculer la décomposition $n = 2^s t$ avec $s \in \mathbb{N}$ et $t \in \mathbb{Z}$ impair.*
3. *Effectuer $k$ fois :*
4. *Tirer un élément aléatoire $z \in \{2, \dots, n-1\}$.*
5. *Pour tout $x \in \{z^{2^0 t} \bmod n, z^{2^1 t} \bmod n, \dots, z^{2^{s-1} t} \bmod n\}$ :*
6. *Si $\operatorname{pgcd}(x-1, n) \neq 1, n$ : renvoyer* `faux`.
7. *Si $x^{2^s t} \neq 1$ : renvoyer* `faux`.
8. *Renvoyer* `vrai`.

**Corollaire.** *Si $n$ est premier, ce programme renvoie systématiquement* `vrai`. *Si $n$ est composé, ce programme renvoie* `faux` *avec probabilité $1 - 4^{-k}$.*

On peut donc ajuster la valeur de $k$ selon la certitude désirée. Notons qu'il existe aussi des tests déterministes [1], c'est-à-dire dont le résultat est inconditionnel, mais que ceux-ci sont bien plus couteux.

**Exercice.** *L'un des deux entiers* 51991 *et* 51997 *n'est pas premier ; lequel ?*

## 5.7 Cryptosystème RSA

Rappelons la méthode de chiffrement à clef publique RSA que nous avions brièvement décrite à la section 2.1.

**Définition.** *La méthode de chiffrement à clef publique RSA [12] fonctionne* ***essentiellement*** *comme il suit :*

1. *Pour construire un couple de clefs, choisir deux nombres premiers $p$ et $q$ aléatoirement. Calculer alors deux entiers $a$ et $b$ vérifiant $ab = 1 \bmod (p-1)(q-1)$. Calculer $n = pq$. Renvoyer comme clef publique $e = (n, a)$ et comme clef privée $d = (n, b)$.*
2. *On chiffre des messages $m \in \{1, \dots, n\}$ par $E : (e, m) \mapsto m^a \bmod n$.*
3. *On déchiffre grâce à $D : (d, m) \mapsto m^b \bmod n$.*

Nous avions alors posé deux questions :
— L'égalité $D(d, E(e, m)) = m$ est-elle toujours satisfaite ?
— Calculer $d$ à partir de la clef publique est-il difficile ?
C'est-à-dire, intuitivement, cette méthode est-elle correcte et est-elle sûre ? Sa correction peut être rigoureusement prouvée :

*Démonstration.* L'égalité $D(d, E(e, m)) = m$ se ré-écrit $(m^a)^b = m \bmod n$ ; comme $ab = 1 \bmod \varphi(n)$, elle est vérifiée lorsque $m$ est inversible modulo $n$. Si $m$ n'est pas premier à $n$, alors il est divisible par $p$ ou par $q$, ce qui se produit pour seulement $p + q - 1$ valeurs de $m \in \{1, \dots, n = pq\}$ ; dans ce cas, on pourra toutefois montrer en appliquant le théorème Chinois que l'égalité est encore vérifiée. □

La sûreté d'une méthode de chiffrement à clef publique peut s'exprimer en ces termes : est-il possible, étant donné la clef publique, de retrouver la clef privée ? Dans le cas de RSA, pour calculer $d$ étant donné la clef publique, la méthode la plus directe, qui est aussi la plus efficace connue, consiste à factoriser $n$ ; cela donne $\varphi(n)$ et on peut alors calculer $d$ comme inverse de $e$ modulo $\varphi(n)$.

**Exercice.** *Calculer la clef privée associée à la clef publique* ($n = 26, a = 5$).

En pratique, on sait factoriser des entiers de 100 bits instantanément, de 300 bits en quelques heures, de 500 bits en quelques mois et de 700 bits en quelques années. Les applications sérieuses utilisent donc des modules $n$ de 2048 bits voire plus.

