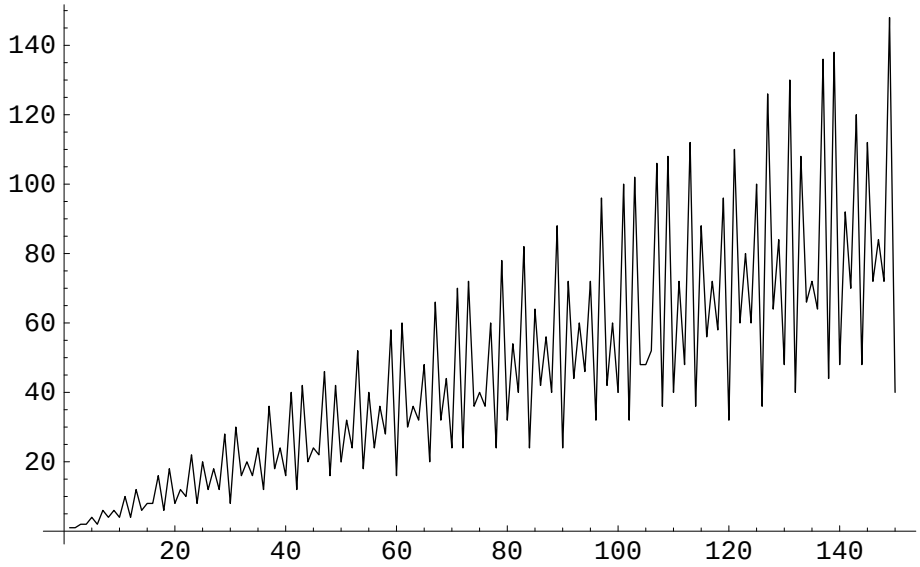
Université de Liège
Faculté des sciences

Mathématiques discrètes



Notes de cours 2009–2010

Michel Rigo

Table des matières

CHAPITRE I

Quelques compléments d'algèbre

Nous rappelons tout d'abord quelques définitions de structures et objets classiques déjà rencontrés à diverses occasions dans les cours d'algèbre. Les cinq premières sections de ce chapitre ne constituent qu'un résumé partiel de notions supposées connues et nous invitons le lecteur à compléter ce rappel, s'il le juge nécessaire. Dans la suite de ce chapitre, nous approfondissons quelques points importants comme les éléments algébriques, les polynômes et leurs racines ou encore la structure des champs finis. En effet, ces derniers disposent, comme nous le verrons dans les chapitres suivants, d'atouts particulièrement intéressants pour les applications (codes correcteurs, cryptographie, combinatoire, etc...). Attirons d'ores et déjà l'attention du lecteur sur le fait que nous considérerons tout au long de ces notes presque exclusivement des structures commutatives.

1. Structures algébriques

Définition I.1.1. Un *groupe* est un ensemble G muni d'une opération interne et partout définie $\circ : G \times G \to G$ telle que

- l'opération $\circ$ est associative : $\forall x, y, z \in G,\ x \circ (y \circ z) = (x \circ y) \circ z$,
- il existe un élément (unique) $e \in G$, appelé *neutre*, tel que
$$x \circ e = x = e \circ x,\ \forall x \in G,$$
- tout élément de G est *inversible*, i.e., pour tout $x \in G$, il existe $y \in G$ (unique, noté x^{-1} ou $-x$ suivant le contexte) tel que $x \circ y = y \circ x = e$.

Enfin, si pour tous $x, y \in G$, on a $x \circ y = y \circ x$, alors on parle de *groupe commutatif* ou *abélien*. S'il est nécessaire de rappeler l'opération ou le neutre du groupe G, on le notera $(G, \circ)$ ou $(G, \circ, e)$.

Remarque I.1.2. Si un ensemble jouit uniquement des deux premières propriétés, on dit alors qu'il s'agit d'un *monoïde*.

Exemple I.1.3. L'ensemble $(\mathbb{Z}/m\mathbb{Z}, +)$, aussi noté $(\mathbb{Z}_m, +)$, des entiers modulo m muni de l'opération d'addition correspondante est un groupe[1]. L'ensemble $(\mathbb{Q} \setminus \{0\}, \cdot)$ en est un aussi. Ces deux premiers exemples sont des groupes commutatifs. L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices carrées inversibles

Nous supposons les entiers modulo connus.

[1]La notation $\mathbb{Z}/m\mathbb{Z}$ prendra rapidement tout son sens. Notez également que $\mathbb{Z}_m$ est souvent utilisé pour désigner l'ensemble des entiers m-adiques (m premier). Il n'y a cependant ici aucune confusion possible.

de dimension n muni de la multiplication matricielle est un groupe non commutatif. Par contre, $(\mathbb{N}, +)$ est un monoïde qui n'est pas un groupe.

Définition I.1.4. Soient $(G, \circ, e_G)$ et $(H, \diamond, e_H)$ deux groupes. Un *homomorphisme de groupes* est une application $f : G \to H$ telle que

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y).$$

Puisque dans un groupe, tout élément est inversible, il découle de cette définition que $f(e_G) = e_H$ et $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$. En effet, pour tout $x \in G$, on a $f(x) = f(x \circ e_G) = f(x) \diamond f(e_G)$. Puisque H est un groupe, nous pouvons multiplier à gauche par $f(x)^{-1}$ pour obtenir $f(x)^{-1} \diamond f(x) = f(x)^{-1} \diamond f(x) \diamond f(e_G)$ et conclure. Fort de cette constatation, il vient pour tout $x \in G$, $f(e_G) = f(x \circ x^{-1}) = f(x) \diamond f(x^{-1}) = e_H$.

Définition I.1.5. Soient $(G, \circ, e_G)$ et $(H, \diamond, e_H)$ deux monoïdes. Un *homomorphisme de monoïdes* est une application $f : G \to H$ telle que

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y) \quad \textbf{et} \quad f(e_G) = e_H.$$

Cette dernière condition ne découle pas de la première car, dans le cas d'un monoïde, on ne dispose généralement pas de la notion d'inverse.

Définition I.1.6. Un *anneau* est un ensemble A muni de deux opérations internes et partout définies, que nous noterons ici $+$ et $\cdot$ et dont les neutres respectifs sont notés 0 et 1, tel que

- $(A, +, 0)$ est un groupe commutatif,
- l'opération $\cdot$ est associative, i.e., $\forall x, y, z \in A$, $(x.y).z = x.(y.z)$,
- 1 est neutre pour $\cdot$, i.e., $\forall x \in A$, $1.x = x.1 = x$,
- l'opération $\cdot$ est distributive par rapport à $+$,

$$\forall x, y, z \in A,\ (x + y).z = x.z + y.z \text{ et } x.(y + z) = x.y + x.z.$$

S'il est nécessaire de rappeler les opérations de l'anneau, on le notera alors $(A, +, \cdot, 0, 1)$ ou $(A, +, \cdot)$. Un anneau est *commutatif* si l'opération $\cdot$ est commutative.

Exemple I.1.7. L'ensemble $(\mathbb{Z}_m, +, \cdot)$ possède une structure d'anneau commutatif. L'ensemble $\mathbb{R}_n^n$ des matrices carrées de dimension n à coefficients réels muni des opérations usuelles d'addition et de multiplication possède une structure d'anneau (non commutatif).

Remarque I.1.8. Si $(A, +, \cdot)$ est un anneau, alors $(A, \cdot, 1)$ possède en particulier une structure de monoïde.

Définition I.1.9. Un anneau pour lequel $0 \neq 1$ et tout élément non nul possède un inverse pour $\cdot$, i.e., pour tout $x \in A \setminus \{0\}$, il existe $y \in A$ tel que $x.y = 1 = y.x$, est qualifié de *corps*. Si de plus, l'anneau est commutatif, on parle alors de *champ*[2].

[2]Nos amis français n'emploient pas cette terminologie et parle exclusivement de corps. Parfois, ils parlent de corps gauche pour insister sur le caractère non commutatif de la multiplication.

Exemple I.1.10. L'ensemble $\mathbb{Z}_p$ est un champ si et seulement si p est un nombre premier. On le note parfois $\mathbb{F}_p$ et cette notation sera justifiée dans les sections suivantes. Le sous-ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de $\mathbb{R}_n^n$ est un corps.

Définition I.1.11. Soient $(A, +_A, \cdot_A, 0_A, 1_A)$ et $(B, +_B, \cdot_B, 0_B, 1_B)$ deux anneaux. Un *homomorphisme d'anneaux* est une application $f : A \to B$ telle que f est un homomorphisme de groupes entre $(A, +_A, 0_A)$ et $(B, +_B, 0_B)$ et aussi un homomorphisme de monoïdes entre $(A, \cdot_A, 1_A)$ et $(B, \cdot_B, 1_B)$. Autrement dit, on a

$$\forall x, y \in A,\ f(x+y) = f(x) + f(y),\ f(x.y) = f(x).f(y)$$

et $f(1_A) = 1_B$.

Définition I.1.12. Soit $\mathbb{K}$ un champ (ou simplement un corps). Un *espace vectoriel* E sur $\mathbb{K}$ ou $\mathbb{K}$-*vectoriel* est un ensemble E muni d'une addition interne $+ : E \times E \to E$ et d'une multiplication interne $\cdot : \mathbb{K} \times E \to E$ tel que

- $(E, +)$ est un groupe commutatif

et pour tous $x, y \in E$ et tous $\lambda, \mu \in \mathbb{K}$

- $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$,
- $1 \cdot x = x$,
- $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
- $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.

Si $\mathbb{K}$ n'est pas un champ, mais simplement un anneau, on parle alors de $\mathbb{K}$-*module*. Un espace vectoriel est de *dimension finie* s'il contient une partie génératrice finie. Sa *dimension* est alors le nombre d'éléments d'une de ses bases[3].

Définition I.1.13. Soient $\mathbb{K}, \mathbb{L}$ deux champs tels que $\mathbb{K}$ soit un sous-champ de $\mathbb{L}$. Dans ce cas, on dit que $\mathbb{L}$ est une *extension de champ* de $\mathbb{K}$. En particulier, il est immédiat de vérifier que $\mathbb{L}$ est un $\mathbb{K}$-vectoriel. Si la dimension de $\mathbb{L}$ comme $\mathbb{K}$-vectoriel est finie et égale à d, alors on parle d'*extension finie* et d est le *degré de l'extension*; on la note $[\mathbb{L} : \mathbb{K}]$. Plus généralement, si $\mathbb{K}$ et $\mathbb{L}$ sont deux champs et s'il existe un plongement $h : \mathbb{K} \to \mathbb{L}$ (i.e., un homomorphisme injectif), alors on dit que $\mathbb{L}$ est une extension de $\mathbb{K}$ car $\mathbb{K}$ est isomorphe à un sous-champ de $\mathbb{L}$.

Remarque I.1.14. Si $\mathbb{K}$ est un champ fini contenant t éléments et si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré fini d, alors on en déduit immédiatement que $\mathbb{L}$ contient t^d éléments. En effet, il existe une base $(\ell_1, \ldots, \ell_d)$ de $\mathbb{L}$ telle que tout élément de $\mathbb{L}$ se décompose de manière unique comme $k_1\ell_1 + \cdots + k_d\ell_d$ avec les $k_i \in \mathbb{K}$.

[3]Un $\mathbb{K}$-vectoriel possède au moins une base et toutes ses bases sont équipotentes. Cela signifie que, dans le cas d'un espace vectoriel de dimension finie, elles ont le même nombre d'éléments. Rappelons aussi qu'un A-module ne possède pas toujours de base.

Exemple I.1.15. L'ensemble $\mathbb{Q}$ est un champ. En adjoignant à $\mathbb{Q}$ le nombre irrationnel $\sqrt{2}$, on obtient l'extension de champ $\mathbb{Q}(\sqrt{2})$ formée de toutes les expressions rationnelles[4] faisant intervenir $\sqrt{2}$ et des éléments de $\mathbb{Q}$. Il s'agit du plus petit champ contenant $\mathbb{Q}$ et $\sqrt{2}$. Ainsi, un élément arbitraire de $\mathbb{Q}(\sqrt{2})$ est de la forme

$$\frac{\sum_{i=0}^{m} q_i\,(\sqrt{2})^i}{\sum_{j=0}^{n} r_j\,(\sqrt{2})^j}, \quad q_i, r_j \in \mathbb{Q}, m, n \in \mathbb{N}.$$

Des manipulations algébriques élémentaires permettent de réécrire cet élément sous la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. Ainsi, on a

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

et $(1, \sqrt{2})$ forment une base de $\mathbb{Q}(\sqrt{2})$ considéré comme $\mathbb{Q}$-vectoriel. Il est clair que le degré de cette extension est 2, i.e., $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Par des raisonnements analogues, il est facile de voir que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

et $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

2. Idéaux

Définition I.2.1. Un *idéal* (*bilatère*) d'un anneau $(A, +, \cdot)$ est un sous-ensemble $I \subset A$ tel que

- $(I, +, 0)$ est un groupe commutatif,
- pour tous $i \in I$ et $a \in A$, $a.i$ et $i.a$ appartiennent à I.

Soient $a_1, \ldots, a_k$ des éléments de A. Dans le cas où A est un anneau commutatif, l'idéal engendré par $a_1, \ldots, a_k$ est

$$\langle a_1, \ldots, a_k \rangle = \left\{ \sum_{i=1}^{k} b_i a_i \mid b_i \in A \right\}.$$

Un idéal engendré par un unique élément $a \in A$, i.e., $I = \langle a \rangle$, est qualifié de *principal*. Un anneau *principal* est un anneau intègre[5] dans lequel tout idéal est principal.

Définition I.2.2. Un idéal I d'un anneau A est *maximal* si I est propre, i.e., $I \neq A$, et s'il n'est contenu strictement dans aucun idéal propre, i.e., si J est un idéal tel que $I \subsetneq J$, alors $J = A$.

Exemple I.2.3. Si $\mathbb{K}$ est un champ, les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$ tout entier. En effet, si un élément $a \neq 0$ appartient à un idéal $I \neq \{0\}$, alors $a^{-1}.a = 1$ doit appartenir à I et de là, on en déduit que tout élément de $\mathbb{K}$ appartient à I. Les idéaux de $\mathbb{Z}$ sont les $m\mathbb{Z} = \langle m \rangle$ et $\mathbb{Z}$ est donc un anneau principal.

[4] On a le droit, dans un champ, d'ajouter, soustraire, multiplier et diviser entre eux des éléments quelconques de $\mathbb{Q} \cup \{\sqrt{2}\}$ (en ne divisant bien sûr pas par 0).

[5] i.e., A ne possède pas de diviseurs de 0. Autrement dit, si $a.b = 0$ avec $a, b \in A$, alors $a = 0$ ou $b = 0$.

2.1. Quotient d'un anneau par un idéal. Nous serons brefs. Soient $(A, +, \cdot, 0, 1)$ un anneau et I un idéal de A. Puisque I est un sous-groupe du groupe commutatif $(A, +, 0)$, on peut tout d'abord considérer le groupe quotient A/I. Rappelons que les éléments de A/I sont les classes de la forme

$$a + I = \{a + i \mid i \in I\}, \quad a \in A.$$

La somme de deux classes $a + I$ et $b + I$ est la classe $(a + b) + I$ et le neutre la classe $0 + I = I$. On peut munir A/I d'une structure supplémentaire d'anneau en le munissant d'une multiplication : le produit des classes $a + I$ et $b + I$ est la classe $(a.b) + I$ et le neutre est alors $1 + I$. La projection canonique $\pi : A \to A/I : a \mapsto a + I$ est alors un homomorphisme d'anneaux.

Exemple I.2.4. L'anneau quotient de $\mathbb{Z}$ par l'idéal $m\mathbb{Z}$ est l'anneau $\mathbb{Z}_m$ des entiers modulo m. Une classe est un élément de la forme $a + \langle m \rangle$. Pour $m = 3$, on a par exemple,

$$(1 + \langle 3 \rangle) + (2 + \langle 3 \rangle) = 3 + \langle 3 \rangle = 0 + \langle 3 \rangle$$

et

$$(2 + \langle 3 \rangle).(2 + \langle 3 \rangle) = 4 + \langle 3 \rangle = 1 + \langle 3 \rangle.$$

En effet, dans $\mathbb{Z}_m$ il est facile de se convaincre que

$$\forall a, b \in \mathbb{Z} : \ a + \langle m \rangle = b + \langle m \rangle \Leftrightarrow a \equiv b \pmod{m}.$$

Remarque I.2.5. Un élément $a + I$ de A/I est nul (i.e., correspond au neutre pour l'addition dans l'anneau quotient) si et seulement si a appartient à I. En effet, $a + I = \{a + i \mid i \in I\} = I$ si et seulement si $a \in I$.

Un résultat fort utile concernant les idéaux maximaux est le suivant.

Premier ingrédient pour construire un champ fini.

Théorème I.2.6. *Soient A un anneau commutatif et I un idéal de A. L'anneau quotient A/I est un champ si et seulement si I est un idéal maximal.*

2.2. Idéaux et divisibilité. La proposition suivante relie la notion d'idéal à celle de la divisibilité. Elle nous sera utile dans la suite et nous avons donc jugé bon de la rappeler. Soient a, b deux éléments d'un anneau A muni d'une division euclidienne. Bien sûr, on dira que a divise b s'il existe $c \in A$ tel que $b = c.a$.

Théorème I.2.7. *Soient A un anneau principal*[6] *et $a, b \in A \setminus \{0\}$. On a*

- $\langle a \rangle \supset \langle b \rangle$ *si et seulement si a divise b.*
- $\langle a \rangle = \langle b \rangle$ *si et seulement si $a = ub$ avec u inversible dans A.*

Démonstration. Supposons que $\langle a \rangle \supset \langle b \rangle$. En particulier, b appartient à $\langle a \rangle$ et il existe donc $c \in A$ tel que $b = ca$. Ainsi, a divise b. Réciproquement, si a divise b, il existe $c \in A$ tel que $b = ca$. Dès lors, pour tout $t \in A$, $tb = tca$ ce qui montre que $\langle b \rangle$ est inclus dans $\langle a \rangle$.

[6] On suppose l'anneau principal muni d'une division euclidienne comme par exemple $\mathbb{Z}$ ou $\mathbb{K}[X]$.

Pour la seconde partie, si $a = ub$ avec u inversible dans A, on a aussi $u^{-1}a = b$ (avec u^{-1} l'inverse de u, i.e., $u^{-1}.u = 1$). Ainsi, a divise b et b divise a. Donc par le premier point, $\langle a\rangle = \langle b\rangle$. Réciproquement, si $\langle a\rangle = \langle b\rangle$, alors il existe u et v dans A tels que $a = ub$ et $b = va$. De là, $b = vub$ et donc $vu = 1$. Ceci signifie que u et v sont inversibles et inverses l'un de l'autre.

■

3. Polynômes et division euclidienne

Dans cette section $\mathbb{K}$ est un champ.

Définition I.3.1. Un *polynôme* à coefficients dans le champ $\mathbb{K}$ est une suite $(\alpha_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ non tous nuls pour laquelle il existe un entier $d \geq 0$ tel que $\alpha_n = 0$ pour tout $n > d$. On notera symboliquement ce polynôme par

$$P = \sum_{i=0}^{d} \alpha_i\, X^i = \alpha_d X^d + \cdots + \alpha_1 X + \alpha_0$$

et d en est le *degré*, noté $\deg P$. La *valeur* $P(\beta)$ de ce polynôme évalué en $\beta \in \mathbb{K}$ est

$$P(\beta) = \sum_{i=0}^{d} \alpha_i\, \beta^i = \alpha_d \beta^d + \cdots + \alpha_1 \beta + \alpha_0.$$

(Nous rappelons au lecteur la distinction faite entre polynôme et *fonction polynomiale*[7].) La suite nulle est appelé *polynôme nul*. Si $\alpha_d = 1$, le polynôme est qualifié de *monique* (ou *unitaire*). Si $d = 0$, le polynôme est *constant*. On définit de manière naturelle (comme dans le cas des polynômes à coefficients réels) la somme et le produit de deux polynômes. L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ possède alors une structure d'anneau.

Il est aisé de munir $\mathbb{K}[X]$ de la divison euclidienne[8].

Proposition I.3.2 (Division euclidienne). *Soit $\mathbb{K}$ un champ. Si $D \in \mathbb{K}[X]$ est non nul, alors pour tout $P \in \mathbb{K}[X]$, il existe des polynômes uniques Q et R tels que*

$$P = Q.D + R, \quad \textit{avec } \deg R < \deg D.$$

Démonstration. En procédant comme dans $\mathbb{C}[z]$ (calcul écrit), le résultat est immédiat.

■

[7] Les polynômes de $\mathbb{Z}_3[X]$, $P(X) = X^2 + 1$ et $Q(X) = X^3 + X^2 - X + 1$ sont distincts mais représentent la même fonction : $\forall z \in \mathbb{Z}_3$, $P(z) = Q(z)$.

[8] On dit parfois que $\mathbb{K}[X]$ est un *anneau euclidien*. En fait, un anneau euclidien est un anneau muni d'une valuation euclidienne permettant de définir une "sorte" de division euclidienne. Si $\mathbb{K}$ n'est pas un champ mais simplement un anneau, pour assurer l'existence des polynômes Q et R, il faut que le coefficient principal de D soit inversible. De plus, l'unicité de Q et R n'est assurée que si l'anneau est intègre.

Soient P, Q, R appartenant à $\mathbb{K}[X]$. Si $P = Q.R$, alors le polynôme Q *divise* le polynôme P. Puisque $\mathbb{K}$ est un champ[9],

$$\deg P.Q = \deg P + \deg Q \tag{1}$$

et dès lors, $\mathbb{K}[X]$ est un anneau *intègre*, i.e., qu'il ne possède pas de diviseur de zéro. Ainsi, $P.Q = 0$ entraîne $P = 0$ ou $Q = 0$.

Définition I.3.3. Un polynôme non constant P est *irréductible* si $P = Q.R$ entraîne que Q ou R est constant. Au vu de (1), P ne peut pas s'écrire comme le produit de deux polynômes de degré strictement inférieur au degré de P. En particulier, tout polynôme de degré 1 est irréductible.

Exemple I.3.4. Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$ car il s'y factorise en $(X + i)(X - i)$.

Remarque I.3.5. Dans $\mathbb{K}[X]$, les seuls éléments inversibles sont les polynômes constants $k \in \mathbb{K} \setminus \{0\}$. C'est immédiat. Si P est un polynôme de degré au moins 1, alors pour tout $Q \in \mathbb{K}[X]$, $\deg P.Q \geq 1$ et P ne peut donc pas posséder d'inverse. Avec le même genre de raisonnement, il est clair que $\langle P \rangle = \mathbb{K}[X]$ si et seulement si $P \neq 0$ est constant.

Le résultat suivant découle principalement du fait que $\mathbb{K}[X]$ est muni de la division euclidienne.

Théorème I.3.6. *Soit $\mathbb{K}$ un champ. L'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est principal.*

Corollaire I.3.7. *Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$. L'idéal $\langle P \rangle$ est un idéal maximal si et seulement si P est irréductible.*

Deuxième ingrédient pour construire un champ fini.

Démonstration. Supposons que $\langle P \rangle$ est un idéal maximal avec $P \neq 0$. Montrons d'abord que P ne peut pas être constant. Supposons qu'il le soit. Dans ce cas, $P = k \in \mathbb{K} \setminus \{0\}$ et $k^{-1}.k = 1$ doit appartenir à $\langle k \rangle$. On en conclut que $\langle P \rangle = \mathbb{K}[X]$, ce qui est impossible. Supposons à présent que P est un polynôme non constant qui se factorise en $P = Q.R$. Au vu du théorème I.2.7, $\langle P \rangle \subseteq \langle Q \rangle$. Si $\langle P \rangle = \langle Q \rangle$, alors en utilisant la seconde partie du théorème I.2.7 et la remarque I.3.5, on conclut que R est constant. Sinon, $\langle P \rangle \subsetneq \langle Q \rangle$ et puisque $\langle P \rangle$ est maximal, on en conclut que $\langle Q \rangle = \mathbb{K}[X]$ et donc que Q est constant.

Réciproquement, si P est un polynôme irréductible, montrons que l'anneau $\mathbb{K}[X]/\langle P \rangle$ est un champ (d'où la conclusion, en utilisant le théorème I.2.6). Il suffit de montrer que tout élément non nul $\pi(Q) = Q + \langle P \rangle$ du quotient $\mathbb{K}[X]/\langle P \rangle$ est inversible. Dire que $\pi(Q)$ est non nul revient à dire que Q n'appartient pas à $\langle P \rangle$ (cf. remarque I.2.5).

Considérons l'idéal $\langle P, Q \rangle$ et montrons qu'il est égal à $\mathbb{K}[X]$. Puisque $\mathbb{K}[X]$ est principal, il existe un polynôme T tel que $\langle P, Q \rangle = \langle T \rangle$. Ainsi,

[9] Si $\mathbb{K}$ est simplement un anneau, une telle propriété est fausse. En effet, considérons les polynômes $2X^2 + 1$ et $2X + 1$ de $\mathbb{Z}_4[X]$. On a $(2X^2 + 1).(2X + 1) = 2X^2 + 2X + 1$.

il existe deux polynômes U et V tels que $P = U.T$ et $Q = V.T$. Par hypothèse, P étant irréductible, U ou T est constant. Si T est constant, alors $\langle P, Q\rangle = \langle T\rangle = \mathbb{K}[X]$. Si U est constant, c'est un élément non nul de $\mathbb{K}$ qui est inversible dans $\mathbb{K}[X]$ et on en tire (cf. théorème I.2.7) que $\langle P\rangle = \langle T\rangle = \langle P, Q\rangle$ ou encore que Q appartient à $\langle P\rangle$ ce qui est impossible.

Puisque $\langle P, Q\rangle = \mathbb{K}[X]$, il contient 1 et il existe $A, B \in \mathbb{K}[X]$ tels que

$$1 = A.P + B.Q.$$

Cela entraîne que dans l'anneau quotient $\mathbb{K}[X]/\langle P\rangle$,

$$(B + \langle P\rangle).(Q + \langle P\rangle) = 1 + \langle P\rangle$$

et donc, $\pi(Q)$ est inversible d'inverse $B + \langle P\rangle$.

■

En utilisant ce dernier corollaire et le théorème I.2.6, on déduit le résultat suivant qui nous permettra de construire des champs finis.

Proposition I.3.8. *Soit $\mathbb{K}$ un champ. L'anneau quotient $\mathbb{K}[X]/\langle P\rangle$ est un champ si et seulement si P est un polynôme irréductible.*

Exemple I.3.9. Considérons l'anneau des polynômes $\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2+1\rangle$. Les classes de l'anneau quotient (il s'agit même d'un champ car $X^2 + 1$ est irréductible[10] sur $\mathbb{Z}_3[X]$) sont de la forme[11] $P + \langle X^2 + 1\rangle$ avec $\deg P < 2$. Par commodité, nous noterons $P + \langle X^2 + 1\rangle$ simplement P. La table ci-dessous est la table de multiplication dans $\mathbb{Z}_3[X]/\langle X^2 + 1\rangle$ (dans laquelle on n'a pas considéré l'élément zéro). Pour l'obtenir, il suffit de travailler "modulo $X^2 + 1$". Ainsi, la multiplication des deux classes $P + \langle X^2 + 1\rangle$ et $Q + \langle X^2 + 1\rangle$ est la classe $R + \langle X^2 + 1\rangle$ où R est le reste de la division dans $\mathbb{Z}_3[X]$ de $P.Q$ par $X^2 + 1$.

$\cdot$	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
1	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
2	2	1	$2X$	$2X+2$	$2X+1$	X	$X+2$	$X+1$
X	X	$2X$	2	$X+2$	$2X+2$	1	$X+1$	$2X+1$
$X+1$	$X+1$	$2X+2$	$X+2$	$2X$	1	$2X+1$	2	X
$X+2$	$X+2$	$2X+1$	$2X+2$	1	X	$X+1$	$2X$	1
$2X$	$2X$	X	1	$2X+1$	$X+1$	2	$2X+2$	$X+2$
$2X+1$	$2X+1$	$X+2$	$X+1$	2	$2X$	$2X+2$	X	1
$2X+2$	$2X+2$	$X+1$	$2X+1$	X	2	$X+2$	1	$2X$

Ainsi, si p est un nombre premier et si P un polynôme irréductible de degré f de $\mathbb{Z}_p[X]$, alors

$$\boxed{\mathbb{Z}_p[X]/\langle P\rangle}$$

[10] Pour le vérifier, un peu de patience. Attendez le résultat I.5.7.

[11] En effet, d'une manière générale, pour tous $P, Q \in \mathbb{K}[X]$, $P+\langle X^2+1\rangle = Q+\langle X^2+1\rangle$ si et seulement si P et Q ont même reste après division par $X^2 + 1$.

est un champ à p^f éléments. Un moyen commode d'en coder les éléments est de considérer les f-uples d'éléments de $\mathbb{Z}_p$ correspondant aux f-uples des coefficients des polynômes sur $\mathbb{Z}_p$ de degré strictement inférieur à f. Ainsi, sur notre exemple, ces couples sont $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,0)$, $(2,1)$ et $(2,2)$. Le table de multiplication reprise ci-dessus est codée comme suit.

$\cdot$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,2)$	$(0,2)$	$(0,1)$	$(2,0)$	$(2,2)$	$(2,1)$	$(1,0)$	$(1,2)$	$(1,1)$
$(1,0)$	$(1,0)$	$(2,0)$	$(0,2)$	$(1,2)$	$(2,2)$	$(0,1)$	$(1,1)$	$(2,1)$
$(1,1)$	$(1,1)$	$(2,2)$	$(1,2)$	$(2,0)$	$(0,1)$	$(2,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(1,2)$	$(2,1)$	$(2,2)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(0,1)$
$(2,0)$	$(2,0)$	$(1,0)$	$(0,1)$	$(2,1)$	$(1,1)$	$(0,2)$	$(2,2)$	$(1,2)$
$(2,1)$	$(2,1)$	$(1,2)$	$(1,1)$	$(0,2)$	$(2,0)$	$(2,2)$	$(1,0)$	$(0,1)$
$(2,2)$	$(2,2)$	$(1,1)$	$(2,1)$	$(1,0)$	$(0,2)$	$(1,2)$	$(0,1)$	$(2,0)$

Pour obtenir un codage encore plus commode, il suffit de considérer les f-uples d'éléments de $\mathbb{Z}_p$ comme des écritures de nombres en base p. Ainsi, à $(x_{f-1},\dots,x_0) \in (\mathbb{Z}_p)^f$ correspond l'entier

$$\sum_{i=0}^{f-1} x_i\, p^i.$$

La table de multiplication précédente peut donc encore se réécrire

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	6	8	7	3	5	4
3	3	6	2	5	8	1	4	7
4	4	8	5	6	1	7	2	3
5	5	7	8	1	3	4	6	1
6	6	3	1	7	4	2	8	5
7	7	5	4	2	6	8	3	1
8	8	4	7	3	2	5	1	6

Proposition I.3.10. *Tout polynôme de $\mathbb{K}[X]$ se décompose de manière unique comme produit de polynômes irréductibles (à des facteurs constants et à l'ordre des facteurs près).*

En effet, $\deg P.Q = \deg P + \deg Q$ assure l'existence de la décomposition (si un polynôme n'est pas irréductible, il se factorise en un produit de deux polynômes de degré inférieur et cette procédure ne peut être répétée qu'un nombre fini de fois). L'unicité de la décomposition découle du lemme suivant.

Lemme I.3.11. *Si $P \in \mathbb{K}[X]$ est irréductible et si P divise $F.G$, alors P divise F ou G.*

Démonstration. Supposons que P ne divise pas F. Cela signifie que F n'appartient pas à $\langle P\rangle$. Dès lors, $\langle P\rangle$ est inclus strictement dans $\langle P, F\rangle$. Or, par le corollaire I.3.7, $\langle P\rangle$ est maximal. Donc, $\langle P, F\rangle = \mathbb{K}[X]$ contient 1 et il existe des polynômes S et T tels que $1 = S.P+T.F$. De là, $G = SPG+TFG$ et puisque P divise chacun des deux termes de la somme, on en conclut que P divise G.

■

Remarque I.3.12. D'une certaine façon, on peut dire que les polynômes irréductibles jouent, dans l'ensemble des polynômes à coefficients dans $\mathbb{K}$, le même rôle que les nombres premiers, dans l'ensemble des entiers.

4. Eléments algébriques

Dans la section précédente, nous avons obtenu un moyen commode pour générer des champs finis (pour l'instant, nous sommes en mesure de construire un champ à p^f éléments pour tout nombre premier $p \geq 2$, à condition qu'il existe au moins un polynôme irréductible de degré f sur $\mathbb{Z}_p$). Dans cette section, nous obtenons une construction alternative en considérant l'extension d'un champ $\mathbb{K}$ par un élément algébrique (cf. proposition I.4.11).

Soient $\mathbb{K}$ et $\mathbb{L}$ deux champs tels que $\mathbb{L}$ est une extension de $\mathbb{K}$. Cette supposition sera employée tout au long de la section.

Définition I.4.1. Un élément $\alpha \in \mathbb{L}$ est *algébrique* sur $\mathbb{K}$ s'il existe un polynôme P à coefficients dans $\mathbb{K}$ tel que $P(\alpha) = 0$. L'ensemble $\mathcal{P}_\alpha$ des polynômes à coefficients dans $\mathbb{K}$ et annulés par α est un idéal de $\mathbb{K}[X]$. Puisque $\mathbb{K}[X]$ est principal, il existe un polynôme M_α que nous pouvons supposer être monique[12] tel que

$$\boxed{\mathcal{P}_\alpha = \{P \in \mathbb{K}[X] \mid P(\alpha) = 0\} = \langle M_\alpha\rangle.}$$

On appelle M_α le *polynôme minimum* de α. Si $\alpha' \in \mathbb{L}$ est tel que $M_\alpha(\alpha') = 0$, alors α' est un *conjugué* de α sur $\mathbb{K}$.

Lemme I.4.2. *Soit $\alpha \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$ ayant M_α comme polynôme minimum.*

i) *Le polynôme M_α est irréductible sur $\mathbb{K}$.*
ii) *Pour tout polynôme $P \in \mathbb{K}[X]$, $P(\alpha) = 0$ si et seulement si M_α divise P.*
iii) *M_α est l'unique polynôme monique de degré minimum dans $\mathbb{K}[X]$ annulé par α.*
iv) *Si P est un polynôme monique irréductible sur $\mathbb{K}$ annulé par α, alors $P = M_\alpha$.*

[12] S'il ne l'était pas, il suffit de le multiplier par l'inverse du coefficient du terme dominant.

Démonstration. i) Supposons que M_α puisse être factorisé en $M_\alpha = P.Q$ avec $0 < \deg P, \deg Q < \deg M_\alpha$. Alors, on a $M_\alpha(\alpha) = P(\alpha).Q(\alpha) = 0$ et on en conclut que P ou Q doit appartenir à $\mathcal{P}_\alpha$. Dès lors, M_α doit diviser P ou Q ce qui est impossible au vu de leur degré respectif.

Le point ii) est immédiat. Passons au point iii). Tout polynôme monique de $\mathbb{K}[X]$ annulé par α appartient à $\mathcal{P}_\alpha$ et est donc un multiple de M_α. Par conséquent, il est soit égal à M_α soit de degré strictement supérieur.

Pour le point iv), cela découle directement du fait que $\mathcal{P}_\alpha = \langle M_\alpha \rangle$. Pour le lecteur peu convaincu, voici une argumentation supplémentaire. Supposons que P est un polynôme monique irréductible sur $\mathbb{K}$ annulé par α. On effectue la division euclidienne de P par M_α, $P = Q.M_\alpha + R$ avec $\deg R < \deg M_\alpha$. Soit $R = 0$ et dans ce cas, puisque P est irréductible, on en conclut que $Q = 1$ et que $P = M_\alpha$. Soit $R \neq 0$. Dans ce cas, on en conclut que $P(\alpha) = R(\alpha) = 0$ ce qui, au vu de iii), est impossible car $\deg R < \deg M_\alpha$.

■

Remarque I.4.3. Si α' est un conjugué de α, alors ils ont le même polynôme minimum, i.e., $M_\alpha = M_{\alpha'}$. En effet, avec les notations précédentes, puisque $M_\alpha(\alpha') = 0$, on a que $M_\alpha \in \mathcal{P}_{\alpha'} = \langle M_{\alpha'} \rangle$ (i.e., $M_{\alpha'}$ divise M_α). La conclusion suit car M_α et $M_{\alpha'}$ sont tous deux des polynômes moniques irréductibles.

Exemple I.4.4. Le nombre d'or $\tau = (1 + \sqrt{5})/2 \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car il est racine du polynôme $M_\tau(X) = X^2 - X - 1$ qui est le polynôme minimum de τ. Son conjugué est $(1 - \sqrt{5})/2$.

Dans l'exemple I.1.15, nous avions considéré l'extension de $\mathbb{Q}$ par l'élément $\sqrt{2} \in \mathbb{R}$ algébrique sur $\mathbb{Q}$ et nous avions vérifié que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ était fini (autrement dit que $\mathbb{Q}(\sqrt{2})$ est une extension finie de $\mathbb{Q}$). Ce résultat est en fait tout à fait général.

Théorème I.4.5. *L'élément $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ si et seulement si $[\mathbb{K}(\alpha) : \mathbb{K}]$ est fini. En particulier, le degré de l'extension $[\mathbb{K}(\alpha) : \mathbb{K}]$ est égal au degré du polynôme minimum de α sur $\mathbb{K}$.*

La démonstration de ce résultat peut se faire à l'aide de quelques remarques.

Remarque I.4.6. Si $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et si son polynôme minimum est de degré d, alors tout élément de l'extension de champ $\mathbb{K}(\alpha)$ s'exprime comme combinaison linéaire à coefficients dans $\mathbb{K}$ des éléments $1, \alpha, \ldots, \alpha^{d-1}$. (Autrement dit, comme un polynôme en α à coefficients dans $\mathbb{K}$ et de degré $< d$.)

En effet, un élément[13]

$$P(\alpha) = \sum_{i=0}^{n} k_i\, \alpha^i, \quad k_i \in \mathbb{K}$$

appartient à $\mathbb{K}(\alpha)$ (on l'obtient en appliquant un nombre fini de sommes, de produits et de différences à des éléments de $\mathbb{K} \cup \{\alpha\}$). En effectuant la division euclidienne de $P(X)$ par M_α, il vient

$$P(X) = Q(X).M_\alpha(X) + R(X) \text{ avec } \deg R < d.$$

La conclusion suit en considérant l'évaluation de cette expression en α ($M_\alpha(\alpha) = 0$).

Cependant, un élément arbitraire de $\mathbb{K}(\alpha)$ est de la forme $P(\alpha).(Q(\alpha))^{-1}$ où nous pouvons supposer, par le point précédent, que $Q(X)$ est de degré $< d$. Puisque $\deg Q < \deg M_\alpha$, on en tire que

$$\langle M_\alpha \rangle \subsetneq \langle Q, M_\alpha \rangle$$

et M_α étant irréductible, $\langle M_\alpha \rangle$ est maximal et $\langle Q, M_\alpha \rangle = \mathbb{K}[X] \ni 1$. De là, il existe des polynômes S, T tels que $1 = S.M_\alpha + T.Q$ et la conclusion suit en évaluant cette dernière expression en α. L'inverse de $Q(\alpha)$ est donc un polynôme en α.

Pour conclure, $P(\alpha).(Q(\alpha))^{-1}$ se ramène donc à un produit de deux polynômes en α, puis par la première partie, à un polynôme en α de degré $< d$. Ainsi, $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ forment une partie génératrice de $\mathbb{K}(\alpha)$. Ces éléments sont aussi linéairement indépendants sur $\mathbb{K}$ car sinon, on disposerait d'une relation linéaire à coefficients dans $\mathbb{K}$ les liant et donc d'un polynôme de degré $< d$ de $\mathbb{K}[X]$ annulé par α, ce qui est impossible.

La réciproque est immédiate.

Remarque I.4.7. Si $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ est fini, alors les $n + 1$ éléments

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

sont linéairement dépendants sur $\mathbb{K}$. On en tire une relation linéaire à coefficients dans $\mathbb{K}$ liant ces éléments, i.e., α est algébrique sur $\mathbb{K}$.

Exemple I.4.8. Un utilisant les constructions développées dans la remarque I.4.6, on peut montrer que

$$\frac{2\tau^2 + \tau - 3}{\tau^3 + \tau^2 - \tau + 4} = \frac{10}{22}\,\tau - \frac{7}{22}$$

où τ est le nombre d'or. Ceci illustre le fait que tout élément de $\mathbb{Q}(\tau)$ se réexprime sous la forme $a\,\tau + b$ avec $a, b \in \mathbb{Q}$.

Proposition I.4.9. *L'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un sous-champ de $\mathbb{L}$.*

[13] L'ensemble des valeurs des polynômes de $\mathbb{K}[X]$ évalués en α se note souvent $\mathbb{K}[\alpha]$.

Démonstration. Montrons que si α et β sont algébriques sur $\mathbb{K}$, alors $\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1} le sont aussi. On va montrer que tous ces éléments appartiennent à une extension convenable de $\mathbb{K}$, contenue dans $\mathbb{L}$ et de dimension finie sur $\mathbb{K}$. Cela suffit au vu du théorème I.4.5.

L'extension $M = \mathbb{K}(\alpha)$ est une extension finie de $\mathbb{K}$ et contient α. L'élément β est algébrique sur $\mathbb{K}$. Il est donc aussi algébrique sur M. En appliquant le même raisonnement, l'extension $M' = M(\beta)$ est contenue dans $\mathbb{L}$ et de dimension finie sur M. En se rappelant le résultat bien connu de "la base télescopique", on a

$$[M' : \mathbb{K}] = [M' : M][M : \mathbb{K}]$$

et donc M' est une extension de $\mathbb{K}$ de dimension finie sur $\mathbb{K}$. Puisque M' est un champ qui contient α et β, il contient $\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1}.