Pour implanter les fonctionnalités ci-dessus en Sage, on pourrait écrire :

```
sage: def premierhasard(n):
....:     r=randint(n/2,n)
....:     while not is_prime(r):
....:         r=r+1
....:     return r
....:
sage: def creation():
....:     p=premierhasard(2**512)
....:     q=premierhasard(2**512)
....:     N=p*q
....:     h=(p-1)*(q-1)
....:     a=65537
....:     while gcd(a,h)>1:
....:         a=a+1
....:     b=inverse_mod(a,h)
....:     p=(N,a)
....:     s=(N,b)
....:     return(p,s)
....:
sage: def message2entier(m):
....:     return sum([ord(m[i])*256**i for i in range(0,len(m))])
....:
sage: def entier2message(e):
....:     m=""
....:     while e%256>0:
....:         m=m+chr(e%256)
....:         e=e//256
....:     return m
....:
sage: def chiffrer(m,p):
....:     (N,a)=p
....:     e=message2entier(m)
....:     return power_mod(e,a,N)
....:
sage: def dechiffrer(c,s):
....:     (N,b)=s
....:     e=power_mod(c,b,N)
....:     return entier2message(e)
....:
sage: (p,s)=creation()
sage: c=chiffrer("un message tres secret",p)
sage: dechiffrer(c,s)
'un message tres secret'
```

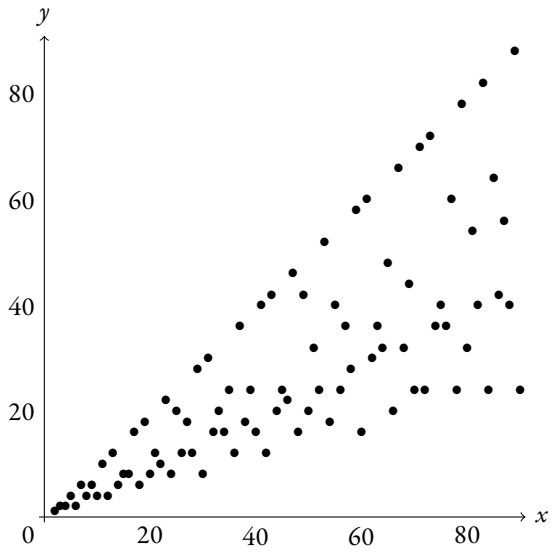



FIGURE 5.1 – Petites valeurs de la fonction indicatrice d'Euler.

# Chapitre 6

# Groupes en cryptographie

La méthode de chiffrement à clef publique RSA est une construction ad hoc : sa sécurité repose sur la difficulté de problèmes spécifiques (pas plus difficiles que celui de la factorisation) et en conséquence peu étudiés. Afin de construire des méthodes de chiffrement plus génériques nous allons étudier plus en détail la structure du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

## 6.1 Ordre d'un élément

**Définition.** *On appelle ordre d'un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ et on note* $\mathrm{ord}(x)$ *le plus petit entier non nul $k \in \mathbb{N}^*$ pour lequel on a $x^k = 1$.*

Cette définition est classique mais fait difficilement transparaître la pertinence de la notion d'ordre ; elle est bien plus visible notamment à travers la propriété que voici.

**Proposition.** *L'ordre de $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est le cardinal de l'ensemble $\{x^\ell : \ell \in \mathbb{Z}\}$.*

*Démonstration.* Si $x^\ell$ est une puissance arbitraire de $x$ alors la division euclidienne $\ell = \mathrm{ord}(x)q + r$ de $\ell$ par $\mathrm{ord}(x)$ implique

$$x^\ell = x^{\mathrm{ord}(x)q+r} = x^{\mathrm{ord}(x)q}x^r = \left(x^{\mathrm{ord}(x)}\right)^q x^r = x^r$$

d'où s'ensuit l'égalité

$$\{x^\ell : \ell \in \mathbb{Z}\} = \{x^r : r \in \{0, \dots, \mathrm{ord}(x) - 1\}\}.$$

Or l'ensemble de droite a exactement $\mathrm{ord}(x)$ éléments car $x^r = x^s$ implique $x^{r-s} = 1$ et, par minimalité de $\mathrm{ord}(x)$, on a nécessairement $r = s$. □

L'ordre d'un élément est une notion fortement liée à la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$, comme le dévoile tout particulièrement le théorème suivant.

**Théorème** (Lagrange)**.** *L'ordre de tout élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ divise $\varphi(n)$.*

*Démonstration.* Écrivons encore la division euclidienne $\varphi(n) = kq + r$ de $\varphi(n)$ par l'ordre $k$ de $x$ ; on a alors

$$1 = x^{\varphi(n)} = x^{kq+r} = x^{kq}x^r = \left(x^k\right)^q x^r = x^r$$

or, par la minimalité de $k$, la seule valeur possible pour $r \in \{0, 1, \dots, k-1\}$ est 0. □

**Exercice.** *Soient $x$ et $y$ deux éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ dont les ordres sont premiers entre eux. Montrer que l'ordre de leur produit est le produit de leurs ordres.*

Les résultats ci-dessus peuvent s'étendre afin de concevoir un algorithme efficace permettant de calculer l'ordre d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$.

**Algorithme.**
*Entrée :* *Deux entiers $x$ et $n$ premiers entre eux.*
*Sortie :* *L'ordre de $x$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$.*

1. *Calculer $h \leftarrow \varphi(n)$.*
2. *Pour chaque facteur premier $p$ de $h$ :*
3. *Tant que $p$ divise $h$ :*
4. *Si $x^{h/p} = 1 \bmod n$, poser $h \leftarrow h/p$.*
5. *Renvoyer $h$.*

## 6.2 Éléments primitifs

La structure du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ serait plus transparente si chaque élément de ce groupe pouvait s'écrire comme puissance d'un élément $x$ fixe. Cela revient à demander que $x$ soit d'ordre maximal.

**Définition.** *On dit qu'un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est primitif, ou que c'est un générateur, si ses puissances décrivent tous les éléments du groupe multiplicatif.*

**Exemple.** *L'entier 2 est primitif modulo 5 car $\{2^0, 2^1, 2^2, 2^3\} = (\mathbb{Z}/5\mathbb{Z})^\times$. Modulo 7 on a $\{2^k : k \in \mathbb{Z}\} = \{1, 2, 4\} \subsetneq (\mathbb{Z}/7\mathbb{Z})^\times$ donc 2 est d'ordre 3, non 6.*

Dans le cas où $n$ admet un unique facteur premier, un tel élément existe toujours.

**Proposition.** *Pour tout $p$ premier, le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ admet un générateur.*

Pour simplifier nous prouverons ce résultat uniquement dans le cas $\alpha = 1$ ; on pourra généraliser les arguments ci-dessous aux puissances $\alpha$ arbitraires en exercice.

*Démonstration.* Soit $x$ un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $k$. Ses puissances décrivent un ensemble $\{x^\ell : \ell \in \mathbb{Z}\}$ de cardinal $k$ dont l'ordre de chaque élément divise $k$. Inversement, tout élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ dont l'ordre divise $k$ est une racine du polynôme $X^k - 1$ ; il y a ainsi au plus $k$ tels éléments et ce sont tous des puissances de $x$. Maintenant, les puissances de $x$ d'ordre exactement $k$ sont celles dont l'exposant est inversible modulo $k$. Le nombre d'éléments d'ordre exactement $k$ est donc $\varphi(k)$ s'il est non nul.

En sommant ces majorations sur les ordres possibles, on obtient :

$$p - 1 \leqslant \sum_{d \mid p-1} \varphi(d)$$

Or le lemme ci-dessous montre l'égalité. Lorsque $k$ divise $p - 1$, il y a donc exactement $\varphi(k)$ éléments d'ordre $k$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Contempler dans quelle mesure ce qui a été démontré ci-dessus est plus fort que le résultat annoncé.