■

Définition I.4.10. On dit que $\mathbb{L}$ est une *extension algébrique* de $\mathbb{K}$ si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

La proposition suivante est à mettre en parallèle avec la proposition I.3.8. Elle permet, comme nous le verrons sur un exemple, de construire des champs finis "par extension" et non par quotient.

Proposition I.4.11. *Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$. L'anneau quotient $\mathbb{K}[X]/\langle M_\alpha\rangle$ est isomorphe à l'extension de champ $\mathbb{K}(\alpha)$.*

Démonstration. Il s'agit d'une simple application du premier théorème d'isomorphie. Soit l'application $A/\ker\Phi \cong \operatorname{Im}\Phi$

$$\Phi : \mathbb{K}[X] \to \mathbb{L} : P \mapsto P(\alpha)$$

qui à un polynôme associe son évaluation en α. Il est clair qu'il s'agit d'un homomorphisme[14] d'anneaux. Le noyau de cette application est $\ker\Phi = \mathcal{P}_\alpha = \langle M_\alpha\rangle$. Par le corollaire I.3.7, $\langle M_\alpha\rangle$ est maximal et donc, par le théorème I.2.6, $\mathbb{K}[X]/\ker\Phi$ est un champ. Par le premier théorème d'isomorphie, ce champ est isomorphe à l'image de Φ. Il nous suffit donc pour conclure de montrer que

$$\operatorname{Im}\Phi = \{P(\alpha) \mid P \in \mathbb{K}[X]\} = \mathbb{K}(\alpha).$$

Il est clair que α appartient à $\operatorname{Im}\Phi$ (il suffit de prendre $P(X) = X$) et que $\mathbb{K}$ est inclus dans $\operatorname{Im}\Phi$ (il suffit de prendre $P(X) = k$, pour tout $k \in \mathbb{K}$). Par conséquent, $\mathbb{K}(\alpha)$ est inclus dans $\operatorname{Im}\Phi$. Montrons l'autre inclusion. Soit $P(\alpha)$ un élément quelconque de $\operatorname{Im}\Phi$, $P \in \mathbb{K}[X]$. Il est évident que $P(\alpha)$ est de la forme

$$P(\alpha) = k_0 + k_1\,\alpha + \cdots + k_d\,\alpha^d, \quad k_0, \ldots, k_d \in \mathbb{K}$$

et appartient donc à $\mathbb{K}(\alpha)$.

[14] $(P+Q)(\alpha) = P(\alpha) + Q(\alpha)$, $(P.Q)(\alpha) = P(\alpha).Q(\alpha)$

	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
1	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	α	2α	$1+2\alpha$	1	$1+\alpha$	$2+\alpha$	$2+2\alpha$	2
$1+\alpha$	$1+\alpha$	$2+2\alpha$	1	$2+\alpha$	2α	2	α	$1+2\alpha$
$2+\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$	2α	2	$2+2\alpha$	1	α
2α	2α	α	$2+\alpha$	2	$2+2\alpha$	$1+2\alpha$	$1+\alpha$	1
$1+2\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	1	$1+\alpha$	2	2α
$2+2\alpha$	$2+2\alpha$	$1+\alpha$	2	$1+2\alpha$	α	1	2α	$2+\alpha$

TABLE I.1. Table de multiplication de $\mathbb{Z}_3(\alpha)$.

■

Exemple I.4.12. Soit le champ $\mathbb{Z}_3$ et le polynôme $P(X) = X^2 + X + 2$ de $\mathbb{Z}_3[X]$. Ce polynôme est irréductible[15] sur $\mathbb{Z}_3[X]$. Dans l'extension de champ $\mathbb{L} = \mathbb{Z}_3[X]/\langle P\rangle$, l'élément $\alpha = X + \langle P\rangle$ annule P. En effet,

$$P(\alpha) = X^2 + X + 2 + \langle P\rangle = 0 + \langle P\rangle$$

est bien le zéro de $\mathbb{L}$. Autrement dit, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{Z}_3$ et possède P comme polynôme minimum. Ainsi, $\mathbb{Z}_3(\alpha)$ est un champ à 9 éléments

$$0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2.$$

On y effectue les sommes et les produits comme dans $\mathbb{Z}_3[\alpha]$ (i.e., avec des polynômes en α) en se rappelant que $\alpha^2 + \alpha + 2 = 0$. La table de multiplication est reprise dans le tableau I.1. Par exemple, dans $\mathbb{Z}_3[\alpha]$, on a $(1+2\alpha)(2+2\alpha) = \alpha^2 + 2$ et en se rappelant que $\alpha^2 + \alpha + 2 = 0$, on trouve $\alpha^2 + 2 = 2\alpha$.

Observons que $\beta = 2X + 2 + \langle P\rangle = 2\alpha + 2$ est aussi tel que $P(\beta) = 0$. En effet,

$$P(\beta) = (2X+2)^2 + 2X + 2 + 2 + \langle P\rangle = X^2 + X + 2 + \langle P\rangle = 0 + \langle P\rangle.$$

Ainsi, on aurait également pu construire l'extension $\mathbb{Z}_3(\beta)$, isomorphe à $\mathbb{Z}_3(\alpha)$ par l'isomorphisme envoyant α sur β et laissant les éléments de $\mathbb{Z}_3$ inchangés.

Remarque I.4.13. L'exemple précédent s'adapte aisément à un champ arbitraire $\mathbb{K}$ et à un polynôme irréductible P de $\mathbb{K}[X]$ de degré d.

Si $\mathbb{K}$ est fini et contient t éléments et si α "annule" P, alors $\mathbb{K}(\alpha)$ est un champ à t^d éléments.

De même, si $\mathbb{K}$ est un champ et si α et β annulent un même polynôme irréductible $P \in \mathbb{K}[X]$, alors les extensions $\mathbb{K}(\alpha)$ et $\mathbb{K}(\beta)$ sont isomorphes par l'isomorphisme envoyant α sur β et laissant les éléments de $\mathbb{K}$ inchangés. La justification est immédiate.

[15] Encore une fois, nous anticipons. Attendez le résultat I.5.7.

4.1. Transcendance. La proposition I.4.11 répond à l'objectif que nous nous étions fixé en début de section. Néanmoins, on peut s'interroger sur la structure de $\mathbb{K}(\alpha)$ si α n'est pas algébrique.

Définition I.4.14. Soit $\mathbb{K}$ un champ (ou même plus simplement un anneau intègre). Le *champ des fractions rationnelles* à coefficients dans $\mathbb{K}$ (ou *champ des quotients*) noté[16] $\mathbb{K}(x)$ est défini comme le quotient de l'ensemble des couples

$$\{(P,Q) \mid P,Q \in \mathbb{K}[x],\, Q \neq 0\}$$

par la relation d'équivalence $(P,Q) \sim (P',Q')$ si et seulement si $P.Q' = P'.Q$. Il s'agit de la même construction que pour $\mathbb{Q}$. On y définit naturellement la somme et le produit de deux éléments du quotient. Par convention, on notera un représentant de la classe d'équivalence de (P,Q) par $\frac{P}{Q}$.

Définition I.4.15. Si $\alpha \in \mathbb{L}$ n'est pas algébrique sur $\mathbb{K}$, alors on dit qu'il est *transcendant* sur $\mathbb{K}$.

Lemme I.4.16. *Soient $\mathbb{K}$ et $\mathbb{L}$ deux champs. Si $\Phi : \mathbb{K} \to \mathbb{L}$ est un homomorphisme, alors il est injectif (i.e., c'est un plongement).*

Démonstration. Puisque Φ est un homomorphisme, son noyau $\ker \Phi$ est un idéal de $\mathbb{K}$. Or $\mathbb{K}$ est un champ (cf. remarque I.2.3), donc $\ker \Phi$ est égal à $\{0\}$ ou $\mathbb{K}$. La seconde possibilité ne peut être envisagée car $\Phi(1_{\mathbb{K}}) = 1_{\mathbb{L}} \neq 0_{\mathbb{L}}$ et donc $1_{\mathbb{K}}$ ne peut appartenir à $\ker \Phi$. Enfin, rappelons que si le noyau d'une application est réduit à $\{0\}$, alors cette application est injective.

■

Proposition I.4.17. *Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$ un élément transcendant sur $\mathbb{K}$. Le champ $\mathbb{K}(\alpha)$ est isomorphe à $\mathbb{K}(x)$.*

La preuve se base sur un schéma identique à celle de la proposition I.4.11.

Démonstration. Soit l'application

$$\Phi : \mathbb{K}(x) \to \mathbb{L} : (P,Q) \mapsto P(\alpha).Q(\alpha)^{-1} =: \frac{P(\alpha)}{Q(\alpha)}.$$

Il est clair qu'il s'agit d'un homomorphisme. Au vu du lemme précédent, Φ est injectif mais est aussi trivialement surjectif sur son image. Autrement dit, $\mathbb{K}(x)$ est isomorphe à $\operatorname{Im}\Phi$ et il nous reste à vérifier que $\operatorname{Im}\Phi = \mathbb{K}(\alpha)$. Il est clair que $\operatorname{Im}\Phi \supseteq \mathbb{K}(\alpha)$. Montrons l'autre inclusion. Un élément quelconque de $\operatorname{Im}\Phi$ est de la forme

$$(k_0 + k_1\,\alpha + \cdots + k_d\,\alpha^d).(\ell_0 + \ell_1\,\alpha + \cdots + \ell_e\,\alpha^e)^{-1},\ k_0,\ldots,k_d,\ell_0,\ldots,\ell_e \in \mathbb{K}$$

et appartient bien évidemment à $\mathbb{K}(\alpha)$.

■

[16] Attention à ne pas confondre les notations $\mathbb{K}(\alpha)$, extension de champ et $\mathbb{K}(x)$, champ des fractions ! Ces notations sont cependant tout à fait compatibles, puisque les éléments de $\mathbb{K}(\alpha)$ ne sont rien d'autres que les fractions rationnelles de $\mathbb{K}(x)$ évaluées en α. On avait déjà fait usage de cette convention pour $\mathbb{K}[\alpha]$, l'ensemble des évaluations des polynômes de $\mathbb{K}[X]$ évalués en α.

5. Racines d'un polynôme

Dans cette section, $\mathbb{K}$ est encore un champ et P est un polynôme de $\mathbb{K}[X]$ de degré $d > 0$.

Définition I.5.1. L'élément $\alpha \in \mathbb{K}$ est une *racine* de P si $P(\alpha) = 0$.

Proposition I.5.2. *L'élément $\alpha \in \mathbb{K}$ est une racine de P si et seulement si $X - \alpha$ divise P.*

Démonstration. La condition est trivialement suffisante. Montrons qu'elle est nécessaire. Effectuons la division euclidienne de P par $X - \alpha$, on trouve $P(X) = Q(X).(X-\alpha)+R$ avec $\deg R < 1$. Puisque $P(\alpha) = 0$, cela entraîne que R doit être nul.

■

Remarque I.5.3. Soit $\alpha \in \mathbb{K}$. L'évaluation de P en α est égale au reste de la division de P par $X - \alpha$. En effet, $P(X) = Q(X).(X - \alpha) + R$ avec $\deg R < 1$.

Définition I.5.4. Si $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P, alors on dit que α est une racine de *multiplicité* m.

Les deux remarques suivantes attirent l'attention du lecteur sur les différences qu'il peut exister entre $\mathbb{K}[X]$ (avec $\mathbb{K}$ un champ quelconque) et les automatismes que l'on connaît sur $\mathbb{C}[z]$.

Remarque I.5.5. Puisque la factorisation d'un polynôme est "essentiellement" unique[17], la somme des racines de P comptées avec leur multiplicité ne peut excéder d. Par exemple, le polynôme $X^3-X^2+X-1 = (X^2+1)(X-1)$ possède une seule racine dans $\mathbb{R}$.

Remarque I.5.6. Si $P \in \mathbb{K}[X]$ ne possède pas de racine dans $\mathbb{K}$, cela n'entraîne pas qu'il soit nécessairement irréductible. En effet, le polynôme $(X^2 + 1)(X^2 + 2) = X^4 + 3X^2 + 2$ de $\mathbb{R}[X]$ ne possède aucune racine réelle mais il n'est pas irréductible.

Proposition I.5.7. *Soit $P \in \mathbb{K}[X]$ un polynôme de degré deux ou trois. Si P n'a pas de racine dans $\mathbb{K}$, alors P est irréductible sur $\mathbb{K}$.*

Démonstration. En effet, sinon, il serait réductible et dans la décomposition de P en un produit de deux facteurs, un des facteurs au moins serait de degré un.

■

[17] En supposant les différents facteurs moniques.

5.1. Dérivation formelle. Sur un champ arbitraire (et en particulier sur un champ fini), il n'est pas possible de dériver une fonction comme en analyse réelle par passage à la limite. Néanmoins, on peut définir la dérivée "formelle" d'un polynôme en copiant la formule usuelle des polynômes réels. Nous allons voir que cette opération conserve certaines propriétés de la dérivée usuelle.

Si k est un élément d'un champ $\mathbb{K}$ et n un entier, alors la notation $n\,k$ désigne en fait l'élément de $\mathbb{K}$, $\underbrace{k+\cdots+k}_{n\times}$.

Définition I.5.8. Soit $P = k_0 + k_1X + k_2X^2 \cdots + k_dX^d$ un polynôme de $\mathbb{K}[X]$. On définit la *dérivée (formelle)* du polynôme P par

$$\mathrm{D}_X P = k_1 + 2\,k_2\,X + \cdots + d\,k_d\,X^{d-1}.$$

Ainsi défini, il s'agit simplement d'une application de $\mathbb{K}[X]$ dans lui-même jouissant des propriétés usuelles

- $\mathrm{D}_X(P+Q) = \mathrm{D}_X P + \mathrm{D}_X Q$,
- $\mathrm{D}_X(P.Q) = \mathrm{D}_X P.Q + P.\mathrm{D}_X Q$,
- $\mathrm{D}_X(k.P) = k\mathrm{D}_X P$, si $k \in \mathbb{K}$.

Proposition I.5.9. *L'élément $\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ de multiplicité au moins deux si et seulement si $P(\alpha) = (\mathrm{D}_X P)(\alpha) = 0$.*

Démonstration. Si α est une racine de multiplicité au moins deux de P, alors $P = (X-\alpha)^2 Q$ et $\mathrm{D}_X P = (X-\alpha)(2Q + (X-\alpha)\mathrm{D}_X Q)$ et donc, $P(\alpha) = (\mathrm{D}_X P)(\alpha) = 0$.

Passons à la réciproque. Si $P(\alpha) = 0$, alors $P = (X-\alpha)Q$ et donc $\mathrm{D}_X P = (X-\alpha)\mathrm{D}_X Q + Q$. Or $(\mathrm{D}_X P)(\alpha) = 0$ et l'on en tire $Q(\alpha) = 0$. Par conséquent, $Q = (X-\alpha)R$ et $P = (X-\alpha)^2 R$ ce qui suffit.

■

Corollaire I.5.10. *Soient $\mathbb{L}$ un extension du champ $\mathbb{K}$ et $\alpha \in \mathbb{L}$, un élément algébrique sur $\mathbb{K}$. L'élément α est racine simple de son polynôme minimum M_α.*

Démonstration. Si $(\mathrm{D}_X P)(\alpha) = 0$, alors le polynôme $\mathrm{D}_X P \in \mathbb{K}[X]$ serait de degré strictement inférieur à α et annulé par α. Ceci est impossible.

■

On peut introduire naturellement la dérivée (formelle) d'ordre $k \geq 2$ comme $\mathrm{D}_X^k P = \mathrm{D}_X^{k-1}(\mathrm{D}_X P)$.

Remarque I.5.11. Dans $\mathbb{C}[z]$ on dispose d'un résultat plus fort que celui énoncé ci-dessus. En effet, dans ce cas, il est bien connu que α est une racine de multiplicité m d'un polynôme $P \in \mathbb{C}[z]$ non nul si et seulement si $P(\alpha) = (\mathrm{D}_X P)(\alpha) = \cdots = (\mathrm{D}_X^{m-1} P)(\alpha) = 0$ et $(\mathrm{D}_X^m P)(\alpha) \neq 0$. Cependant, un tel résultat n'est en général pas vrai sur un champ fini ! Ainsi, le polynôme de $\mathbb{Z}_3[X]$, $X^4 - X = (X^3-1)X = (X-1)^3 X$ possède 1 comme racine triple

mais pourtant toutes les dérivées de ce polynôme évaluées en 1 sont nulles ! (Cela dépend bien évidemment de la caractéristique du champ $\mathbb{K}$. . . .)

Nous rappelerons plus loin la définition de la caractéristique.

Ainsi, pour un champ $\mathbb{K}$ de **caractéristique nulle**, la formule de Taylor bien connue reste valable dans $\mathbb{K}[X]$.

Proposition I.5.12 (Formule de Taylor). *Soient $\mathbb{K}$ un champ de caractéristique nulle, $P \in \mathbb{K}[X]$ un polynôme de degré d et α un élément de $\mathbb{K}$. On a*

$$P(X) = \sum_{i=0}^{d} \frac{(\mathrm{D}_X^i P)(\alpha)}{i!}(X-\alpha)^i.$$

Corollaire I.5.13. *Soit $\mathbb{K}$ un champ de caractéristique nulle. Un élément $\alpha \in \mathbb{K}$ est racine de multiplicité m d'un polynôme $P \in \mathbb{K}[X]$ non nul si et seulement si*

$$P(\alpha) = (\mathrm{D}_X P)(\alpha) = \cdots = (\mathrm{D}_X^{m-1} P)(\alpha) \text{ et } (\mathrm{D}_X^m P)(\alpha) \neq 0.$$

Démonstration. Cela résulte directement de la formule de Taylor. ∎

5.2. Corps de rupture d'un polynôme.

Définition I.5.14. Etant donné le polynôme $P \in \mathbb{K}[X]$ de degré d, il existe une plus petite extension de champ $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P se factorise en un produit de polynômes de degré un. De manière équivalente, cela signifie que P a exactement d racines dans $\mathbb{L}$ comptées avec leur multiplicité. Cette extension est **unique** à un isomorphisme près (cf. remarque I.5.21) et on l'appelle[18] le *corps*[19] *de rupture* de P sur $\mathbb{K}$.

Remarque I.5.15. Soit $P \in \mathbb{K}[X]$ de degré d. L'extension $\mathbb{L}$ est le corps de rupture de P sur $\mathbb{K}$ s'il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ tels que

$$P(X) = k\,(X-\alpha_1)\cdots(X-\alpha_d)$$

où $k \in \mathbb{K}$ est le coefficient dominant de P et

$$\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_d).$$

Exemple I.5.16. Comme nous le vérifierons très vite, le corps de rupture de $X^2 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2})$.

Nous nous contenterons de démontrer les deux résultats suivants prouvant l'existence d'un champ dans lequel P se factorise. Le premier de ces résultats correspond au lemme de (Gauss-) d'Alembert vu dans le cas des polynômes à coefficients complexes. Sa preuve utilise le même argument que celui développé dans l'exemple I.4.12.

[18] Certains auteurs parlent parfois de corps de rupture d'un polynôme pour désigner une extension contenant une racine de P et dès lors, pour ces mêmes auteurs, ce que nous avons décidé d'appeler "corps de rupture" est alors appelé *corps de décomposition*.

[19] Il s'agit même d'un champ.

Théorème I.5.17. *Soit $P \in \mathbb{K}[X]$ un polynôme à coefficients dans le champ $\mathbb{K}$. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P admette au moins une racine dans $\mathbb{L}$.*

Démonstration. Il suffit de démontrer le résultat pour un facteur irréductible Q de P. Ainsi, l'anneau quotient $\mathbb{K}[X]/\langle Q\rangle$, noté $\mathbb{L}$, est un champ (cf. proposition I.3.8). Clairement, $\mathbb{K}$ est isomorphe à un sous-champ de $\mathbb{L}$ (il suffit de considérer le plongement $\Phi : \mathbb{K} \to \mathbb{L} : k \mapsto k + \langle Q\rangle$). Considérons à présent l'homomorphisme canonique

$$\pi : \mathbb{K}[X] \to \mathbb{L} = \mathbb{K}[X]/\langle Q\rangle : R \mapsto R + \langle Q\rangle$$

et notons $\alpha = \pi(X) \in \mathbb{L}$. Ainsi[20], puisque que π est un homomorphisme d'anneaux

$$Q(\alpha) = Q(\pi(X)) = \pi(Q(X)) = 0$$

car le zéro de $\mathbb{K}[X]/\langle Q\rangle$ est $0 + \langle Q\rangle = \pi(Q)$.

■

Exemple I.5.18. Nous considérons le polynôme irréductible $Q = X^2 + 1$ de $\mathbb{R}[X]$ et montrons que l'anneau quotient

$$\mathbb{R}[X]/\langle X^2 + 1\rangle = \{a + bX + \langle X^2 + 1\rangle \mid a, b \in \mathbb{R}\}$$

est un champ isomorphe à $\mathbb{C}$. En effet, si on dénote une classe de l'anneau quotient simplement par $a + bX$, alors le produit de deux classes est donné par

$$(a + bX).(a' + b'X) = aa' + (ab' + a'b)X + bb'X^2 = aa' - bb' + (ab' + a'b)X$$

car $bb'X^2 = bb'(X^2 + 1) - bb'$. Dès lors, l'application

$$\Phi : \mathbb{R}[X]/\langle X^2 + 1\rangle \to \mathbb{C} : a + bX + \langle X^2 + 1\rangle \mapsto a + i\,b$$

est bien un isomorphisme. On retrouve la multiplication usuelle des nombres complexes,

$$(a + i\,b).(a' + i\,b') = aa' - bb' + i\,(ab' + a'b).$$

Exemple I.5.19. Poursuivons l'exemple I.5.16 et considérons le quotient

$$\mathbb{Q}[X]/\langle X^2 - 2\rangle.$$

Une fois encore, nous noterons les éléments du quotient $a + bX$, $a, b \in \mathbb{Q}$. Il vient,

$$(a + bX).(a' + b'X) = aa' + (ab' + a'b)X + bb'X^2 = aa' + 2bb' + (ab' + a'b)X$$

car

$$bb'X^2 = bb'(X^2 - 2) + 2bb'$$

[20]Grâce au plongement Φ, les éléments de $\mathbb{K}$ peuvent être vus comme des éléments de $\mathbb{L}$. Ainsi, on peut considérer le polynôme Q non pas comme un polynôme à coefficients dans $\mathbb{K}$, mais comme un polynôme de $\mathbb{L}[X]$. De cette manière, il est naturel d'évaluer Q en un élément de $\mathbb{L}$.

et $\Phi : \mathbb{Q}[X]/\langle X^2-2\rangle \to \mathbb{Q}(\sqrt{2}) : a+bX+\langle X^2-2\rangle \mapsto a+\sqrt{2}\,b$ est un isomorphisme. En effet, on retrouve la règle du produit

$$(a+b\sqrt{2}).(a'+b'\sqrt{2}) = aa'+2bb'+\sqrt{2}(ab'+a'b).$$

Voici à présent l'analogue du théorème fondamental de l'algèbre pour les polynômes de $\mathbb{C}[z]$.

Corollaire I.5.20. *Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P se factorise en un produit de polynômes de degré un de $\mathbb{L}[X]$.*

Démonstration. On procède par récurrence sur le degré du polynôme en appliquant le théorème précédent. On peut observer, au vu de la proposition I.4.11, que pour construire cette extension, on peut adjoindre progressivement à $\mathbb{K}$ des racines de P. En particulier, l'extension de $\mathbb{K}$ ainsi obtenue est de degré fini.

■

Remarque I.5.21. On peut montrer que si l'on dispose de deux corps de rupture sur $\mathbb{K}$ d'un polynôme $P \in \mathbb{K}[X]$, alors ces deux champs sont isomorphes par un isomorphisme laissant les éléments de $\mathbb{K}$ invariants et permutant les racines de P. A isomorphisme près, il n'existe donc qu'un corps de rupture de P sur $\mathbb{K}$.

Remarque I.5.22. Un champ $\mathbb{K}$ est *algébriquement clos* si tout polynôme non constant de $\mathbb{K}[X]$ se factorise complètement en un produit de polynômes de degré un. Cela revient à dire que chaque polynôme non constant de $\mathbb{K}[X]$ possède une racine dans $\mathbb{K}$. La plus petite extension de champ de $\mathbb{K}$ qui est algébriquement close est la *clôture algébrique* de $\mathbb{K}$, dénotée $\overline{\mathbb{K}}$. Par exemple, $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$ et $\mathbb{C}$ est algébriquement clos.

6. Champs finis

Rappelons tout d'abord que le théorème de Wedderburn stipule que tout corps fini est commutatif. Autrement dit, tout corps fini est un champ. Dès lors, dans cette section, nous nous intéressons uniquement aux *champs* finis.

Définition I.6.1. Si $(A,+,\cdot)$ est un anneau, on dénote par $(A^*,\cdot)$ le groupe multiplicatif des éléments inversibles dans A. En particulier, si on désigne par $\mathbb{F}_q$ un champ contenant q éléments[21], alors $\mathbb{F}_q^*$ est un groupe commutatif (pour la loi de multiplication) formé des $q-1$ éléments non nuls de $\mathbb{F}_q$.

[21] On rencontre aussi la notation équivalente $GF(q)$ où GF sont les initiales de "Galois Field".

Exemple I.6.2. On a $\mathbb{Z}_6^* = (\{1,5\},\cdot)$ et $\mathbb{Z}_5^* = (\{1,2,3,4\},\cdot)$. En effet, les tables de multiplication respectives sont données par

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

6.1. Caractéristique d'un champ. Commençons par rappeler ce qu'est la caractéristique d'un champ. Soit $\mathbb{K}$ un champ (ou même simplement un anneau intègre). Considérons l'*homomorphisme caractéristique* $\Phi : \mathbb{Z} \to \mathbb{K}$ qui est un homomorphisme d'anneaux défini par

$$\Phi(m) = \underbrace{1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}}}_{m \text{ fois}} =: m.1 \quad \text{, si } m \geq 0$$

et $\Phi(m) = -\Phi(-m)$, si $m < 0$ (en particulier, Φ est complètement caractérisé par le fait qu'il envoie $1 \in \mathbb{Z}$ sur l'unité de $\mathbb{K}$, $1_{\mathbb{K}}$ que l'on notera simplement 1).

Il est immédiat[22] que le noyau de Φ, $\ker\Phi$, est un idéal de $\mathbb{Z}$. Puisque $\mathbb{Z}$ est principal, il existe $n \geq 0$ tel que $\ker\Phi = \langle n\rangle = n\mathbb{Z}$. Cet entier n est appelé la *caractéristique* de $\mathbb{K}$. En vertu du premier théorème d'isomorphie, $\mathbb{Z}/\ker\Phi$ est isomorphe à l'image de Φ dans $\mathbb{K}$.

Si $n = 0$, alors $\ker\Phi = \{0\}$ et $\mathbb{Z}/\ker\Phi = \mathbb{Z}$ s'identifie à un sous-anneau de $\mathbb{K}$. Puisque le plus petit champ contenant $\mathbb{Z}$ est $\mathbb{Q}$, on en conclut que $\mathbb{K}$ contient un sous-champ isomorphe à $\mathbb{Q}$.

Si $n = 1$, alors $\ker\Phi = \mathbb{Z}$ et en particulier, $\Phi(1) = 0$. De plus, puisque Φ est un homomorphisme, on a aussi $\Phi(1) = 1$ et on aurait dans $\mathbb{K}$, $0 = 1$. Ceci est impossible dans un champ.

Si $n > 1$, puisque $\mathbb{K}$ est intègre, l'image de Φ dans $\mathbb{K}$ est un sous-anneau intègre. Pour conclure, rappelons que $\mathbb{Z}/n\mathbb{Z}$ est intègre (et même un champ) si et seulement si $n > 1$ est premier. Dans ce cas, la caractéristique n de $\mathbb{K}$ est un nombre premier et $\mathbb{K}$ contient donc un sous-champ isomorphe à $\mathbb{Z}_n$. (Remarquons en particulier que cela signifie que $\mathbb{K}$ est une extension de $\mathbb{Z}_n$.)

Remarque I.6.3. Nous venons donc de démontrer que tout champ fini $\mathbb{K}$ contient un champ isomorphe à $\mathbb{Z}_p$ avec p premier, appelé le *sous-champ premier* de $\mathbb{K}$. En effet, puisque $\mathbb{K}$ est fini, il ne peut contenir une copie de $\mathbb{Q}$. De plus, nous montrerons aisément l'unicité du sous-champ premier (cf. corollaire I.6.6), c'est-à-dire que $\mathbb{Z}_p$ est l'unique champ de la forme $\mathbb{Z}_m$ inclus dans $\mathbb{K}$.

Comme nous le verrons rapidement, deux champs de même caractéristique partagent de nombreuses propriétés. Dans un champ de caractéristique $p > 0$, on dispose du résultat suivant.

[22] Le noyau de tout homomorphisme est un idéal.

Théorème I.6.4 (Binôme de Newton "stupide"). *Si $\mathbb{K}$ est un champ de caractéristique p (p premier), alors pour tout $n \geq 1$, on a*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Démonstration. On procède par récurrence sur n. Si $n = 1$, alors la formule du binôme de Newton[23] donne

$$(a+b)^p = \sum_{k=0}^{p} \mathrm{C}_p^k a^k b^{p-k}.$$

On a

$$\mathrm{C}_p^k = \frac{p!}{k!\,(p-k)!}$$

et pour $0 < k < p$, le nombre premier p apparaît au numérateur mais pas au dénominateur. Ainsi, $p! = k!\,(p-k)!\,\mathrm{C}_p^k$, p ne divisant pas $k!\,(p-k)!$. On en conclut que C_p^k est un multiple de la caractéristique p et donc que $\mathrm{C}_p^k = 0$ dans $\mathbb{K}$.

Supposons le résultat satisfait pour $n-1$ et vérifions-le pour n. Il vient

$$(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n}.$$

Pour l'avant-dernière égalité, on a utilisé l'hypothèse de récurrence et pour la dernière, le cas $n = 1$.

■

Proposition I.6.5. *Soit $\mathbb{K}$ un champ fini de caractéristique $p > 1$. Il existe $n > 0$ tel que $\mathbb{K}$ contienne exactement p^n éléments.*

Démonstration. Le champ $\mathbb{K}$ contient un sous-champ isomorphe à $\mathbb{Z}_p$. On peut donc considérer $\mathbb{K}$ comme un $\mathbb{Z}_p$-vectoriel et si $[\mathbb{K} : \mathbb{Z}_p] = n$, alors $\#\mathbb{K} = p^n$ (comme nous l'avions déjà remarqué au point I.1.14.

■

Corollaire I.6.6. *Soit $\mathbb{K}$ un champ fini, le seul champ de la forme $\mathbb{Z}_q$, $q \geq 2$, inclus dans $\mathbb{K}$ est son sous-champ premier.*

Démonstration. Soit $\mathbb{K}$ un champ fini de caractéristique p, i.e., ayant $\mathbb{Z}_p$ comme sous-champ premier. Il contient p^n éléments. Si $\mathbb{Z}_q$ est un sous-champ de $\mathbb{K}$, on en tire que q doit diviser p^n (l'ordre d'un sous-groupe divise l'ordre du groupe). De plus, puisque $\mathbb{Z}_q$ est un champ, q est premier. Par conséquent, $q = p$.

■

[23] Que l'on peut appliquer ici car un champ est commutatif.

6.2. La fonction indicatrice d'Euler.

Définition I.6.7. La *fonction indicatrice d'Euler*[24] est définie par

$$\varphi(n) = \#\{x \mid 1 \leq x \leq n, \text{ pcgd}(x, n) = 1\}.$$

Elle compte donc le nombre de nombres $< n$ et premier avec n. Ainsi, les premières valeurs de cette fonction sont

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

et un graphique de la fonction est donné à la figure I.1.

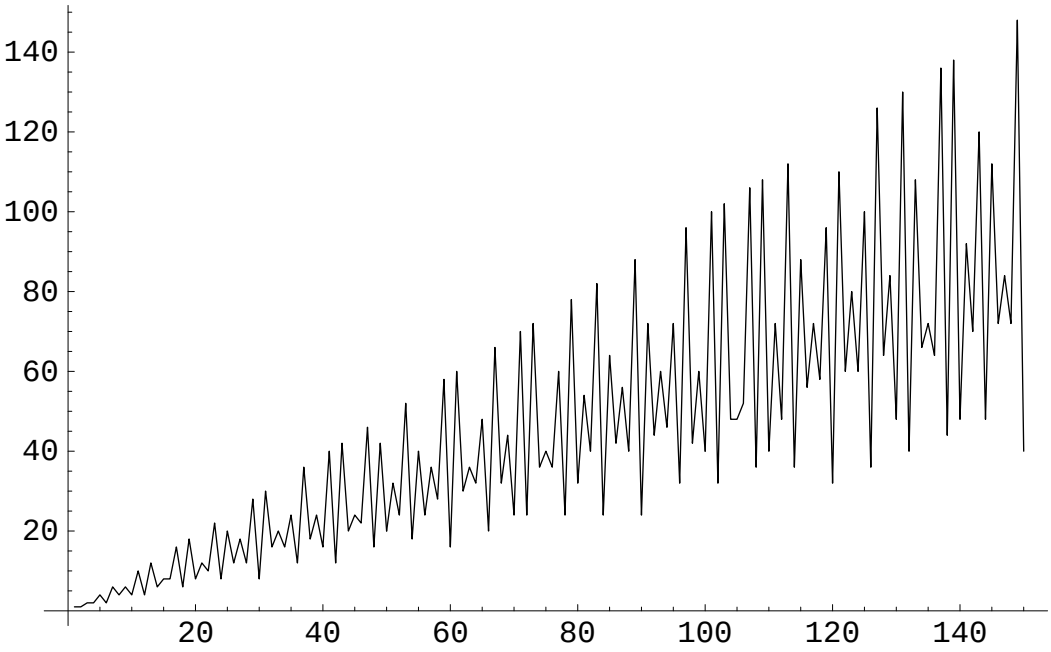


FIGURE I.1. Les premières valeurs de $\varphi(n)$.

Remarque I.6.8. Dans l'anneau $\mathbb{Z}_n$, le nombre d'éléments inversibles est exactement $\varphi(n)$. Autrement dit, le groupe multiplicatif $\mathbb{Z}_n^*$ est d'ordre $\varphi(n)$.

Lemme I.6.9. *La fonction φ est multiplicative, i.e., si m et n sont des entiers premiers entre eux, alors*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

[24]Dans `Mathematica`, on utilise la fonction `EulerPhi[n]`. On rencontre parfois la nomenclature *fonction totient* introduite par J.J. Sylvester.

Démonstration. Nous savons que, puisque m et n sont premiers entre eux, l'anneau $\mathbb{Z}_{mn}$ est isomorphe à $\mathbb{Z}_m \times \mathbb{Z}_n$. On en déduit un isomorphisme[25] de groupes entre $\mathbb{Z}_{mn}^*$ et $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

■

Corollaire I.6.10. *Si le nombre $n \geq 2$ se factorise en un produit de nombres premiers sous la forme $n = p_1^{k_1} \cdots p_r^{k_r}$, alors*

$$\boxed{\varphi(n) = \prod_{j=1}^{r} (p_j - 1)\, p_j^{k_j - 1}.}$$

Démonstration. D'après le lemme précédent, il nous suffit de vérifier que $\varphi(p^k) = (p-1)\, p^{k-1}$, p premier, $k \geq 1$. Pour ce faire, remarquons que les nombres entiers de l'intervalle $[1, p^k]$ qui ne sont pas premiers avec p^k sont les multiples de p appartenant à cet intervalle, i.e.,

$$p, 2p, 3p, \ldots, (p^{k-1} - 1)\, p, p^{k-1}\, p$$

qui sont en nombre p^{k-1}.

■

6.3. Deux applications classiques. Bien qu'immédiat, le résultat suivant est à la base du cryptosystème à clé publique RSA.

Théorème I.6.11 (Petit théorème de Fermat[26]). *Si* $\operatorname{pgcd}(a, m) = 1$, *alors*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Démonstration. Puisque $\operatorname{pgcd}(a, m) = 1$, a appartient au groupe multiplicatif $\mathbb{Z}_m^*$ des éléments inversibles de $\mathbb{Z}_m$. La conclusion découle du fait que l'ordre d'un élément divise l'ordre du groupe.

■

Remarque I.6.12. Le lecteur pourrait s'interroger sur le fait qu'il n'est nullement précisé dans l'énoncé précédent si $a < m$ ou si $a > m$. Il suffit de remarquer que si $a > m$, alors, en effectuant la division euclidienne $a = q.m + a'$ avec $a' < m$. Bien évidemment, si $\operatorname{pgcd}(a, m) = 1$, alors il en est de même pour $\operatorname{pgcd}(a', m) = 1$ et $a \equiv a' \mod m$.

Remarque I.6.13. Dans la littérature, on trouve parfois une autre formulation d'un résultat également appelé petit théorème de Fermat. Soient p un nombre premier et $n < p$ un entier. On a

$$n^p \equiv n \mod p.$$

[25] Soit $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ l'isomorphisme en question. Ainsi, à tout élément $z \in \mathbb{Z}_{mn}$, il correspond un unique couple $\varphi(z) = (z_1, z_2)$ et réciproquement. Si z est inversible et a z' pour inverse, alors $\varphi(z.z') = \varphi(z).\varphi(z') = \varphi(1) = (1, 1)$. En particulier, $(z_1, z_2).(z_1', z_2') = (1, 1) = (z_1 z_1', z_2 z_2')$ ce qui montre que z_1 (resp. z_2) est un élément inversible de $\mathbb{Z}_m$ (resp. $\mathbb{Z}_n$). La réciproque étant également vraie, on en tire l'isomorphisme annoncé.

[26] Ce résultat est, sous cette forme, attribué à Euler.

Il s'agit d'un cas particulier du théorème I.6.11. En effet, si n est premier, $\varphi(n) = n - 1$.

Théorème I.6.14 (Wilson). *Soit p un nombre premier. On a*

$$(p-1)! \equiv -1 \mod p.$$

Démonstration. On suppose $p \geq 3$. Classons les éléments du groupe multiplicatif $\mathbb{Z}_p^*$ selon qu'ils sont ou non égaux à leur inverse.

Un élément x qui est égal à son inverse est tel que $x = x^{-1}$ et donc $x^2 = 1$. Cela signifie que si un élément x est égal à son inverse, alors x est racine du polynôme $X^2 - 1 \in \mathbb{Z}_p[X]$. Or ce polynôme n'a que deux racines -1 et 1. Ainsi, 1 et -1 sont les deux seuls éléments de $\mathbb{Z}_p^*$ égaux à leur inverse.

Les $p-3$ autres éléments de $\mathbb{Z}_p^*$ se groupent par paires d'éléments distincts (x_i, y_i), $i = 1, \ldots, (p-3)/2$, tels que $x_i y_i = 1$. Puisque $(p-1)!$ est le produit de tous les éléments de $\mathbb{Z}_p^*$, on a

$$(p-1)! = 1.(-1). \prod_{i=1}^{(p-3)/2} x_i y_i = -1.$$

■

Remarque I.6.15. On a même mieux. Etant donné $m > 1$, m est premier **si et seulement si** $(m-1)! \equiv -1 \mod m$. En effet, si m n'est pas premier, il est de la forme $m = a.b$ avec $1 < a < m$. Par conséquent, a divise $(m-1)!$. De là, on en tire que a et, *a fortiori* m, ne divisent pas $(m-1)!+1$. Ainsi, on pourrait tester qu'un nombre m est ou non premier en calculant $(m-1)! \mod m$ et en vérifiant si le résultat est ou non congru à -1. Bien évidemment, un tel test est peu effectif.

6.4. Existence de générateurs pour $\mathbb{F}_q$. Nous revenons à présent sur la structure des champs finis à q éléments. En fait, si un champ contient q éléments, q est puissance d'un nombre premier p (qui est la caractéristique du champ).

Remarque I.6.16. Nous ne faisons que de paraphraser la proposition I.6.5. Soit $\mathbb{F}_q$ un champ à q éléments. Nous avons vu précédemment que la caractéristique de $\mathbb{F}_q$ est un nombre premier p et que $\mathbb{F}_q$ est une extension du sous-champ premier $\mathbb{Z}_p$ (cf. section 6.1). Ainsi, $\mathbb{F}_q$ peut être considéré comme un $\mathbb{Z}_p$-vectoriel de dimension finie. Posons $[\mathbb{F}_q : \mathbb{Z}_p] = f$ (f étant nécessairement fini). Cela signifie que, par l'intermédiaire d'une base[27], les éléments de $\mathbb{F}_q$ sont en bijection avec les f-uples d'éléments de $\mathbb{Z}_p$. Ainsi, on a

$$\boxed{q = p^f.}$$

[27] Si $y_1, \ldots, y_f \in \mathbb{F}_q$ forment une base de $\mathbb{F}_q$ considéré comme $\mathbb{Z}_p$-vectoriel, alors tout élément $x \in \mathbb{F}_q$ se décompose de manière unique comme $x = \alpha_1 y_1 + \cdots + \alpha_f y_f$. Ainsi, à x correspond le f-uple $(\alpha_1, \ldots, \alpha_f)$ des composantes de x et inversement, à tout f-uple correspond un élément de $\mathbb{F}_q$.

Définition I.6.17. Si $\mathbb{F}_q$ est un champ à q éléments, on appelle *générateur (multiplicatif)* de $\mathbb{F}_q$ tout élément d'ordre $q-1$ pour le groupe multiplicatif $\mathbb{F}_q^*$ (on parle aussi d'*élément primitif*[28]). Autrement dit, si g est un générateur de $\mathbb{F}_q$,

$$\mathbb{F}_q^* = \{g^n \mid n = 1, \ldots, q-1\}.$$

Exemple I.6.18. Considérons un exemple simpliste : $\mathbb{Z}_5$. Dans ce cas, 2 est un générateur car

i	1	2	3	4
2^i	2	4	3	1

Remarque I.6.19. Lorsqu'on dispose d'un générateur β de $\mathbb{F}_q$, on peut introduire la notion de *logarithme discret* en base β comme suit. Pour tout α non nul, $\mathrm{dlog}_\beta \alpha = n$ si $\beta^n = \alpha$ avec $n < q$.

Le résultat suivant stipule que $\mathbb{F}_q^*$ est un groupe cyclique.

Théorème I.6.20. *On dispose des résultats suivants.*

- *Tout champ fini $\mathbb{F}_q$ possède un générateur.*
- *Si g est un générateur de $\mathbb{F}_q$, alors g^j en est un aussi si et seulement si* $\mathrm{pgcd}(j, q-1) = 1$.
- *Le nombre de générateurs de $\mathbb{F}_q$ est $\varphi(q-1)$.*

Lemme I.6.21. *Pour tout entier $N \geq 1$, on a*

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

Démonstration. On partitionne l'ensemble $E = \{1, 2, \ldots, N\}$ en ensembles disjoints E_d de la façon suivante. Pour chaque diviseur d de N, on définit

$$E_d = \{k \in E \mid \mathrm{pgcd}(k, N) = d\}.$$

Il est clair que ces ensembles forment une partition de E. Cherchons la valeur du cardinal de E_d. Soit $k \in E_d$. Puisque $\mathrm{pgcd}(k, N) = d$, il existe k' et N' tels que

$$k = k'd, \ N = N'd \ \text{ et } \mathrm{pgcd}(k', N') = 1.$$

De plus, $1 \leq k \leq N$ donc $1 \leq k' \leq N'$ et $\mathrm{pgcd}(k', N') = 1$. Cela signifie qu'il y a $\varphi(N')$ nombres k' satisfaisant les propriétés données ci-dessus. A chacun de ces k' correspond exactement un entier k de E_d. On en tire donc

$$\#E_d = \varphi(N') = \varphi(\frac{N}{d}).$$

Si $d_1, \ldots, d_r$ sont tous les diviseurs de N, on a

$$N = \#E = \sum_{i=1}^{r} \#E_{d_i} = \sum_{i=1}^{r} \varphi(\frac{N}{d_i}).$$

[28] Rappelez-vous par exemple de la terminologie "*racine primitive de l'unité*". Il s'agit des racines n-ièmes de l'unité de la forme $\omega_k = e^{2ik\pi/n}$ avec $k < n$ premier avec n. Dans ce cas, les puissances de ω_k décrivent exactement l'ensemble des racines n-ièmes de 1.

Pour conclure, il suffit de remarquer[29] que $\{N/d_i \mid i = 1, \ldots, r\} = \{d_1, \ldots, d_r\}$. En effet, chaque N/d_i est lui-même un diviseur de N. Par conséquent, lorsqu'on parcourt l'ensemble des N/d_i possibles, on parcourt en fait l'ensemble de tous les diviseurs de N.

■

Exemple I.6.22. Avec les notations de la preuve, on a

$$18 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) = 1 + 1 + 2 + 2 + 6 + 6.$$

De plus,

$$18 = \varphi(18/1) + \varphi(18/2) + \varphi(18/3) + \varphi(18/6) + \varphi(18/9) + \varphi(18/18)$$

et

$$E_1 = \{1, 5, 7, 11, 13, 17\}, \quad E_2 = \{2, 4, 8, 10, 14, 16\},$$
$$E_3 = \{3, 15\}, \quad E_6 = \{6, 12\}, \quad E_9 = \{9\} \text{ et } E_{18} = \{18\}.$$

Démonstration. Considérons à présent la preuve du théorème I.6.20. Soit a un élément d'ordre d du groupe multiplicatif $\mathbb{F}_q^*$ (pour l'instant, nous supposons qu'un tel élément existe). Puisque l'ordre d'un élément divise l'ordre du groupe, d divise $q-1$. Par définition, d est le plus petit entier tel que $a^d = 1$. Ainsi, $a, a^2, \ldots, a^d$ sont des éléments distincts.

Montrons que les éléments d'ordre d de $\mathbb{F}_q^*$ sont exactement les a^j tels que $\text{pgcd}(j, d) = 1$. Il est clair que les d éléments $a, a^2, \ldots, a^d$ sont tous des racines de $X^d - 1$. Or un polynôme de degré d sur un champ possède au plus d racines. Dès lors, les puissances de a parcourent l'ensemble des racines de $X^d - 1$. Un élément quelconque d'ordre d de $\mathbb{F}_q^*$ étant racine de $X^d - 1$, nous avons montré que tout élément d'ordre d de $\mathbb{F}_q^*$ est de la forme a^j pour un certain j. Cela n'est pas suffisant, un élément de la forme a^j n'est pas nécessairement d'ordre d. Si $\text{pgcd}(j, d) = d' > 1$, alors

$$(a^j)^{d/d'} = (a^d)^{j/d'} = 1$$

et a^j a un ordre qui divise $d/d' < d$. Dans ce cas, a^j n'est pas d'ordre d. De plus, si $\text{pgcd}(j, d) = 1$, alors il existe des entiers[30] u et v tels que $1 = ju - dv$. De là,

$$a = a^{1+dv} = (a^j)^u.$$

Ainsi, a et a^j sont puissances l'un de l'autre. Ils sont donc de même[31] ordre d.

[29] On a en fait une bijection de l'ensemble des diviseurs de N dans lui-même qui à d_i, associe N/d_i. On pourra en particulier observer que r, le nombre de diviseurs de N, est impair si et seulement si N est un carré.

[30] Pensez au théorème de Bezout.

[31] C'est immédiat. S'il existe m et n tels que $x^m = y$ et $y^n = x$, autrement dit, si x et y sont puissances l'un de l'autre, alors x et y sont de même ordre. En effet, si x (resp. y) est d'ordre k (resp. ℓ), alors $y^k = (x^m)^k = (x^k)^m = 1$ et donc $\ell \leq k$. Par symétrie, on tire aussi $k \leq \ell$.

Par conséquent, si un élément d'ordre d existe dans $\mathbb{F}_q^*$, il y en a alors exactement $\varphi(d)$. Ainsi, pour tout entier d divisant $q-1$, il n'y a que deux possibilités : aucun élément de $\mathbb{F}_q^*$ n'est d'ordre d ou il y a exactement $\varphi(d)$ éléments d'ordre d.

Il suffit alors d'un argument de comptage pour conclure. Au vu du lemme précédent, si on prend $N = q-1$ et puisque, dans $\mathbb{F}_q^*$, l'ordre de tout élément divise $q-1$, il faut nécessairement $\varphi(d)$ éléments d'ordre d pour tout diviseur de $q-1$. En particulier, $\mathbb{F}_q^*$ contient $\varphi(q-1)$ éléments d'ordre $q-1$.

■

Exemple I.6.23. Reprenons l'exemple I.3.9. Au vu de la table de multiplication obtenue précédemment, on trouve facilement l'ordre des éléments de $\mathbb{F}_9 = \mathbb{Z}_3[X]/\langle X^2+1\rangle$ en calculant leurs puissances (par convention, on note un élément du quotient simplement P au lieu de $P + \langle X^2+1\rangle$)

P	P^2	P^3	P^4	P^5	P^6	P^7	P^8
1							
2	1						
X	2	$2X$	1				
$2X$	2	X	1				
$X+1$	$2X$	$2X+1$	2	$2X+2$	X	$X+2$	1
$X+2$	X	$2X+2$	2	$2X+1$	$2X$	$X+1$	1
$2X+1$	X	$X+1$	2	$X+2$	$2X$	$2X+2$	1
$2X+2$	$2X$	$X+2$	2	$X+1$	X	$2X+1$	1

On trouve $\varphi(8) = 4$ (resp. $\varphi(4) = 2$, $\varphi(2) = 1$, $\varphi(1) = 1$) éléments d'ordre 8 (resp. 4, 2, 1).

6.5. Existence et unicité d'un champ à p^f éléments. Nous montrons ici qu'un champ à $q = p^f$ éléments est le corps de rupture du polynôme $X^q - X$. (Vu l'unicité, à isomorphisme près, du corps de rupture, on pourra parler du champ à q éléments et lui consacrer la notation $\mathbb{F}_q$.) En d'autres termes, si A et B sont deux champs contenant p^f éléments, alors il s'agit en fait de deux copies du même objet.

Théorème I.6.24. *Soit $\mathbb{F}_q$ un champ à $q = p^f$ éléments. Tout élément de $\mathbb{F}_q$ satisfait l'équation $X^q - X = 0$ et $\mathbb{F}_q$ est précisément l'ensemble des racines de cette équation. Autrement dit, pour tout sous-champ $\mathbb{K}$ de $\mathbb{F}_q$, $\mathbb{F}_q$ est le corps de rupture du polynôme $X^q - X$ sur $\mathbb{K}$.*

Réciproquement, pour tout $q = p^f$, puissance d'un nombre premier p, le corps de rupture du polynôme $X^q - X$ sur $\mathbb{Z}_p$ est un champ à q éléments.

Démonstration. Si $\mathbb{F}_q$ est un champ fini[32], puisque l'ordre de tout élément non nul divise $q-1$, on en déduit que tout élément non nul satisfait l'équation $X^{q-1} = 1$ et donc également l'équation $X^q = X$. L'élément nul

[32]Au vu de la remarque I.6.16, sa caractéristique vaut p: $\mathbb{F}_q$ est une extension de $\mathbb{Z}_p$.

satisfait aussi cette dernière équation. Ainsi, tout élément de $\mathbb{F}_q$ est racine du polynôme $X^q - X$ de degré q (considéré comme polynôme à coefficients dans $\mathbb{K}$). Puisque ce polynôme a au plus q racines, ses racines décrivent donc exactement $\mathbb{F}_q$, i.e., $\mathbb{F}_q$ est le corps de rupture de $X^q - X$ sur $\mathbb{K}$ (la plus petite extension de $\mathbb{K}$ contenant toutes les racines de $X^q - X$).

Réciproquement, soit $q = p^f$ et considérons le corps de rupture $\mathbb{F}$ du polynôme $P = X^q - X$ sur $\mathbb{Z}_p$. Puisque $\mathrm{D}_X(X^q - X) = qX^{q-1} - 1 = -1$ dans $\mathbb{Z}_p[X]$ ou $\mathbb{F}[X]$ (car q est un multiple de la caractéristique p), on en conclut que $X^q - X$ n'a pas de racine mutliple[33] (cf. proposition I.5.9). Le corps de rupture $\mathbb{F}$ doit donc contenir au moins les q racines distinctes de P. Il nous suffit de montrer que l'ensemble de ces racines est un champ (en effet, le corps de rupture est le plus petit champ contenant ces racines). Soient a et b, deux racines du polynôme, i.e., $a^q = a$ et $b^q = b$. Le produit des racines est encore une racine car $(ab)^q = ab$. Pour la somme, en utilisant[34] le théorème I.6.4, on a $(a + b)^q = a^q + b^q = a + b$. Pour l'inverse d'une racine, il vient $a^q = a$ et donc $a^{-q-1}.a^q = a^{-q-1}.a$, c'est-à-dire $a^{-1} = (a^{-1})^q$. Enfin, pour l'opposé d'une racine $(a + (-a))^q = 0 = a^q + (-a)^q$, et donc $(-a)^q = -(a^q)$. Ceci suffit.

∎

Remarque I.6.25. Soit $\mathbb{K}$ un sous-champ de $\mathbb{F}_q$. Puisque $\mathbb{F}_q$ est le corps de rupture de $X^q - X$ sur $\mathbb{K}$, on a

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha).$$

Puisque le corps de rupture d'un polynôme est unique (à un isomorphisme près, cf. définition I.5.14), nous pourrons donc parler du champ $\mathbb{F}_q$. (Ainsi, le champ $\mathbb{Z}_p$ des entiers modulo est une copie du champ $\mathbb{F}_p$ à isomorphisme près. Nous emploierons indifféremment les deux notations.)

Remarque I.6.26. Le théorème I.6.24 affirme en particulier que tout élément de $\mathbb{F}_q$ est algébrique sur $\mathbb{F}_p$ (et même sur tout sous-champ $\mathbb{K}$ de $\mathbb{F}_q$). En effet, tout élément de $\mathbb{F}_q$ est racine du polynôme $X^q - X \in \mathbb{F}_p[X]$ (ou de manière analogue, on peut considérer que $X^q - X \in \mathbb{K}[X]$).

6.6. Sous-champs de $\mathbb{F}_q$. Cette courte section contient un unique résultat présentant la structure des sous-champs de $\mathbb{F}_q$. De plus, le résultat présenté ici nous sera utile pour obtenir une formule comptant le nombre de polynômes moniques irréductibles sur $\mathbb{F}_p$ de degré fixé.

[33] Il est possible de démontrer que $X^q - X$ n'a pas de racine multiple sans avoir recours à la notion de dérivation formelle, voir l'article de I. N. Herstein, *Amer. Math. Monthly* (1987).

[34] Il est clair que le corps de rupture $\mathbb{F}$ étant une extension de $\mathbb{Z}_p$, il est encore de caractéristique p.

Lemme I.6.27. *Soient $m > n$. Le pgcd de $X^{p^m} - X$ et de $X^{p^n} - X$ est $X^{p^h} - X$ où $h = \mathrm{pgcd}(m, n)$. En particulier, si d divise f, alors $X^{p^d} - X$ divise $X^{p^f} - X$.*

Démonstration. Effectuons la division euclidienne, $m = a.n + r$ avec $0 \leq r < n$. Alors, on obtient

$$p^m - 1 = (p^n - 1)\,(\underbrace{p^{(a-1)n} + p^{(a-2)n} + \cdots + p^n + 1}_{:=\alpha})\,p^r + p^r - 1$$

(pour s'en convaincre, il suffit de "redistribuer" le membre de droite faisant apparaître une somme télescopique). De là, on trouve facilement

$$X^{p^m-1} - 1 = X^{(p^n-1)\,\alpha\,p^r+p^r-1} - 1 = X^{p^r-1}(X^{(p^n-1)\,\alpha\,p^r} - 1) + X^{p^r-1} - 1.$$

De plus, on a aussi

$$X^{(p^n-1)\,\alpha\,p^r} - 1 = (X^{p^n-1} - 1)(\underbrace{(X^{p^n-1})^{\alpha\,p^r-1} + (X^{p^n-1})^{\alpha\,p^r-2} + \cdots + 1}_{:=Q}).$$

En combinant les deux derniers développements et en multipliant par X, il vient

$$X^{p^m} - X = X^{p^r-1}\,(X^{p^n} - X)\,Q + X^{p^r} - X.$$

Autrement dit, le reste de la division de $X^{p^m} - X$ par $X^{p^n} - X$ vaut $X^{p^r} - X$. On peut alors conclure en utilisant l'algorithme d'Euclide et en procédant par divisions euclidiennes successives. (Le pgcd de $X^{p^m} - X$ et de $X^{p^n} - X$ est égal à celui de $X^{p^n} - X$ et de $X^{p^r} - X$, et ainsi de suite.)

■

Proposition I.6.28. *Les sous-champs de $\mathbb{F}_q = \mathbb{F}_{p^f}$ sont exactement les $\mathbb{F}_{p^d}$ pour d divisant f. Plus précisément, si $\mathbb{K}$ est un sous-champ de $\mathbb{F}_q$, alors il contient p^d éléments où d divise f. Réciproquement, si d divise f, alors $\mathbb{F}_q$ contient exactement un sous-champ contenant p^d éléments.*

En particulier, si on étend $\mathbb{F}_p$ par un élément de $\mathbb{F}_{p^f}$, alors on obtient un de ces sous-champs $\mathbb{F}_{p^d}$.

Démonstration. Soit $\mathbb{K}$ un sous-champ de $\mathbb{F}_q$ contenant t éléments. En particulier, si on pose $[\mathbb{F}_q : \mathbb{K}] = s$, alors $\#\mathbb{F}_q = t^s$. De là, on tire que $p^f = t^s$. Puisque p est premier et que s et t sont entiers, il existe d tel que $t = p^d$ et $ds = f$ (autrement dit, d divise f).

Soit d un diviseur de f. Au vu du lemme précédent, $X^{p^d} - X$ divise $X^{p^f} - X = X^q - X$ (nous allons considérer ces deux polynômes comme polynômes sur $\mathbb{Z}_p$). Ainsi, toute racine de $X^{p^d} - X$ est racine de $X^q - X$ et appartient donc à $\mathbb{F}_q$ (cf. première partie du théorème I.6.24). Par conséquent, $\mathbb{F}_q$ doit contenir comme sous-champ, le corps de rupture de $X^{p^d} - X$ sur $\mathbb{Z}_p$. Vu la deuxième partie du théorème I.6.24, ce corps de rupture est un champ à p^d éléments. Autrement dit, $\mathbb{F}_q$ contient un sous-champ à p^d éléments. Supposons que $\mathbb{F}_q$ contienne au moins deux tels sous-champs distincts. Ensemble, ils contiendraient plus de p^d racines de $X^{p^d} - X$ ce qui est impossible. Ceci prouve l'unicité du sous-champ d'ordre p^d.

Considérons à présent le cas particulier. Il est clair que $\mathbb{F}_p(\alpha)$ est un sous-champ de $\mathbb{F}_q$. Il est donc de la forme $\mathbb{F}_{p^d}$ pour un certain d divisant f.

■

Exemple I.6.29. Considérons le champ $\mathbb{F}_{2^8} = \mathbb{F}_{256}$. Puisque les diviseurs de 8 sont $1, 2, 4, 8$, les sous-champs propres de $\mathbb{F}_{2^8}$ sont $\mathbb{F}_2$, $\mathbb{F}_{2^2}$ et $\mathbb{F}_{2^4}$. On obtient un treillis "linéaire" représenté à la figure I.2 et symbolisant les inclusions de ces différents sous-champs. Inspectons à présent pour chacun

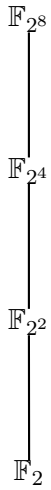


FIGURE I.2. Sous-champs de $\mathbb{F}_{256}$.

de ces sous-champs, l'ordre des différents éléments qui y interviennent ainsi que leur nombre. Pour rappel, pour tout d diviseur de $q-1$, il y a dans $\mathbb{F}_q^*$ exactement $\varphi(d)$ éléments d'ordre d. Le tableau suivant récapitule la structure des différents sous-champs emboîtés en précisant l'ordre et le nombre d'éléments y apparaissant. Dans ce tableau, il faut comprendre que tous les éléments repris dans les k premières lignes appartiennent aussi aux sous-champs apparaissant "plus bas" (à cause de l'emboîtement).

	ord	#
$\mathbb{F}_2^*$	1	1
$\mathbb{F}_4^*$	3	2
$\mathbb{F}_{16}^*$	5	4
	15	8
$\mathbb{F}_{256}^*$	17	16
	51	32
	85	64
	255	128
		255

La figure I.3 reprend la situation au sein de $\mathbb{F}_{256}$. On y a dessiné les sous-champs et indiqués l'ordre des différents éléments.

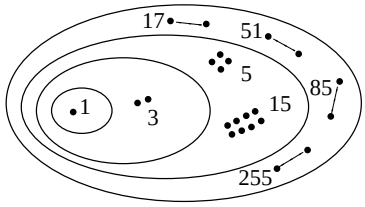


FIGURE I.3. $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^8}$ et leurs éléments (ordre respectif).

Exemple I.6.30. Considérons le champ $\mathbb{F}_{2^{30}}$. Ses sous-champs sont $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^{10}}$ et $\mathbb{F}_{2^{15}}$. On dispose des inclusions reprises sur le trellis de la figure I.4.

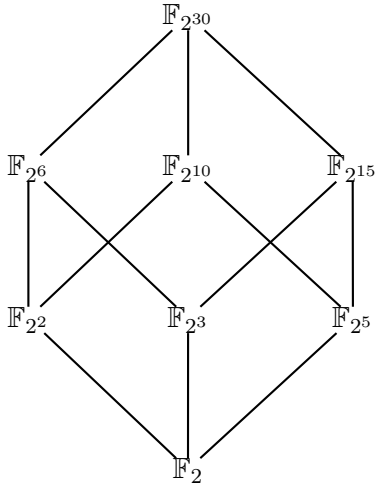


FIGURE I.4. Sous-champs de $\mathbb{F}_{2^{30}}$.

On peut faire le même exercice de description que pour $\mathbb{F}_{2^8}$. Puisqu'ici la structure est plus compliquée, on rappelle dans la dernière colonne du tableau, les éléments déjà pris en compte dans des sous-champs plus petits

(cela permet de retrouver en quelque sorte le treillis de la figure I.4).

	ord	#	déjà pris en compte
$\mathbb{F}_2^*$	1	1	
$\mathbb{F}_{2^2}^*$			1
	3	2	
$\mathbb{F}_{2^3}^*$			1
	7	6	
$\mathbb{F}_{2^5}^*$			1
	31	30	
$\mathbb{F}_{2^6}^*$			1, 3, 7
	9	6	
	21	12	
	63	36	
$\mathbb{F}_{2^{10}}^*$			1, 3, 31
	11	10	
	33	20	
	93	60	
	341	300	
	1023	600	
$\mathbb{F}_{2^{15}}^*$			1, 7, 31
	151	150	
	217	180	
	1057	900	
	4681	4500	
	32767	27000	
$\mathbb{F}_{2^{30}}^*$			1, 3, 7, 9, 11, 21, 31, 33, 63, 93, 151, 217, 341, 1023, 1057, 4681, 32767
	77	60	
	99	60	
	231	120	
	⋮	⋮	
	1073741823	534600000	

Les “points de suspension” évitent de passer en revue[35] les 79 diviseurs de $2^{30} - 1$ non rencontrés comme ordre d'éléments de sous-champs plus petits.

[35] 77, 99, 231, 279, 331, 453, 651, 693, 993, 1359, 1661, 1953, 2317, 2387, 2979, 3069, 3171, 3641, 4983, 6951, 7161, 9513, 10261, 10923, 11627, 14043, 14949, 20853, 21483, 25487, 30783, 32769, 34881, 42129, 49981, 51491, 71827, 76461, 92349, 98301, 104643, 112871, 149943, 154473, 215481, 229383, 294903, 338613, 349867, 360437, 449829, 463419, 549791, 646443, 790097, 1015839, 1049601, 1081311, 1549411, 1649373, 2370291, 3148803, 3243933, 3848537, 4648233, 4948119, 7110873, 10845877, 11545611, 13944699, 17043521, 32537631, 34636833, 51130563, 97612893, 119304647, 153391689, 357913941, 1073741823.

Les éléments de $\mathbb{F}_{2^{30}}^*$ n'appartenant à aucun sous-champ propre sont en nombre 1073708010. La figure I.5 symolise les différents sous-champs et les éléments des différents ordres qui y apparaissent.

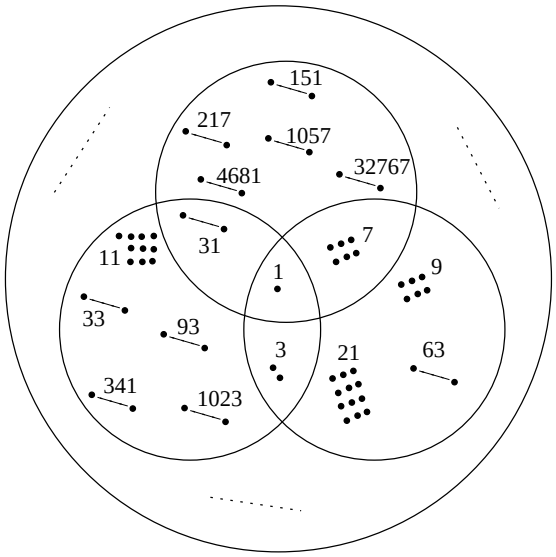


FIGURE I.5. Les éléments de $\mathbb{F}_{2^{30}}$ suivant leur ordre.

7. Construction de champs finis

Dans ce cours, nous avons décidé d'utiliser le logiciel `Mathematica` pour des illustrations informatiques. Nous avons choisi ce logiciel, non pas pour sa vitesse d'exécution (en effet, l'implémentation efficace d'algorithmes devrait très certainement être réalisée avec un langage de plus bas niveau comme le `C` ou même l'assembleur) mais pour sa simplicité d'utilisation : gestion des grands nombres, programmation fonctionnelle et même multi-paradigmes, implémentation de nombreuses fonctions mathématiques et en particulier des fonctions issues de la théorie des nombres, utilitaires graphiques directement accessibles, etc .... Ce cours ne se veut pas non plus être une introduction à ce logiciel. Nous espérons que les exemples fournis permettront au lecteur de réaliser lui-même d'autres expérimentations et d'en apprendre un peu plus par lui-même (n'hésitez jamais à consulter l'aide en ligne !).

Au vu des sections précédentes, nous avons exactement deux situations possibles.

- Si p est premier, alors $\mathbb{Z}_p$ est un champ (le champ $\mathbb{F}_p$) et nous connaissons très bien sa structure et l'arithmétique modulo p.
- Si $q = p^f$, alors on obtient le champ $\mathbb{F}_q$ en quotientant l'anneau $\mathbb{F}_p[X]$ par un polynôme irréductible de degré f. La question qui se pose est alors l'existence de polynômes irréductibles sur $\mathbb{F}_p$ de degré f. (Une variante, en se rappelant la proposition I.4.11, revient

à considérer une extension de $\mathbb{F}_p$ par une racine d'un polynôme irréductible de degré f sur $\mathbb{F}_p$).

Considérons tout d'abord un petit exemple.

Exemple I.7.1. Nous montrons ici comment obtenir la table de multiplication de $\mathbb{F}_9 = \mathbb{Z}_3[X]/\langle X^2+1\rangle$ donnée à l'exemple I.3.9 grâce à `Mathematica`. La liste des polynômes de degré au plus un sur $\mathbb{Z}_3$ est encodée dans la variable `t` comme suit :

```
:> t = {0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2}
```

Ceci peut être automatisé comme suit :

Pensez au produit scalaire.

```
:> p = 3;
:> deg = 1;
:> t=Flatten[Table[{i,j}, {i,0,p-1}, {j,0,p-1}], 1]
     .Table[x^(deg-i), {i,0,deg}]
```

Nous définissons une fonction `reduire` qui, en deux étapes, calcule le reste de la division d'un polynôme `p` par X^2+1 puis en réduit les coefficients modulo 3 (pour ce faire, nous utilisons[36] deux fois la fonction `PolynomialMod`).

```
:> reduire[p_]:=PolynomialMod[PolynomialMod[p,x^2+1],3]
```

Enfin, nous stockons la table de multiplication dans une variable `m`.

```
:> m=Table[reduire[t[[i]] t[[j]]], {i,1,9}, {j,1,9}]
```

Pour l'affichage, on pourra utiliser

```
:> TableForm[m]
```

Remarquons que pour vérifier au préalable que le polynôme X^2+1 est bien irréductible sur $\mathbb{Z}_3[X]$, puisqu'il s'agit d'un polynôme de degré deux, il suffit de vérifier qu'il n'a pas de racines.

```
:> Table[Mod[x^2+1 /. x->i, 3], {i,0,2}]
Out[]= {1,2,2}
```

Notre but est de montrer que le produit de tous les polynômes moniques irréductibles de $\mathbb{F}_p[X]$ et de degré divisible par f est exactement $X^{p^f} - X$. Pour y parvenir, nous avons besoin d'un résultat préalable.

Théorème I.7.2. *Pour tout $q = p^f$, le polynôme $X^q - X$ est le produit dans $\mathbb{F}_p[X]$ de tous les polynômes minimums (distincts) des éléments de $\mathbb{F}_q$.*

Démonstration. Nous savons déjà que $\mathbb{F}_q$ est précisément l'ensemble des racines de $X^q - X$ et que ce polynôme ne possède pas de racine multiple (cf. théorème I.6.24). En particulier, si $\beta \in \mathbb{F}_q$, il est algébrique sur $\mathbb{F}_p$ (en effet, $X^q - X$ peut être vu comme un polynôme de $\mathbb{F}_p[X]$ qui est annulé par β). Il possède donc un polynôme minimum M_β sur $\mathbb{F}_p$ divisant $X^q - X$.

Remarquons que si α, β appartiennent à $\mathbb{F}_q$ (ayant respectivement M_α, M_β comme polynôme minimum sur $\mathbb{F}_p$), alors soit $M_\alpha = M_\beta$ (autrement dit, α

[36] Dans les versions récentes de `Mathematica`, on dispose d'une version améliorée de la fonction `PolynomialMod[p,x^2+1,Modulus->3]` pour n'utiliser qu'une seule fonction.

et β sont conjugués) soit $M_\alpha \neq M_\beta$ et ces polynômes n'ont aucune racine commune (car sinon, ils auraient une racine commune γ, conjugué de α et β; on pourrait alors conclure que $M_\alpha = M_\gamma = M_\beta$).

Ainsi, $\mathbb{F}_q$ peut être partitionné en classes telles que deux éléments quelconques $\alpha, \beta \in \mathbb{F}_q$ appartiennent à une même classe si et seulement si $M_\alpha = M_\beta$ (il s'agit en fait d'une relation d'équivalence). Si $\mathbb{F}_q$ est partitionné en t classes et en choisissant un représentant $\alpha_1, \ldots, \alpha_t$ dans chaque classe, on trouve

$$X^q - X = M_{\alpha_1} \cdots M_{\alpha_t}.$$

En effet, il suffit de procéder de proche en proche. On a d'abord $X^q - X = M_{\alpha_1} Q$. Dans cette factorisation, puisque les racines de $X^q - X$ sont simples, M_{α_1} et Q n'ont pas de racine commune et les racines de $X^q - X$ non conjugées à α_1 sont exactement les racines de Q. On continue de proche en proche jusqu'à avoir épuisé $\mathbb{F}_q$.

■

Théorème I.7.3. *Pour tout $q = p^f$, le polynôme $X^q - X$ se factorise dans $\mathbb{F}_p[X]$ en le produit de tous les polynômes moniques irréductibles (distincts) dont le degré divise f.*

Démonstration. Au vu du théorème précédent, nous savons déjà que $X^q - X$ est le produit dans $\mathbb{F}_p[X]$ de tous les polynômes minimums (distincts) des éléments de $\mathbb{F}_q$. Soit P un tel polynôme de degré d, polynôme minimum de $\alpha \in \mathbb{F}_q$. Puisqu'il est irréductible, $\mathbb{F}_p[X]/\langle P \rangle$ est un champ contenant p^d éléments. Ce champ est aussi bien sûr isomorphe à $\mathbb{F}_p(\alpha)$ (cf. proposition I.4.11). Il s'agit donc d'un sous-champ de $\mathbb{F}_q$. On conclut par le théorème de structure des sous-champs de $\mathbb{F}_q$, que d divise f.

Il nous reste à montrer que tout polynôme monique P irréductible sur $\mathbb{F}_p$ dont le degré d divise f est le polynôme minimum sur $\mathbb{F}_p$ d'un élément de $\mathbb{F}_q$. Considérons le champ $\mathbb{L} = \mathbb{F}_p[X]/\langle P \rangle$ contenant p^d éléments. Par le théorème de structure des sous-champs de $\mathbb{F}_q$, $\mathbb{L}$ est (isomorphe à) un sous-champ de $\mathbb{F}_q$. De plus, par construction, $\mathbb{L}$ (et donc $\mathbb{F}_q$) contient une racine β de P. Autrement dit, P est un polynôme monique irréductible sur $\mathbb{F}_p$ ayant $\beta \in \mathbb{F}_q$ comme racine : P est le polynôme minimum de β sur $\mathbb{F}_p$.

■

Corollaire I.7.4. *Si f est un nombre premier, il y a alors exactement $\frac{p^f - p}{f}$ polynômes moniques irréductibles de degré f dans $\mathbb{F}_p[X]$.*

Remarque I.7.5. Par le petit théorème de Fermat, $p^f \equiv p \mod f$ et donc $\frac{p^f - p}{f}$ est un entier.

Démonstration. Soit $N_p(f)$ le nombre de polynômes moniques irréductibles de degré f dans $\mathbb{F}_p[X]$. Par le théorème précédent, puisque les seuls diviseurs de f sont 1 et f, le polynôme $X^{p^f} - X$ se factorise en un produit des $N_p(f) = k$ polynômes $P_1, \ldots, P_k$ moniques irréductibles sur $\mathbb{F}_p$ de degré f et des p polynômes de degré un : $X - \alpha_i$, pour $\alpha_i \in \mathbb{F}_p$, $i = 1, \ldots, p$.

Autrement dit,

$$X^{p^f} - X = \underbrace{P_1(X) \cdots P_k(X)}_{k \text{ polynômes de degré } f} \underbrace{(X-\alpha_1)\cdots(X-\alpha_p)}_{p \text{ polynômes de degré } 1}$$

et en s'intéressant au degré des deux membres, on obtient

$$p^f = f.N_p(f) + p \tag{2}$$

d'où la formule annoncée.

■

Remarque I.7.6. Si f n'est pas premier, notons $N_p(d)$ le nombre de polynômes moniques irréductibles de degré d sur $\mathbb{F}_p$. Au vu du théorème I.7.3, la formule (2) devient

$$p^f = \sum_{d|f} d.N_p(d) = f.N_p(f) + \sum_{\substack{d|f \\ d<f}} d.N_p(d)$$

et de là,

$$N_p(f) = \left(p^f - \sum_{\substack{d|f \\ d<f}} d.N_p(d)\right)/f.$$

Cette formule permet donc de calculer, de proche en proche, les valeurs de $N_p(f)$ (On remarque que (2) n'est qu'un cas particulier de cette formule). En particulier, cette formule permet de se convaincre de l'existence d'un polynôme irréductible de degré f dans $\mathbb{F}_p[X]$.

En utilisant la formule donnée à la remarque I.7.6 ci-dessus, on calcule aisément le nombre de polynômes moniques irréductibles sur $\mathbb{F}_p$ de degré f pour les premières valeurs de p et de f. On peut procéder comme suit.

```
:> n[p_,f_] :=
   (p^f-Map[n[p,#]&,Drop[Divisors[f],-1]].Drop[Divisors[f],-1])/f
:> Table[n[Prime[i],j], {i,1,10}, {j,1,7}]
```

On obtient alors le tableau I.2.

On peut montrer que le nombre $N_p(f)$ de polynômes moniques irréductibles sur $\mathbb{F}_p$ de degré f est tel que

$$\frac{N_p(f)}{p^f} \sim \frac{1}{f}.$$

(Un argument en faveur de ce résultat sera fourni par la proposition I.7.7.) Cela signifie que la probabilité pour qu'un polynôme monique de degré f sur $\mathbb{F}_p$ soit irréductible est proche de $\frac{1}{f}$ (ce qu'il est possible de montrer explicitement).

A titre indicatif, reprenons la dernière ligne de notre tableau et divisons chacun des éléments par 29^f. On trouve comme approximation numérique

f	1	2	3	4	5	6	7
p	2	1	2	3	6	9	18
	3	3	8	18	48	116	312
	5	10	40	150	624	2580	11160
	7	21	112	588	3360	19544	117648
	11	55	440	3630	32208	295020	2783880
	13	78	728	7098	74256	804076	8964072
	17	136	1632	20808	283968	4022064	58619808
	19	171	2280	32490	495216	7839780	127695960
	23	253	4048	69828	1287264	24670536	486403632
	29	406	8120	176610	4102224	99133020	2464268040

TABLE I.2. $N_p(f)$: nombre de polynômes moniques irréductibles sur $\mathbb{F}_p$ de degré f.

```
:> Table[N[n[29,j]/29^j], {j,1,7}]
Out[] =
  {1., 0.482759, 0.332937, 0.249703, 0.2, 0.16666, 0.142857}
```

et comparons-le aux valeurs approchées de $1/f$,

```
:> Table[N[1/j], {j,1,7}]
Out[] =
  {1., 0.5,      0.333333, 0.25,     0.2, 0.166667, 0.142857}
```

En pratique, pour générer un polynôme monique irréductible sur $\mathbb{F}_p$ de degré f, on choisit de manière aléatoire un polynôme monique puis on teste[37] si le polynôme obtenu est ou non irréductible. On répète la procédure jusqu'à obtenir un polynôme irréductible. A titre indicatif, cette méthode requiert $\mathcal{O}(f^3.\ln f\,.\ln p)$ opérations dans $\mathbb{F}_p$.

Pour conclure cette section, voici un autre argument assurant l'existence de polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$. En effet, le lecteur pourrait, à juste titre, ne pas être entièrement convaincu par les développements menés jusqu'ici. Pour prouver facilement la proposition I.7.7, nous devons tout d'abord introduire la notion de générateur d'extension de champ.

Proposition I.7.7. *Pour tout $n > 2$, le nombre de polynômes moniques irréductibles de degré n dans $\mathbb{F}_p[X]$ est minoré par*

$$\frac{p^n - p\sqrt{p^n}}{n}.$$

Définition I.7.8. Soient $\mathbb{K} \subset \mathbb{L}$ deux champs. Un élément $\alpha \in \mathbb{L}$ est un *générateur* de $\mathbb{L}$ sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}[\alpha]$ (où, pour rappel, $\mathbb{K}[\alpha]$ désigne l'ensemble des polynômes en α à coefficients dans $\mathbb{K}$).

[37] Nous ne parlons pas ici des algorithmes permettant de tester le caractère irréductible d'un polynôme.

Exemple I.7.9. Si on construit $\mathbb{F}_{16}$ comme $\mathbb{Z}_2[X]/\langle X^4+X^3+1\rangle$, on peut se convaincre par simple calcul que X (sous-entendu $X+\langle X^4+X^3+1\rangle$ en est un générateur (au sens de la définition I.6.17) mais que $X+1$ n'en est pas un.

```
:> Union[Table[
    PolynomialMod[PolynomialMod[x^i, x^4+x^3+1], 2],
         {i,1,15}]]

Out[] = {1, x, ...

:> Length[%]
Out[] = 15

:> Union[Table[
    PolynomialMod[PolynomialMod[(x+1)^i, x^4+x^3+1], 2],
         {i,1,15}]]

Out[] = {1, x^3, 1+x, 1+x^2, 1+x+x^2+x^3}
```

Par contre, $X+1$ est un générateur de $\mathbb{F}_{16}$ sur $\mathbb{Z}_2$. Il suffit de montrer que $X+\langle X^4+X^3+1\rangle$ s'obtient comme un polynôme à coefficients dans $\mathbb{Z}_2$ de $X+1+\langle X^4+X^3+1\rangle$ et on vérifie que

$$(X+1)^5+X+1=X \mod X^4+X^3+1.$$

Autrement dit, tout élément de $\mathbb{Z}_2[X]/\langle X^4+X^3+1\rangle$ s'obtient comme puissance de X ou comme une expression polynomiale de $X+1$.

Proposition I.7.10. *Soient $\mathbb{F}_{p^s}\subset\mathbb{F}_{p^{sn}}$ deux champs, $n>2$. Le nombre de générateurs de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ est minoré par*

$$p^{sn}-p^{s(1+\frac{n}{2})}.$$

Démonstration. Un élément α n'est pas un générateur de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ si et seulement si α appartient à un sous-champ propre de $\mathbb{F}_{p^{sn}}$ qui contient $\mathbb{F}_{p^s}$. Un tel sous-champ est de la forme $\mathbb{F}_{p^{sd}}$ où $d<n$ est un diviseur de n. Donc, le nombre de non-générateurs de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ est[38]

$$\leq\sum_{\substack{d|n\\ d<n}}p^{sd}.$$

Ainsi, le nombre de générateurs de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ est minoré par

$$p^{sn}-\sum_{\substack{d|n\\ d<n}}p^{sd}\geq p^{sn}-\sum_{r=1}^{\lfloor n/2\rfloor}p^{sr}=p^{sn}-p^s\frac{p^{s\lfloor n/2\rfloor}-1}{p^s-1}\geq p^{sn}-p^{s(1+n/2)}$$

[38] On a une majoration car un même élément pourrait être compté plusieurs fois, rien n'empêche *a priori* plusieurs sous-champs propres de $\mathbb{F}_{p^s}$ d'être emboités.

p n	3	4	5	6	7
2	1	3	5	9	17
3	7	18	47	120	311
5	38	153	622	2602	11158
7	110	596	3358	19605	117646
11	437	3654	32205	295255	2783877
13	724	7133	74252	804462	8964068
17	1627	20871	283963	4022921	58619804
19	2275	32570	495211	7840972	127695955
23	4042	69948	1287258	24672638	486403626
29	8112	176805	4102216	99137208	2464268033

TABLE I.3. Premières valeurs de $\lfloor (p^n - p\sqrt{p^n})/n \rfloor$

où, pour la dernière inégalité, on remarque que $\frac{p^{s\lfloor n/2 \rfloor}-1}{p^s-1} \leq p^{sn/2}$.

■

Lemme I.7.11. *Soient $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^{sn}}$ deux champs, $n \geq 2$. L'élément $\alpha \in \mathbb{F}_{p^{sn}}$ est un générateur de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ si et seulement si son polynôme minimum sur $\mathbb{F}_{p^s}$ est de degré n.*

Démonstration. Soit M_α le polynôme minimum de α sur $\mathbb{F}_{p^s}$ (bien sûr, α est algébrique sur $\mathbb{F}_{p^s}$, cf. remarque I.6.26).