**Lemme.** *Pour tout entier naturel $n$ on a $n = \sum_{d \mid n} \varphi(d)$.*

*Démonstration.* Supposons d'abord $n = p^\alpha$ avec $p$ premier et $\alpha \in \mathbb{N}^*$ ; on a alors

$$\sum_{d\,|\,p^\alpha} \varphi(d) = \sum_{\ell=0}^{\alpha} \varphi(p^\ell) = 1 + \sum_{\ell=1}^{\alpha} (p-1)p^{\ell-1} = 1 + (p-1)\sum_{\ell=0}^{\alpha-1} p^\ell$$

et le résultat s'obtient en calculant cette dernière somme géométrique.

Soient maintenant $m$ et $n$ deux entiers premiers entre eux ; on a

$$\sum_{d\,|\,mn} \varphi(d) = \sum_{\substack{a\,|\,m \\ b\,|\,n}} \varphi(ab) = \sum_{a\,|\,m} \varphi(a) \sum_{b\,|\,n} \varphi(b)$$

et le résultat en découle par récurrence sur le nombre de facteurs premiers. □

La structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est moins explicite, mais peut s'étudier, via le théorème Chinois, en combinant plusieurs instances du du résultat ci-dessus.

**Exercice.** *Combien y a-t-il d'éléments de chaque ordre possible dans* $(\mathbb{Z}/77\mathbb{Z})^\times$ *?*

## 6.3 Notion de groupe

Plutôt que de travailler exclusivement et de manière ad hoc sur l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ muni de sa loi de multiplication, nous allons introduire un cadre plus général auquel la plupart de nos résultats et constructions s'étend.

**Définition.** *On appelle groupe tout ensemble $G$ muni d'une loi de composition*

$$\cdot : \begin{cases} G \times G \longrightarrow G \\ (x, y) \longmapsto x \cdot y \end{cases}$$

*qui vérifie les propriétés :*

— $\forall x \in G, \forall y \in G, \forall z \in G, x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativité)
— $\exists 0 \in G, \forall x \in G, x \cdot 0 = x$ (élément neutre)
— $\forall x \in G, \exists y \in G, x \cdot y = 0$ (inverse)

*De surcroit, on dit qu'il est abélien ou commutatif si :*

— $\forall x \in G, \forall y \in G, x \cdot y = y \cdot x$ (commutativité)

Beaucoup d'ensembles de nombres que vous connaissez sont des groupes lorsqu'on les muni de leur loi de composition naturelle :

— $\mathbb{Z}$, les entiers relatifs munis de l'addition ;
— $\mathbb{Q}$, les nombres rationnels munis de l'addition ;
— $\mathbb{R}$, les nombres réels munis de l'addition ;
— $\mathbb{C}$, les nombres complexes munis de l'addition ;
— $\mathbb{Q}^\times$, les nombres rationnels non nuls munis de la multiplication ;
— $\mathbb{R}^\times$, les nombres réels non nuls muni de la multiplication ;
— $\mathbb{C}^\times$, les nombres complexes non nuls munis de la multiplication ;
— $\mathbb{Z}/n\mathbb{Z}$, les entiers modulo $n$ munis de l'addition modulaire ;
— $(\mathbb{Z}/n\mathbb{Z})^\times$, les entiers inversibles modulo $n$ munis de la multiplication modulaire ;
— $\mathrm{Mat}_{n,m}(\mathbb{R})$, les matrices de taille $n \times m$ munies de l'addition matricielle ;
— $\mathrm{GL}_n(\mathbb{R})$, les matrices carrées $n \times n$ inversibles munies de la multiplication matricielle ;

Attention, la loi de composition est aussi importante que l'ensemble sous-jacent. Par exemple, $\mathbb{Q}^\times$ n'est pas un groupe pour l'addition car il n'admet pas d'élément neutre ; inversement, $\mathbb{Q}$ n'est pas un groupe pour la multiplication car 0 n'admet pas d'inverse.

Remarquons enfin que les espaces vectoriels (que vous connaissez déjà) ne sont autres, lorsqu'on oublie leur loi de multiplication par un scalaire, des groupes abéliens.