Si $\deg M_\alpha = n$, alors $\mathbb{F}_{p^s}[\alpha]$ n'est autre que $\mathbb{F}_{p^s}(\alpha)$ (le lecteur peu convaincu peut se rapporter à la remarque I.4.6) qui est isomorphe au champ $\mathbb{F}_{p^s}[X]/\langle M_\alpha \rangle$ (cf. proposition I.4.11) et qui possède p^{sn} éléments. Autrement dit, $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^{sn}}$, i.e., α est un générateur de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$.

Passons à la réciproque et supposons que $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^{sn}}$. Par conséquent, $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^s}(\alpha) \simeq \mathbb{F}_{p^s}[X]/\langle M_\alpha \rangle$ possède p^{sn} éléments et on en déduit que $\deg M_\alpha = n$.

■

Nous pouvons à présent passer à la preuve de la proposition I.7.7.

Démonstration. Le champ $\mathbb{F}_{p^n}$ contient $\mathbb{F}_p$ comme sous-champ. Au vu de la proposition I.7.10, le nombre de générateurs de $\mathbb{F}_{p^n}$ sur $\mathbb{F}_p$ est minoré par $p^n - p\sqrt{p^n}$. Soit α un tel générateur. Par le lemme précédent, son polynôme minimum sur $\mathbb{F}_p$ (qui est monique et irréductible) est de degré n. Ce polynôme possède au plus n racines. Autrement dit, il est le polynôme minimum d'au plus n des générateurs envisagés. Par conséquent, le nombre de polynômes moniques irréductibles de $\mathbb{F}_p[X]$ est minoré par $(p^n - p\sqrt{p^n})/n$.

■

Le tableau I.3 reprend le minorant de $N_p(n)$ donné par la proposition I.7.7. On en comparera les valeurs avec celles obtenues au tableau I.2.

Terminons cette section par un algorithme naïf permettant de générer par degrés croissants les polynômes irréductibles sur $\mathbb{F}_p$. On maintient les

polynômes déjà obtenus dans une liste. A la première étape, cette liste contient uniquement les polynômes de degré 1.

A l'étape $k+1$, la liste contient les polynômes irréductibles de degré au plus k. Il suffit alors d'énumérer tous les polynômes de degré $k+1$ et de tester pour chacun d'eux s'il est divisible par un polynôme de la liste. Si tel est le cas, on passe au polynôme suivant, sinon, ce polynôme est ajouté à la liste.

```
p = 3;

(* genere tous les polynomes de degre d sur Z_p *)

:> genere[d_] :=  Table[IntegerDigits[i,p].
        Reverse[Table[x^i, {i,0,d}]], {i,p^d,p^(d+1)-1}]

(* initialise la liste avec ceux de deg=1 *)

:> liste = genere[1]

Out[] = {x, 1+x, 2+x, 2x, 1+2x, 2+2x}

(* teste si un poly. est irreductible en recherchant le reste
   de la division euclidienne par tous les poly. de la liste *)

:> irreductible[pol_] := If[CoefficientList[Apply[Times,
 Map[PolynomialMod[pol,#,Modulus->p]&,liste]],x]=={}, False, True]

:> Select[genere[2], irreductible[#] &]

Out[] = {1+x^2, 2+x+x^2, 2+2x+x^2, 2+2x^2, 1+x+2x^2, 1+2x+2x^2}

(* generer tous les poly. irreductibles de deg< 5 *)

:> For[i=2, i<5,
    liste=Flatten[Append[liste,Select[genere[i],irreductible[#] &]]];
    i++]
:> liste

Out[] = {x, 1+x, 2+x, 2x, 1+2x, 2+2x, 1+x^2, 2+x+x^2, 2+2x+x^2,
  2+2x^2, 1+x+2x^2, 1+2x+2x^2, 1+2x+x^3, 2+2x+x^3, 2+x^2+x^3, ...
```

8. Représentation en base entière et exponentiation modulaire

Soit $b \geq 2$. Tout nombre $n \in \mathbb{N} \setminus \{0\}$ se décompose de manière unique sous la forme

$$n = \sum_{i=0}^{\ell-1} \sigma_i \, b^i, \qquad \text{avec } \sigma_i \in \{0, \ldots, b-1\} \text{ et } \sigma_{\ell-1} \neq 0.$$

C'est une conséquence de la division euclidienne. Le mot $\rho_b(n) = \sigma_{\ell-1} \cdots \sigma_0$ de longueur ℓ est la *représentation* en base b de n. On dit que $\sigma_{\ell-1}$ (resp. σ_0) est le chiffre de poids fort ou chiffre le plus significatif (resp. le chiffre de poids faible ou le chiffre le moins significatif).

Pour tout entier n, il existe ℓ tel que $b^{\ell-1} \leq n < b^\ell$. Dans ce cas, $\rho_b(n)$ est un mot de longueur ℓ. Ainsi, la longueur $L_b(n) = \ell$ de la représentation en base b de n est donnée par

$$L_b(n) = \lfloor \log_b(n) \rfloor + 1 = \left\lfloor \frac{\ln n}{\ln b} \right\rfloor + 1.$$

Par abus de langage, on s'autorisera à parler de la "longueur de l'entier n" en place de la longueur de la représentation, la base b considérée étant sous-entendue.

Exemple I.8.1. La représentation en base 2 de 73 est donnée par

```
:> BaseForm[73,2]
Out[]= 1001001
```

et on vérifie que

```
:> Log[2,73]//N
Out[]= 6.18982
```

Nous allons voir comment l'écriture en base 2 permet de calculer rapidement une exponentiation modulo m. Ainsi, nous voulons rechercher

$$x^e \mod m \quad \text{avec} \quad e = \sum_{i=0}^{k} e_i \, 2^i.$$

Il est clair que

$$x^e = x^{\sum_{i=0}^{k} e_i \, 2^i} = \prod_{i=0}^{k} (x^{2^i})^{e_i} = \prod_{\substack{0 \leq i \leq k \\ e_i = 1}} x^{2^i}.$$

Si on remarque que $x^{2^{i+1}} = (x^{2^i})^2$, pour calculer $x^e \mod m$, il suffit donc de calculer les $x^{2^i} \mod m$ au moyen de $k = L_b(e) - 1$ élévations successives au carré (modulo m) ainsi que $k = L_b(e) - 1$ produits (modulo m). Ainsi, la complexité de l'algorithme sous-jacent est logarithmique en l'exposant et non pas linéaire comme l'aurait été un algorithme naïf !

Exemple I.8.2. Pour calculer $6^{73} \mod 100$, on a tout d'abord

$$73 = 2^0 + 2^3 + 2^6, \quad \rho_2(73) = 1001001.$$

Ensuite, on calcule le tableau suivant

i	0	1	2	3	4	5	6
$(6^{2^{i-1}})^2$		6^2	36^2	$(-4)^2$	16^2	56^2	36^2
$6^{2^i} \mod 100$	6	36	-4	16	56	36	-4

Enfin, $6^{73} \mod 100 = 6^{2^0}.6^{2^3}.6^{2^6} = 6.16.(-4) = 16 \mod 100$. Pour effectuer ce calcul, nous avons donc eu besoin de 6 élévations au carré et de deux produits dans $\mathbb{Z}_{100}$. Ceci est bien plus efficace qu'une méthode naïve qui aurait nécessité 73 multiplications. Dans `Mathematica`, cette fonction est implémentée comme suit.

```
:> PowerMod[6,73,100]
Out[]= 16
```

9. Complexité d'algorithmes

Dans cette section, nous nous intéressons au temps nécessaire pour réaliser des calculs (addition, produit, inversion,...) dans un champ fini au moyen d'un ordinateur. Nous simplifierons notre propos en considérant uniquement comme opérations élémentaires les opérations sur les bits (par exemple, on ne prendra pas en compte les problèmes liés à l'allocation mémoire et nous négligerons les coûts temporels correspondant). Ces opérations sont supposées être réalisées en un temps constant (bien évidemment cette constante dépend de l'ordinateur employé). Rappelons qu'un *bit* est un élément fondamental de la mémoire ne pouvant prendre que deux valeurs et permettant de coder de l'information.

9.1. Addition de deux entiers. Intéressons-nous tout d'abord à l'addition de deux entiers représentés en base 2. Le choix de la base 2 a une vocation principalement pédagogique. Les processeurs actuels utilisent plutôt une puissance de 2 comme base de représentation. Néanmoins, les raisonnements développés sont assez facilement transposables à un cadre plus réaliste. Ainsi, on peut procéder comme à l'école primaire en effectuant un "calcul écrit". Additionnons 120 et 30 en base deux (ils sont donc représentés chacun par une suite de bits).

report		1	1	1	1				
$\rho_2(120)$			1	1	1	1	0	0	0
$\rho_2(30)$	+				1	1	1	1	0
		1	0	0	1	0	1	1	0

Ainsi, pour chacune des colonnes de bits et en commençant par la droite (par le bit de poids faible), pour obtenir un bit s de la réponse (plus un bit r' de report éventuel), on regarde trois bits (un bit pour chacun des deux nombres à ajouter, a et b, plus un bit r provenant d'un éventuel report). La situation est résumée dans la table I.4.

a	b	r	$\to$	s	r'
0	0	0		0	0
0	1	0		1	0
1	0	0		1	0
1	1	0		0	1
0	0	1		1	0
0	1	1		0	1
1	0	1		0	1
1	1	1		1	1

TABLE I.4. Addition bit à bit.

Le nombre d'opérations élémentaires sur les bits (et par conséquent, le temps nécessaire) pour additionner deux entiers x et y est donc proportionnel à $\max(L_2(x), L_2(y))$, ce qui s'écrit encore[39] $\mathcal{O}(\max(\ln x, \ln y))$.

9.2. Multiplication de deux entiers. Considérons encore notre calcul écrit de l'école primaire pour multiplier deux entiers 25 et 13 représentés en base 2.

				1	1	0	0	1
$\times$					1	1	0	1
				1	1	0	0	1
		1	1	0	0	1		
$+$	1	1	0	0	1			
1	0	1	0	0	0	1	0	1

Ne devrait-on pas enseigner à l'école primaire la multiplication en base 2 ? C'est en fait plus simple qu'en base 10. On recopie simplement !

Dans cet exemple, on a recopié le mot 11001 correspondant au premier facteur autant de fois qu'il y a de "1" dans le second facteur représenté par 1101. Chacune de ces copies est décalée d'un cran vers la gauche (un cran supplémentaire par zéro rencontré). En effet, 13 étant égal à $2^3 + 2^2 + 1$,

$$25 \times 13 = 25 \times 2^3 + 25 \times 2^2 + 25 \times 2^0$$

et multiplier un nombre par une puissance k-ième de la base revient à ajouter k zéros à la fin de la représentation de ce nombre (c'est-à-dire, revient à un décalage de k positions vers la gauche).

On remarque donc que, d'une manière générale, pour multiplier deux entiers x et y, on doit réaliser, de proche en proche, au plus[40] $L_2(y) - 1$ additions entre deux nombres de longueur $L_2(x)$. En effet, pour réaliser une addition arbitraire comme $a_1 + \cdots + a_k$, on peut décider de grouper les termes comme suit,

$$(\cdots((a_1 + a_2) + a_3) + \cdots) + a_k$$

ce qui requiert exactement $k - 1$ additions de deux termes.

[39] Rappelons qu'une fonction $f = \mathcal{O}(g)$ s'il existe N et $C > 0$ tels que pour tout $n \geq N$, $f(n) \leq C\, g(n)$.

[40] Cette borne est atteinte lorsque y est de la forme $1 \cdots 1$, c'est-à-dire si $y = 2^m - 1$.

Expliquons à présent pourquoi on peut considérer être en présence de nombres de longueur $L_2(x)$ lorsqu'on effectue une addition intermédiaire de deux termes. Pour la première addition, on dispose de deux copies de $\rho_2(x)$ dont la seconde a été décalée vers la gauche de $n \geq 1$ positions. A cause de ce décalage, les n bits les plus à droite du premier terme sont simplement recopiés dans la réponse finale et on peut donc considérer être en présence de deux nombres de même longueur $L_2(x)$ (plus exactement, on doit réaliser l'addition d'un nombre de longueur $L_2(x)$ avec un nombre de longueur $L_2(x) - n$). Sur notre exemple, on a

$$\begin{array}{cccccc|cc} & & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & \downarrow & \downarrow \\ \hline 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{array}$$

Ensuite, c'est ce résultat intermédiaire qui sera ajouté à une copie de $\rho_2(x)$ décalée vers la gauche et le même raisonnement s'applique à nouveau,

$$\begin{array}{cccccccc|ccc} & & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 0 & 0 & 1 & \downarrow & \downarrow & \downarrow \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}$$

De là, on en conclut que le temps nécessaire pour multiplier x et y est proportionnel à $L_2(x).L_2(y)$ ou encore $\mathcal{O}(\ln x.\ln y)$ (puisqu'on effectue au maximum $L_2(y) - 1$ additions de deux nombres dont la longueur n'excède pas $L_2(x)$).

Remarque I.9.1. Il existe des techniques plus évoluées pour multiplier deux entiers en réduisant le nombre d'opérations à réaliser. Ainsi, il est possible de calculer le produit de deux nombres de k bits en $\mathcal{O}(k.\ln k.\ln\ln k)$ opérations. Cette borne est même meilleure que $\mathcal{O}(k^{1+\varepsilon})$ et ce, quel que soit $\varepsilon > 0$.

Le cas de la division euclidienne se traite de manière semblable. Signalons que la division euclidienne (quotient et diviseur) d'un entier x tel que $L_2(x) = k$ par un entier y tel que $L_2(y) = \ell$ nécessite un nombre d'opérations élémentaires proportionnel à $\ell(k - \ell + 1)$.

9.3. Algorithme d'Euclide étendu. Rappelons le résultat classique suivant.

Proposition I.9.2 (Algorithme d'Euclide). *Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. En appliquant successivement la division euclidienne, on obtient la suite d'équations*

$$\begin{array}{rcll} b & = & a\,q_1 + r_1, & 0 < r_1 < a \\ a & = & r_1\,q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2\,q_3 + r_3 & 0 < r_3 < r_2 \\ & \vdots & & \\ r_{j-2} & = & r_{j-1}\,q_j + r_j & 0 < r_j < r_{j-1} \\ r_{j-1} & = & r_j\,q_{j+1}. & \end{array}$$

Le pgcd de a et de b est le dernier reste non nul r_j.

Pour la suite, nous posons $r_0 = a$. De cet algorithme, on tire un autre résultat fort utile.

Théorème I.9.3 (Théorème de Bezout). *Soient $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Il existe des entiers relatifs α_0 et β_0 tels que*

$$\mathrm{pgcd}(a, b) = a\,\alpha_0 + b\,\beta_0.$$

Exemple I.9.4. On a

$$\begin{aligned} 735 &= 6.121 + 9 \\ 121 &= 13.9 + 4 \\ 9 &= 2.4 + 1 \\ 4 &= 4.1 \end{aligned}$$

ce qui montre que $\mathrm{pgcd}(735, 121) = 1$ ou encore que 121 est inversible dans $\mathbb{Z}_{735}$. En "remontant" l'algorithme, on peut trouver des coefficients α_0 et β_0 du théorème de Bezout tels que

$$1 = \alpha_0.121 + \beta_0.735$$

et ainsi rechercher l'inverse de 121 dans $\mathbb{Z}_{735}$.

$$\begin{aligned} 1 &= 9 - 2.4 \\ &= 9 - 2.(121 - 13.9) = -2.121 + 27.9 \\ &= -2.121 + 27.(735 - 6.121) = -164.121 + 27.735. \end{aligned}$$

Donc, dans $\mathbb{Z}_{735}$, $121^{-1} = -164 = 571$.

L'algorithme d'Euclide étendu permet de calculer simultanément $\mathrm{pgcd}(a, b)$ et les coefficients α_0 et β_0 du théorème de Bezout. Avec les notations de la proposition I.9.2, on introduit deux suites $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ telles que

$$A_0 = 0,\ A_1 = 1,\ B_0 = 1,\ B_1 = 0,$$

et pour tout $n \geq 1$,

$$A_{n+1} = q_n A_n + A_{n-1} \quad \text{et} \quad B_{n+1} = q_n B_n + B_{n-1}.$$

Avec ces définitions, on obtient le résultat suivant.

Proposition I.9.5. *On a*

$$r_n = (-1)^n A_{n+1}\, a + (-1)^{n+1} B_{n+1}\, b,\ \forall n \geq 0.$$

Démonstration. On procède par récurrence sur n. Pour $n = 0$, c'est immédiat et pour $n = 1$, on a

$$r_1 = -A_2\, a + B_2\, b = -q_1\, a + b.$$

Supposons le résultat vérifié pour les valeurs inférieures à n et vérifions-le pour n.

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_n \\ &= (-1)^n A_{n-1}\, a + (-1)^{n+1} B_{n-1}\, b - ((-1)^{n+1} A_n\, a + (-1)^n B_n\, b) q_n \\ &= (-1)^n (A_{n-1} + A_n\, q_n)\, a + (-1)^{n+1} (B_{n-1} + B_n\, q_n)\, b \\ &= (-1)^n A_{n+1}\, a + (-1)^{n+1} B_{n+1}\, b. \end{aligned}$$

■

Exemple I.9.6. Reprenons le pgcd de $a = 121$ et $b = 735$. On a obtenu

$$q_1 = 6,\ q_2 = 13,\ q_3 = 2,\ q_4 = 4 \text{ et } r_1 = 9,\ r_2 = 4,\ r_3 = 1,\ r_4 = 0.$$

En même temps que le calcul des divisions euclidiennes successives, on peut aussi rechercher les premiers termes des suites A_n et B_n,

$$A_0 = 0,\ A_1 = 1,\ A_2 = q_1 A_1 + A_0 = 6,$$
$$A_3 = q_2 A_2 + A_1 = 79,\ A_4 = q_3 A_3 + A_2 = 164,$$
$$B_0 = 1,\ B_1 = 0,\ B_2 = q_1 B_1 + B_0 = 1,$$
$$B_3 = q_2 B_2 + B_1 = 13,\ B_4 = q_3 B_3 + B_2 = 27.$$

De là, par la proposition précédente, il vient

$$1 = r_3 = (-1)^3 A_4\, 121 + (-1)^4 B_4\, 735 = (-164).121 + 27.735.$$

Remarque I.9.7. Si $b > a > 0$, on peut montrer que la complexité de l'algorithme d'Euclide est $\mathcal{O}(\ln b)$ et pour la version étendue, on a $\mathcal{O}(\ln a . \ln b)$. L'algorithme d'Euclide et sa version étendue peuvent facilement être adaptés au cas de deux polynômes.

Exemple I.9.8. Dans `Mathematica`, on dispose des fonctions suivantes :

```
:> GCD[121,735]
Out[]= 1
:> ExtendedGCD[121,735]
Out[]= {1, {-164,27}}
```

9.4. Opérations dans $\mathbb{F}_q$. Nous savons que les éléments du champ $\mathbb{F}_q$, avec $q = p^f$ (p premier), peuvent être vus comme des polynômes à coefficients dans $\mathbb{F}_p$ (c'est-à-dire dans l'anneau $\mathbb{Z}_p$ des entiers modulo p) regardés modulo un polynôme irréductible M de degré f. Ainsi, un tel élément est caractérisé par un polynôme

$$a_{f-1} X^{f-1} + \cdots + a_0, \quad a_i \in \mathbb{F}_p.$$

Ainsi, l'addition de deux tels objets nécessite f sommes modulo p (on additionne entre eux les coefficients respectifs des deux polynômes, un polynôme de degré $f-1$ ayant f coefficients),

$$[a_{f-1} X^{f-1} + \cdots + a_0] + [b_{f-1} X^{f-1} + \cdots + b_0]$$

$$= (\underbrace{a_{f-1}+b_{f-1}}_{(\mathrm{mod}\ p)})X^{f-1} + \cdots + (\underbrace{a_0+b_0}_{(\mathrm{mod}\ p)}).$$

Si on travaille modulo p, cela signifie que les nombres a_i, b_i rencontrés sont inférieurs à p. Dès lors, la somme de deux éléments de $\mathbb{F}_q$ requiert au total

$$\mathcal{O}(f \ln p)$$

opérations car nous avons vu que la somme de deux nombres $< p$ se réalise (en base 2) en $\mathcal{O}(\ln p)$ opérations (nous admettrons que sur $\mathbb{F}_p$, les coûts sont semblables à ceux obtenus pour les développpements en base 2, il ne serait pas difficile de s'en convaincre).

Une multiplication de deux éléments de $\mathbb{F}_q$ est effectuée grâce à des additions et à des multiplications modulo p. La complexité des additions étant bien inférieure à celle des multiplications, pour estimer le coût d'une multiplication dans $\mathbb{F}_q$, on peut uniquement regarder le nombre de multiplications qui y interviennent. Ainsi, si on réalise le produit de deux polynômes P et Q de degré inférieur à f, $\mathcal{O}(f^2)$ multiplications de coefficients modulo p sont nécessaires pour déterminer tous les coefficients du polynôme $P.Q$,

$$[a_{f-1}X^{f-1} + \cdots + a_0].[b_{f-1}X^{f-1} + \cdots + b_0] = \sum_{j=0}^{2f-2} \underbrace{\left(\sum_{k+\ell=j} a_k.b_\ell \right)}_{(\mathrm{mod}\ p)} X^j.$$

En effet, on remarque que les produits $a_k.b_\ell$ apparaissent tous exactement une fois dans l'expression ci-dessus, $k, \ell \in \{0, \ldots, f-1\}$. De plus chaque multiplication requiert $\mathcal{O}(\ln^2 p)$ opérations. (Comme pour les additions, nous admettrons que sur $\mathbb{F}_p$, les coûts sont semblables à ceux obtenus pour les développpements en base 2 et puisque nous travaillons modulo p, cela revient à considerer le produit de 2 entiers $< p$.) Le coût total de la multiplication est donc $\mathcal{O}(f^2 \ln^2 p) = \mathcal{O}(\ln^2 q)$. Ce n'est pas tout, le polynôme obtenu est de degré au plus $2f-2$ et doit encore être réduit modulo M. Il faut donc réaliser la division euclidienne de $P.Q$ par M. Cette division emploie $\mathcal{O}(f)$ divisions d'entiers modulo p (une division se fait en $\mathcal{O}(\ln^2 p)$) et aussi $\mathcal{O}(f^2)$ multiplications d'entiers modulo p. Ainsi la division prend un temps $\mathcal{O}(f^2 \ln^2 p) = \mathcal{O}(\ln^2 q)$. Les deux étapes nécessitant le même ordre d'opérations, la complexité temporelle d'une multiplication dans $\mathbb{F}_q$ est donc d'ordre

$$\mathcal{O}(\ln^2 q).$$

Effectuer une division dans $\mathbb{F}_q$ revient à multiplier par l'inverse. Ceci peut être réalisé grâce à l'algorithme d'Euclide étendu (adapté aux polynômes de $\mathbb{F}_p[X]$). On peut montrer que la recherche de l'inverse se fait en $\mathcal{O}(\ln^2 q)$ opérations élémentaires.

Le calcul d'une puissance n-ième dans $\mathbb{F}_q$ peut se faire sur la même base que l'exponentiation modulaire présentée à la section 8. Cela nécessite donc $\mathcal{O}(\ln n)$ multiplications dans $\mathbb{F}_q$. Le coût total est donc $\mathcal{O}(\ln n . \ln^2 q)$.

10. A propos des nombres premiers

Nous énonçons dans cette section, quelques faits relatifs à l'ensemble des nombres premiers. En effet, de nombreux cryptosystèmes sont basés sur ces nombres et une connaissance de base de ceux-ci nous paraît dès lors indispensable.

Proposition I.10.1. *Il existe une infinité de nombres premiers.*

Démonstration. Procédons par l'absurde en supposant qu'il n'existe qu'un nombre fini de nombres premiers $2 = p_1 < \ldots < p_k$. Alors, le nombre

$$N = p_1 \cdot p_2 \cdots p_k + 1$$

ne peut être premier puisqu'il est supérieur à p_k. Il est dès lors composé et divisible par un nombre premier p_i. De là, $1 = N - p_1 \cdot p_2 \cdots p_k$ doit donc être divisible par p_i et nous avons obtenu une contradiction.

■

Corollaire I.10.2. *Soit p_k, le k-ième nombre premier. On a*

$$p_k \leq 2^{2^{k-1}}.$$

Démonstration. En effet, tout nombre premier divisant $p_1 \cdots p_k + 1$ est distinct de $p_1, \ldots, p_k$. Ainsi, $p_{k+1} \leq p_1 \cdots p_k + 1$. On procède alors par récurrence. On a $p_1 \leq 2$ et de là[41],

$$p_{k+1} \leq 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 < 2^{2^k}.$$

■

Remarque I.10.3. On peut trouver des plages arbitrairement longues d'entiers consécutifs tous composés. Il suffit de considérer les n entiers consécutifs

$$(n+1)! + 2,\ (n+1)! + 3,\ \ldots,\ (n+1)! + n + 1.$$

Par contre, il est conjecturé qu'il existe une infinité de *nombres premiers jumeaux*, i.e., tels que p et $p+2$ soient premiers.

Nous énonçons sans démonstration les deux résultats suivants.

Théorème I.10.4 (Théorèmes de raréfaction des nombres premiers). *Si $\pi(n)$ désigne le nombre de nombres premiers inférieurs ou égaux à n, alors*

$$\lim_{n\to\infty} \frac{\pi(n) \ln n}{n} = 1.$$

Autrement dit, le quotient $\pi(n)/n$ se comporte asymptotiquement comme $1/\ln n$.

41

$$\underbrace{2.2}_{2\times}\underbrace{2.2.2.2}_{4\times}\cdots\underbrace{2\cdots 2}_{2^{k-1}} = 2^{\sum_{i=1}^{k-1} 2^i} = 2^{2^k-2}.$$

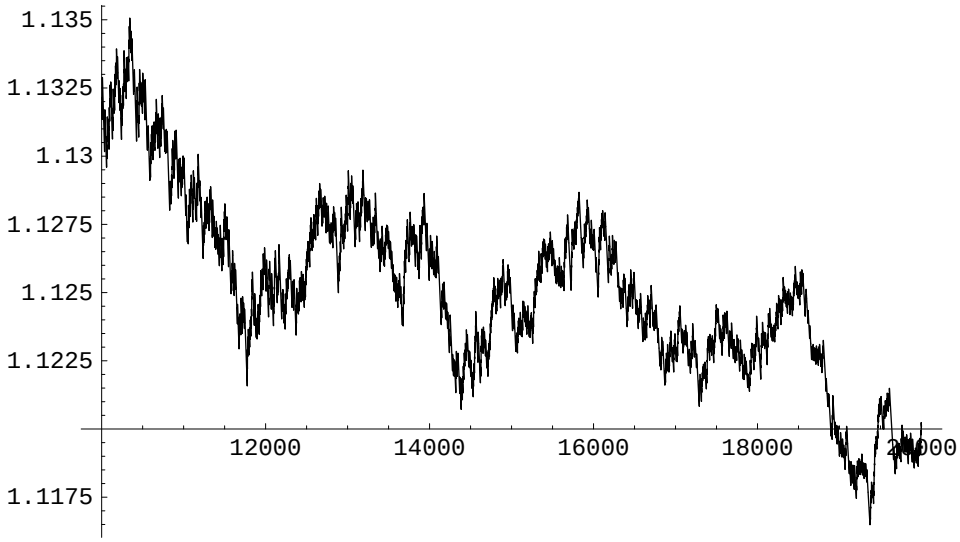


FIGURE I.6. Graphique de $\pi(n)\ \frac{\ln n}{n}$ pour $10^4 \leq n \leq 2.10^4$.

Théorème I.10.5 (Dirichlet). *Si a et b sont premiers entre eux, alors il existe une infinité de nombres premiers de la forme $a + n\,b$.*

Remarque I.10.6. La démonstration de ce résultat général sort du cadre de ce cours. Il est cependant facile de montrer qu'il existe une infinité de nombres premiers de la forme $4n+3$. Supposons qu'il n'existe qu'un nombre fini de nombres premiers $q_1 < \cdots < q_k$ de cette forme. Le nombre

$$N = 4q_1q_2\cdots q_k - 1 = 4(q_1q_2\cdots q_k - 1) + 3$$

est de la forme $4n + 3$. Il ne peut être premier car il serait plus grand que q_k. Dès lors, N est composé. Aucun nombre premier, hormis 2, n'est de la forme $4n + 2$ ou $4n$. Donc aucun facteur de ce type n'intervient dans la décomposition de N en facteurs premiers. De plus, N ne peut contenir dans sa décomposition uniquement des facteurs de la forme $4n + 1$ car il serait alors lui-même de cette forme. On en conclut que N doit contenir un facteur premier q_i de la forme $4n + 3$. On en tire alors que $1 = 4q_1q_2\cdots q_k - N$ doit être divisible par q_i, ce qui est impossible.

Une *progression arithmétique de nombres premiers* de longueur ℓ est un ensemble de la forme $\{p + k\,d \text{ premier},\ k = 0, \ldots, \ell - 1\}$. Par exemple, voici une progression de longueur 10.

$$199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089$$

Un résultat récent (2004) et remarquable, dont la preuve est hautement difficile montre que des progressions arithmétiques arbitrairement longues de nombres premiers existent. Il s'agit d'une sorte de "réciproque" au théorème de Dirichlet.

Théorème I.10.7 (Ben Green - Terence Tao [**7**]). *Pour tout entier ℓ, l'ensemble des nombres premiers contient une progression arithmétique de longueur ℓ.*

CHAPITRE II

Cryptographie

1. Introduction

L'objectif premier de la cryptographie est de permettre l'échange d'informations de manière "sécurisée" entre deux personnes (typiquement appelées Alice et Bob) par l'intermédiaire d'un canal peu sûr pouvant être espionné par un opposant (typiquement appelé Oscar). On peut imaginer que le canal employé est une ligne téléphonique ou le réseau Internet. L'information que désire transmettre Alice peut par exemple être un texte en français ou une suite de bits ou d'entiers. On l'appellera le *texte clair*. Pour ne pas permettre à Oscar de comprendre le contenu du texte clair, Alice transforme ce texte par un procédé de *chiffrement* en utilisant une clé déterminée. Le texte obtenu après chiffrement est appelé *texte chiffré* et c'est ce dernier qui est envoyé à Bob au moyen du canal de transmission. Bob, connaissant la clé utilisée par Alice, peut alors *déchiffrer* le texte chiffré pour réobtenir le texte clair. L'opposant Oscar ne connaissant pas la clé de chiffrement ne peut quant à lui réobtenir "facilement" le texte clair.

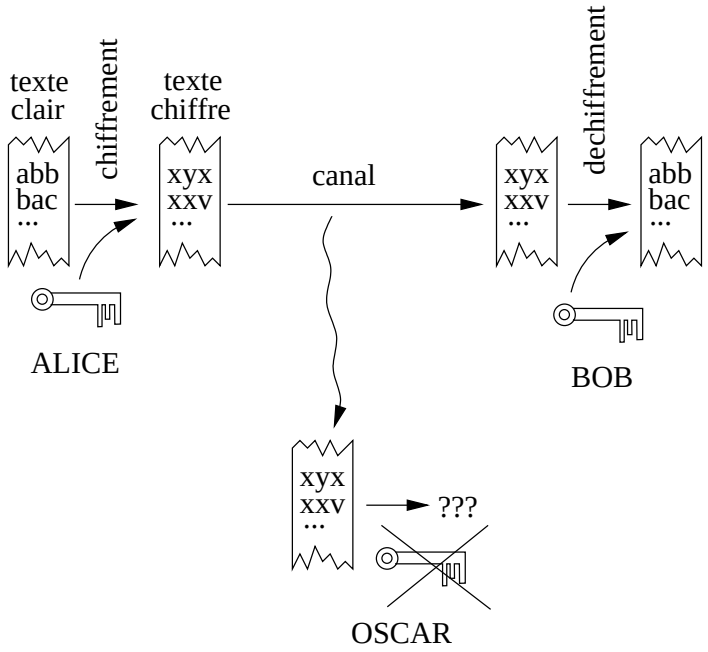


FIGURE II.1. Le canal de communication.

De manière plus formelle, on dispose de la définition suivante.

Définition II.1.1. On appelle *système cryptographique* ou *cryptosystème* un triplet[1] $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ satisfaisant les conditions suivantes :

- $\mathcal{P}$ est l'ensemble fini des *textes clairs* possibles (*plaintexts*),
- $\mathcal{C}$ est l'ensemble fini des *textes chiffrés* possibles (*ciphertexts*),
- $\mathcal{K}$ est l'ensemble fini des clés possibles, appelé parfois espace des clés (*keys*),
- Pour tout $k \in \mathcal{K}$, il existe une *fonction de chiffrement* (*encryption rule*) e_k telle que

$$e_k : \mathcal{P} \to \mathcal{C} : t \mapsto e_k(t)$$

et il existe une *fonction de déchiffrement* (*decryption rule*) d_k telle que

$$d_k : \mathcal{C} \to \mathcal{P} : t \mapsto d_k(t) \quad \text{et} \quad \forall t \in \mathcal{P},\ d_k(e_k(t)) = t.$$

Remarque II.1.2. Pour permettre le déchiffrage, la fonction e_k doit bien évidemment être injective pour tout $k \in \mathcal{K}$.

Exemple II.1.3. Ce premier exemple simpliste consiste en la présentation du *chiffrement par décalage*. Ici, nous prenons $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ et pour tout $k \in \{0, \ldots, 25\}$, on pose

$$e_k(x) = (x + k) \mod 26 \quad \text{et} \quad d_k(y) = (y - k) \mod 26.$$

Si Alice désire envoyer à Bob sur le canal peu sûr une suite

$$\mathbf{x} = x_1 x_2 \cdots x_\ell, \quad x_i \in \mathcal{P},$$

elle la chiffrera au préalable avec une fonction e_k (pour un $k \in \mathcal{K}$ choisi de commun accord avec Bob dans un lieu supposé à l'abri de l'opposant Oscar) et transmettra alors à Bob, la suite

$$\mathbf{y} = e_k(x_1)e_k(x_2)\cdots e_k(x_\ell).$$

Une étape souvent préalable au chiffrement est le *codage*. Nous appelons codage l'ensemble des conventions prises pour modifier le texte clair en un texte équivalent[2] plus simple à traiter du point de vue cryptographique. Expliquons notre propos sur un exemple. Si Alice veut transmettre le message "`bonsoir`", nous pouvons convenir que chaque lettre est remplacée par sa position dans l'alphabet $\Sigma = \{\mathtt{a}, \ldots, \mathtt{z}\}$ (en commençant par coder `a` par 0). Ainsi, le texte clair "`bonsoir`" est *codé* en "$\mathbf{x}$ = 1,14,13,18,14,8,17". Notre codage est simplement une bijection entre l'alphabet Σ et l'ensemble $\{0, \ldots, 25\}$. L'application inverse sera naturellement appelée *décodage*. Attirons l'attention du lecteur sur le fait que codage et chiffrement sont deux notions distinctes. Si la clé choisie est $k = 3$ (il est de coutume d'attribuer

[1] Nous avons choisi de conserver ici les notations anglo-saxonnes.

[2] Le codage est donc une bijection.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

TABLE II.1. Un premier codage.

le cryptosystème par décalage avec le choix de la clé $k = 3$ à Jules César), alors le texte devient

$$\mathbf{y} = e_3(1)e_3(14)e_3(13)e_3(18)e_3(14)e_3(8)e_3(17) = 4, 17, 16, 21, 17, 11, 20.$$

Ce texte chiffré s'écrit sous forme équivalente, grâce à nos conventions de codage, "`erqvrlu`". On comprend aisément comment Bob pourra décoder ce message et retrouver le texte clair original.

Il est assez facile de se convaincre que ce cryptosystème est peu sûr. En effet, si Oscar obtenait le texte "`erqvrlu`", il pourrait aisément retrouver le texte clair ne serait-ce qu'en essayant de manière exhaustive les 26 clés possibles et en regardant si les textes obtenus ont ou non un sens. On appelle *cryptanalyse* l'ensemble des moyens et techniques mis en oeuvre pour retrouver le texte clair ou au moins une certaine information contenue dans celui-ci. Si Oscar ne connaît pas le cryptosystème utilisé pour chiffrer le texte clair, la cryptanalyse sera plus ardue mais il serait illusoire de baser la sécurité d'un système sur la protection (plus qu'incertaine) de la description des fonctions cryptographiques employées. Le *principe de Kerckhoff* suppose qu'Oscar connaît le cryptosystème utilisé. La sécurité du système réside alors dans la protection de la clé k choisie par Alice et Bob. Les types d'attaque dont dispose Oscar sont les suivantes (par ordre de difficulté décroissante)

- **Texte chiffré connu** : Oscar connaît uniquement un fragment de texte chiffré $\mathbf{y}$ qu'il a intercepté. Dans des cryptosystèmes évolués, il est souvent nécessaire pour réaliser la cryptanalyse de connaître de longs fragments de texte.
- **Texte clair connu** : Oscar connaît un texte clair $\mathbf{x}$ et le texte chiffré $\mathbf{y}$ correspondant. Dans le cryptosystème de César, pour réaliser la cryptanalyse, il suffit simplement de connaître une lettre et son équivalent chiffré pour retrouver la clé.
- **Texte clair choisi** : Oscar a accès à une machine chiffrante. Il peut choisir un texte clair $\mathbf{x}$ et obtenir le texte chiffré $\mathbf{y}$ correspondant. Une telle attaque est souvent utile au cryptanalyste ayant déjà énoncé des conjectures sur la clé du cryptosystème. Une attaque à texte clair choisi peut par exemple être réalisée par Oscar, lorsque ce dernier peut masquer son identité et avoir accès à une machine réalisant le chiffrement (sans pour autant connaître la clé utilisée).

- **Fonction de chiffrement connue** : Oscar connaît précisément la fonction utilisée pour le chiffrement. Son but est alors de découvrir la fonction de déchiffrement. Cette situation est typique des cryptosystèmes à clé publique que nous rencontrerons dans le chapitre suivant.
- **Texte chiffré choisi** : Oscar a temporairement accès à une machine déchiffrante. Il peut choisir un texte chiffré $\mathbf{y}$ et obtenir le texte clair $\mathbf{x}$ correspondant.

Nous reviendrons plus loin sur quelques techniques de cryptanalyse.

2. Implémentation et codage

Comme nous l'a montré l'exemple précédent, la première étape dans l'élaboration d'un procédé cryptographique consiste en le *codage* du texte clair. Il ne s'agit pas de chiffrement à proprement parler, mais simplement de l'application des conventions choisies comme base préalable au chiffrement. Nous avons décidé ici de prendre un alphabet contenant 32 symboles. En effet, il est souvent commode, pour des raisons d'efficacité d'implémentation, de travailler sur un alphabet (mais aussi modulo une puissance de deux). Sans entrer dans les détails, un choix convenable de la "base" permet parfois d'accélérer certains calculs. Pour ne pas alourdir l'exposé, nous avons réduit notre alphabet à 32 symboles comprenant les lettres minuscules, un espace et quelques signes de ponctuation. On aurait tout aussi bien pu considérer l'ensemble des 256 caractères du codage ASCII, voir même l'ensemble des 2^{16} caractères UNICODE. Ainsi, nous définissons la liste suivante.

```
:> alphabet = {" ", "a", "b", "c", "d", "e", "f", "g", "h", "i",
     "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u",
     "v", "w", "x", "y", "z", ",", ".", "'", ":", "?"};
```

La fonction `code` prend comme argument une chaîne de caractères et renvoie une liste d'entiers compris entre 0 et 31 correspondant aux positions occupées par les lettres de la chaîne dans l'alphabet.

```
:> code[mot_] :=
    Map[Position[alphabet,#][[1,1]]-1 &, Characters[mot]]
```

Ainsi, si on considère le texte clair suivant,

```
:> texteclair =  "le jour de ses onze ans, harry potter, un
     orphelin eleve par un oncle et une tante qui le detestent,
     voit son existence bouleversee.";
```

l'application de la fonction `code` donne

```
:> codetxclair = code[texteclair]
Out[]= {12, 5, 0, 10, 15, 21, 18, 0, 4, 5, 0, 19, 5, 19, 0, 15, 14,
 26, 5, 0, 1, 14, 19, 27, 0, 8, 1, 18, 18, 25, 0, 16, 15, 20, 20, 5,
 18, 27, 0, 21, 14, 0, 15, 18, 16, 8, 5, 12, 9, 14, 0, 5, 12, 5, 22,
 5, 0, 16, 1, 18, 0, 21, 14, 0, 15, 14, 3, 12, 5, 0, 5, 20, 0, 21,
 14, 5, 0, 20, 1, 14, 20, 5, 0, 17, 21, 9, 0, 12, 5, 0, 4, 5, 20, 5,
```

```
 19, 20, 5, 14, 20, 27, 0, 22, 15, 9, 20, 0, 19, 15, 14, 0, 5, 24, 9,
 19, 20, 5, 14, 3, 5, 0, 2, 15, 21, 12, 5, 22, 5, 18, 19, 5, 5, 28}
```

Implémentons directement la fonction de décodage qui à une liste de nombres associe une chaîne de caractères.

```
:> decode[liste_] :=
    StringJoin[
      Table[alphabet[[liste[[i]] +1]], {i,1,Length[liste]}] ]
```

On pourra vérifier que `decode[codetxclair]` rend bien le texte initial. Considérons à présent la méthode de chiffrement par décalage de Jules César introduite dans l'exemple II.1.3.

```
:> cesar[n_] := Mod[n+3,32]
:> codetxchiffre = cesar[codetxclair]
Out[]={15, 8, 3, 13, 18, 24, 21, 3, 7, 8, 3, 22, 8, 22, 3, 18, 17,
 29, 8, 3, 4, 17, 22, 30, 3, 11, 4, 21, 21, 28, 3, 19, 18, 23, 23,
 8, 21, 30, 3, 24, 17, 3, 18, 21, 19, 11, 8, 15, 12, 17, 3, 8, 15,
 8, 25, 8, 3, 19, 4, 21, 3, 24, 17, 3, 18, 17, 6, 15, 8, 3, 8, 23,
 3, 24, 17, 8, 3, 23, 4, 17, 23, 8, 3, 20, 24, 12, 3, 15, 8, 3, 7,
 8, 23, 8, 22, 23, 8, 17, 23, 30, 3, 25, 18, 12, 23, 3, 22, 18, 17,
 3, 8, 27, 12, 22, 23, 8, 17, 6, 8, 3, 5, 18, 24, 15, 8, 25, 8, 21,
 22, 8, 8, 31}
```

Sous forme de texte, on obtient

```
:> txchiffre = decode[codetxchiffre]
Out[]= "ohcmrxucghcvhvcrq'hcdqv:ckduu.csrwwhu:cxqcruskholqchohy
   hcsducxqcrqfohchwcxqhcwdqwhctxlcohcghwhvwhqw:cyrlwcvrqch,lvw
   hqfhcerxohyhuvhh?"
```

Plaçons-nous un instant dans la peau de l'opposant Oscar. Imaginons ne pas savoir au moyen de quelle clé ce texte a été chiffré et supposons disposer uniquement du texte chiffré (ou de manière équivalente, de la variable `codetxchiffre`). En vertu du principe de Kerckhoff, nous supposons également savoir que le texte a été chiffré par décalage. Pour la cryptanalyse du texte (i.e., tenter de déterminer la clé secrète), on peut réaliser une analyse de la fréquence des lettres apparaissant dans le texte de la manière suivante.

```
:> Map[Count[codetxchiffre,#] &, Table[i, {i,0,31}]]
Out[]={0, 0, 0, 23, 4, 1, 2, 2, 24, 0, 0, 2, 4, 1, 0, 6,
       0, 11, 8, 3, 1, 7, 7, 10, 6, 3, 0, 1, 1, 1, 3, 1}
```

Cette analyse montre que la lettre la plus fréquemment rencontrée est la huitième lettre de notre alphabet, i.e., le "h". De là, puisque la lettre "e" apparaît le plus souvent en français (cf. table II.2), on peut penser que le cryptosystème employé remplace "e" par "h" et de là, on retrouve la clé secrète 3.

Remarque II.2.1. A titre indicatif, voici la table des fréquences d'apparition des différentes lettres apparaissant dans les textes écrits en français.

lettre	%
e	15,87
a	9,42
i	8,41
s	7,90
t	7,26
n	7,15
r	6,46
u	6,24
l	5,34

TABLE II.2. Fréquence d'apparition des lettres en français.

On peut considérer comme unité fondamentale pour réaliser le codage d'une chaîne de caractères, non pas une simple lettre, mais un bloc de m lettres consécutives (ou de manière équivalente, m entiers). Un bloc $t_1 \cdots t_m$ de $m \geq 1$ entiers consécutifs, tous inférieurs à 32, représente un nombre n écrit en base 32,

$$n = \sum_{j=1}^{m} t_j \, 32^{m-j}.$$

Ce bloc de longueur m représente donc un nombre $0 \leq n \leq 32^m - 1$. Ainsi, une méthode alternative pour le codage d'un texte clair, revient à considérer m lettres consécutives et à en calculer la valeur correspondante. Avec notre définition II.1.1, $\mathcal{P} = \mathcal{C}$ est maintenant égal à $\mathbb{Z}_{32^m}$ et non plus $\mathbb{Z}_{32}$.

Remarque II.2.2. Utiliser un codage dans lequel on considère des blocs de m éléments augmente la sécurité du cryptosystème. En effet, sur notre exemple, l'espace des clés passe de $\mathcal{K} = \mathbb{Z}_{32}$ à $\mathcal{K} = \mathbb{Z}_{32^m}$. Puisque le nombre de clés augmente, une recherche exhaustive menée par Oscar et qui consisterait à passer en revue l'ensemble de toutes les clés possibles jusqu'à l'obtention d'un texte clair raisonnable prendrait beaucoup plus de temps (si $m = 5$, $32^5 \simeq 33 \times 10^6$ et en testant 1000 clés par seconde, il faudrait à Oscar un peu plus de 9 heures pour parcourir l'espace des clés).

Si nous découpons le texte clair en tronçons de longueur m, il faudrait que ce texte soit de longueur divisible par m. S'il ne l'était pas, on ajouterait[3] au préalable des symboles à la fin du texte pour que sa longueur soit divisible par m. Cette première fonction est réalisée par `ajout` qui prend comme arguments une liste d'entiers et un entier m et renvoie une liste d'entiers

[3]Par facilité, c'est la méthode que nous décidons d'employer ici. Attirons néanmoins l'attention du lecteur sur le fait qu'un tel choix peut mettre en péril la sécurité du cryptosystème. En effet, si Oscar connaît cette convention (et on ne peut pas supposer qu'il ne la connaisse pas), alors cette information pourrait lui permettre d'obtenir des renseignements sur la clé choisie k.

éventuellement complétée par des zéros pour que sa longueur soit divisible par m.

```
:> ajout[liste_,m_] :=
      PadRight[liste, Length[liste]+Mod[-Length[liste],m]]
```

Notre texte clair est de longueur 132. En effet, on a

```
:> Length[codetxclair]
Out[] = 132
```

Ce nombre n'est pas divisible par 5. Appliquons alors notre nouvelle fonction et remplaçons directement notre codage du texte clair.

```
:> codetxclair = ajout[codetxclair,5]
Out[] = {12, 5, 0, 10, 15, 21, 18, 0, 4, 5, ...
       ... , 21, 12, 5, 22, 5, 18, 19, 5, 5, 28, 0, 0, 0}
```

Trois zéros ont donc bien été ajoutés à la fin de notre liste. Nous pouvons à présent considérer un bloc de m entiers comme la représentation en base 32 d'un entier. Pour ce faire, utilisons la fonction suivante.

```
:> codebloc[liste_,m_] :=
           Map[FromDigits[#,32] &, Partition[liste,m]]
```

Ainsi, chaque suite de 5 entiers est remplacée par la valeur qu'elle représente en base 32.

```
:> codetxclair = codebloc[codetxclair,5]
Out[] = {12747087, 22610053, 628320, 16214176, 1527648, 8440409,
 540308, 5860373, 14696016, 8565038, 176310, 5259314, 702479,
 14790816, 5898926, 5263406, 21135925, 9449632, 4378803,
 21150363, 736564, 638400, 6039156, 5704864, 2610565, 23251557,
 6160384}
```

Par exemple, $\mathbf{12}.32^4+\mathbf{5}.32^3+\mathbf{0}.32^2+\mathbf{10}.32+\mathbf{15} = 12747087$. Implémentons directement une fonction de décodage qui, à une liste d'entiers compris entre 0 et 32^m-1, fournit une chaîne de caractères (m caractères sont fournis par entier).

```
:> decodebloc[liste_,m_] :=
    decode[Flatten[Map[IntegerDigits[#,32,m] &, liste]]]
```

On peut vérifier que cette fonction rend bien le texte clair lorsqu'on l'applique à `codetxclair`. Pour procéder à un chiffrement semblable au chiffrement de César, nous avons ici la possibilité de translater par une constante $k < 32^m$ et nous travaillons bien évidemment modulo 32^m (sur notre exemple, $m = 5$). Par exemple, on a

```
:> codetxchiffre = Mod[codetxclair+12345678, 32^5]
Out[] = {25092765, 1401299, 12973998, 28559854, 13873326,
  20786087,12885986, 18206051, 27041694, 20910716, 12521988,
  17604992, 13048157, 27136494, 18244604, 17609084, 33481603,
  21795310, 16724481, 33496041, 13082242, 12984078, 18384834,
  18050542, 14956243, 2042803, 18506062}
```

`code[mot]`	chaîne de longueur n $\mapsto$ liste de n éléments de $\mathbb{Z}_{32}$
`decode[liste]`	liste de n éléments de $\mathbb{Z}_{32}$ $\mapsto$ chaîne de longueur n
`ajout[liste,m]`	liste quelconque $\mapsto$ liste de longueur divisible par m
`codebloc[liste,m]`	liste de $n.m$ éléments de $\mathbb{Z}_{32}$ $\mapsto$ liste de n éléments de $\mathbb{Z}_{32^m}$
`decodebloc[liste,m]`	liste de n éléments de $\mathbb{Z}_{32^m}$ $\mapsto$ chaîne de longueur $n.m$.

TABLE II.3. Fonctions implémentées.

Ceci donne sous forme d'une chaîne de caractères chiffrée, le résultat suivant.

```
:> decodebloc[codetxchiffre, 5]
Out[]= "w'xt'ajxnslk''n,gronmglenszj'glig?bqkskcyyg.:s:ds.k:dpd
  pyhl lnfj'y.donqlx?.pylk.?'x.ctydono:lpa?:f?ilogtbllgxnqqa:bq
  f,onnhmvsa:j'sqtxjn"
```

Pour que Bob puisse retrouver le texte original, il lui suffit d'effectuer

```
:> decodebloc[Mod[codetxchiffre-12345678, 32^5],5]
```

Cette méthode consistant à considérer des blocs de m lettres comme unité de base, ne modifie en rien les techniques employées (par exemple ici, le chiffrement par décalage). La sécurité du cryptosystème est "artificiellement" augmentée simplement parce qu'on a à sa disposition 32^m clés de longueur m au lieu des 32 clés initiales. Pour cette simple raison, la cryptanalyse est dès lors plus délicate (il est bien plus long et difficile de deviner la clé.). Par exemple, dans la première version ($m = 1$), chaque "`e`" du texte clair était remplacé par un "`h`", alors qu'ici, des "`e`" différents peuvent être remplacés par des lettres différentes lorsqu'ils se trouvent dans des blocs distincts de longueur m. Néanmoins, un bloc donné $x_1 \cdots x_m \in \mathcal{P} = \mathbb{Z}_{32^m}$ est toujours transformé en un même bloc $e_k(x_1 \cdots x_m)$. Pour cette raison, on parle de cryptosystème monoalphabétique.

En résumé, dans les autres sections de ce chapitre, nous supposerons disposer des cinq fonctions suivantes reprise à la table II.3.

3. Quelques cryptosystèmes classiques

3.1. Chiffrement par substitution. Si $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32}$ (on pourrait sans aucune restriction considérer d'autres ensembles de textes clairs et chiffrés), alors $\mathcal{K}$ est l'ensemble des permutations de $\{0, \ldots, 31\}$, i.e.,

$$\mathcal{K} = \{\nu \in \mathcal{S}_{32} \mid \nu : \mathbb{Z}_{32} \to \mathbb{Z}_{32} \text{ bijection}\}.$$

Par rapport au chiffrement par décalage, le chiffrement par substitution présente l'avantage que $\#\mathcal{K}$ est grand : ici, $32! \simeq 2,6 \times 10^{35}$. Les fonctions de chiffrement et déchiffrement sont pour la clé $k = \nu$,

$$e_k(x) = \nu(x) \quad \text{et} \quad d_k(y) = \nu^{-1}(y).$$

Exemple II.3.1. Considérons la permutation suivante

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
e	:	d	k	,	l	p	n		q	x	f	s	z	.	u

p	q	r	s	t	u	v	w	x	y	z	,	.	’	:	?
’	a	c	i	g	?	t	v	o	y	w	r	b	m	j	h

Il est facile de voir que le texte clair :

```
le jour de ses onze ans, harry potter, un orphelin eleve par
un oncle et une tante qui le detestent, voit son existence
bouleversee.
```

est chiffré en

```
slexu?ce,leilieu.wle:.i,e :ccye’ugglc,e?.euc’ lsq.elsltle’:c
e?.eu.kslelge?.leg:.glea?qesle,lgligl.g,etuqgeiu.eloqigl.kl
edu?sltlcillb
```

Bien que le nombre de clés disponibles soit important, ce cryptosystème peut être aisément cassé en effectuant une analyse des fréquences. On peut non seulement rechercher les lettres apparaissant le plus souvent, mais aussi les couples ou les triplets. De là, il est aisé de retrouver le texte clair. Ce cryptosystème ne peut dès lors être considéré comme sûr et son seul intérêt réside dans les cryptogrammes que l'on trouve dans les livres de jeux.

3.2. Chiffrement affin. Prenons $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Soient a et b appartenant à $\mathbb{Z}_n$ avec a inversible dans $\mathbb{Z}_n$ (i.e., $pgcd(a, n) = 1$). Ainsi, on a

$$\mathcal{K} = \{(a, b) \mid a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$$

et pour une clé $k = (a, b)$ choisie dans $\mathcal{K}$, on a

$$e_k(x) = ax + b \mod n \quad \text{et} \quad d_k(y) = a^{-1}(y - b) \mod n.$$

Il faut prendre a inversible pour que la fonction e_k soit injective. Le nombre de clés est bien évidemment $n\,\varphi(n)$. Avec les fonctions dont nous disposons, le chiffrement affin est très simple à mettre en oeuvre.

Exemple II.3.2. Dans Mathematica, considérons le texte suivant.

```
:> texteclair = "ving minutes plus tard, harry sortit du magasin
     de hiboux avec une grande cage a l’interieur de laquelle
     une magnifique chouette aux plumes blanches comme la neige
     dormait paisiblement.";
```

Pour chiffrer ce texte, on peut procéder comme suit (ici $k = (13, 8)$),

```
:> decode[Mod[13 code[texteclair]+8, 32]]
Out[]= "f':chq':yli?hxdy?hlur.gpurrmh?krl'lh.yhqucu?':h.ihp'bk
  y hufiohy:ihcru:.ihoucihuhda':lir'iyrh.ihdueyiddihy:ihquc:'v
  'eyihopkyillihuy hxdyqi?hbdu:opi?hokqqihduh:i'cih.krqu'lhxu'
  ?'bdiqi:lt"
```

Le chiffrement affin étant un cas particulier de chiffrement par substitution, on réalise sa cryptanalyse en recourant à des méthodes d'analyse statistique des fréquences d'apparition des lettres.

3.3. Chiffrement de Vigenère. Les chiffrements par décalage, par substitution et affin sont des exemples de systèmes *monoalphabétiques*. En effet, la fonction de chiffrement e_k s'applique à un seul élément de $\mathcal{P}$ à la fois (le plus souvent une lettre ou de manière équivalente un élément de $\mathbb{Z}_{32}$) et à chaque élément de $\mathcal{P}$ est appliquée la même fonction de chiffrement. Même lorsqu'on a considéré un bloc de m symboles consécutifs, il s'agissait une fois encore d'un système monoalphabétique car dans ce cas, l'ensemble $\mathcal{P}$ était $\mathbb{Z}_{32^m}$ et la fonction de chiffrement s'appliquait toujours à un unique élément de $\mathcal{P}$ à la fois. Le chiffrement de Vigenère[4] est *polyalphabétique* car il traite m symboles simultanément. Il s'agit en quelque sorte de m chiffrements par décalage. Ici,

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{32})^m,$$

si $k = (k_1, \ldots, k_m) \in (\mathbb{Z}_{32})^m$, alors

$$e_k(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m) \mod 32$$

et

$$d_k(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m) \mod 32.$$

On peut convenir que pour chiffrer une suite de longueur $rm + s$ constituée de r m-uples d'éléments de $\mathbb{Z}_{32}$ suivie d'un s-uple d'éléments de $\mathbb{Z}_{32}$ avec $0 \leq s < m$,

$$\mathbf{x} = x_1 \cdots x_m \,|\, \cdots \,|\, x_{(r-1)m+1} \cdots x_{rm} \,|\, x_{rm+1} \cdots x_{rm+s},$$

on calculera

$$\begin{aligned} \mathbf{y} \;=\; & (x_1 + k_1) \cdots (x_m + k_m) \,|\, \cdots \,|\, (x_{(r-1)m+1} + k_1) \cdots (x_{rm} + k_m) \,| \\ & (x_{rm+1} + k_1) \cdots (x_{rm+s} + k_s) \mod 32. \end{aligned}$$

Exemple II.3.3. L'implémentation est presque immédiate.

```
:> codetxclair = code[texteclair]
Out[] = {22, 9, 14, 7, 0, 13, 9, 14, 21, 20, ...}

:> vigenere[liste_,cle_] :=
     Mod[liste+PadRight[cle,Length[liste],cle],32]

:> codetxchiffre = vigenere[codetxclair,{10,8,20}]
```

[4] Blaise de Vigenère, XVIè siècle.

```
Out[] = {0, 17, 2, 17, 8, 1, 19, 22, 9, 30, ...}
:> decode[codetxchiffre]
Out[] = "qbqhasvi:mgjx ?,t:ifnc.kzfchgyzhs.tn'twi,k,'xhxoh.sjc? t
k:ymhixmtqzuxlyjkuqmtkh gqb:mfsmi.hxoh kyiot ohixmtwi,xqzsyiohwrw
io.hohu? tztiwmgjj kvwrmgjkcwuyjtujvysoyjlc.uus.tzi''qvvmaovhf"
```

Pour le déchiffrement, c'est immédiat !

```
:> vigenere[codetxchiffre, -{10,8,20}]
Out[] = {22, 9, 14, 7, 0, 13, 9, 14, 21, 20, ...}
```

Dans le chiffrement de Vigenère, un même symbole peut être transformé en m symboles distincts suivant la position qu'occupe ce symbole dans un m-uple donné.

Nous ne parlerons pas de la cryptanalyse du chiffrement de Vigenère. Celle-ci peut être réalisée assez facilement (test de Kasiski ou utilisation d'un indice de coïncidence) et n'apporte pas d'arguments utiles à la suite de notre exposé.

3.4. Chiffrement de Hill. Tout comme dans l'exemple précédent, le chiffrement de Hill[5] est un cryptosystème polyalphabétique. On prend $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{32})^m$ et l'espace des clés est

$$\mathcal{K} = GL_m(\mathbb{Z}_{32}),$$

l'ensemble des matrices inversibles à coefficients dans $\mathbb{Z}_{32}$. Il est clair qu'on peut une fois encore remplacer $\mathbb{Z}_{32}$ par un $\mathbb{Z}_n$ quelconque. Il faudra cependant au lecteur une certaine dose de courage (voire une dose certaine), pour aller relire les développements réalisés dans le cours d'algèbre linéaire (calcul matriciel) et pour remarquer que les propriétés que nous utiliserons dans $\mathbb{Z}_n$ ne font intervenir que des notions telles que linéarité du déterminant, définition du produit matriciel, existence éventuelle d'un inverse, etc... et sont donc transposables à un anneau quelconque, comme par exemple $\mathbb{Z}_n$.

La proprosition suivante montre qu'il faut perdre le reflexe habituel acquis sur un champ comme $\mathbb{R}$ ou $\mathbb{C}$.

Proposition II.3.4. *Une matrice carrée A à coefficients dans $\mathbb{Z}_n$ est inversible, i.e., il existe B tel $AB = BA = I$, si et seulement si son déterminant est inversible dans $\mathbb{Z}_n$.*

Démonstration. Il est bien connu (règle des mineurs) que

$$A\,\widetilde{\mathrm{cof}(A)} = \det A\; I = \widetilde{\mathrm{cof}(A)}\,A$$

où $\mathrm{cof}(A)$ désigne la matrice des cofacteurs (ou mineurs algébriques) de A. Cette proposition est classiquement démontrée sur $\mathbb{R}$ ou sur $\mathbb{C}$ et s'étend aisément à $\mathbb{Z}_n$. Ainsi, si $\det A$ est inversible, l'inverse de A est donné par $(\det A)^{-1}\widetilde{\mathrm{cof}(A)}$.

[5] Lester S. Hill (1929).

Réciproquement, si A est inversible et d'inverse A^{-1}, alors

$$1 = \det(AA^{-1}) = \det A \det A^{-1}$$

ce qui montre que $\det A$ est inversible.

■

Remarque II.3.5. Pour que le chiffrement soit réalisable, il suffit d'observer que *la matrice A détermine une bijection $x \mapsto Ax$ de $(\mathbb{Z}_n)^m$ dans lui-même si et seulement si A est inversible.*

Supposons A inversible. Pour tous x, y tels que $Ax = Ay$, en multipliant par A^{-1}, on trouve $x = y$ et l'application est donc injective. Elle est aussi surjective: pour tout $y \in (\mathbb{Z}_n)^m$, $x = A^{-1}y$ est tel que $Ax = y$.

Passons à la réciproque. Puisque l'application $x \mapsto Ax$ est en particulier surjective, pour tout vecteur unitaire e_i, $i = 1, \ldots, m$, il existe un vecteur colonne C_i tel que $AC_i = e_i$. De là, la matrice dont les colonnes sont $C_1, \ldots, C_m$ est inverse de A.

Ainsi, si A n'est pas inversible, alors l'application $x \mapsto Ax$ n'est ni injective ni surjective (car $(\mathbb{Z}_n)^m$ étant fini, elle est injective si et seulement si elle est surjective). Dès lors, il existe des vecteurs $x, y \in (\mathbb{Z}_n)^m$ distincts tels que $Ax = Ay$. Ceci est bien évidemment problématique, des textes clairs distincts ne peuvent pas avoir même chiffrement.

Si la clé choisie est $k = (a_{ij}) \in GL_m(\mathbb{Z}_{32})$, la fonction de chiffrement $e_k : \mathbb{Z}_{32}^m \to \mathbb{Z}_{32}^m : (x_1, \ldots, x_m) \mapsto (y_1, \ldots, y_m)$ est donnée par

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Appliquons ce chiffrement à l'exemple suivant.

Exemple II.3.6. Voici tout d'abord les données.

```
:> code[texteclair]="le phenix sur lequel a ete preleve la plume
qui se trouve dans votre baguette a egalement fourni une autre
plume a une autre baguette."

:> a= {{5,17}, {4,21}};
```

Ainsi, la matrice A réalisant le chiffrement de Hill est

$$A = \begin{pmatrix} 5 & 17 \\ 4 & 21 \end{pmatrix}.$$

Nous décidons de couper le texte clair en tronçon de longueur 2 et ajoutons éventuellement des zéros à la fin.

```
:> codetxclair = ajout[code[texteclair],2]
Out[] = {12, 5, 0, 16, 8, 5, 14, 9, 24, 0, ...}
```

et pour le chiffrement de Hill, on procède comme suit.

```
:> hill[a_,liste_] :=
    Flatten[Map[Mod[a.#,32] &, Partition[liste, Length[a]]]]
:> codetxchiffre = hill[a, codetxclair]
Out[] = {17, 25, 16, 16, 29, 9, 31, 21, 24, 0, 4, 5, 26, ...}
```

Pour le déchiffrement, il suffit de connaître l'inverse de A.

```
:> Inverse[a, Modulus -> 32]
Out[] = {{17,3}, {12,1}}
```

Pour trouver cet inverse manuellement, on calcule le déterminant de A, $\det A = 5$, son inverse modulo 32 grâce à l'algorithme d'Euclide étendu, $(\det A)^{-1} = 13$ et enfin, la matrice des cofacteurs transposée,

$$\widetilde{\operatorname{cof} A} = \begin{pmatrix} 21 & -17 \\ -4 & 5 \end{pmatrix}.$$

On trouve, $13.21 = 273 \equiv 17 \mod 32$, $13.(-17) = -221 \equiv 3 \mod 32$, $13.(-4) = -52 \equiv 12 \mod 32$ et $13.5 = 65 \equiv 1 \mod 32$.

```
:> hill[Inverse[a,Modulus -> 32], codetxchiffre]
Out[] = {12, 5, 0, 16, 8, 5, 14, 9, 24, 0, 19, 21, ...}
```

Pour la cryptanalyse de ce chiffrement, envisageons uniquement le cas où un texte clair de longueur m^2 est connu. Si Oscar connaît la valeur $m = 2$, le texte clair $12, 5, 0, 16$ et le texte chiffré correspondant $17, 25, 16, 16$, alors il en déduit que

$$A \begin{pmatrix} 12 & 0 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 17 & 16 \\ 25 & 16 \end{pmatrix}.$$

Ici, pas de chance pour Oscar car la matrice du membre de gauche n'est pas inversible. Son déterminant vaut 0 et n'est pas premier avec 32. Oscar doit construire une matrice inversible dont les colonnes correspondent à des couples de texte clair lorsque ce dernier est décomposé en m-uples consécutifs. On peut par exemple prendre pour premier couple $(12, 5)$ correspondant au texte chiffré $(17, 25)$ et comme second couple $(19, 21)$ qui correspond à $(4, 5)$

$$A \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix} = \begin{pmatrix} 17 & 4 \\ 25 & 5 \end{pmatrix}.$$

Puisque

$$\det \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix} \equiv 29 \mod 32, \quad A = \begin{pmatrix} 17 & 4 \\ 25 & 5 \end{pmatrix} \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix}^{-1}$$

et Oscar retrouve A.

Remarque II.3.7. Le *chiffrement par permutation* est un cas particulier du chiffrement de Hill. On considère comme matrice pour le chiffrement, une matrice de permutation[6] P de dimension m. Le chiffrement de Hill revient alors à permuter les lettres d'un même m-uple au moyen de la permutation définie par P.

[6]Rappelons qu'une telle matrice possède exactement un 1 sur chaque ligne et sur chaque colonne.

Exemple II.3.8. Considérons la matrice de permutation

```
:> p = {{0,1,0}, {0,0,1}, {1,0,0}}
```

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} b \\ c \\ a \end{pmatrix}$$

et dès lors,

```
:> decode[hill[p, codetxclair]]
Out[] = "e lhepixnsu  lrquel e eae trepevl le pauml qei ue sro
tveuda s notve ragbetue t eaalgmeet noufnirun  aetru peuml aeu
n  aetru beguatte"
```

3.5. Chiffrement par flot ou en chaîne. Dans ce type de chiffrement, on génère une suite de clés $\mathbf{z} = z_1 z_2 \cdots$ utilisées successivement pour chiffrer une suite $\mathbf{x} = x_1 x_2 \cdots$. Commençons par un exemple. Soient $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{32}$. Pour chiffrer

$$\mathbf{x} = x_1 x_2 x_3 \cdots, \quad \forall i \geq 1,\ x_i \in \mathcal{P}$$

avec une clé k fixée initialement, on procède comme suit :

$$\mathbf{y} = (x_1 + k)(x_2 + x_1)(x_3 + x_2) \cdots \mod 32$$

ce qui revient à ajouter à la suite $\mathbf{x}$, la suite décalée d'une unité vers la droite.

Exemple II.3.9. Nous utilisons une fois encore nos conventions habituelles et choisissons la clé $k = 5$.

```
:> texteclair = "essayer un chapeau valait beaucoup mieux que
   d'etre oblige de jeter un sort, mais il aurait prefere ne
   pas avoir a le faire devant tout le monde."
:> codetxclair = code[texteclair]
Out[] = {5, 19, 19, 1, 25, 5, 18, 0, 21, 14, 0, 3, 8, 1, ...}

:> flot[liste_,k_] := Mod[ Drop[Prepend[liste,k],-1]+liste, 32]
:> flot[codetxclair,5]
Out[] = {10, 24, 6, 20, 26, 30, 23, 18, 21, 3, 14, 3, 11, 9, ...}
:> decode[%]
Out[] = "jxftz:wrucnckiqufvuvwmmj'tbgfvxrdepmvnzmxqfzedabyfwe
   oqnupledie joyywrucnsbafohnj.siulavgsj'tpbwkkwwensepqtsawex
   ,raalqefgj,wedi,wobttcditlqem.'ria"
```

En effet, on obtient en recopiant et décalant :

	5	19	19	1	25	5	18	0	21	14	0	3	8	1	$\cdots$
5		5	19	19	1	25	5	18	0	21	14	0	3	8	$\cdots$
10	24	6	20	26	30	23	18	21	3	14	3	11	9	$\cdots$	

Nous reviendrons par après sur d'autres exemples de chiffrements par flot mais donnons-en une définition formelle.

Définition II.3.10. Un *chiffrement par flot* est un quintuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F})$ où $\mathcal{P}, \mathcal{C}, \mathcal{K}$ sont définis comme dans le cas des chiffrements classiques,

- $\mathcal{L}$ est un ensemble fini, appelé *alphabet du flot de clés* (*keystream alphabet*),
- $\mathcal{F}$ est une suite de fonctions $(f_n)_{n\geq 1}$, appelée *générateur du flot de clés* et telle que pour tout $n \geq 1$,
$$f_n : \mathcal{K} \times \mathcal{P}^{n-1} \to \mathcal{L},$$
- pour tout $z \in \mathcal{L}$, il existe une fonction de chiffrement e_z telle que $e_z : \mathcal{P} \to \mathcal{C}$ et une fonction de déchiffrement d_z telle que $d_z : \mathcal{C} \to \mathcal{P}$ et $d_z(e_z(x)) = x$ pour tout $x \in \mathcal{P}$.

A une suite $\mathbf{x} = x_1x_2x_3\cdots$ d'éléments de $\mathcal{P}$ et à une clé $k \in \mathcal{K}$, correspond une unique suite de fonctions $\mathcal{F} = (f_1, f_2, f_3, \ldots)$. Chaque fonction f_n donne un élément z_n appartenant à l'ensemble fini $\mathcal{L}$ et à ce z_n, il correspond deux fonctions e_{z_n} et d_{z_n}. Le chiffrement de $\mathbf{x}$ est alors
$$e_{z_1}(x_1)e_{z_2}(x_2)e_{z_3}(x_3)\cdots$$

Remarque II.3.11. Dans cette définition, on voit que le n-ième élément du flot de clé dépend de la clé $k \in \mathcal{K}$ choisie et des $n-1$ éléments de texte clair lus précédemment.

Exemple II.3.12. Dans l'exemple précédent et avec les notations de la définition, $e_{z_1}(x_1) = x_1 + k \pmod{32}$ et pour $n > 1$, $e_{z_n}(x_n) = x_n + x_{n-1} \pmod{32}$. Il s'agit donc d'un cas très particulier de chiffrement par flot. La clé $k \in \mathcal{K}$ n'est utilisée que dans la fonction de chiffrement e_{z_1} et pour tout $n > 1$, la fonction de chiffrement e_{z_n} est entièrement déterminée par un seul élément de texte clair x_{n-1}. En toute généralité, un chiffrement par flot admet plus de souplesse.

Définition II.3.13. Un chiffrement en chaîne est dit *synchrone* si la suite de clés $(z_n)_{n\geq 1}$ est indépendante du texte clair. L'exemple II.3.9 n'est pas synchrone. Un chiffrement est dit *(ultimement) périodique* si la suite $(z_n)_{n\geq 1}$ est (ultimement) périodique, i.e., s'il existe $N, p \geq 1$ tels que $z_n = z_{n+p}$ pour tout $n \geq N$.

4. Le chiffrement DES

Tous les chiffrements rencontrés jusqu'à présent sont à clé secrète (ou privée), i.e., la sécurité du système réside dans la non-divulgation de la clé $k \in \mathcal{K}$ choisie. Ces systèmes sont tous peu sûrs car, comme nous l'avons vu, ils peuvent être aisément cryptanalysés. Dans cette section, nous présentons un cryptosystème à clé secrète considéré jusqu'il y a peu comme sûr et utilisé en pratique (ou alors, l'une de ses variantes plus récentes). Il s'agit du DES (*Data Encryption Standard*) développé initialement par IBM comme une variante de LUCIFER. Ce système a été officiellement publié en 1977 et

aujourd'hui, on emploie généralement des variantes du système initial (par exemple, des banques ou des ministères américains).

Les cryptosystèmes à clé secrète comme le chiffrement par décalage, par substitution, de Hill ou encore de Vigenère sont *idempotents*. Cela signifie que composer successivement deux cryptosystèmes du même type, par exemple deux chiffrements par décalage de clés k et ℓ, est encore un chiffrement de même type, par exemple un chiffrement par décalage de clé $k+\ell$. Si un cryptosystème est idempotent, il n'y a donc aucun intérêt à l'itérer (on a besoin de plus de clés mais cela n'apporte aucune sécurité supplémentaire).

DES, quant à lui, n'est pas idempotent (on le construit sur le produit de deux systèmes qui ne commutent pas[7], le *produit* de deux cryptosystèmes consistant à composer successivement les deux chiffrements). La sécurité est dès lors augmentée en l'itérant plusieurs fois. Ici, nous l'itérerons 16 fois. Brossons rapidement son fonctionnement.

On construit une clé secrète k comme suit. Tout d'abord, on détermine une suite aléatoire s de 56 bits, i.e., un élément de $s = s_1 \cdots s_{56} \in \{0,1\}^{56}$. On définit alors une suite de 64 bits $k = k_1 \cdots k_{64}$ de la manière suivante,

$$k_1, \ldots, k_7, k_9, \ldots, k_{15}, \ldots, k_{57}, \ldots, k_{63} = s_1, \ldots, s_{56}$$

et

$$\forall j \in \{0, \ldots, 7\}, \quad \sum_{i=1}^{8} k_{j8+i} \equiv 1 \mod 2.$$

Cette dernière condition stipule simplement que la somme de 8 bits consécutifs est toujours impaire (cela permet donc de détecter une éventuelle erreur dans le stockage ou le transfert d'une clé, on parle souvent de bit de parité). Ces 8 bits ajoutés aux 56 bits de départ ne jouent pas de rôle dans la suite.

On considère un texte clair de 64 bits $\mathbf{x} = x_1 \cdots x_{64} \in \{0,1\}^{64}$. On lui applique initialement une permutation ν de $\{1, \ldots, 64\}$ donnée par

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Ainsi, on considère $\nu(\mathbf{x}) = x_{\nu(1)} \cdots x_{\nu(64)} = x_{58}\, x_{50} \cdots x_7$. Ce mot $\nu(\mathbf{x})$ est divisé en deux mots de longueur 32,

$$\nu(\mathbf{x}) = L_0 R_0 = \left(x_{\nu(1)} \cdots x_{\nu(32)}\right) \left(x_{\nu(33)} \cdots x_{\nu(64)}\right).$$

Connaissant L_n et R_n ($n \geq 0$), on calcule L_{n+1} et R_{n+1} comme suit

$$L_{n+1} = R_n \tag{3}$$

et

$$R_{n+1} = L_n \oplus f(R_n, K_{n+1}) \tag{4}$$

[7] Si S et T sont idempotents et commutent, alors $S \circ T$ est aussi idempotent. En effet, $(S \circ T) \circ (S \circ T) = S \circ (T \circ S) \circ T = S \circ (S \circ T) \circ T = (S \circ S) \circ (T \circ T) = S \circ T$.

où $\oplus$ représente le "ou-exclusif", autrement dit l'addition bit à bit modulo 2, i.e.,

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

On peut dès lors calculer de proche en proche les L_n et R_n jusqu'à obtenir le mot $L_{16}R_{16}$ auquel on applique la permutation ν^{-1}. Le chiffrement de $\mathbf{x}$ est $\mathbf{y} = \nu^{-1}(L_{16}R_{16})$. On dit qu'on applique le DES en seize tours.

Il nous faut encore expliciter comment obtenir les clés $K_1, \ldots, K_{16}$ (processus de diversification des clés) et aussi définir la fonction f. On définit d'abord K_0. On l'obtient à partir de k en sélectionnant dans l'ordre les bits (on ne prend pas en compte ici les bits de parité k_{j8}, $j = 1, \ldots, 8$) de k en suivant la permutation ci-dessous

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36

pour former une chaîne de longueur 28

$$C_0 = k_{57}\, k_{49} \cdots k_{44}\, k_{36}$$

et aussi la permutation

63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

pour former une seconde chaîne de longueur 28

$$D_0 = k_{63}\, k_{55} \cdots k_{12}\, k_4.$$

Ainsi, $K_0 = C_0D_0$. Pour construire K_{n+1}, $n \geq 0$, on procède en deux étapes. Tout d'abord, disposant de C_n et D_n, on construit C_{n+1} et D_{n+1} en effectuant une permutation circulaire d'une ou de deux unités vers la gauche sur C_n et D_n de la manière suivante

$n+1$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
# permut.	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Ainsi,

$$C_1 = k_{49}\, k_{41} \cdots k_{44}\, k_{36}\, k_{57},\ C_2 = k_{41} \cdots k_{44}\, k_{36}\, k_{57}\, k_{49},\ \ldots$$

et

$$D_1 = k_{55}\, k_{47} \cdots k_{12}\, k_4\, k_{63},\ D_2 = k_{47} \cdots k_{12}\, k_4\, k_{63}\, k_{55},\ \ldots.$$

Connaissant C_n et D_n, $n \geq 1$, on obtient K_n en sélectionnant 48 des 56 bits de C_nD_n dans l'ordre suivant

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Passons à la définition de f. Rappelons que f prend comme argument un bloc R_n de 32 bits et une clé K_{n+1} de 48 bits (cette dernière ne dépend que de la clé k) pour produire un bloc de 32 bits.

On remplace R_n par un bloc R'_n de 48 bits en recopiant certains des bits de R_n plusieurs fois de la manière suivante (on parle de l'expansion de R_n)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Ainsi, si R_n est de la forme $r_1 r_2 \cdots r_{32}$, on obtient la suite

$$R'_n = r_{32}\, r_1\, r_2\, r_3\, r_4\, r_5\, r_4\, r_5 \cdots r_{31}\, r_{32}\, r_1.$$

On additionne à présent bit à bit R'_n et K_{n+1} modulo 2 pour obtenir B et cette suite est alors découpée en 8 blocs de 6 bits, i.e.,

$$B = R'_n \oplus K_{n+1} = \underbrace{b_1 \cdots b_6}_{B_1}\, \underbrace{b_7 \cdots b_{12}}_{B_2} \cdots \underbrace{b_{43} \cdots b_{48}}_{B_8}.$$

Il nous faut maintenant transformer chacun de ces 8 blocs en 8 nouveaux blocs B'_i de longueur 4. La valeur de la fonction f est alors une permutation de $B'_1 \cdots B'_8$ qui est bien de longueur 32, on a

$$\mu(B'_1 \cdots B'_8).$$

La transformation de B_i en B'_i est réalisée au moyen d'une table S_i. Considérons tout d'abord la table S_1.

S_1 :

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

On l'utilise comme suit pour calculer B'_1 à partir de $B_1 = b_1 b_2 b_3 b_4 b_5 b_6$. Le mot $b_1 b_6$ (resp. $b_2 b_3 b_4 b_5$) représente un entier $0 \leq x \leq 3$ (resp. $0 \leq y \leq 15$) écrit en base 2. Dans le tableau S_1, on considère l'élément $(S_1)_{x,y}$ se trouvant à la ligne x et à la colonne y. La représentation binaire de $(S_1)_{x,y}$ (éventuellement complétée par des zéros de tête pour obtenir un mot de longueur 4) est alors B'_1. On procède de manière semblable pour $B'_2, \ldots, B'_8$ avec les tables données ci-après. La dernière table reprend la permutation μ.

Exemple II.4.1. Soit $B_1 = 100101$. Le mot $b_1b_6 = 11$ (resp. $b_2b_3b_4b_5 = 0010$) correspond à $x = 3$ (resp. $y = 2$). Dans la table S_1, cela correspond[8] à l'élément 8 dont la représentation binaire est 0100 qui est B_1'.

Ceci termine la définition de DES. Notons que les tables S sont souvent appelées *S-boxes* (ou *substitution-boxes*) et sont vitales pour la sécurité de DES car elles constituent des composantes non linéaires du cryptosystème. En effet, aucune des boîtes n'est une fonction linéaire ou affine. Certaines personnes ont même imaginé que ces boîtes pouvaient cacher des "trappes" permettant à la National Security Agency de déchiffrer des messages tout en affirmant que le DES était "sûr".

Un avantage certain du DES est sa rapidité. En effet, l'implémentation du cryptosystème peut être réalisée de manière efficace logiciellement ou physiquement sur des circuits électroniques élémentaires à faible coût pouvant par exemple être placés sur une carte de crédit. Comparé aux cryptosystèmes à clé publique comme le RSA dont nous parlerons au chapitre suivant, la rapidité de DES est indéniable.

La critique principale faite à DES réside dans son espace des clés de taille $2^{56} \simeq 7,2 \times 10^{16}$ jugée trop petite. En effet, en 1993, on estimait pouvoir construire une puce capable de tester 5×10^7 clés par seconde pour un coût proche de 8 euros. Ainsi, en regroupant un grand nombre de telles puces, on pourrait trouver la clé secrète en quelques heures. On pourrait aussi imaginer une recherche réalisée à grande échelle par des milliers d'ordinateurs partagés sur internet. Il ne faut pas sous-estimer l'acharnement d'Oscar (par exemple, si le chiffrement concerne des transferts bancaires aux montants astronomiques, des secrets d'états ou industriels, des plans militaires, etc...)

Les sept autres S-boxes sont données ci-dessous.

S_2 :

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3 :

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4 :

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

[8] Les lignes sont numérotées de 0 à 3 et les colonnes de 0 à 15.

S_5 :

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6 :

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7 :

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8 :

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

et la permutation μ

μ :

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Notons pour conclure que, pour le déchiffrement, les équations (3) et (4) se réécrivent

$$R_n = L_{n+1}$$

et

$$L_n = R_{n+1} \oplus f(L_{n+1}, K_{n+1}).$$

De là, connaissant L_{16} et R_{16}, on peut retrouver L_0 et R_0.