**Définition.** *On appelle sous-groupe d'un groupe $(G, \cdot)$ tout groupe de la forme $(H, \cdot)$ avec $H \subset G$.*

Comme dans le cas des sous-espaces vectoriels, on peut montrer qu'un sous-ensemble d'un groupe forme un sous-groupe sans à nouveau vérifier entièrement chacune les hypothèses de la définition de groupe.

**Proposition.** *Pour que $H \subset G$ soit un sous-groupe, il faut et il suffit qu'il contienne l'élément neutre et soit stable par la loi de composition et son inverse.*

Généralisons maintenant la notion d'ordre que nous avons étudiée dans le cas de $(\mathbb{Z}/n\mathbb{Z})^\times$ et regardons comment elle se comporte vis-à-vis des sous-groupes.

**Définition.** *L'ordre d'un groupe est son cardinal.*

On a par exemple $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ et $\#\mathbb{Z} = \infty$.

**Théorème** (Lagrange)**.** *L'ordre de tout sous-groupe divise celui du groupe.*

*Démonstration.* Si $H$ est un sous-groupe de $G$ alors on a le partitionnement

$$G = \bigcup_{x \in G} \underbrace{\{xy : y \in H\}}_{xH}$$

où les termes $xH$ sont tous de cardinal $\#H$ et sont, deux à deux, soit disjoints soit identiques. □

**Exercice.** *Démontrer que $\mathbb{U}_n \subset \mathbb{U}_m$ si et seulement si $n \mid m$.*

Il est naturel (et fort utile) de se demander quel sous-groupe on obtient en « combinant » certains éléments donnés d'un groupe.

**Définition.** *Soit $(g_1, \dots, g_k)$ une famille d'éléments d'un groupe $G$. On appelle sous-groupe engendré et on note $\langle g_1, \dots, g_k \rangle$ le plus petit sous-groupe de $G$ contenant chacun des $g_i$.*

*On dit qu'un groupe $G$ est monogène s'il est engendré par un seul élément ; s'il est de surcroit fini on dit qu'il est cyclique.*

Si $G$ est commutatif, alors on peut écrire ces sous-groupes explicitement :

$$\langle g_1, \dots, g_k \rangle = \left\{ g_1^{\alpha_1} \cdot \colon \cdot \, g_k^{\alpha_k} : \alpha \in \mathbb{Z}^k \right\}.$$

**Exemple.** *Le groupe $\mathbb{Z}$ est monogène, mais le groupe $\mathbb{Z}^\times$ ne l'est pas. Le groupe $\mathbb{U}_n$ est cyclique, mais le groupe $\mathbb{U}$ ne l'est pas.*

**Définition.** *L'ordre d'un élément $g$ d'un groupe $G$ est l'ordre du sous-groupe $< g >$ qu'il engendre.*

Par le théorème de Lagrange, l'ordre de tout élément divise celui du groupe.

## 6.4 Racines de l'unité

Afin de nous familiariser davantage avec la notion de groupe nous allons maintenant présenter un autre exemple classique. Nous verrons notamment que cet exemple n'est en fait pas bien éloigné des groupes $(\mathbb{Z}/n\mathbb{Z}, +)$.

**Définition.** *Pour tout entier $n \in \mathbb{N}^*$, on dit qu'un nombre complexe $z \in \mathbb{C}$ est une racine $n^e$ de l'unité lorsqu'il vérifie $z^n = 1$ et on note $\mathbb{U}_n$ l'ensemble des tels nombres.*

**Exemple.** *On peut calculer les racines de l'unité de petit ordre explicitement :*
- $\mathbb{U}_1 = \{1\}$
- $\mathbb{U}_2 = \{1, -1\}$
- $\mathbb{U}_4 = \{1, -1, i, -1\}$
- $\mathbb{U}_3 = \{1, j, \overline{j}\}$ *avec* $j = e^{\frac{2\pi i}{3}}$ *a*

On peut déjà remarquer sur ces petits exemples que ces ensembles forment des groupes pour la multiplication complexe.