Exemple II.4.2. Considérons le premier tour d'un chiffrement par DES. Soit la clé k qui, avec les bits de parité, est stockée en hexadécimal[9] par

133457799BBCDFF1

[9]Remarquons que $2^{64} = 16^{16}$. Ainsi, chaque chiffre en base 16 fournit quatre chiffres en base 2.

et en binaire

13	0	0	0	1	0	0	1	1
34	0	0	1	1	0	1	0	0
57	0	1	0	1	0	1	1	1
79	0	1	1	1	1	0	0	1
$9B$	1	0	0	1	1	0	1	1
BC	1	0	1	1	1	1	0	0
DF	1	1	0	1	1	1	1	1
$F1$	1	1	1	1	0	0	0	1

On ne considèrera pas la dernière colonne formée des bits de parité. On a

$$C_0 = k_{57}k_{49}\cdots k_{44}\,k_{36} = 11110000110011001010101011111$$

et

$$D_0 = k_{63}\,k_{55}\cdots k_{12}\,k_4 = 01010101011001100111100011111.$$

En permutant d'une unité vers la gauche, on obtient

$$C_1 = 11100001100110010101010111111$$

et

$$D_1 = 10101010110011001111100011110.$$

De là, on construit la clé K_1 en sélectionnant 48 des 56 bits de C_1D_1,

$$K_1 = 000110110000001011101111111111000111000001110010.$$

Considérons le texte clair écrit en hexadécimal

$$\mathbf{x} = 0123456789ABCDEF$$

et en binaire

$$\mathbf{x} = 0000000100100011010001010110011111000100110101011110011011110111101111.$$

On lui applique la permutation ν pour obtenir L_0 et R_0,

$$\nu(\mathbf{x}) = \underbrace{11001100000000000110011001111111}_{L_0}\underbrace{11110000101010101111000010101010}_{R_0}.$$

Il vient

$$L_1 = R_0 = 11110000101010101111000010101010$$

et

$$R_1 = L_0 \oplus f(R_0, K_1).$$

On étend d'abord R_0 de longueur 32 en R_0' de longueur 48 et on obtient

$$R_0' = 011110100001010101010101011110100001010101010101.$$

Ensuite, on calcule

$$B = R_0' \oplus K_1 = \underbrace{011000}_{b_1}\underbrace{010001}_{b_2}\underbrace{011110}_{b_3}\underbrace{111010}_{b_4}\underbrace{100001}_{b_5}\underbrace{100110}_{b_6}\underbrace{010100}_{b_7}\underbrace{100111}_{b_8}.$$

En regardant le contenu des 8 S-boxes, on peut calculer la valeur de f. Tout d'abord, les S-boxes donnent

$$\underbrace{0101}_{b'_1}\underbrace{1100}_{b'_2}\underbrace{1000}_{b'_3}\underbrace{0010}_{b'_4}\underbrace{1011}_{b'_5}\underbrace{0101}_{b'_6}\underbrace{1001}_{b'_7}\underbrace{0111}_{b'_8}$$

et enfin,

$$f(R_0, K_1) = \mu(b'_1 b'_2 b'_3 b'_4 b'_5 b'_6 b'_7 b'_8) = 00100011010010101010100110111011$$

et

$$R_1 = L_0 \oplus f(R_0, K_1) = 11101111010010100110010101000100.$$

Ceci achève un tour de DES ! L'implémentation Mathematica est donnée ci-dessous (il serait illusoire de réaliser tous ces calculs à la main).

```
:> k=IntegerDigits[16^^133457799bbcdff1,2,64]
Out[]={0,0,0,1,0,0,0,1,1,0,0,0,1,1,0,1,0,0,0,0,1,0,1,0,1,1,1,0,1,1,1,1,1,0,
0,1,1,0,0,1,1,0,1,1,1,0,1,1,1,1,0,0,1,1,0,1,1,1,1,1,1,1,1,1,0,0,0,1}

:> c0=Map[Part[k,#]&,
          {57,49,41,33,25,17,9,1,58,50,42,34,26,18,
           10,2,59,51,43,35,27,19,11,3,60,52,44,36}]
Out[]={1,1,1,1,0,0,0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,0,1,0,1,1,1,1}

:> d0=Map[Part[k,#]&,
          {63,55,47,39,31,23,15,7,62,54,46,38,30,22,
           14,6,61,53,45,37,29,21,13,5,28,20,12,4}]
Out[]={0,1,0,1,0,1,0,1,0,1,1,0,0,1,1,0,0,1,1,1,1,0,0,0,1,1,1,1}

:> c1=RotateLeft[c0,1]
Out[]={1,1,1,0,0,0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,0,1,0,1,0,1,1,1,1,1}

:> d1=RotateLeft[d0,1]
Out[]={1,0,1,0,1,0,1,0,1,1,0,0,1,1,0,0,1,1,1,1,0,0,0,1,1,1,1,0}

:> c1d1=Join[c1,d1]
Out[]={1,1,1,0,0,0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,0,1,0,1,1,1,1,1,
       1,0,1,0,1,0,1,0,1,1,0,0,1,1,0,0,1,1,1,1,0,0,0,1,1,1,1,0}

:> k1=Map[Part[c1d1,#]&,
          {14,17,11,24,1,5,3,28,15,6,21,10,23,19,12,4,26,8,16,7,
           27,20,13,2,41,52,31,37,47,55,30,40,51,45,33,48,44,49,
           39,56,34,53,46,42,50,36,29,32}]
Out[]={0,0,0,1,1,0,1,1,0,0,0,0,0,0,1,0,1,1,1,0,1,1,1,1,
       1,1,1,1,1,1,0,0,0,1,1,1,0,0,0,0,0,1,1,1,0,0,1,0}

:> x=IntegerDigits[16^^0123456789abcdef,2,64]
Out[]={0,0,0,0,0,0,0,1,0,0,1,0,0,0,1,1,0,1,0,0,0,1,0,1,0,1,1,0,0,1,
1,1,1,0,0,0,1,0,0,1,1,0,1,0,1,0,1,1,1,1,0,0,1,1,0,1,1,1,1,0,1,1,1,1}
```

```
:> l0r0=Map[Part[x,#]&,
             {58,50,42,34,26,18,10,2,60,52,44,36,28,20,12,4,62,54,
              46,38,30,22,14,6,64,56,48,40,32,24,16,8,57,49,41,33,
              25,17,9,1,59,51,43,35,27,19,11,3,61,53,45,37,29,21,
              13,5,63,55,47,39,31,23,15,7}]
Out[]={1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,1,1,1,1,
1,1,1,1,1,1,0,0,0,0,1,0,1,0,1,0,1,0,1,1,1,1,0,0,0,0,1,0,1,0,1,0,1,0}

:> l0=Take[l0r0,32]
Out[]={1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,1,1,1,1,1,1}

:> r0=Take[l0r0,-32]
Out[]={1,1,1,1,0,0,0,0,1,0,1,0,1,0,1,0,1,1,1,1,0,0,0,0,1,0,1,0,1,0,1,0}

:> r1=l0
Out[]={1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,1,1,1,1,1,1}

:> r0'=Map[Part[r0,#]&,
            {32,1,2,3,4,5,4,5,6,7,8,9,8,9,10,11,12,13,12,13,14,15,16,
             17,16,17,18,19,20,21,20,21,22,23,24,25,24,25,26,27,28,29,
             28,29,30,31,32,1}]
Out[]={0,1,1,1,1,0,1,0,0,0,0,1,0,1,0,1,0,1,0,1,0,1,0,1,
       0,1,1,1,1,0,1,0,0,0,0,1,0,1,0,1,0,1,0,1,0,1,0,1}

:> b=Mod[r0'+k1,2]
Out[]={0,1,1,0,0,0,0,1,0,0,0,1,0,1,1,1,1,0,1,1,1,0,1,0,
       1,0,0,0,0,1,1,0,0,1,1,0,0,1,0,1,0,0,1,0,0,1,1,1}

:> b=Partition[b,6]
Out[]={{0,1,1,0,0,0},{0,1,0,0,0,1},{0,1,1,1,1,0},{1,1,1,0,1,0},
       {1,0,0,0,0,1},{1,0,0,1,1,0},{0,1,0,1,0,0},{1,0,0,1,1,1}}

:> g[l_]:={FromDigits[{l[[1]],l[[6]]},2]+1,FromDigits[Take[l,{2,5}],2]+1}

:> position=Map[g[#]&,b]
Out[]= {{1,13},{2,9},{1,16},{3,14},{4,1},{3,4},{1,11},{4,4}}

:>
s1={{14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7},{0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8},
    {4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0},{15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13}};
s2={{15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10},{3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5},
    {0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15},{13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9}};
s3={{10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8},{13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1},
    {13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7},{1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12}};
s4={{7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15},{13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9},
    {10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4},{3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14}};
s5={{2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9},{14,11,2,12,4,7,13,1,5,0,15,10,3,9,8,6},
    {4,2,1,11,10,13,7,8,15,9,12,5,6,3,0,14},{11,8,12,7,1,14,2,13,6,15,0,9,10,4,5,3}};
```

```
s6={{12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11},{10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8},
    {9,14,15,5,2,8,12,3,7,0,4,10,1,13,11,6},{4,3,2,12,9,5,15,10,11,14,1,7,6,0,8,13}};
s7={{4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1},{13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6},
    {1,4,11,13,12,3,7,14,10,15,6,8,0,5,9,2},{6,11,13,8,1,4,10,7,9,5,0,15,14,2,3,12}};
s8={{13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7},{1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2},
    {7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8},{2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11}};

:> s={s1,s2,s3,s4,s5,s6,s7,s8};

:> valsboxes= Flatten[
    Table[IntegerDigits[Part[s[[i]],position[[i,1]],position[[i,2]]],2,4], {i,1,8}]]
Out[]={0,1,0,1,1,1,0,0,1,0,0,0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,0,1,0,1,1,1}

:> f=Map[Part[valsboxes,#]&,
          {16,7,20,21,29,12,28,17,1,15,23,26,5,18,31,10,
           2,8,24,14,32,27,3,9,19,13,30,6,22,11,4,25}]
Out[]={0,0,1,0,0,0,1,1,0,1,0,0,1,0,1,0,1,0,1,0,1,0,0,1,1,0,1,1,1,0,1,1}

:> r1=Mod[l0+f,2]
Out[]={1,1,1,0,1,1,1,1,0,1,0,0,1,0,1,0,0,1,1,0,0,1,0,1,0,1,0,0,0,1,0,0}
```

Cet exemple Mathematica peut convaincre le lecteur que DES peut être implémenté de façon efficace.

Remarque II.4.3. Depuis juin 2001, DES a été officiellement remplacé par l'AES (*Advanced Encryption Standard*) dont l'algorithme cryptographique *Rijndael* est d'origine belge[10], voir par exemple :

`www.chi-publishing.com/portal/backissues/pdfs/ISB_2001/ISB0602/ISB0602RW.pdf`
`www.esat.kuleuven.ac.be/~rijmen/rijndael/`

La sélection de cet l'algorithme a été réalisée par un concours initié par le *National Institute of Standards and Technology* (NIST). Notons enfin que pour palier à l'insécurité grandissante de DES (dûe principalement à l'amélioration constante des perfomances de calcul des machines), on a encore parfois recours à un triple DES.

[10] Joan Daemen, Viincent Rijmen.

CHAPITRE III

RSA et cryptographie à clé publique

Dans tous les cryptosystèmes étudiés jusqu'à présent, la connaissance de la fonction de chiffrement e_k permettait de retrouver aisément la fonction de déchiffrement d_k. Ainsi, connaître l'une de ces deux fonctions est équivalent à connaître la clé k. En effet, même dans le cas *a priori* plus complexe du DES, si on sait comment un message a été chiffré, on peut le déchiffrer en reprenant les seize tours dans l'ordre inverse. Pour tous ces cryptosystèmes, qualifiés de *symétriques*, la nécéssité d'échanger une clé au moyen d'un canal sûr en est le problème principal pour les mettre en oeuvre. Ainsi, par exemple, si Alice et Bob n'ont que l'échange de courriers électroniques comme moyen de communication, on voit mal comment ils pourraient se mettre d'accord sur une clé k sans qu'Oscar ne puisse l'intercepter. En effet, ni Alice ni Bob ne sauraient maîtriser le cheminement de leurs messages électroniques sur le réseau[1].

L'idée d'un cryptosystème à clé publique est de construire un couple de fonctions (e_k, d_k) de manière telle que la connaissance de la fonction de chiffrement e_k n'apporte aucun renseignement sur la fonction de déchiffrement d_k. De cette façon, e_k peut être rendu publique sans mettre en danger la sécurité du système cryptographique. On parle parfois de cryptosystème *asymétrique*. Ainsi, si Alice désire envoyer un message à Bob, ce dernier publie une fonction de chiffrement e_{k_B} qui lui est propre et conserve soigneusement la fonction d_{k_B} correspondante. Alice peut donc envoyer un message chiffré $e_{k_B}(x)$ à Bob. Ce dernier étant l'unique personne à connaître d_{k_B}, il est théoriquement le seul en mesure de déchiffrer le message d'Alice.

Ces idées ont à l'origine été développées par Diffie et Hellman (1976), puis par Rivest, Shamir et Adleman (1977). Elles reposent sur le principe de fonction à sens unique.

1. Fonction à sens unique

On appelle *fonction à sens unique* une fonction $f : A \to B$ (par exemple, une bijection) qui est telle que $f(x)$ est "facile" à calculer pour tout $x \in A$ et $f^{-1}(y)$ est "difficile à calculer". La notion de "facilité" fait référence aux ressources à mettre en oeuvre pour effectuer les calculs de f et f^{-1} (complexité temporelle).

[1]Il faut savoir qu'entre les deux serveurs de courrier, les messages transitent en clair par une série de relais et peuvent donc être facilement espionnés.

Exemple III.1.1. Illustrons ce concept sur l'exemple suivant. Imaginons disposer d'un annuaire téléphonique contenant 200000 entrées composées d'un nom et d'un numéro. Les entrées étant classées par ordre alphabétique, si on demande de retrouver le numéro de téléphone d'une personne x, il ne faudra certainement pas plus d'une minute à l'exécutant pour trouver ce numéro, c'est-à-dire la valeur $f(x)$. On peut par exemple procéder par dichotomie (et l'estimation du nombre de comparaisons à réaliser est proportionnelle à $\log_2 200000 \sim 17,61$).

Dumbeldore, A.	03189228
⋮	⋮
Fudge, C.	02162276
Ganger, H.	04122782
⋮	⋮
Hagrid, R.	02765100
Potter, H.	04378128
⋮	⋮

Par contre, connaissant le numéro d'une personne, retrouver le nom correspondant demandera bien plus de temps car on ne dispose pas de l'annuaire inversé. Ceci constitue donc une tâche bien plus rédibitoire puisque l'exécutant est obligé de passer en revue l'ensemble des numéros (comparez 200000 à son logarithme !). On peut dire que la fonction qui, à un nom, associe le numéro de téléphone correspondant est une fonction à sens unique.

Pour mettre en oeuvre un cryptosystème à clé publique, si on utilise une fonction à sens unique "pure" comme fonction de chiffrement, il sera dès lors très difficile de calculer les valeurs de la fonction de déchiffrement. Ce type de fonctions n'aurait donc que peu d'intérêt pratique puisque personne, pas même l'utilisateur légal, ne pourrait déchiffrer un message chiffré. C'est pour cette raison qu'on introduit le concept de fonction à sens unique "*à trappe cachée*" (trapdoor one-way function). La *trappe cachée* est en fait une information supplémentaire qui, lorsqu'on en dispose, permet de calculer facilement l'inverse de la fonction.

Remarque III.1.2. Bien que cruciales en cryptographie, les fonctions que nous utiliserons seront supposées à sens unique, mais aucune fonction n'a été jusqu'à ce jour *démontrée* comme telle.

Remarque III.1.3. On utilise parfois des fonctions à sens unique "pures" dans le cadre de la gestion des mots de passe. Sur une machine Linux (ou même maintenant Windows NT, XP et MacOS X), à chaque utilisateur u correspond un mot de passe m_u. Si f est une fonction à sens unique, lorsque l'utilisateur entre son mot de passe m_u, on calcule $f(m_u)$ et un fichier contenant les couples $(u, f(m_u))$ est maintenu à jour sur la machine. En comparant la valeur fournie par l'utilisateur et la valeur contenue dans

le fichier, on peut décider si l'utilisateur est ou non admis à travailler sur l'ordinateur. Un pirate mal intentionné obtenant le fichier des mots de passe $(u, f(m_u))$ n'est théoriquement pas en mesure de retrouver les mots de passe m_u. En effet, seules les valeurs $f(m_u)$ sont stockées et f étant à sens unique, il lui est impossible de retrouver m_u. Par conséquent, il lui faudra recourir à d'autres moyens pour usurper l'identité d'un utilisateur légal. C'est aussi pour cette raison qu'on demande aux utilisateurs de ne pas employer de noms communs comme mots de passe m_u. En effet, il est facile d'établir la liste des valeurs de f sur les mots d'un dictionnaire et ainsi, retrouver le mot de passe initial par simple comparaison.

2. RSA

Le cryptosystème RSA (du nom de ses inventeurs Rivest, Shamir et Adleman) que nous allons présenter maintenant fournit en particulier une illustration du concept de fonction à sens unique (à trappe cachée).

Détaillons-en les ingrédients. Bob choisit deux grands nombres premiers distincts p et q. Il en calcule le produit

$$n = p.q.$$

Puisque p et q sont premiers, il est clair que

$$\varphi(n) = (p-1).(q-1).$$

Bob choisit à présent deux nombres e et d tels que

$$d.e \equiv 1 \mod \varphi(n).$$

Pour ce faire, il choisit e tel que

$$1 < e < \varphi(n) \quad \text{et} \quad \text{pgcd}(e, \varphi(n)) = 1.$$

Ensuite, Bob obtient d grâce à l'algorithme d'Euclide étendu. Bob publie n et e et conserve secret les autres éléments $d, p, q, \varphi(n)$. On appelle e (resp. d) l'*exposant de chiffrement* (resp. *de déchiffrement*). On dira de plus que le couple $k = (e, n)$ est la clé du système. Si l'ensemble des textes clairs est $\mathcal{P} = \mathbb{Z}_n$, alors

$$\forall x \in \mathbb{Z}_n,\ e_k(x) := x^e \mod n.$$

Le chiffrement s'obtient aisément au moyen de l'exponentiation modulaire dont la complexité temporelle est raisonnable (cf. section 9 du chapitre I).

Proposition III.2.1. *Avec les notations précédentes, si $k = (e, n)$ et si $y = e_k(x)$, alors*

$$y^d \mod n = x.$$

Remarque III.2.2. Cette proposition nous montre que pour déchiffrer un message, il suffit d'élever le texte chiffré à la puissance d et on posera donc

$$d_k(y) := y^d \mod n.$$

Démonstration. Rappelons que le petit théorème de Fermat (cf. théorème I.6.11) stipule que si $\text{pgcd}(x, n) = 1$, alors

$$x^{\varphi(n)} \equiv 1 \mod n.$$

Ici, $y = x^e$. Ainsi, il existe $\alpha \in \mathbb{N}$ tel que

$$y^d = (x^e)^d = x^{ed} = x^{1+\alpha\,\varphi(n)}$$

car $ed \equiv 1 \mod \varphi(n)$. Si x est premier avec n, le résultat est donc démontré en appliquant le petit théorème de Fermat.

Supposons à présent que x n'est pas premier avec n. Il est cependant premier avec p ou q car sinon, il serait multiple de n, or $x < n$. Supposons dès lors, x premier avec p mais pas avec q. Par le petit théorème de Fermat,

$$x^{ed} = x\,(x^{p-1})^{\alpha(q-1)} \equiv x \mod p$$

car $x^{p-1} \equiv 1 \mod p$. On a aussi trivialement

$$x^{ed} \equiv x \mod q$$

car les deux membres sont congrus à zéro modulo q. De ces deux égalités, puisque p et q sont premiers et distincts, on en tire[2] que

$$x^{ed} \equiv x \mod n.$$

■

Connaissant d, le déchiffrement est semblable au chiffrement et utilise une fois encore l'exponentiation modulaire.

En résumé, on a les données suivantes :

- Bob publie : $k = (e, n)$,
- Bob conserve secret : d, p, q, $\varphi(n)$,
- fonction de chiffrement : $e_k(x) = x^e \mod n$,
- fonction de déchiffrement : $d_k(y) = y^d \mod n$.

Remarque III.2.3. Supposons qu'Alice et Bob désirent converser par courrier électronique en utilisant le RSA. Dans ce cas, Alice construit des nombres n_A, e_A, d_A et publie $k_A = (e_A, n_A)$. Bob fait de même. Il construit n_B, e_B, d_B et publie $k_B = (e_B, n_B)$. Alice (resp. Bob) utilisera alors e_{k_B} (resp. e_{k_A}) pour chiffrer des messages destinés à Bob (resp. Alice). En pratique, on peut donc supposer disposer d'une sorte d'annuaire reprenant les utilisateurs et leur clé publique respective[3].

[2] Si $y \equiv x \mod p$ et $y \equiv x \mod q$, alors cela signifie qu'il existe $m_1, m_2 \in \mathbb{Z}$ tels que $y = x + m_1 p$ et $y = x + m_2 q$. De là, $m_1 p = m_2 q$. Puisque p et q sont premiers et distincts, on en tire que p divise m_2 et que q divise m_1. Autrement dit, il existe α_1 et α_2 tels que $m_1 = \alpha_1 q$ et $m_2 = \alpha_2 p$. De $m_1 p = m_2 q$, on tire $\alpha_1 pq = \alpha_2 pq$. D'où $\alpha_1 = \alpha_2$ et $y = x + \alpha_1 pq = x + \alpha_1 n$.

[3] Par exemple, de nombreuses personnes utilisent le logiciel de protection du courrier électroniquePGP (Pretty Good Privacy) conçu à l'origine par Philip Zimmermann et dont l'un des algorithmes cryptographiques permettant l'échange de clés repose sur le RSA.

Remarque III.2.4. Oscar a bien évidemment lui aussi accès à la clé publique (e, n) de Bob. Pour retrouver l'exposant d de déchiffrement, il lui faut connaître $\varphi(n)$ pour ensuite calculer l'inverse de e modulo $\varphi(n)$. Un moyen lui permettant de trouver $\varphi(n)$ est de factoriser n. Ainsi, la sécurité du RSA réside dans le fait qu'il est facile de faire le produit n de deux grands nombres premiers p et q mais qu'il est par contre *supposé difficile* de factoriser n. Nous verrons plus loin que la connaissance de d ou de $\varphi(n)$ revient à la factorisation de n.

Exemple III.2.5. Considérons un exemple rudimentaire (et très peu réaliste). Soient les entiers :

$$p = 11,\ q = 23,\ n = p.q = 253,\ e = 3.$$

Puisque $220 = 3.73 + 1$, on en déduit que l'exposant de déchiffrement d est tel que

$$3^{-1} = -73 \mod 220 = 147 \mod 220.$$

Bob publie $k = (3, 253)$. Si Alice veut envoyer le texte clair $x = 165$ à Bob, elle calcule

$$e_k(x) = 165^3 \mod 253 = 110.$$

Si Bob reçoit le message $y = 110$, il lui suffit de calculer

$$d_k(y) = 110^{147} = 110^{128}.110^{16}.110^2.110^1 \mod 253 = 165.$$

Ce calcul nécéssite 7 élévations au carré ($2^7 = 128$) et trois produits modulo 253.

3. Chiffrement RSA en pratique

Pour assurer la sécurité du RSA, il est de coutûme de prendre des nombres premiers p et q de l'ordre de 2^{512} (voir plus tard, la remarque III.10.5). Un nombre de cette taille écrit en base 10 possède environ

$$\lfloor \log_{10} 2^{512} \rfloor = \left\lfloor 512 \underbrace{\log_{10} 2}_{\sim 0,3} \right\rfloor = 154$$

chiffres décimaux. Si nous supposons travailler, avec nos conventions habituelles, sur un alphabet Σ de 32 symboles, ou plus généralement sur un alphabet de N symboles (on utilise un N majuscule pour le distinguer de $n = pq$), alors $N = 26, 32$ ou encore 256 pour le code ASCII est bien trop petit par rapport à $n \sim 2^{1024}$. En effet, si on utilisait comme ensemble de textes clairs $\mathbb{Z}_N$ au lieu de $\mathbb{Z}_n$, alors une recherche exhaustive de toutes les images $x^e \mod n$ pour $x \in \mathbb{Z}_N$ permettrait de réduire à néant la sécurité du RSA. Avec un N petit, une telle recherche est rapide à réaliser.

On implémente dès lors en général le RSA en considérant comme unité de base, les blocs de k symboles consécutifs de l'alphabet Σ avec k défini par

$$k := \left\lfloor \log_N n \right\rfloor,$$

autrement dit, $N^k \leq n < N^{k+1}$. Comme d'habitude (se rappeler le chapitre II, section 2), k éléments consécutifs de $\mathbb{Z}_N$ correspondent à un nombre $x \in \mathbb{Z}_{N^k}$ écrit en base N et compris entre 0 et $N^k - 1$. En fait, il est clair que k est la plus grande valeur possible permettant ce codage. Ainsi, si $x \in \mathbb{Z}_{N^k}$, le chiffrement de x est donné par

$$y = x^e \mod n$$

qui est un entier $y < n$ et $n < N^{k+1}$. Donc la représentation de y en base N peut être de longueur $k+1$. Ainsi, les blocs de k éléments consécutifs de $\mathbb{Z}_N$ sont envoyés de manière injective sur des blocs de longueur $k+1$. Il suffit donc dans l'implémentation du RSA d'utiliser les conventions ad hoc[4].

Exemple III.3.1. Considérons encore une fois un exemple simpliste. Comme dans l'exemple III.2.5, on prend $n = 253$ et $e = 3$. L'alphabet utilisé est $\Sigma = \{a, b, c, d\}$ et le codage de Σ fait correspondre a (resp. b, c, d) à 0 (resp. 1, 2, 3). Ici, $N = \#\Sigma = 4$ et donc

$$k = \left\lfloor \log_4 253 \right\rfloor = 3$$

car $4^3 = 64$ et $4^4 = 256$. Si Alice désire envoyer à Bob le message

bccadb,

elle procède comme suit. Tout d'abord, le premier bloc de longueur 3, *bcc*, correspond à l'entier

$$1.4^2 + 2.4 + 2.1 = 26 < 64$$

et son chiffrement est donné par

$$26^3 \mod 253 = 119 = 1.4^3 + 3.4^2 + 1.4^2 + 3.4^0$$

qui correspond au mot *bdbd*. Le second bloc de texte clair, *adb*, correspond à

$$0.4^2 + 3.4 + 1 = 13$$

et son chiffrement

$$13^3 \mod 253 = 173 = 2.4^3 + 2.4^2 + 3.4^1 + 1.4^0$$

fournit le mot *ccdb*. Ainsi, Alice transmet le texte chiffré

bdbdccdb.

Quant à Bob, il sait qu'il doit redécouper le texte chiffré en blocs de longueur $k + 1 = 4$ avant déchiffrement.

Exemple III.3.2. Considérons un exemple quelque peu plus réaliste en utilisant Mathematica. La mise en oeuvre ne nécéssite pas de nouvelles fonctions par rapport à celles introduites au chapitre précédent. Considérons les dix- et vingt-millionièmes nombres premiers,

[4]En particulier, le choix de k est univoquement déterminé par n et par la taille N l'alphabet.

```
:> p=Prime[10000000]
Out[]=179424673
:> q=Prime[20000000]
Out[]=373587883
```

Il s'agit ici de deux nombres de taille trop petite pour une application cryptographique réelle[5].

```
:> n=p*q
Out[]=67030883744037259
:> phi=(p-1)(q-1)
Out[]=67030883191024704
```

Cherchons à présent deux nombres e et d inverses l'un de l'autre modulo $\varphi(n)$. Essayons par exemple, $e = 13673$.

```
:> ExtendedGCD[13673, phi]
Out[]={1, {-23629697724035623, 4820}}
```

Cela signifie que e est inversible et

$$-23629697724035623.13673 + 4820.\,\varphi(n) = 1.$$

De là, on calcule

```
:> Mod[-23629697724035623,phi]
Out[]=43401185466989081
```

Par conséquent, $d = 43401185466989081$.

```
:> e=13673
:> d=43401185466989081
```

Nous utilisons toujours notre alphabet de taille 32. Il vient

```
:> N[Log[32,n]]
Out[]=11.1791
```

Par conséquent, on va considérer des blocs de longueur $k = 11$. Soit le texte clair,

```
:> texteclair = "pour votre information, sachez que le melange
d'asphodele et d'armoise donne un sommifere si puissant qu'on
l'appelle la goutte du mort vivant.";
:> codetxclair=code[texteclair]
Out[]={16, 15, 21, 18, 0, 22, 15, 20, 18, 5, 0, 9, 14, 6, 15,
 18, 13, 1, 20, 9, 15, 14, 27, 0, 19, 1, 3, 8, 5, 26, 0, 17,
 21, 5, 0, 12, 5, 0, 13, 5, ...
                                    ... , 9, 22, 1, 14, 20, 28}
```

Ici, nous pouvons vérifier que la liste est un multiple de $k = 11$. En effet,

```
:> Length[codetxclair]
Out[]=143
```

[5]En pratique, il n'est pas conseillé d'utiliser des nombres premiers provenant d'une table car Oscar, s'il dispose de la même table, pourrait tester si les nombres présents dans cette table divisent n

et $143 = 13.11$. Ainsi, nous ne devons même pas utiliser la fonction `ajout`[6]. Si un bloc de 11 éléments consécutifs de $\mathbb{Z}_{32}$ représente un entier inférieur à 32^{11}, ces entiers sont donnés par

```
:> liste=codebloc[codetxclair,11]
Out[]= {18565873064888480, 10632812601943534, 30420226061173301,
   5642865914283463, 5634895741467781, 13686914021230157,
  17226220621478048, 24137148644235442, 5650700051992161,
  16466893790970269, 1706627137810464, 8432863510942733,
  17543831480220316}
```

En effet, on pourrait vérifier que pour le premier élément, on a bien

$$\begin{aligned} 18565873064888480 &= 16.32^{10} + 15.32^9 + 21.32^8 + 18.32^7 + 0.32^6 \\ &\quad +22.32^5 + 15.32^4 + 20.32^3 + 18.32^2 + 5.32^1 + 0.32^0. \end{aligned}$$

Nous pouvons à présent chiffrer cette liste en utilisant la clé publique (e, n).

```
:> listechiffree=PowerMod[liste, e, n]
Out[]= {35842157597020710, 23309826535758073, 7668972335977207,
   33354174667033896, 47013455444144299, 1288299963418294,
    6381507244972354, 54508071251259, 56798681894838301,
   16862311291641331, 41363332544598199, 27747396549481814,
     877008501014677}
```

Le possesseur de l'exposant d peut, à partir de cette liste, retrouver la liste initiale en calculant

```
:> PowerMod[listechiffree, d, n]
Out[]= {18565873064888480, 10632812601943534, ...
 ..., 17543831480220316}
```

Si on désire décoder la liste chiffrée, il faut avoir à l'esprit que les éléments de cette liste doivent correspondre à des blocs de longueur $k + 1 = 12$ qui sont des représentations d'entiers en base $N = 32$. Avec nos conventions de codage, il vient donc comme texte chiffré

```
:> decodebloc[listechiffree,12]
Out[]="?zvhbox,tqf tvpegugafgy fy:.oa:atww 's?ngzl.cihaixfotk
vr.ek adsvnzz:auv euk:ixgovjb  aqrlscr,i,arnjcfu zx ' n?he,ej
bwosadwswmkpxdew xttcpyllejv  x'tizbv du"
```

Naturellement, ce texte est de longueur $13.12 = 156$ comme on le vérifie avec

```
:> StringLength[%]
Out[]=156
```

4. Un procédé de signature

Supposons qu'Alice veuille envoyer un message par courrier électronique à Bob. Comment Bob peut-il être certain que le message provient bien

[6]Rappelons qu'ajouter des zéros pourrait donner une information partielle à Oscar.

d'Alice et non pas d'Oscar se faisant passer pour Alice ? Nous allons voir dans cette courte section que le RSA permet de répondre à cette question[7]. Soient (e_A, n_A) et (e_B, n_B) les clés publiques d'Alice et de Bob respectivement. On notera d_A et d_B les exposants de déchiffrement correspondants. Nous savons que $(x^{e_A})^{d_A} = x \mod n_A$ donc, en particulier, nous avons aussi

$$(x^{d_A})^{e_A} = x \mod n_A.$$

Sans se soucier dans un premier temps des détails techniques, Alice peut procéder comme suit pour envoyer un message $x \in \mathbb{Z}_n$ à Bob. Tout d'abord, Alice calcule $x' = x^{d_A} \mod n_A$. Ensuite, elle chiffre le résultat obtenu en utilisant la clé publique de Bob et calcule

$$y' = x'^{e_B} \mod n_B.$$

Elle envoie y' à Bob. Pour le déchiffrement, Bob calcule $y'^{d_B} \mod n_B$ et réobtient x'. Enfin, il emploie la clé publique d'Alice pour retrouver x,

$$x = x'^{e_A} \mod n_A.$$

Cela assure l'authenticité du message car seule Alice connaît d_A et donc, elle est la seule à pouvoir produire x'.

En pratique, cette procédure doit être quelque peu adaptée. En effet, si $n_A > n_B$, alors des $x' < n_A$ distincts peuvent être égaux modulo n_B et le protocole proposé ne serait dès lors plus injectif. On procède alors comme suit. Alice et Bob décident d'une valeur commune t (cette valeur peut être publiée à cet effet). Ensuite ils construisent chacun deux cryptosystèmes RSA, l'un utilisé pour les signatures, l'autre pour les chiffrements (on convient d'employer un indice s ou c pour préciser s'il s'agit d'une signature ou d'un chiffrement). Ainsi, Alice publie $(e_{A,s}, n_{A,s})$ et $(e_{A,c}, n_{A,c})$. De même, Bob publie $(e_{B,s}, n_{B,s})$ et $(e_{B,c}, n_{B,c})$. La construction suppose que

$$n_{A,s} < t < n_{A,c} \quad \text{et} \quad n_{B,s} < t < n_{B,c}.$$

De cette manière, Alice signe son message en utilisant l'exposant $d_{A,s}$ pour obtenir un nombre inférieur à $n_{A,s}$. Enfin, le message est chiffré avec les clé $(e_{B,c}, n_{B,c})$ et on a bien $n_{A,s} < n_{B,c}$, ce qui suffit.

Remarque III.4.1. Il ne serait pas raisonnable qu'Alice et Bob emploient la même valeur pour n, car alors, connaissant tous deux la factorisation de n, ils pourraient déchiffrer les messages destinés à l'autre utilisateur.

Remarque III.4.2. [8] Nous simplifions ici notre propos en nous intéressant uniquement à la signature du message par Alice. Pour être complet, on pourrait bien sûr également considérer le chiffrement avant l'envoi à Bob.

[7] On suppose que le détenteur de l'annuaire des clés publiques est une personne de confiance.

[8] Cette remarque m'a été proposée par P. Paquay. Merci Pierre !

Cela ne changerait rien à notre présentation. Nous utilisons les mêmes conventions que précédemment, sans pour autant rappeler l'indice A propre à la signataire Alice. Il est clair que pour tous $x_1, x_2 \in \mathbb{Z}_n$,

$$(x_1x_2)^d = x_1^d\, x_2^d \mod n.$$

Par conséquent, si Alice signe (disons à des moments différents) les messages $x = x_1x_2$ et x_2, elle signe également, sans pour autant le vouloir, le message x_1. En effet, si on dispose de x^d et de x_2^d, on trouve

$$x_1^d = x^d(x_2^d)^{-1} \mod n$$

et ce même[9] sans avoir connaissance de l'exposant d. Ceci est appelé le problème de la *signature cachée*. En effet, on pourrait imaginer qu'Oscar puisse utiliser le message x_1 authentifié par la signature d'Alice sans que cette dernière ne l'ait jamais signer. Pour remédier à cette situation, on essaie de construire des *fonctions de hachage* qui sont telles que

$$\mu(x_1x_2) \neq \mu(x_1)\mu(x_2)$$

et telles qu'il est "difficile" de trouver $x_1 \neq x_2$ tels que $\mu(x_1) = \mu(x_2)$. En général, on applique la fonction de hachage μ au texte T à signer *dans son intégralité* et le résultat est un texte $\mu(T)$ de taille fixe (souvent 160 bits). C'est ensuite uniquement le résultat qui est signé : $(\mu(T))^d \mod n$. Bien évidemment la fonction de hachage μ n'est pas injective, mais on cherche à minimiser la probabilité que deux textes distincts ayant du sens possèdent la même image par μ. De plus, cela permet également de diminuer le nombre de calculs à effectuer pour une signature puisqu'on signe à chaque un texte de taille fixe et non un texte T arbitrairement long.

5. Connaissance de d et $\varphi(n)$

Dans cette section, nous montrons que trouver d (resp. $\varphi(n)$) est aussi difficile que factoriser n. Plus précisément, nous allons montrer que si on dispose de d (resp. de $\varphi(n)$) , alors on peut construire un algorithme permettant de factoriser n. En particulier, cette section va nous donner un premier exemple d'algorithme probabiliste.

5.1. Si d est connu. On pose

$$s = \max\{t \in \mathbb{N} \mid 2^t \text{ divise } ed-1\}$$

et

$$k = \frac{ed-1}{2^s}.$$

Autrement dit, 2^s est la plus grande puissance de 2 qui divise $ed-1$.

[9] A condition bien sûr que x_2^d soit inversible. Mais ceci se produit avec une probabilité $\varphi(n)/n = (p-1)(q-1)/pq$ qui est très élevée.

Lemme III.5.1. *Si a est premier avec n, l'ordre de a^k dans le groupe multiplicatif*[10] *$\mathbb{Z}_n^*$ est de la forme 2^i pour un $i \in \{0, \ldots, s\}$.*

Démonstration. Puisque a est premier avec n, le petit théorème de Fermat stipule que

$$a^{ed-1} \equiv 1 \mod n.$$

Par définition de k, on a $ed - 1 = k2^s$ et donc

$$(a^k)^{2^s} \equiv 1 \mod n.$$

Par définition de l'ordre d'un élément, cette dernière égalité signifie que l'ordre de a^k divise 2^s.

■

Proposition III.5.2. *Soit a premier avec n. Si les ordres de a^k modulo p et modulo q diffèrent, alors il existe $t \in \{0, \ldots, s-1\}$ tel que*

$$1 < \text{pgcd}(a^{2^t k} - 1, n) < n.$$

Démonstration. Par le lemme précédent, on sait qu'il existe $i \leq s$ tel que

$$(a^k)^{2^i} = 1 + \alpha n = 1 + (\alpha p)q.$$

Cela signifie que 2^i est un multiple de l'ordre de a^k modulo q. Ainsi, l'ordre de a^k modulo q est de la forme 2^t et pour les mêmes raisons, l'ordre de a^k modulo p est de la forme $2^{t'}$. Par hypothèse, les ordres étant différents, on peut supposer $t < t' \leq s$. De là, on a

$$(a^k)^{2^t} \equiv 1 \mod q \quad \text{et} \quad (a^k)^{2^t} \not\equiv 1 \mod p.$$

Ainsi, $(a^k)^{2^t} - 1$ est un multiple de q mais pas de p et

$$\text{pgcd}(a^{2^t k} - 1, n) = q.$$

■

On dispose dès lors d'un algorithme pour factoriser n :

Algorithme III.5.3. La donnée est n.
Choisir aléatoirement $a \in \{1, \ldots, n-1\}$.
Calculer $g = \text{pgcd}(a, n)$.
    Si $g > 1$, on a trouvé un facteur de n.
    Si $g = 1$,
        pour $t = s-1, s-2, \ldots$
            calculer $g' = \text{pgcd}(a^{2^t k} - 1 \mod n, n)$
        jusqu'à obtenir $g' > 1$ ou arriver à $t = 0$.
    Si $g' > 1$, on a trouvé un facteur de n.
    Sinon, $t = 0$, recommencer l'algorithme avec un nouveau choix de a.

[10] Rappelons que $\mathbb{Z}_n^*$ désigne le groupe des éléments inversibles de $\mathbb{Z}_n$ muni de l'opération de multiplication.

La question qui se pose est de déterminer parmi les $\varphi(n)$ candidats "a" premiers avec n combien sont tels que a^k possède des ordres différents modulo p et q. En effet, de tels a permettent de factoriser n. Le résultat suivant est admis sans démonstration[11].

Proposition III.5.4. *Le nombre d'entiers $a < n$, premiers avec n et tels que a^k possède des ordres différents modulo p et q est au moins égal à $\varphi(n)/2$.*

Corollaire III.5.5. *La probabilité de tirer consécutivement k nombres "a" au hasard dans l'algorithme III.5.3 et qu'aucun de ceux-ci ne permette de factoriser n est inférieure*[12] *à*

$$2^{-k}.$$

5.2. Si $\varphi(n)$ est connu. Les développements sont immédiats. En effet, nous savons que

$$n = p.q \quad \text{et} \quad \varphi(n) = (p-1)(q-1).$$

En remplaçant q par n/p dans la seconde équation, on obtient

$$\varphi(n) = (p-1)(\frac{n}{p} - 1)$$

c'est-à-dire,

$$p^2 + p\,[\varphi(n) - n - 1] + n = 0.$$

Puisque $\varphi(n)$ est connu, il s'agit d'une simple équation du second degré permettant de retrouver le facteur p de n.

6. Rapidité du RSA

Typiquement, si l'exposant de déchiffrement est du même ordre de grandeur que $n = p.q$ et si l'on suppose que son écriture binaire contient autant de bits 0 que de 1, alors travaillant avec un entier $n \sim 2^{1024}$, pour réaliser une exponentiation modulaire, on a besoin de 1024 élévations au carré et 512 multiplications modulo n. Par conséquent, la quantité de calculs à effectuer, bien que pouvant être traitée en pratique, est bien supérieure au nombre de calculs nécessaires dans la mise en oeuvre des cryptosystèmes à clé secrète comme par exemple le DES. On peut en effet estimer le RSA de 1000 à 10000 fois plus lent. Ainsi, il arrive souvent qu'on utilise le RSA pour échanger en toute sécurité une clé d'un cryptosystème à clé secrète puis, une fois cette initialisation réalisée, utiliser uniquement le cryptosystème symétrique bien plus rapide. C'est par exemple la technique employée par le logiciel PGP (voir `http://www.pgpi.org/`).