**Théorème.** *Pour tout entier $n \in \mathbb{N}^*$, le couple $(\mathbb{U}_n, \times)$ est un groupe.*

*Démonstration.* On montre que c'est un sous-groupe de $\mathbb{C}^\times$ en vérifiant :
- $1 \in \mathbb{U}_n$
- $a \in \mathbb{U}_n, b \in \mathbb{U}_n \Rightarrow ab \in \mathbb{U}_n$
- $a \in \mathbb{U}_n \Rightarrow a^{-1} \in \mathbb{U}_n$

□

La décomposition polaire $z = \rho e^{\theta i}$ (avec $\rho \in \mathbb{R}_+$ et $\theta \in \mathbb{R}$) permet d'écrire ses éléments explicitement :

$$\begin{aligned} z^n = 1 &\iff (\rho e^{\theta i})^n = 1 \\ &\iff \rho^n e^{n\theta i} = 1 \\ &\iff \begin{cases} \rho^n = 1 \\ n\theta = 2k\pi \end{cases} && \text{pour un certain } k \in \mathbb{Z} \\ &\iff \begin{cases} \rho = 1 \\ \theta = \frac{2k\pi}{n} \end{cases} \end{aligned}$$

On a ainsi :

$$\mathbb{U}_n = \left\{ e^{\frac{2k\pi i}{n}} : k \in \{0, \dots, n-1\} \right\}$$

Mais cette égalité est en réalité bien plus qu'une simple assertion ensembliste.

**Proposition.** *L'application*

$$e : \begin{cases} \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n \\ k + n\mathbb{Z} \longmapsto e^{\frac{2k\pi i}{n}} \end{cases}$$

*est bijective et vérifie les propriétés suivantes :*
- $e(0) = 1$
- $e(k + \ell) = e(k) \cdot e(\ell)$
- $e(-k) = e(k)^{-1}$

Cette application transforme donc, de manière parfaitement réversible, le groupe $\mathbb{Z}/n\mathbb{Z}$ muni de sa loi en le groupe $\mathbb{U}_n$ muni de sa loi. Si l'on fait abstraction des « noms » des éléments de ces deux groupes, la structure restante est alors identique. On dit que ces deux groupes sont isomorphes.

Mettons cette bijection en application.

**Proposition.** *Les éléments primitifs du groupe $\mathbb{U}_n$ sont les $e^{\frac{2k\pi i}{n}}$ pour lesquels* $\operatorname{pgcd}(k,n)=1$*; il y en a donc $\varphi(n)$.*

*Démonstration.* L'application ci-dessus permet de ramener ce problème dans $(\mathbb{Z}/n\mathbb{Z},+)$. L'élément 1 y est évidemment primitif et, inversement, un élément $k$ est primitif si et seulement si 1 est dans le sous-groupe engendré par $k$, c'est-à-dire si $k$ est inversible. □

## 6.5 Logarithme discret

Il nous a été bénéfique d'exploiter l'écriture de chaque élément de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ comme puissance d'un élément $g$ fixé, c'est-à-dire la surjectivité de l'application

$$\begin{cases} \mathbb{Z} \longrightarrow \mathbb{Z}/p^\alpha\mathbb{Z} \\ \ell \longmapsto g^\ell \end{cases} ;$$

cette écriture n'est toutefois pas complètement explicite car, si évaluer l'application ci-dessus est une tache algorithmiquement aisée, l'inverser est un problème très difficile.

Nous allons à présent nous placer dans le cadre plus général des groupes abéliens finis. Cependant, on pourra parfaitement penser au cas $G=(\mathbb{Z}/n\mathbb{Z})^\times$ si nécessaire pour fixer les idées.

**Définition.** *Soient $x$ et $y$ deux éléments d'un groupe $G$. On appelle logarithme discret de $y$ en base $x$ toute solution $k\in\mathbb{Z}$ de l'équation $y=x^k$.*

Remarquons que si $k$ et $\ell$ sont deux solutions, alors $x^{k-\ell}=1$ ; les solutions sont donc bien définies modulo l'ordre de $x$.