[11] La preuve de ce résultat n'est pas difficile mais n'apporte pas d'élément essentiel à la suite de notre discussion.

[12] A titre indicatif, si $k = 10$, $1 - 2^{-k} = 1023/1024 \sim 0,999$.

7. Quelques éléments de sécurité à prendre en considération

Dans cette section, nous présentons quelques remarques à prendre en compte pour ne pas permettre à Oscar de retrouver facilement la factorisation de n ou l'exposant de déchiffrement. Bien évidemment, le lecteur soucieux de mettre en pratique le RSA devra passer en revue l'ensemble des cas connus pour éviter tout éceuil de sécurité. Notre liste n'est certes pas exhaustive. Dans cette section, certains termes restent volontairement "vagues". Par exemple, on parle de "petit" nombre premier. L'adjectif "petit" est à mettre en rapport avec les tailles d'entiers qui peuvent être aisément traités par un ordinateur actuel. Ainsi, sans l'utilisation de l'ordinateur, on peut imaginer qu'un nombre de l'ordre de 10^8 est considéré comme "grand" (car les calculs à la main deviennent vite pénibles). Avec la technologie d'il y a dix ans, 2^{128} était certes considéré comme "grand" et maintenant, on considérera comme "grand" un nombre de l'ordre de 2^{256}. Il faut donc, en cryptographie, toujours tenir compte des évolutions tant théoriques que matérielles.

1. Les deux facteurs p et q ne doivent pas être petits, ni provenir d'une table. En effet, par recherche exhaustive ou en testant les nombres de la table, Oscar pourrait facilement (c'est-à-dire en un temps raisonnable) factoriser n. Par exemple, avec la technologie actuelle, il est tout à fait réaliste de rechercher de manière exhaustive si n est divisible par l'un des 10^7 premiers nombres premiers.

Exemple III.7.1. Sous Mathematica , tester si 15485863 est divisible par l'un des cent mille premiers nombres premiers prend sur un pentium III à 600 Mhz un peu moins de $3,4$ secondes.

```
:> Timing[Table[Mod[15485863, Prime[i]],{i,1,100000}]]
Out[]={3.37 Second, {1, 1, 3, 1, 8, 3, 2, 8, 9, ... }}
```

2. Les facteurs p et q ne doivent pas être trop proches. En effet, dans cette situation, on dispose d'une attaque élémentaire pour factoriser n. Dans cette situation, si $p > q$, alors $(p-q)/2$ est petit et $(p+q)/2$ est un peu plus grand[13] que $\sqrt{n}$. Par ailleurs, il est clair que

$$\left(\frac{p+q}{2}\right)^2 - n = \left(\frac{p-q}{2}\right)^2.$$

Ainsi, il suffit de considérer successivement tous les entiers $x > \sqrt{n}$ et pour ceux-ci, de calculer $x^2 - n$ jusqu'à obtenir un carré parfait y^2. Dans ce cas, $x^2 - y^2 = n$ et on trouve $p = x + y$ et $q = x - y$.

Exemple III.7.2. Soit $n = 97343$. On a $\sqrt{n} > 311$ et

$$312^2 - n = 1.$$

[13]Rappelons que la moyenne géométrique $\sqrt{pq}$ est majorée par la moyenne arithmétique $(p+q)/2$. "AM-GM Inequality" : pour tous $a_1, \ldots, a_n \geq 0$, $\sum_{i=1}^n a_i/n \geq \prod_{i=1}^n a_i^{1/n}$.

Par conséquent, $n = 311.313$.

Exemple III.7.3. Soit $n = 239812789091371$. On a $\sqrt{n} > 15485889$ et

$$15485890^2 - 239812789091371 = 729 = 27^2.$$

Donc,

$$239812789091371 = (15485890 + 27)(15485890 - 27).$$

Il s'agit en fait du produit des millionième et $(10^6 + 2)$-ième nombres premiers.

3. Les nombres $p-1$ et $q-1$ ne doivent pas avoir un large facteur commun (i.e., un pgcd trop grand). En effet, sinon leur plus petit commun multiple

$$u = \text{ppcm}\{(p-1), (q-1)\}$$

sera "relativement petit" en comparaison de $\varphi(n)$ (on peut avoir $u \sim \sqrt{n}$). On peut alors exploiter le fait suivant. *Si* $u = \text{ppcm}\{(p-1), (q-1)\}$, *alors tout inverse de* e *modulo* u *peut être utilisé comme exposant de déchiffrement*[14].

Bien que u (tout comme $\varphi(n)$ d'ailleurs) soit inconnu, puisqu'on ne connaît pas p et q, u peut être suffisamment petit pour procéder à une recherche exhaustive d'un exposant de déchiffrement. Ainsi, il suffit à Oscar de tester des candidats u successifs et pour chacun d'entre eux de calculer l'inverse de e modulo u. Si ces candidats ne sont pas trop nombreux, Oscar obtiendra alors en un temps raisonnable un exposant de déchiffrement. Par contre si u est "grand", il ne sera pas possible à Oscar de procéder à cette recherche exhaustive.

Exemple III.7.4. Soient $p = 61$, $q = 181$, $n = 11041$ et $e = 4013$. Ici, $\varphi(n) = 60.180 = 10800$ et nous sommes dans la situation extrême où le ppcm de $p-1$ et de $q-1$ est égal à $q-1 = 180$. Le ppcm étant pair, il suffit de tester successivement pour candidats $u = 2, 4, \ldots, 180$. Après un maximum de 90 tests, Oscar est en mesure de construire un exposant de déchiffrement et ce bien que $\varphi(n)$ soit bien plus grand.

Exemple III.7.5. Modifions légèrement l'exemple précédent. Soient $p = 61$, $q = 179$, $n = 10919$ et $e = 4013$. Ici, $\varphi(n) = 60.178 = 10680$. Du point de vue de l'ordre de grandeur, les différences sont minimes. Néanmoins, ici

$$\text{ppcm}(60, 178) = 60.89 = 5340$$

[14]En effet, si $z.e \equiv 1 \mod u$, alors $z.e = 1 + \alpha(p-1) = 1 + \beta(q-1)$ et il suffit d'adapter la seconde partie de la preuve de la proposition III.2.1 à ce cas. Soit $x \in \mathbb{Z}_n$. On a

$$(x^e)^z = x^{ez} = x(x^\alpha)^{p-1}.$$

Si x est premier avec p, alors x^α aussi et $x.(x^\alpha)^{p-1} \equiv x.1$ modulo p. Si x est un multiple de p, $(x^e)^z$ et x sont tous deux congrus à 0 modulo p. Par conséquent, pour tout $x \in \mathbb{Z}_n$, $(x^e)^z \equiv x$ modulo p. Le raisonnement est également valide pour q. On en tire que pour tout $x \in \mathbb{Z}_n$, $(x^e)^z \equiv x$ modulo n, z est bien un exposant de déchiffrement.

et par conséquent, la recherche exhaustive nécéssite de l'ordre de 2770 essais (à comparer aux 90 tests de l'exemple précédent).

4. Supposons que $\varphi(n)$ ne possède que de petits facteurs premiers, i.e.,

$$\varphi(n) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad p_i \leq r$$

où r est une borne suffisamment petite (dans l'écriture ci-dessus $p_1, \ldots, p_k$ représentent tous les nombres premiers inférieurs à r et α_i vaut 0 lorsque p_i n'apparaît pas effectivement dans la décomposition de $\varphi(n)$ en facteurs premiers). Il est clair que

$$p_i^{\lfloor \log_{p_i} n \rfloor}$$

est la plus grande puissance de p_i qui peut éventuellement diviser $\varphi(n)$ (en effet, $\varphi(n) < n$ et ne connaissant pas la valeur de $\varphi(n)$, on utilise alors n comme estimation). On peut alors décider de passer en revue les candidats potentiels pour $\varphi(n)$: ils sont de la forme

$$u = p_1^{\beta_1} \cdots p_k^{\beta_k} \text{ avec } \beta_i \leq \lfloor \log_{p_i} n \rfloor, \forall i \leq k.$$

Pour chaque candidat potentiel u, si $(u+1)/e$ est un entier d', on essaye d' comme exposant de déchiffrement (c'est assez naturel, car alors $ed' = 1 + u$). Si r n'est pas trop grand, les candidats potentiels à tester ne sont pas trop nombreux et une recherche exhaustive est réalisable. Par contre, si r est grand, i.e., si $\varphi(n)$ contient un grand facteur premier, alors la recherche exhaustive devient impraticable.

Exemple III.7.6. Soit n le produit des 100- et 101-ièmes nombres premiers,

$$n = 295927 \text{ et } \varphi(n) = 2^3.3^4.5.7.13.$$

Si on adopte les conventions précédentes, on a

$$\varphi(n) = 2^3.3^4.5.7.11^0.13$$

et $\log_2 n = 18$, $\log_3 n = 11$, $\log_5 n = 7$, $\log_7 n = 6$, $\log_{11} n = 5$, $\log_{13} n = 4$. Ainsi, les candidats u sont (en considérant la borne $r = 13$) de la forme

$$2^{i_1}.3^{i_2}.5^{i_3}.7^{i_4}.11^{i_5}.13^{i_6}$$

avec $0 \leq i_1 \leq 18$, $0 \leq i_2 \leq 11$, $0 \leq i_3 \leq 7$, $0 \leq i_4 \leq 6$, $0 \leq i_5 \leq 5$ et $0 \leq i_6 \leq 4$. Le nombre total de candidats est donc

$$19.12.8.7.6.5 = 383040.$$

Par contre, pour n, produit des 101- et 102-ièmes nombres premiers, on a

$$n = 304679 \text{ et } \varphi(n) = 2^3.3.7.13.139.$$

Ici, le plus grand facteur premier apparaissant dans la décomposition de $\varphi(n)$ est 139 (qui est le 34-ième nombre premier) et si on procède comme ci-dessus, les candidats u sont de la forme

$$2^{i_1}.3^{i_2}.5^{i_3}.7^{i_4} \cdots 131^{i_{32}}.137^{i_{33}}.139^{i_{34}}$$

et le nombre total de candidats est

$$5149048008867840.$$

5. Signalons encore que si les exposants e et d sont petits, il existe également des attaques possibles du RSA. Ainsi, pour la sécurité du système, il est conseillé d'avoir de grands exposants. Cependant, il est clair qu'au point de vue temps de calcul, des exposants petits seraient bien plus avantageux puisqu'ils réduiraient le nombre de multiplications et d'élévations au carré dans une exponentiation modulaire. Il est donc parfois nécessaire de faire un compromis entre sécurité et temps de calcul (par exemple, pour un système RSA placé sur une carte à puce pour laquelle les ressources de calcul sont limitées).

8. Génération de grands nombres premiers

Remarque III.8.1. Cette section ne tient pas compte des résultats récents d'Agrawal *et al.* fournissant un algorithme polynomial permettant de tester la primalité d'un entier (et fournissant par la même occasion une réponse positive à la conjecture $\texttt{Primes} \in P$). Bien que polynomial et prometteur, leur algorithme est difficile à mettre en oeuvre et nous avons préféré présenter ici les algorithmes probabilistes classiques (Fermat ou Miller-Rabin) permettant de tester la primalité d'un entier.

Pour mettre en oeuvre le RSA, il est nécessaire de pouvoir générer de grands nombres premiers. Pratiquement, si on désire trouver un nombre premier de k bits lorsqu'il est écrit en base 2, on considère un vecteur appartenant à $\{0,1\}^k$ dont les première et dernière composantes valent 1. En effet, voulant obtenir un nombre ayant exactement k chiffres, celui-ci ne commence donc pas par 0 et pour avoir un nombre premier, le dernier chiffre doit être 1 sinon le nombre serait pair. Une fois ce nombre obtenu, on effectue des tests de primalité pour déterminer si le nombre tiré est bel et bien premier. Le théorème de raréfaction des nombres premiers (cf. théorème I.10.4) nous donne une approximation du nombre de tirages à réaliser pour obtenir un nombre premier de k bits : le nombre de nombres premiers de k bits est

$$\pi(2^k) - \pi(2^{k-1}) \sim \frac{2^k}{\ln 2^k} - \frac{2^{k-1}}{\ln 2^{k-1}}$$

et le nombre total d'entiers impairs de k bits est 2^{k-2}. Ainsi, en quotientant les deux grandeurs, pour $k = 100$, la probabilité de tirer au hasard un nombre premier est proche de $0,0285$ et pour $k = 512$, cette probabilité passe à $0,0056$.

Le petit théorème de Fermat fournit un test de primalité probabiliste. En effet, si m est premier, alors $x^{m-1} \equiv 1 \mod m$. Donc, si pour x premier avec m, on a $x^{m-1} \not\equiv 1 \mod m$, alors on en conclut directement que m n'est pas premier. L'algorithme pour tester m est le suivant .

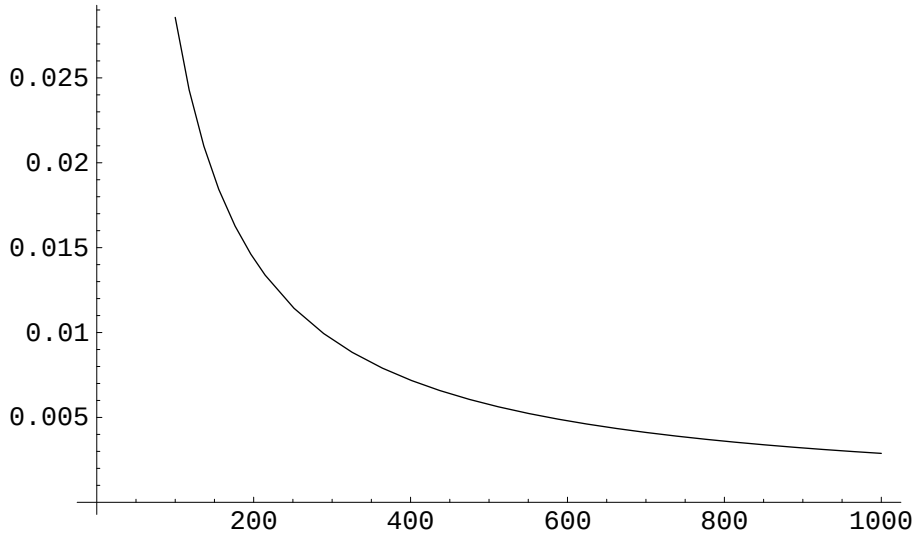


FIGURE III.1. Probabilité de tirer un nombre premier de k bits.

Algorithme III.8.2 (Test de primalité de Fermat). La donnée est m.
Choisir aléatoirement x tel que $1 \leq x < m$.
Calculer $g = \text{pgcd}(x, m)$.
  Si $g > 1$, alors m n'est pas premier.
  Sinon, calculer $t = x^{m-1} \mod m$.
    Si $t \not\equiv 1$, alors m est composé.
    Si $t \equiv 1$, alors m est peut-être premier.

Ainsi, la réponse fournie par l'algorithme est : soit "m est composé" (on ne dispose pas de la factorisation de m mais on est certain que ce nombre n'est pas premier) soit "m est peut-être premier". En effet, pour m composé, il existe des entiers x tels que $x^{m-1} \equiv 1 \mod m$. La détermination du caractère composé de m dépend de l'entier x tiré aléatoirement.

Définition III.8.3. Si x est tel que $1 \leq x < m$, $\text{pgcd}(x, m) = 1$ et $x^{m-1} \equiv 1 \mod m$, alors on dit que x est un *témoin de la primalité* de m ou que m est un nombre *pseudo-premier relativement à la base* x.

au plus m a de témoins, au plus on peut croire en sa primalité...

Exemple III.8.4. Le nombre 91 est composé, $91 = 13.7$. Considérons les deux calculs suivants,

$$2^{90} = 2^{64}.2^{16}.2^{8}.2^{2} \equiv 64 \mod 91.$$

Ainsi, si dans l'algorithme, on avait tiré aléatoirement $x = 2$, on aurait montré que 91 n'est pas premier. Autrement dit, 2 n'est pas témoin de la primalité de 91. Par contre,

$$3^{90} = 3^{64}.3^{16}.3^{8}.3^{2} \equiv 1 \mod 91.$$

Dès lors, si dans l'algorithme on avait choisi $x = 3$, on n'aurait pas été en mesure de prouver la non primalité de 91. On peut dire que 91 est pseudo-premier relativement à 3.

Pour déterminer la probabilité avec laquelle l'algorithme pourra détecter qu'un nombre n'est pas premier, on recourt au résultat suivant.

Proposition III.8.5. *Considérons un entier m. Soit tous, soit au plus la moitié des entiers x tels que $1 \leq x < m$ et $\text{pgcd}(x, m) = 1$ sont témoins de la primalité de m.*

Remarque III.8.6. Dans la situation où un entier composé m est tel qu'au plus la moitié des entiers x sont témoins de la primalité de m, si on effectue k tests consécutifs, la probabilité que m soit considéré comme pseudo-premier à l'issue de ces k tests est inférieure à 2^{-k}. En effet, il faudrait lors des k choix aléatoires, tirer, à chaque fois, des nombres témoins de la primalité de m.

Ainsi, sous l'hypothèse que les entiers non premiers testés possèdent au moins un élément non témoin de la primalité, alors le tableau suivant reprend la probabilité qu'un nombre soit premier s'il passe avec succès k tests consécutifs.

k	1	2	3	4	5	6	7	8
P	0.5	0.75	0.875	0.9375	0.96875	0.984375	0.992188	0.996094

k	9	10	11	12	13	14
P	0.998047	0.999023	0.999512	0.999756	0.999878	0.999939

Démonstration. Supposons que x n'est pas témoin de la primalité de m, i.e.,

$$x^{m-1} \not\equiv 1 \mod m.$$

Soient $w_1, \ldots, w_t$ tous les témoins (distincts) de primalité de m. Posons

$$u_i = x\, w_i \mod m.$$

Les u_i sont tous distincts car x est premier avec m donc inversible modulo m. Si $u_i = u_j$ avec $i \neq j$, alors on en déduirait que $w_i = w_j$, ce qui est impossible. De plus, $1 \leq u_i < m$ et $\text{pgcd}(u_i, m) = 1$ car x et les w_i, par définition, sont premiers avec m. Il est facile de voir que les u_i ne sont pas témoins de la primalité de m. En effet,

$$u_i^{m-1} = \underbrace{x^{m-1}}_{\not\equiv 1} \underbrace{w_i^{m-1}}_{\equiv 1} \not\equiv 1 \mod m.$$

En conclusion, s'il existe x qui n'est pas témoin de la primalité de m, alors il y a au moins autant de nombres u_i non témoins que de w_i qui sont témoins. Ceci conclut la preuve.

■

Définition III.8.7. Il existe des nombres composés m pour lesquels tout $x < m$ et premier avec m est témoin de primalité de m, i.e., $x^{m-1} \equiv 1 \mod m$. Un tel nombre est appelé nombre de *Carmichael*. Bien évidemment, la probabilité de détection de la non primalité de m donnée à la remarque III.8.6 ne s'applique pas aux nombres de Carmichael. Le seul espoir bien faible de détecter la non primalité d'un tel nombre m est de tirer au hasard un nombre x ayant un facteur commun avec m.

Proposition III.8.8. *Un nombre composé m est de Carmichael si et seulement si il n'est divisible par aucun carré parfait (on dit parfois qu'il est square-free ou quadratfrei) et pour tout p premier divisant m, $p-1$ divise $m-1$.*

Exemple III.8.9. Le nombre $561 = 3.11.17$ est un nombre de Carmichael (c'est même le plus petit). En effet, $560 = 280.2$, $560 = 56.10$ et $560 = 35.16$. On pourrait vérifier que tout $x < m$ et premier avec m est tel que $x^{m-1} \equiv 1 \mod m$.

Démonstration. Soit $m \geq 3$ un nombre de Carmichael. Soit p un diviseur premier de m. Soit a une racine primitive modulo p (i.e., un générateur de $\mathbb{Z}_p^*$) qui est première avec m.

Un choix d'un tel a est toujours possible. En effet, nous savons que $\mathbb{Z}_p$ est un champ et par le théorème I.6.20, $\mathbb{Z}_p^*$ possède exactement $\varphi(p-1)$ générateurs. Soit u un de ces générateurs modulo p. Si m se décompose en produit de facteurs premiers sous la forme $p^\alpha q_1^{\beta_1} \cdots q_r^{\beta_r}$, alors a s'obtient par exemple comme solution du système

$$\begin{cases} a \equiv u & \mod p, \\ a \equiv 1 & \mod q_1, \\ \vdots & \\ a \equiv 1 & \mod q_r. \end{cases}$$

(En effet, si a est solution de ce système, il est nécessairement premier avec m puisqu'il n'a aucun facteur commun avec m. Il suffit en fait d'assurer qu'aucune de ces congruences ne soit nulle.) Le théorème des restes chinois[15] assure l'existence d'un tel a.

Puisque a est premier avec m qui est un nombre de Carmichael, on a $a^{m-1} \equiv 1 \mod m$ et donc $a^{m-1} \equiv 1 \mod p$ (car p divise m). De plus, a

[15]Théorème des restes chinois. Si $m_1, \ldots, m_n$ sont deux à deux premiers, le système

$$x \equiv a_1 \mod m_1, \ldots, x \equiv a_n \mod m_n$$

possède une unique solution modulo $m = m_1 \cdots m_n$. Si, pour tout $i = 1, \ldots, n$, on pose $M_i = m/m_i$ et $y_i = M_i^{-1} \mod m_i$, alors cette solution est donnée par

$$x = \left(\sum_{i=1}^{n} a_i y_i M_i \right) \mod m.$$

étant une racine primitive modulo p, son ordre modulo p est exactement $p-1$ et donc $p-1$ divise $m-1$.

Il nous reste à vérifier que p^2 ne divise pas m. Supposons que p^2 divise m. Dans ce cas, $\varphi(m)$ est alors divisible par $p(p-1)$ et en particulier par p. Dès lors, $\mathbb{Z}_m^*$ qui est un groupe contenant $\varphi(m)$ éléments contient un sous-groupe[16] d'ordre p et donc aussi un élément $b \in \mathbb{Z}_m^*$ premier avec m et d'ordre p modulo m. Puisque m est de Carmichael, $b^{m-1} \equiv 1 \mod m$ donc p doit diviser $m-1$. Ceci est impossible car p divise m.

Passons à la réciproque. Supposons que m est sans carré et que $p-1$ divise $m-1$ pour tout facteur premier p de m. Soient a premier avec m et p un diviseur premier de m. Nous devons vérifier que $a^{m-1} \equiv 1 \mod m$. Puisque p est premier, par le petit théorème de Fermat, on a

$$a^{p-1} \equiv 1 \mod p.$$

Puisque $m-1$ est un multiple de $p-1$, on a aussi

$$a^{m-1} \equiv 1 \mod p.$$

Cette dernière congruence est valable pour tous les diviseurs premiers de m. Ainsi, si $m = p_1 \cdots p_r$ (avec $p_i \neq p_j$, si $i \neq j$ car m est sans carré), alors pour tout $i = 1, \ldots, r$,

$$a^{m-1} \equiv 1 \mod p_i.$$

De là, on en tire que

$$a^{m-1} \equiv 1 \mod m.$$

■

Corollaire III.8.10. *Un nombre m de Carmichael est toujours impair.*

Démonstration. En effet, si $p \geq 3$ est un facteur premier de m, vu la proposition précédente, $p-1$ divise $m-1$. Or $p-1$ est pair donc $m-1$ l'est aussi.

■

Remarque III.8.11. Signalons qu'il a été démontré récemment qu'il existe une infinité de nombres de Carmichael[17]. A titre indicatif, le nombre de nombres de Carmichael inférieurs à 10^{17} est

$$585355$$

ce qui est bien peu en comparaison des $\pi(10^{17}) \sim 2,5.\,10^{15}$ nombres premiers inférieurs à 10^{17}. Pour la fonction comptant le nombre de nombres de Carmichael inférieurs à n, on ne dispose pas de résultats analogues à ceux

[16] C'est une conséquence directe du lemme de Cauchy : tout groupe commutatif fini dont l'ordre est divisible par un nombre premier p contient un élément d'ordre p. On peut aussi le voir, dans le cas général, comme une conséquence du premier théorème de Sylow : tout groupe fini dont l'ordre est divisible par un nombre premier p contient un élément d'ordre p.

[17] W. R. Alford, A. Granville, C. Pomerance, *There Are Infinitely Many Carmichael Numbers*, Ann. Math. **139**, 703–722, (1994).

dont on dispose pour $\pi(n)$. Il faut alors recourir à des techniques[18] de calcul élaborées pour énumérer ces nombres.

8.1. Test de Miller-Rabin. Un autre test de primalité souvent employé est le test de Miller-Rabin. L'avantage de ce test probabiliste est qu'il n'existe pas dans cette situation d'analogue aux nombres de Carmichael. Le principe suit la même ligne que le test de Fermat.

Soit $m > 1$ un nombre impair. On pose

$$s = \max\{r \in \mathbb{N} \mid 2^r \text{ divise } m-1\}$$

et

$$d = \frac{m-1}{2^s}.$$

On dispose du résultat suivant[19], analogue du petit théorème de Fermat.

Théorème III.8.12. *Si m est un nombre premier et si $x \in \mathbb{Z}$ est premier avec m, alors l'une des deux conditions est satisfaite :*

- $x^d \equiv 1 \mod m$,
- *il existe $r \in \{1, \ldots, s-1\}$ tel que $x^{2^r d} \equiv -1 \mod m$.*

On dispose par conséquent d'un algorithme pour tester la primalité d'un entier m. Si un entier x premier avec m est tel que aucune des deux conditions du théorème III.8.12 n'est satisfaite, alors m est composé. On dit alors qu'un tel x est *témoin du caractère composé de m*. Dans le cas contraire, on dit que m est un nombre *pseudo-premier fort* (*strong pseudoprime*) pour la base x, l'adjectif "fort" faisant une référence au fait que le test de Miller-Rabin est plus puissant que celui de Fermat.

Tout comme dans le test basé sur le théorème de Fermat, il suffit de tirer au hasard "suffisamment" d'entiers x pour être convaincu de la primalité de m. La probabilité avec laquelle le test de Miller-Rabin peut déterminer le caractère composé d'un nombre est donnée par le résultat suivant.

Proposition III.8.13. *Si $m \geq 3$ est impair, il y a au plus $(m-1)/4$ entiers $x < m$ premiers avec m et non témoins du caractère composé de m.*

Corollaire III.8.14. *Si on applique k fois consécutivement le test de Miller-Rabin à un nombre composé m, la probabilité de ne pas découvrir son caractère composé est inférieure à 4^{-k}.*

Exemple III.8.15. Nous avons vu précédemment que $m = 561$ est un nombre de Carmichael (et par conséquent impossible à déterminer comme composé par le test de Fermat). Si on applique le test de Miller-Rabin, on peut par exemple choisir $x = 2$. La plus grande puissance de 2 qui divise

[18] Bien qu'il existe de nombreux articles, on pourra par exemple voir : R.G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Mathematics of Computation **61**, 381–391 (1993).

[19] Pour une démonstration, on se référera par exemple à : J.A. Buchmann, *Introduction to cryptography*, Springer (2001).

560 est $16 = 2^4$ (car $560 = 16.35$). Ainsi, $s = 4$ et $d = 560/16 = 35$. On calcule

$$x^d = 2^{35} \mod 561 = 263.$$

Puisque le résultat n'est pas 1, on calcule $x^{2^r d}$ pour $r = 1, 2, \ldots, s-1$:

$$2^{2.35} \mod 561 = 166,\ 2^{4.35} \mod 561 = 67,\ 2^{8.35} \mod 561 = 1.$$

Par conséquent, aucune congruence ne donnant -1, on en déduit que 561 est composé et 2 en est le témoin.

Remarque III.8.16. On peut même montrer, en supposant l'hypothèse[20] de Riemann généralisée vérifiée, que si m est composé, alors il existe toujours un témoin x du caractère composé de m tel que

$$x < 2(\ln m)^2.$$

Ceci permet donc d'utiliser le test de Miller-Rabin de manière déterministe en testant tous les x jusqu'à cette borne.

9. RSA et nombres composés

La section précédente nous a montré qu'utiliser l'algorithme découlant du petit théorème de Fermat pour obtenir des nombres premiers peut très bien mener à des nombres composés. Soit, par "malchance", m est composé et les tirages aléatoires ont tous fourni des témoins de primalité de m, soit m est de Carmichael. Analysons donc le chiffrement RSA dans le cas où p et q ne sont pas nécessairement premiers. On suppose ici que

$$p = p_1 p_2$$

et que p_1, p_2, q sont premiers. On a $n = p.q = p_1.p_2.q$ et

$$\varphi(n) = (p_1 - 1)(p_2 - 1)(q - 1).$$

Par contre, ne sachant pas que p n'est pas premier (les tests effectués n'ont par exemple pas su détecter son caractère composé), la valeur de $\varphi(n)$ effectivement calculée est

$$\varphi'(n) = (p - 1)(q - 1)$$

et on choisit des exposants e, d tels que

$$e.d \equiv 1 \mod \varphi'(n) \tag{5}$$

[20] L'*hypothèse de Riemann* stipule que tous les zéros complexes de la fonction

$$\zeta : \mathbb{C} \to \mathbb{C} : s \mapsto \sum_{n=1}^{\infty} \frac{1}{n^s}$$

dont la partie réelle se trouve entre 0 et 1 ont leur partie réelle exactement égale à 1/2. Par exemple, il est facile de voir que si $\operatorname{Re} s > 1$, alors $\zeta(s) \neq 0$ et que si $\operatorname{Re} s < 0$, alors les seuls zéros de la fonction ζ sont $-2, -4, -6, \ldots$ (appelés zéros triviaux). L'hypothèse de Riemann généralisée est du même type mais pour une généralisation de la fonction ζ, à savoir les L-séries de Dirichlet.

Soit

$$u = \text{ppcm}(p_1 - 1, p_2 - 1, q - 1)$$

et supposons que le texte clair x est premier avec n (si x est multiple de p_1, p_2 ou q, on procède comme on l'a déjà fait à plusieurs reprises, cf. proposition III.2.1 et note en bas de la page 90, cela ne ferait que compliquer l'exposé). Par conséquent, x est premier avec p_1, p_2, q et

$$x^{p_1-1} \equiv 1 \mod p_1,\ x^{p_2-1} \equiv 1 \mod p_2,\ x^{q-1} \equiv 1 \mod q.$$

Puisque u est multiple de $p_1 - 1$, de $p_2 - 1$ et de $q - 1$, on a aussi

$$x^u \equiv 1 \mod p_1,\ x^u \equiv 1 \mod p_2,\ x^u \equiv 1 \mod q.$$

De là, p_1, p_2, q étant premiers et distincts, on en tire

$$x^u \equiv 1 \mod n.$$

Il est clair que u divise $\varphi(n)$ (par définition, u est le ppcm des facteurs apparaissant dans $\varphi(n)$).

Pour un texte clair x chiffré en $x^e \mod n$, nous avons à présent deux situations à envisager :

- soit u divise le $\varphi'(n)$ erroné,
- ou bien, u ne divise pas le $\varphi'(n)$ erroné.

Dans le premier cas, $\alpha\, u = \varphi'(n)$ et donc, au vu de (5),

$$(x^e)^d = x^{1+k\varphi'(n)} = x^{1+k\,\alpha\,u} \equiv x \mod n.$$

Par conséquent, toute paire (e, d) d'exposants de chiffrement et de déchiffrement telle que $e.d \equiv 1 \mod \varphi'(n)$ convient. (En effet, les exposants ont été calculés avec le $\varphi'(n)$ erroné.)

Dans le second cas, les choses ne se passent pas aussi bien. En général, $d_k(e_k(x)) \neq x$! Ceci est vérifié sur l'exemple suivant.

Exemple III.9.1. Soient

$$p = 391 (= 17.23) \quad \text{et} \quad q = 281.$$

Ici, $n = 109871$ et le $\varphi'(n)$ calculé (lorsqu'on ne s'est pas aperçu que p n'était pas premier) est $\varphi'(n) = 390.280 = 109200$. Avec nos notations,

$$u = \text{ppcm}\,(16 = 2^4, 22 = 2.11, 280 = 2^3.5.7) = 2^4.5.7.11 = 6160.$$

Ici, u ne divise pas $\varphi'(n)$ ($109200 = 17.6160 + 4480$). Si on décide de prendre $e = 19$, on obtient l'inverse de e modulo $\varphi'(n)$ par l'algorithme d'Euclide étendu et on trouve $d = 45979$. Le texte clair $x = 8$ est bien premier avec n. Nous devrions avoir (dans le cas d'un vrai RSA) $x^{ed} \equiv x \mod n$, mais ici on trouve

$$x^{ed} \mod 109871 = 95548 \neq 8.$$

10. Algorithmes de factorisation

Dans ce cours introductif, nous ne voulons pas développer plus en avant les algorithmes de factorisation connus pour tenter de factoriser n. On peut par exemple citer : le crible d'Eratostène, le crible quadratique (quadratic sieve), des algorithmes sur les courbes elliptiques, le crible algébrique (number field sieve), l'algorithme ρ, la méthode $p-1$ de Pollard, la méthode $p+1$ de Williams ou encore l'algorithme de factorisation par fractions continues. Bien évidemment, toute personne désirant implémenter de manière sûre le RSA doit être au courant de ces algorithmes pour adapter son choix de p et q. Actuellement, aucun algorithme de factorisation connu ne peut factoriser en un temps raisonnable un entier $n \sim 2^{1024}$.

Le crible d'Eratostène bien que simpliste — on teste la divisibilité de n par les entiers successifs[21] — peut être utilisé pratiquement pour des $n < 10^{12}$. Pour donner une idée des ordres de grandeurs, imaginons un ordinateur capable de réaliser 10^9 divisions par seconde ! Si n est de l'ordre de 2^{1024}, $\sqrt{n} \sim 10^{150}$. Il faudrait donc au crible d'Eratostème près de 10^{140} secondes ce qui dépasse de très loin l'âge de l'univers !

Illustrons la méthode $p-1$ de Pollard (1974). Il s'agit d'un algorithme simple qui peut parfois s'appliquer à de grands nombres.

Algorithme III.10.1 (Méthode $p-1$ de Pollard). On se donne un nombre n à factoriser et une borne B.

Choisir aléatoirement $g \in \{2, \ldots, n-1\}$.
Calculer $t = \mathrm{pgcd(g, n)}$.
  Si $t > 1$, alors on a trouvé un facteur de n.
  Sinon, calculer $a = g^{B!} \mod n$.
  Calucler $d = \mathrm{pgcd}(a-1, n)$.
    Si $d > 1$, d est un facteur.
    Sinon, facteur non trouvé, recommencer avec un B supérieur.

Remarquons dès à présent que le calcul de a nécéssite $B-1$ exponentiations modulaires. Ainsi, quand nous parlons de borne B "suffisamment petite", cela signifie qu'il s'agit d'une borne réaliste par rapport à la puissance de calcul disponible. Montrons comment fonctionne cet algorithme.

Soit p un facteur premier de n tel que toute puissance r^α d'un nombre premier r apparaissant dans la décomposition en facteurs premiers de $p-1$, soit inférieure à la borne B, i.e., cette décomposition est de la forme

$$p - 1 = r_1^{\alpha_1} \cdots r_t^{\alpha_t} \text{ avec } r_i^{\alpha_i} \leq B, \ \forall i.$$

Si cette borne B est suffisamment petite, il est alors facile de déterminer par cette méthode un multiple de $p-1$ sans pour autant connaître la valeur de $p-1$.

[21] On peut raffiner la méthode en ne considérant que les nombres non multiples des nombres considérés précédemment.

Puisque $a \equiv g^{B!} \mod n$, on a aussi $a \equiv g^{B!} \mod p$ car p divise n. Par le petit théorème de Fermat, $g^{p-1} \equiv 1 \mod p$ (si g est premier avec p, ce que nous pouvons supposer au vu de l'algorithme). Puisque nous supposons que tout facteur r^α de $p-1$ est inférieur à B, on en déduit que

$$p-1 \text{ divise } B!.$$

En effet, les $r_i^{\alpha_i}$ sont distincts deux à deux et tous $\leq B$. De là,

$$a \equiv g^{B!} = g^{m\,(p-1)} = (g^{p-1})^m \equiv 1 \mod p$$

et $a-1$ est un multiple de p. Par conséquent, il ne reste plus qu'à calculer le pgcd de n et de $a-1$.

Remarque III.10.2. On retrouve donc d'une certaine façon la mise en garde **4.** de la section 7 concernant le choix de p et q dans l'élaboration du RSA. Cette technique est aussi l'analogue d'une technique plus récente basée sur les courbes elliptiques sur $\mathbb{F}_p$ et proposée par H. W. Lenstra (cf. par exemple, [**10, 12**]).

Exemple III.10.3. Considérons l'entier (composé)

$$n = 15770708441.$$

Avec $g = 2$ et B fixé à 200, on calcule[22]

$$g^{200!} \mod n = 6094850739.$$

Ensuite, on calcule le pgcd de $6094850739 - 1$ et de n et on trouve

$$135979$$

qui est donc un facteur de n. En fait, n est le produit des deux nombres premiers suivants :

$$p = 115979 \ (p-1 = 2.103.563) \text{ et } q = 135979 \ (q-1 = 2.3.131.173).$$

Ainsi, une borne $B \geq 173$ permettra toujours la factorisation de n. On pourra observer qu'une borne $B \geq 563$ ne donnera plus de résultat, car dans ce cas, a sera congru à 1 modulo p et q donc aussi modulo n. De toute façon, en pratique, on considère les bornes les plus petites possibles.

Remarque III.10.4. On peut montrer que cet algorithme fonctionne en un temps polynomial en n à condition que la borne convenanble B soit en $\mathcal{O}((\log n)^i)$. Cependant, pour un grand nombre n arbitraire, il est probable que la borne B doive augmenter jusque $\sqrt{n}$ et dans ce cas, la méthode $p-1$ n'est pas plus rapide que le crible d'Eratostène.

Nous terminons cette section par quelques repères concernant l'état actuel de la factorisation de grands entiers.

[22] `PowerMod[2,Factorial[200],15770708441]`

Remarque III.10.5. Voici un petit aperçu de l'état actuel de la factorisation des grands nombres premiers. (Rappelons que 2^{1024} comporte un peu plus de 300 chiffres décimaux).

- En 1998, des nombres de taille 10^{70} pouvaient être factorisés en près de 10 heures sur une station de travail.
- A cette même époque, il fallait un an pour factoriser un nombre de 100 chiffres décimaux sur une station.
- En 1999, un nombre de 155 chiffres a été factorisé en plus de 5 mois par 292 ordinateurs en réseau. Des calculs préalables à la factorisation ont pris près de 4 mois à des super-ordinateurs CRAY.
- En décembre 2003, le "*RSA Challenge number*" `RSA-576` de 576 bits (174 chiffres décimaux) a été factorisé[23]. Ce concours consiste à trouver la factorisation de grands nombres premiers et veut ainsi démontrer la sécurité du RSA pour des choix de clés appropriés.
- Le "*RSA Challenge number*" `RSA-640` de 640 bits suivant

  3107418240490043721350750035888567930037346022842727545720
  1619488232064405180815045563468296717232867824379162728380
  3341547107310850191954852900733772482278352574238645401469
  1736602477652346609

  a été factorisé le 5 novembre 2005 (193 chiffres décimaux). Un prix de 20000 dollars avait été proposé à quiconque en fournirait la factorisation. Cette factorisation a nécessité plus de quatre mois de calculs sur un réseau de machines ce qui représente plus de 30 ans de calcul pour un seul processeur Opteron cadencé à 2,2 Ghz. A titre indicatif, on propose 100000 dollars pour le challenge number `RSA-1024` ...

On peut souvent lire des messages comme ceux-ci :

"*Using a minimal key length of* 1024 *bits, it is guaranteed that RSA can be considered safe for the near future as long as thre will be no fundamental advance in the factoring of large numbers.*"

"*Clearly, the factoring of a challenge-number of specific length does not mean that the RSA cryptosystem is "broken." It does not even mean, necessarily, that keys of the same length as the factored challenge number must be discarded. It simply gives us an idea of the amount of work required to factor a modulus of a given size. This can be translated into an estimate of the cost of breaking a particular RSA key pair.*

Suppose, for example, that in the year 2010 a factorization of RSA-768 is announced that requires 6 months of effort on 100,000 workstations. In this hypothetical situation, would all 768-bit RSA keys need to be replaced? The answer is no. If the data being protected needs security for significantly less than six months, and its value is considerably less than the cost of running

[23] `http://www.rsasecurity.com/rsalabs/`

100,000 workstations for that period, then 768-bit keys may continue to be used."

11. Logarithme discret

Soit G un groupe multiplicatif cyclique contenant n éléments et γ un générateur de G.