**Exemple.** *Dans* $(\mathbb{Z}/11\mathbb{Z})^\times$ *on a* $\log_3(5)=3$ *car* $3^3=27=5 \bmod 11$.
*Cependant,* $\log_3(2)$ *n'existe pas, car* $\{3^k : k\in\mathbb{Z}\}=\{1,3,4,5,9\}$.

Pour calculer un logarithme discret, on peut évidemment « essayer » toutes les possibilités :

**Algorithme** (force brute).
*Entrée :* *Deux éléments $x$ et $y$ d'un groupe $G$.*
*Sortie :* *Un logarithme de $y$ en base $x$.*

1. *Pour tout $k$ dans $\{1,\dots,\#G\}$ :*
2. *Si $x^k=y$ renvoyer $k$.*

Cela nécessite $O(\#G)$ opérations ; on peut cependant faire bien mieux en « partageant » le travail entre $x$ et $y$ :

**Algorithme** (Shanks [14]).
*Entrée :* *Deux éléments $x$ et $y$ d'un groupe $G$.*
*Sortie :* *Un logarithme de $y$ en base $x$.*

1. *Pour tout $\ell$ dans $\{1,\dots,\sqrt{\#G}\}$ :*
2. *Calculer $y^\ell$.*
3. *Pour tout $k$ dans $\{1,\dots,\sqrt{\#G}\}$ :*
4. *Calculer $x^k$.*
5. *Si $x^k=y^\ell$ alors renvoyer $k\ell^{-1} \bmod \#G$.*

Cet algorithme est efficace car on sait stocker les éléments calculés à l'étape 2 dans une structure où on peut ensuite les rechercher à l'étape 5 en temps $O(\log(n)^2)$. La racine carrée vous rappelle le paradoxe des anniversaires à juste titre : c'est ce sur quoi la version probabiliste de cet algorithme reposerait.

Insistons sur le fait que les deux algorithmes ci-dessus s'appliquent à tout groupe abélien fini ; on dit qu'ils sont *génériques*. Il existe d'autres algorithmes plus rapides dans certains cas particuliers comme $G = (\mathbb{Z}/n\mathbb{Z})^\times$ ou $G = \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ mais aucun qui soit générique.

## 6.6 Cryptosystème ElGamal

Le cryptosystème RSA repose entièrement sur la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ ; toute avancée théorique sur ces groupes particuliers serait donc à même de remettre en cause sa sécurité. C'est justement le cas : depuis l'invention de RSA, les tailles de clef considérées sûres ne font qu'augmenter pour pallier les avancées algorithmiques concernant le problème de la factorisation.

Il serait plus satisfaisant de concevoir des cryptosystèmes reposant sur un problème plus générique, de sorte qu'on puisse espérer qu'aucun algorithme autre que générique ne permette de le résoudre efficacement.

**Définition.** *La méthode de chiffrement à clef publique ElGamal [3] fonctionne* ***essentiellement*** *comme il suit :*

1. *Pour construire un couple de clefs, choisir un groupe $G$ et un générateur $g$. Poser $L = \{1, \dots, \#G - 1\}$. Choisir un entier $x \in L$ aléatoirement et calculer $h = g^x$. Renvoyer alors la clef privée $(x)$ et la clef publique $(G, g, h)$.*
2. *Pour chiffrer un message $m \in G$, choisir un entier $y \in L$ aléatoirement et calculer $s = mh^y$ et $t = g^y$. Renvoyer le chiffré $(s, t)$.*
3. *Pour déchiffrer $(s, t)$, renvoyer $st^{-x}$.*

La sécurité de ce cryptosystème repose donc sur la difficulté de calculer $x = \log_g(h)$ à partir de la clef publique, c'est-à-dire de la description du groupe $G$ et de ses éléments $g$ et $h$.

**Exemple.** *Soit $p$ un grand nombre premier.*

— *Si $G = \mathbb{Z}/p\mathbb{Z}$ la sécurité est exécrable.*

— *Si $G = (\mathbb{Z}/p\mathbb{Z})^\times$ la sécurité est similaire à celle de RSA.*

— *Si $G = \left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 : x^2 + y^2 = 1 + d\,x^2 y^2\right\}$ avec la loi de composition*

$$(u, v) \oplus (x, y) = \left( \frac{uy + vx}{1 + d\,uvxy}, \frac{vy - ux}{1 - d\,uvxy} \right)$$

*pour un entier $d$ vérifiant $d^{\frac{p-1}{2}} = -1 \bmod p$ alors la sécurité est (autant que l'on sache) similaire à celle d'un groupe générique.*

# Bibliographie


[1] Manindra Agrawal, Neeraj Kayal et Nitin Saxena. "PRIMES is in P".
In : *Annals of Mathematics* 160.2 (2004), pages 781-793.
doi : 10.4007/annals.2004.160.781.

[2] Whitfield Diffie et Martin E. Hellman. "New directions in cryptography".
In : *IEEE Transactions on Information Theory* 22.6 (1976), pages 644-654.
doi : 10.1109/TIT.1976.1055638.

[3] Taher ElGamal.
"A public key cryptosystem and a signature scheme based on discrete logarithms".
In : *Advances in Cryptology — CRYPTO 1984*.
Sous la direction de George Robert Blakley et David Chaum. Tome 196.
Lecture Notes in Computer Science. Springer, 1985, pages 10-18.
doi : 10.1007/3-540-39568-7_2.

[4] Oded Goldreich. *Foundations of Cryptography. Basic Tools*. Tome 1.
Cambridge University Press, 2001. isbn : 0521035368.
doi : 10.1017/CBO9780511546891.

[5] Oded Goldreich. *Foundations of Cryptography. Basic Applications*. Tome 2.
Cambridge University Press, 2004. isbn : 051172165X.
doi : 10.1017/CBO9780511721656.

[6] Ralph C. Merkle et Martin E. Hellman.
"Hiding information and signatures in trapdoor knapsacks".
In : *IEEE Transactions on Information Theory* 24.5 (1978), pages 525-530.
doi : 10.1109/TIT.1978.1055927.

[7] Gary L. Miller. "Riemann's hypothesis and tests for primality".
In : *Symposium on Theory of Computing — STOC 1975*.
Sous la direction de William C. Rounds et al.
Association for Computing Machinery, 1975, pages 234-239.
doi : 10.1145/800116.803773.

[8] Satoshi Nakamoto. *Bitcoin : A Peer-to-peer Electronic Cash System*. 2008.
url : https://bitcoin.org/bitcoin.pdf.

[9] John M. Pollard. "A Monte Carlo method for factorization".
In : *BIT Numerical Mathematics* 15.3 (1975), pages 331-334.
doi : 10.1007/BF01933667.

[10] Michael O. Rabin. "Probabilistic algorithm for testing primality".
In : *Journal of Number Theory* 12.1 (1980), pages 128-138.
doi : 10.1016/0022-314X(80)90084-0.

[11] Ron L. Rivest. “The RC5 Encryption Algorithm”.
In : *Fast Software Encryption — FSE 1994*. Sous la direction de Bart Preneel. Tome 1008. Lecture Notes in Computer Science. Springer, 1995, pages 86-96. doi : 10.1007/3-540-60590-8_7.

[12] Ron L. Rivest, Adi Shamir et Leonard Adleman.
“A method for obtaining digital signatures and public-key cryptosystems”.
In : *Communications of the ACM* 21.2 (1978), pages 120-126.
doi : 10.1145/359340.359342.

[13] Adi Shamir.
“A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem”.
In : *Foundations of Computer Science — FOCS 1982*. IEEE Computer Society, 1982, pages 145-152. doi : 10.1109/SFCS.1982.55.

[14] Daniel Shanks. “Class number, a theory of factorization, and genera”.
In : *1969 Number Theory Institute*. Sous la direction de Donald J. Lewis. Tome 20. Proceedings of Symposia in Pure Mathematics. American Mathematical Society, 1971, pages 415-440.

[15] Claude Shannon. “Communication theory of secrecy systems”.
In : *Bell System Technical Journal* 28.4 (1949), pages 656-715.