Définition III.11.1. Soit $x \in G$. Par analogie avec la fonction logarithme usuelle, le *logarithme discret* de x est le plus petit exposant d tel que

$$x = \gamma^d.$$

On utilise alors la notation $\operatorname{dlog} x = d$ ou même $\operatorname{dlog}_\gamma x = d$. Ainsi,

$$\operatorname{dlog}_\gamma : G \to \{1, \ldots, |G|\}.$$

Exemple III.11.2. Dans $\mathbb{Z}_{17}^*$, un générateur est donné par 3. Autrement dit, 3 est une racine primitive modulo 17. On dispose des valeurs suivantes modulo 17 des puissances de 3 :

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Ainsi, par exemple,

$$\operatorname{dlog}_3 15 = 6 \text{ et } \operatorname{dlog}_3 14 = 9.$$

Remarque III.11.3. On peut parfois considérer une version quelque peu plus générale que le problème de la détermination du logarithme discret de x. Soit G un groupe quelconque (pas nécessairement cyclique), dans lequel on considère deux éléments $x, y \in G$. La question qui est posée est alors de savoir s'il existe d tel que $x^d = y$ et dans ce cas, de rechercher le plus petit d ayant cette propriété. En particulier, certains cryptosystèmes considèrent le problème du logarithme discret dans des groupes construits sur des courbes elliptiques ou encore sur le groupe multiplicatif $\mathbb{F}_{p^f}^*$. Il est souvent utile de considérer cette version généralisée du problème car même si $\mathbb{F}_{p^f}^*$ possède $\varphi(p^f - 1)$ générateurs, il n'est pas toujours aisé d'en obtenir un.

Si $G = \mathbb{Z}_p^*$ où p est un grand nombre premier, alors $\mathbb{Z}_p^*$ est cyclique. Si on se donne un générateur γ et un élément $x \in \mathbb{Z}_p^*$, le calcul du logarithme discret est conjecturé être difficile. Une technique basique pour le calculer serait simplement d'énumérer les puissances de γ jusqu'à retrouver x. Ceci est déraisonnable dans le cas d'un p grand. Ainsi, on se retrouve dans une situation semblable à celle du RSA. L'exponentiation $x = \gamma^a \mod p$ est facile à calculer si on se donne γ et a. Par contre retrouver a à partir de γ et x est considéré comme difficile. Nous avons donc les bases d'une nouvelle fonction à sens unique.

Tout comme pour la factorisation des grands nombres, il existe ici des algorithmes de recherche du logarithme discret (citons par exemple : l'algorithme "baby-step giant-step" de Shanks, la ρ-méthode de Pollard, l'algorithme de Pohlig-Hellman, le calcul d'indices,...). Cependant aucun algorithme connu à ce jour ne donne de résultats satisfaisant pour des nombres premiers p arbitraires suffisamment grands. Les cryptosystèmes construits sur ce problème sont dès lors considérés comme sûr. Les complexités des algorithmes de factorisation de grands nombres et de recherche de logarithme discret sont fort proches.

Remarque III.11.4. Si $G = (\mathbb{Z}_p^*, \cdot)$, alors $\mathbb{Z}_p^*$ est cyclique d'ordre $p-1$ donc isomorphe au groupe additif $(\mathbb{Z}_{p-1}, +)$. Il existe une bijection

$$\psi : (\mathbb{Z}_p^*, \cdot) \to (\mathbb{Z}_{p-1}, +)$$

telle que

$$\psi(xy \mod p) = \psi(x) + \psi(y) \mod p-1.$$

De là, on en tire que

$$\psi(\gamma^a \mod p) = a\,\psi(\gamma) \mod p-1.$$

Donc, il vient

$$\begin{aligned} x \equiv \gamma^a \mod p &\Leftrightarrow \psi(x) \equiv a\,\psi(\gamma) \mod p-1 \\ &\Leftrightarrow \operatorname{dlog}_\gamma x = a \equiv \psi(x)(\psi(\gamma))^{-1} \mod p-1. \end{aligned}$$

Ainsi, si on dispose d'une méthode efficace pour calculer cet isomorphisme ψ, on obtient alors un algorithme efficace pour calculer le logarithme discret dans $\mathbb{Z}_p^*$ car les calculs dans $(\mathbb{Z}_{p-1}, +)$ sont simples à effectuer. Cependant, on ne connaît pas de méthode générale pour déterminer ψ pour un nombre premier arbitraire p. Ainsi, la détermination de ψ est aussi difficile que la détermination du logarithme discret.

Si on applique cette méthode à un groupe G quelconque et si pour ce groupe, l'isomorphisme est facile à obtenir, alors il vaut mieux ne pas utiliser un tel groupe pour construire un cryptosystème, puisque dans ce cas, le problème du logarithme discret sera considéré comme facile.

Néanmoins, signalons que pour des groupes construits sur des courbes elliptiques ou encore sur le groupe multiplicatif $\mathbb{F}_{p^f}^*$, on ne dispose pas de méthode générale de recherche de ψ.

12. Protocole d'échange des clés de Diffie-Hellman

Si on suppose le problème du logarithme discret difficile, alors on dispose d'un protocole d'échange de clés ne recourant pas à un canal de communication sûr.

Bob et Alice choisissent un grand nombre premier p et une racine primitive γ modulo p. Ces deux nombres peuvent être publiés (ou être espionnés

par Oscar). Alice choisit un exposant a qu'elle conserve soigneusement secret et elle envoie alors à Bob

$$A = \gamma^a \mod p.$$

Bob fait de même. Il choisit un exposant b et envoie à Alice

$$B = \gamma^b \mod p.$$

Alice (connaissant a) peut calculer

$$B^a = \gamma^{ab} \mod p$$

et de même, Bob (connaissant b) peut lui aussi calculer

$$A^b = \gamma^{ab} \mod p.$$

Cette valeur commune leur sert à présent de clé secrète commune.

Si l'opposant Oscar espionnait les échanges entre Alice et Bob, alors il a sa disposition les éléments suivants :

$$p,\ \gamma, A \text{ et } B.$$

Si le problème du logarithme discret est difficile, ne connaissant ni a ni b, il n'est pas en mesure de retrouver la clé secrète $B^a = A^b \mod p$.

Remarque III.12.1. Considérons l'attaque du "man in the middle". Si Oscar a le moyen d'intercepter les messages d'Alice et de Bob et par la même occasion, d'usurper leur identité, il est alors en mesure d'obtenir les messages échangés par ceux-ci et de les altérer à loisir. Avec une telle configuration et

FIGURE III.2. Attaque du "man in the middle".

en utilisant le protocole présenté ci-dessus, Alice calcule A et croit l'envoyer à Bob. C'est Oscar qui reçoit en fait A. Oscar se faisant passer pour Bob, choisit o, calcule

$$O = \gamma^o \mod p$$

et l'envoie à Alice. Ainsi, $\gamma^{ao} \mod p$ sert de clé secrète aux échanges entre Alice et Oscar. De plus, Alice pense que cette clé sert à communiquer entre elle et Bob. De la même façon, Bob calcule B et l'envoie à Oscar pensant l'envoyer à Alice. Cette fois, $\gamma^{bo} \mod p$ sert de clé entre Bob et Oscar. Ainsi, Oscar servant d'intermédiaire peut à sa guise modifier les messages entre Alice et Bob.

Pour se prémunir d'une telle attaque, il est dès lors nécessaire de recourir à un procédé de signature.

13. Cryptosystème d'ElGamal

Ce cryptosystème est encore basé sur la difficulté à résoudre le problème du logarithme discret. Nous allons l'envisager dans $\mathbb{Z}_p^*$ mais il s'adapte aisément à d'autres groupes (comme $\mathbb{F}_{p^f}^*$ ou encore, les groupes sur les courbes elliptiques). Pour assurer la sécurité du cryptosystème, il est conseillé de prendre p supérieur à 2^{768} (il faudrait bien sûr également ne pas considérer des nombres premiers particuliers pour lesquels les algorithmes connus permettraient de résoudre raisonnablement le problème).

Décrivons ce cryptosystème. On choisit tout d'abord un grand nombre premier p (en utilisant par exemple, le test de Fermat ou celui de Miller-Rabin) et un élément $\gamma \in \mathbb{Z}_p^*$. Il serait préférable que γ soit une racine primitive modulo p, mais cela n'est pas nécessaire (cf. remarque III.11.3).

Remarque III.13.1. Dans $\mathbb{F}_p^*$, le nombre de générateurs est égal à $\varphi(p-1)$ (cf. théorème I.6.20). On peut montrer[24] que pour tout $n \geq 5$, on a

$$\varphi(n) \geq \frac{n}{\log\log n}.$$

Ainsi, en tirant un élément γ au hasard dans $\mathbb{Z}_p^*$, on a de "bonnes chances" qu'il s'agisse d'une racine primitive puisque la proportion de tels éléments dans $\mathbb{Z}_p^*$ est d'au moins $1/\log\log(p-1)$. Comme le montre la figure III.3, cette fonction décroît lentement. A titre indicatif, $1/\log\log 2^{768} \sim 0,1593$.

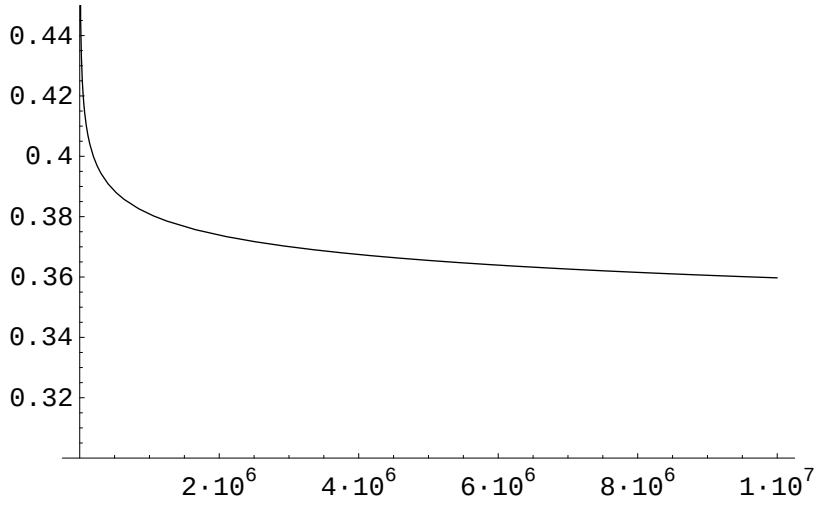


FIGURE III.3. Graphique de $1/\log\log x$ pour $x \leq 10^7$.

De plus, cette borne donne la situation la plus défavorable. En effet, si $p-1 = 2.q$ avec q un nombre premier, alors $\varphi(p-1) = q-1$ et la probabilité de tirer au hasard une racine primitive est dès lors proche de $1/2$.

[24] J. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. of Math. **6**, 69–94, (1962).

L'ensemble des textes clairs est $\mathcal{P} = \mathbb{Z}_p$ (on emploie, si nécessaire, des conventions de codage). Bob choisit aléatoirement un exposant $0 < d < p-1$ qu'il garde soigneusement secret et il calcule

$$e = \gamma^d \mod p.$$

Bob publie

$$k = (p, \gamma, e).$$

On appelle parfois e la clé de Diffie-Hellman de Bob. Si Alice veut envoyer un message x à Bob, elle choisit un nombre aléatoire $0 < b < p-1$ et envoie à Bob le couple

$$(\gamma^b \mod p,\ e^b x \mod p).$$

Remarquons dès à présent que $e^b = (\gamma^d)^b = (\gamma^b)^d$.

Pour le déchiffrement, Bob reçoit le couple ci-dessus et doit retrouver x. Pour éviter de calculer $(e^b)^{-1} \mod p$ (ce qui, par ailleurs, est supposé difficile pour Bob puisqu'il lui faudrait calculer le logarithme discret $\mathrm{dlog}_\gamma\, \gamma^b$ pour retrouver l'exposant b), Bob connaissant d, connaît aussi $p-1-d$ et il lui suffit alors de calculer

$$(\gamma^b)^{p-1-d} e^b x \mod p$$

pour retrouver x. En effet,

$$(\gamma^b)^{p-1-d} e^b x \equiv (\gamma^{p-1})^b (\gamma^b)^{-d} e^b x \equiv (\gamma^{p-1})^b (\gamma^b)^{-d} (\gamma^b)^d x \equiv x \mod p.$$

Que γ soit ou non une racine primitive modulo p, on a toujours $\gamma^{p-1} \equiv 1 \mod p$ car l'ordre d'un élément de $\mathbb{Z}_p^*$ divisant l'ordre du groupe, $p-1$ est un multiple de l'ordre de γ.

Remarque III.13.2. Les calculs nécessaires à ce cryptosystème sont du même type que ceux envisagés dans le RSA; néanmoins, le RSA est bien plus lent. Il s'agit simplement d'exponentiations modulaires. Le déchiffrement nécéssite une exponentiation et le chiffrement en nécéssite deux. Cependant, les calculs de $\gamma^b \mod p$ et $e^b \mod p$ peuvent être réalisés une fois pour toutes par Alice (elle choisit un seul b pour tous ces textes clairs x) et donc être supposés précalculés. Par conséquent, le chiffrement d'ElGamal ne nécéssite en fin de compte qu'une multiplication modulo p ce qui est de loin bien plus efficace que le RSA.

Exemple III.13.3. Nous utilisons une fois encore Mathematica. Construisons un cryptosystème comme suit.

```
:> p=Prime[123456789]
Out[]= 2543568463
:> gamma=Prime[12345678]
Out[]= 224284387
:> d=12345678;
:> e=PowerMod[gamma,d,p]
Out[]= 831108609
```

Ainsi, Bob publie

$$(2543568463,\ 224284387,\ 831108609).$$

Supposons qu'Alice désire envoyer le texte suivant.

```
:> texteclair = "une douleur foudroyante lui traversa la
tete,une douleur comme il n'en avait encore jamais ressenti.
c'etait comme si sa cicatrice avait soudain pris feu."
```

Nous utilisons la même convention que dans la mise en pratique du RSA. Ici, on a

```
:> N[Log[32,p]]
Out[]= 6.24884
```

On utilisera donc des blocs de 6 lettres consécutives comme unité de base ($32^6 < p < 32^7$). Ainsi, pour coder le texte clair, il vient (en ajoutant éventuellement des zéros pour obtenir un texte de longueur divisible par 6),

```
:> codetxclair = ajout[code[texteclair], 6]
Out=[] {21, 14, 5, 0, 4, 15, 21, 12, 5, 21, 18, 0, 6, 15, ...
         ..., 9, 14, 0, 16, 18, 9, 19, 0, 6, 5, 21, 28, 0, 0}
```

En remplaçant six éléments consécutifs de $\mathbb{Z}_{32}$ par l'entier correspondant, on trouve

```
:> liste=codebloc[codetxclair,6]
Out[]=   {719487119, 717411904, 217748047, 840388768, 424968850,
   56805985, 12616325, 677238213, 4707717, 723521005, 441460096,
  500348929, 739561477, 473417888, 337020211, 19058277,
  491057155, 978978100, 3650981, 20218465, 3443764, 613520385,
  739561491, 525468974, 17376864, 207286272}
```

Comme toujours, on peut vérifier

```
:> {21, 14, 5, 0, 4, 15}.Table[32^(5-i),{i,0,5}]
```

que

$$719487119 = 21.32^5 + 14.32^4 + 5.32^3 + 0.32^2 + 4.32 + 15.$$

Alice choisit à présent un nombre b et calcule une fois pour toutes γ^b et e^b modulo p,

```
:> b = Random[Integer, {1, p - 1}]
Out[]= 2077626273
:> PowerMod[gamma,b,p]
Out[]= 2174065976
:> temp=PowerMod[e,b,p]
Out[]= 401303819
```

Elle est à présent en mesure de chiffrer son texte :

```
:> codetxchiffre = Mod[temp*liste, p]
Out[]= {1224703372, 1813996580, 879587936, 965469907,
   1572901588, 1078313219, 1291506749, 397171217, 2052820288,
   1630733064, 162334271, 1346975257, 1481548401, 31283547,
```

```
452298537, 2531435220, 2538016017, 2419180759, 1225202253,
373714894, 1135501389, 1561257229, 2012664941, 1607195455,
371515150, 1134385436}
```

Elle envoie alors à Bob, en plus du texte chiffré, la valeur

$$\gamma^b \mod p = 2174065976.$$

Pour décoder le texte chiffré, tout comme pour le RSA, on considère des blocs de longueur 7. En effet, les nombres $e^b x \mod p$ calculés sont inférieurs à p, mais puisque $32^6 < p < 32^7$, ils peuvent être supérieurs à 32^6. Ainsi, on obtient

```
:> decodebloc[codetxchiffre,7]
Out[]= "ado:?llava:yad zfz.s  .xwyvsan.advta dkphcafouua' kz
   xvpqa'ewcj apsf xh dzzaq?ahdrmpyald'hsq  'zvj, mokayibkne
   hvtbktnchqbhccqfwadpnfrm kdl,:naaz.xbmanp'yhma,?mucmao.wv
   y? kbiwxnaayzvh."
```

Pour que Bob puisse déchiffrer ce message, partant de la liste `codetxchiffre`, il calcule d'abord $(\gamma^b)^{p-1-d}$ puis il ne lui reste plus qu'à effectuer des multiplications modulo p :

```
:> temp = PowerMod[2174065976, p-1-d, p]
Out[]= 438045370
:> Mod[temp*codetxchiffre, p]
Out[]= {719487119, 717411904, 217748047, 840388768, 424968850,
  56805985, 12616325, 677238213, 4707717, 723521005, 441460096,
  500348929, 739561477, 473417888, 337020211, 19058277, 491057155,
  978978100, 3650981, 20218465, 3443764, 613520385, 739561491,
  525468974, 17376864, 207286272}
```

ceci rend bien le codage du texte clair original. Pour s'en convaincre, il suffirait de calculer

```
:> decodebloc[%,6]
```

CHAPITRE IV

Suites linéaires récurrentes

1. Introduction

Dans cette section introductive, nous allons considérer le "*problème de Josephus*[1]". L'histoire, bien que douteuse, raconte que Josephus faisait partie d'un groupe de rebelles juifs. Lorsque ce groupe fut sur le point d'être capturé par les romains pendant la guerre qui les opposait, les membres de ce groupe décidèrent de se donner tour à tour la mort plutôt que d'être faits prisonniers par leurs ennemis. Il avait été décidé, que placés en cercle, ils exécuteraient un membre sur deux. Josephus ne partageant pas cette folie meurtrière, se devait de trouver la position à occuper pour être le dernier survivant.

Exemple IV.1.1. Si le groupe comporte dix personnes — numérotées $1, 2, \ldots, 10$ — placées en cercle et si la première personne à être exécutée porte le numéro 2, la suite des exécutions est la suivante :

$$2, 4, 6, 8, 10, 3, 7, 1, 9.$$

Ainsi, la position que doit occuper Josephus si le groupe comporte 10 personnes, est la position 5, ce que l'on notera par

$$J(10) = 5.$$

Dans Mathematica, on dispose de la fonction de Josephus. Après avoir chargé l'extension appropriée, on a

```
:> << DiscreteMath‘Combinatorica‘
:> Josephus[10,2]
Out[]= {8, 1, 6, 2, 10, 3, 7, 4, 9, 5}
```

qui représente l'inverse de la permutation obtenue en éliminant une personne sur deux, ce qui nous intéresse ici est le dernier élément de cette liste.

Notre but, dans cet exemple introductif, est d'obtenir une formule close[2] pour $J(n)$. Pour ce faire, nous allons tout d'abord distinguer deux cas, selon la parité de n.

[1] Ce problème est extrait de l'excellent livre de L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics*, Addison Wesley, Second edition (1994). On peut noter que la suite de Josephus est k-régulière, cf. J.-P. Allouche, J. Shallit, The ring of k-regular sequences II, *Theoret. Comput. Sci.* **307** (2003), 3–29.

[2] i.e., mettre $J(n)$ sous une forme ne faisant intervenir que des fonctions élémentaires bien connues.

Si n est pair, alors $n = 2m$ et après le premier tour d'exécutions, on aura supprimé les membres $2, 4, 6, \ldots, 2m$. On se ramène dès lors à un problème semblable avec m personnes numérotées cette fois

$$1, 3, \ldots, 2m - 1.$$

De là, on en tire que

$$J(2m) = 2\,J(m) - 1. \tag{6}$$

Si n est impair, alors $n = 2m + 1$ et après le premier tour d'exécutions, on aura supprimé les membres $2, 4, 6, \ldots, 2m$. Ensuite, la première personne exécutée porte le numéro 1 et on se ramène à un problème semblable avec m personnes numérotées

$$3, 5, \ldots, 2m - 1, 2m + 1.$$

On tire alors que

$$J(2m + 1) = 2\,J(m) + 1. \tag{7}$$

De plus, on a trivialement que $J(1) = 1$ et ainsi, on peut calculer, pour tout $n \geq 1$, la valeur de $J(n)$ au moyen des relations

$$\begin{cases} J(1) = 1 \\ J(2m) = 2\,J(m) - 1, \text{ si } m \geq 1 \\ J(2m + 1) = 2\,J(m) + 1, \text{ si } m \geq 1. \end{cases}$$

N'oubliez pas qu'il s'agit d'une question de vie ou de mort !

A ce stade, on dispose d'un algorithme pour calculer $J(n)$ quel que soit $n \geq 1$, mais pas encore de formule close (bien plus avantageuse). Par exemple, avec ces relations, on calcule les premières valeurs de $J(n)$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1

Au vu de ce tableau, on peut proposer la formule close suivante pour $J(n)$. Pour tout $n \geq 1$, il existe m unique tel que $2^m \leq n < 2^{m+1}$. Ainsi, $n = 2^m + r$ avec $0 \leq r < 2^m$ et nous proposons

$$\boxed{J(2^m + r) = 2r + 1.}$$

Il nous suffit de vérifier cette proposition par récurrence sur m. Pour le cas de base, si $m = 0$, alors $r = 0$ et $J(1) = 1$. Passons à la récurrence proprement dite et considérons une fois encore deux cas.

Si r est pair, $2^m + r$ est pair ($m > 0$), alors en utilisant (6) et l'hypothèse de récurrence, on a

$$J(2^m + r) = 2\,J\left(\frac{2^m + r}{2}\right) - 1 = 2\,\underbrace{J\left(2^{m-1} + \frac{r}{2}\right)}_{r+1} - 1 = 2r + 1.$$

Si r est impair, $2^m + r$ l'est aussi et on utilise cette fois (7) et l'hypothèse de récurrence pour obtenir

$$J(2^m + r) = 2\,J\left(\frac{2^m + r - 1}{2}\right) + 1 = 2\,\underbrace{J\left(2^{m-1} + \frac{r-1}{2}\right)}_{r} + 1 = 2r + 1.$$

Remarque IV.1.2. Dans la solution fournie ci-dessus, les puissances de 2 jouent un rôle particulier. En effet, si nous représentons $n = 2^m + r$ en base 2, on a

$$\rho_2(n) = x_m x_{m-1} \cdots x_0$$

où $x_m = 1$ car $2^m \leq n < 2^{m+1}$ et

$$\rho_2(r) = x_{m-1} \cdots x_0$$

car $r < 2^m$. Pour multiplier un nombre par deux en base 2, il suffit de placer un zéro à la droite de sa représentation. Ainsi, si on dispose de la représentation en base 2 de n, alors la représentation en base 2 de $J(n)$ est donnée par

$$\rho_2(J(n)) = x_{m-1} \cdots x_0 1.$$

Puisque $x_m = 1$, on peut encore l'écrire

$$\rho_2(J(n)) = x_{m-1} \cdots x_0 x_m$$

ce qui signifie que pour obtenir $J(n)$, il suffit de réaliser une permutation circulaire d'une unité vers la gauche des chiffres de la représentation en base 2 de n. Cette observation permet de montrer que pour tout $n \geq 1$, la suite $(J^k(n))_{k\in\mathbb{N}}$ décroît (on a toujours $J(n) \leq n$) puis devient stationnaire. Considérons un exemple. Soit $n = 53$ avec $\rho_2(n) = 110101$. Il vient (en prenant comme convention de représenter les nombres en base 2),

$$\begin{aligned} J(\mathbf{1}10101) &= 10101\mathbf{1} \\ J(\mathbf{1}01011) &= 1011\mathbf{1} \\ J(\mathbf{1}0111) &= 111\mathbf{1} \\ J(\mathbf{1}111) &= 111\mathbf{1} \\ &\vdots \end{aligned}$$

Il est facile de voir que si la représentation de n comprend t chiffres 1, la suite $(J^k(n))_{k\in\mathbb{N}}$ se stabilise à $2^t - 1$ car

$$\rho_2(2^t - 1) = \underbrace{11\cdots1}_{t\times}$$

et on a stabilisation lorsque k est au moins égal au nombre de "1" se trouvant à gauche du "0" le plus à droite dans $\rho_2(n)$.

Remarque IV.1.3. On peut généraliser le problème de Josephus en recherchant une formule close pour $f(n)$ lorsque ce dernier satisfait des relations

généralisées comme suit

$$\begin{cases} f(1) &= \alpha \\ f(2m) &= 2\,f(m) + \beta, \text{ si } m \geq 1 \\ f(2m+1) &= 2\,f(m) + \gamma, \text{ si } m \geq 1. \end{cases}$$

Considérons tout d'abord les premières valeurs de $f(n)$:

n	$f(n)$
1	α
2	$2\alpha + \beta$
3	$2\alpha + \gamma$
4	$4\alpha + 3\beta$
5	$4\alpha + 2\beta + \gamma$
6	$4\alpha + \beta + 2\gamma$
7	$4\alpha + 3\gamma$
8	$8\alpha + 7\beta$
9	$8\alpha + 6\beta + \gamma$
$\vdots$	

Au vu des premières valeurs, si on exprime $f(n)$ sous la forme générale

$$f(n) = A(n)\,\alpha + B(n)\,\beta + C(n)\,\gamma$$

et si $n = 2^m + r$ avec $0 \leq r < 2^m$, alors on peut émettre l'hypothèse que

$$A(n) = 2^m, \quad B(n) = 2^m - r - 1, \quad \text{et} \quad C(n) = r.$$

Tout comme précédemment, on peut vérifier cette dernière conjecture par récurrence. Nous proposons ici une autre approche pour déterminer les fonctions A, B, C. La construction d'un "*répertoire*" s'avère dans bien des cas plus simple et plus rapide.

Si on considère le cas particulier $\alpha = 1$ et $\beta = \gamma = 0$, on obtient par une récurrence immédiate que $A(2^m + r) = 2^m$.

Maintenant, utilisons la définition de $f(n)$ donnée ci-dessus et recherchons s'il existe des valeurs de α, β et γ pouvant définir une fonction particulièrement simple comme par exemple, la fonction constante $f(n) = 1$. Il vient

$$\begin{cases} 1 = f(1) = \alpha \\ 1 = f(2m) = 2\,f(m) + \beta = 2 + \beta, \text{ si } m \geq 1 \\ 1 = f(2m+1) = 2\,f(m) + \gamma = 2 + \gamma, \text{ si } m \geq 1 \end{cases}$$

et on en tire $\alpha = 1$, $\beta = \gamma = -1$. Un tel choix de constantes définit donc la fonction $f(n) = 1$. Autrement dit, on a

$$1 = A(n) - B(n) - C(n).$$

On recommence la procédure décrite ci-dessus pour voir s'il existe des valeurs de α, β et γ pouvant définir la fonction $f(n) = n$. On a

$$\begin{cases} 1 = f(1) = \alpha \\ 2m = f(2m) = 2\,f(m) + \beta = 2m + \beta, \text{ si } m \geq 1 \\ 2m+1 = f(2m+1) = 2\,f(m) + \gamma = 2m + \gamma, \text{ si } m \geq 1 \end{cases}$$

et on en tire $\alpha = \gamma = 1$ et $\beta = 0$, c'est-à-dire

$$n = A(n) + C(n).$$

En regroupant l'ensemble des informations que nous avons obtenues, il vient

$$\begin{cases} A(n) &= 2^m \quad \text{, si } n = 2^m + r \text{ avec } 0 \leq r < 2^m \\ A(n) - B(n) - C(n) &= 1 \\ A(n) + C(n) &= n. \end{cases}$$

De là, on vérifie aisément que notre conjecture s'avère être la bonne.

Tout au long de ce chapitre, nous allons essayer de développer des outils permettant d'obtenir des formes closes pour le n-ième terme d'une suite satisfaisant une relation de récurrence linéaire (à coefficients constants). Précisons ce que l'on entend par suite linéaire récurrente.

2. Définitions et premières propriétés

Sauf mention explicite, on se place sur un anneau commutatif $(A, +, \cdot)$. On dénote par $A^{\mathbb{N}}$ l'ensemble des suites sur A. En définissant terme à terme la somme de deux suites et le produit d'une suite par un élément de A, $A^{\mathbb{N}}$ jouit trivialement d'une structure de A-module.

Définition IV.2.1. Une suite $(x_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ est dite *linéaire récurrente homogène* si elle satisfait, pour tout $n \geq 0$, une *relation de récurrence linéaire homogène* (à coefficients constants) de la forme

$$x_{n+k} = a_{k-1}\,x_{n+k-1} + \cdots + a_0\,x_n \tag{8}$$

avec $a_{k-1}, \ldots, a_0 \in A$. On dit que k est le *degré* ou l'*ordre* de la relation. La relation de récurrence linéaire est parfois notée

$$x_{n+k} - a_{k-1}\,x_{n+k-1} - \cdots - a_0\,x_n = 0.$$

On emploie aussi les termes *équation de récurrence linéaire* et *solution* pour désigner respectivement la relation de récurrence et une suite la satisfaisant.

Exemple IV.2.2 (Suite de Fibonacci). Soit la relation de récurrence linéaire[3]

$$x_{n+2} = x_{n+1} + x_n, \ \forall n \geq 0.$$

Son polynôme caractéristique est

$$X^2 - X - 1$$

[3]Par exemple, E. Zeckendorf s'est intéressé à la suite de Fibonacci : Les suites linéaires récurrentes à 2 termes, *Bulletin de la Société Royale des Sciences de Liège* **25** (1956), 574–584.

et pour les conditions initiales $x_0 = 1$, $x_1 = 2$, on trouve la suite bien connue

$$(F_n)_{n\in\mathbb{N}} = 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots .$$

Pour d'autres conditions initiales, par exemple $x_0 = 2$ et $x_1 = 4$, on obtient une autre suite

$$2, 4, 6, 10, 16, 26, 42, 68, 110, 178, \ldots .$$

Remarque IV.2.3. Si, dans (8), il existe $\ell \geq 1$ tel que $a_0 = \cdots = a_{\ell-1} = 0$ et $a_\ell \neq 0$, alors, bien que la suite satisfasse par définition une relation d'ordre k, on remarque qu'elle satisfait *ultimement* (c'est-à-dire pour tout n *suffisamment grand*) une relation d'ordre $k - \ell$. Par exemple, la suite $(x_n)_{n\geq 0} = 100, 200, 1, 1, 2, 3, 5, 8, \ldots$ satisfait, pour tout $n \geq 0$, la récurrence d'ordre 4, $x_{n+4} = x_{n+3} + x_{n+2} + 0x_{n+1} + 0x_n$. Mais, ultimement, c'est-à-dire pour tout $n > 1$, elle satisfait la relation d'ordre 2, $x_{n+2} = x_{n+1} + x_n$.

Autrement dit, la suite translatée $1, 1, 2, 3, 5, 8, \ldots$ satisfait une relation d'ordre 2, mais la suite initiale $100, 200, 1, 1, 2, 3, 5, 8, \ldots$ satisfait quant à elle une relation d'ordre 4. De plus, on remarque que cette dernière suite ne satisfait aucune relation d'ordre 3 (ni d'ordre 2). En effet, si, pour tout $n \geq 0$, $x_{n+3} = ax_{n+2} + bx_{n+1} + cx_n$, alors

$$\begin{cases} 1 &= a + 200b + 100c \\ 2 &= a + b + 200c \\ 3 &= 2a + b + c \\ 5 &= 3a + 2b + c \end{cases}$$

et ce système ne possède aucune solution.

Ainsi, quitte à considérer un translaté $(x_{n+k})_{n\geq 0}$ de la suite initiale, on pourra toujours supposer, si nécessaire, $a_0 \neq 0$.

Remarque IV.2.4. L'ensemble des suites vérifiant pour tout $n \geq 0$

$$x_{n+k} = a_{k-1}\, x_{n+k-1} + \cdots + a_0\, x_n$$

est un A-sous-module de $A^{\mathbb{N}}$ isomorphe à A^k. En effet, à tout k-uple $(x_0, \ldots, x_{k-1})$ de *conditions initiales* correspond une suite linéaire récurrente satisfaisant la relation (8) et réciproquement. De plus, si $\mathbf{x} = (x_n)_{n\in\mathbb{N}}$ et $\mathbf{y} = (y_n)_{n\in\mathbb{N}}$ satisfont (8), alors il en est de même pour $\mathbf{x}+\mathbf{y} = (x_n + y_n)_{n\in\mathbb{N}}$ et $a.\mathbf{x} = (a\, x_n)_{n\in\mathbb{N}}$, $a \in A$.

Définition IV.2.5. A l'équation (8), on associe le polynôme de $A[X]$

$$\chi(X) = X^k - a_{k-1}\, X^{k-1} - \cdots - a_1\, X - a_0.$$

Ce polynôme de degré k est le *polynôme caractéristique de la relation de récurrence*. On rencontrera aussi le *polynôme réciproque de la relation de récurrence* définit par

$$X^k.\chi(1/X) = 1 - a_{k-1}\, X - \cdots - a_1\, X^{k-1} - a_0 X^k.$$

Définition IV.2.6. Une suite $(x_n)_{n\in\mathbb{N}}$ est dite *linéaire récurrente non homogène* si elle satisfait une relation de récurrence linéaire non homogène (à coefficients constants) de la forme

$$x_{n+k} = a_{k-1}\, x_{n+k-1} + \cdots + a_0\, x_n + b \tag{9}$$

avec $a_{k-1}, \ldots, a_0, b \in A$ et $b \neq 0$. La relation de récurrence *homogène associée* est simplement

$$x_{n+k} = a_{k-1}\, x_{n+k-1} + \cdots + a_0\, x_n.$$

Remarque IV.2.7. Si $\mathbf{x} = (x_n)_{n\in\mathbb{N}}$ satisfait (9) et si $\mathbf{y} = (y_n)_{n\in\mathbb{N}}$ satisfait la relation homogène associée, alors $\mathbf{x} + \mathbf{y}$ satisfait encore (9). Réciproquement, si $\mathbf{z} = (z_n)_{n\in\mathbb{N}}$ satisfait (9), alors $\mathbf{x} - \mathbf{z}$ satisfait l'équation homogène associée. De là, on en conclut que l'ensemble des solutions de (9) s'obtient en ajoutant au A-sous-module des solutions de l'équation homogène associée une solution particulière de (9). Ainsi, cet ensemble de solutions possède une structure de variété affine[4].

Pensez à l'analogie avec les équations différentielles linéaires à coefficients constants

Remarque IV.2.8. La suite nulle $\mathbf{0} = (0)_{n\in\mathbb{N}}$ est solution de toute équation de récurrence linéaire homogène et n'est solution d'aucune équation non homogène.

Nous allons nous concentrer principalement sur des équations linéaires récurrentes homogènes.

Définition IV.2.9. A l'équation (8), on associe la *matrice compagnon* de la récurrence définie par

$$\mathcal{M} = \begin{pmatrix} a_{k-1} & a_{k-2} & \cdots & \cdots & a_0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

Il est clair que si $(x_n)_{n\in\mathbb{N}}$ est solution de (8), alors

$$\begin{pmatrix} x_{n+k} \\ x_{n+k-1} \\ \vdots \\ x_{n+1} \end{pmatrix} = \mathcal{M} \begin{pmatrix} x_{n+k-1} \\ x_{n+k-2} \\ \vdots \\ x_n \end{pmatrix}$$

et en particulier, pour tout $n \geq 0$,

$$\begin{pmatrix} x_{n+k-1} \\ x_{n+k-2} \\ \vdots \\ x_n \end{pmatrix} = \mathcal{M}^n \begin{pmatrix} x_{k-1} \\ x_{k-2} \\ \vdots \\ x_0 \end{pmatrix}.$$

[4]Une variété affine est le translaté d'un sous-vectoriel. Nous admettons l'analogie dans le cas plus général de la translation d'un sous-module.

Exemple IV.2.10. Poursuivons l'exemple IV.2.2. La méthode décrite ici est en fait tout à fait générale. Pour cette suite, la matrice compagnon est donnée par

$$\mathcal{M} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ainsi,

$$\begin{pmatrix} x_{n+1} \\ x_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} x_1 \\ x_0 \end{pmatrix}.$$

Si $\mathcal{M}$ n'est pas diagonalisable, on a alors recours à la forme de Jordan.

Une formule close pour le terme général x_n peut s'obtenir en diagonalisant, si possible, la matrice compagnon. En posant $\tau = \frac{1+\sqrt{5}}{2}$ et $\tau' = \frac{1-\sqrt{5}}{2}$, il vient

$$S = \begin{pmatrix} \tau' & \tau \\ 1 & 1 \end{pmatrix} \text{ et } S^{-1}\mathcal{M}S = \begin{pmatrix} \tau' & 0 \\ 0 & \tau \end{pmatrix}.$$

Ainsi,

$$\begin{aligned} \mathcal{M}^n &= S \begin{pmatrix} \tau'^n & 0 \\ 0 & \tau^n \end{pmatrix} S^{-1} = \begin{pmatrix} \tau' & \tau \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \tau'^n & 0 \\ 0 & \tau^n \end{pmatrix} \frac{\sqrt{5}}{5} \begin{pmatrix} -1 & \tau \\ 1 & -\tau' \end{pmatrix} \\ &= \frac{\sqrt{5}}{5} \begin{pmatrix} \tau^{n+1} - \tau'^{n+1} & \tau^n - \tau'^n \\ \tau^n - \tau'^n & \tau\,\tau'^n - \tau'\,\tau^n \end{pmatrix}. \end{aligned}$$

De là, on obtient, pour tout $n \geq 0$,

$$x_n = x_1 \frac{\sqrt{5}}{5}(\tau^n - \tau'^n) + x_0 \frac{\sqrt{5}}{5}(\tau\tau'^n - \tau'\tau^n)$$

et en particulier, pour la suite de Fibonacci dont les conditions initiales sont $x_0 = 1$ et $x_1 = 2$,

$$F_n = \frac{\sqrt{5}}{5}(2\tau^n - 2\tau'^n + \tau\,\tau'^n - \tau'\,\tau^n) = \underbrace{\frac{\sqrt{5}}{5}(2-\tau')}_{\frac{3\sqrt{5}+5}{10}}\tau^n + \underbrace{\frac{\sqrt{5}}{5}(\tau-2)}_{\frac{5-3\sqrt{5}}{10}}\tau'^n.$$

3. Structure des solutions sur un anneau commutatif

Dans cette section, on désire obtenir la forme générale des solutions d'une équation linéaire récurrente homogène à coefficients dans un anneau. Les résultats obtenus concernent tout d'abord un anneau commutatif intègre quelconque et sont ensuite particularisés au cas des champs de nombres réels et complexes.

On supposera se placer sur une extension convenable de l'anneau $(A, +, \cdot)$ dans laquelle le polynôme caractéristique

$$\chi(X) = X^k - a_{k-1}X^{k-1} - \cdots - a_1X - a_0$$

de l'équation linéaire récurrente homogène (8) se factorise complètement. (Par exemple, si A est un champ, on considèrera le corps de rupture de χ sur A). Ainsi, on peut supposer que

$$\chi(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}$$

où $\alpha_1, \ldots, \alpha_r$ sont les racines de χ de multiplicité respective $m_1, \ldots, m_r$.

Le résultat principal de cette section est le suivant.

Théorème IV.3.1. *Si* $\chi(X) = \prod_{j=1}^{r}(X-\alpha_j)^{m_j}$, *alors pour tout* $j \in \{1,\dots,r\}$ *et tout* $t < m_j$, *la suite*

$$(n^t\,\alpha_j^n)_{n\in\mathbb{N}}$$

est une solution de l'équation linéaire homogène (8).

Avant de démontrer ce résultat, quelques compléments sur les racines d'un polynôme sont nécessaires. Rappelons qu'un élément α est racine de multiplicité m d'un polynôme P si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne le divise pas (cf. définition I.5.4).

Le corollaire I.5.13 applicable à un champ $\mathbb{K}$ de caractéristique nulle n'est pas valable sur un anneau quelconque A. Par exemple, le polynôme de $\mathbb{Z}_3[X]$, $X^4 - X = (X^3-1)X = (X-1)^3X$ possède 1 comme racine triple mais pourtant toutes les dérivées de ce polynôme évaluées en 1 sont nulles (en ce y compris les dérivées d'ordre 3 et plus et le résultat I.5.13 n'est donc pas vérifié ici). Il faut être quelque peu plus soigneux. En fait, on dispose des deux résultats suivants.

Lemme IV.3.2. *Soit* A *un anneau commutatif. Si* $\alpha \in A$ *est racine de multiplicité au moins* m *d'un polynôme* $P \in A[X]$, *alors* $(\mathrm{D}^iP)(\alpha) = 0$, $\forall i = 0,\dots,m-1$.

Démonstration. Par définition d'une racine de multiplicité m, on a

$$P(X) = (X-\alpha)^m\,Q(X).$$

Dès lors, pour tout $i \in \{1,\dots,m-1\}$,

$$\mathrm{D}^iP = \sum_{k=0}^{i} \mathrm{C}_i^k\ \underbrace{\mathrm{D}^k(X-\alpha)^m}_{\frac{m!}{(m-k)!}(X-\alpha)^{m-k}}\ \mathrm{D}^{i-k}Q$$

et puisque $i < m$, tous les termes de la somme contiennent au moins un facteur $X-\alpha$. De là, on en conclut que $(\mathrm{D}^iP)(\alpha) = 0$.

■

Proposition IV.3.3. *Soient* A *un anneau commutatif intègre et* m *un entier strictement inférieur à la caractéristique de* A. *La multiplicité de* α *comme racine de* $P \in A[X]$ *est au moins* $m+1$ *si et seulement si*

$$P(\alpha) = (\mathrm{D}P)(\alpha) = \cdots = (\mathrm{D}^mP)(\alpha) = 0.$$

Démonstration. La condition est nécessaire. Cela découle directement du lemme précédent.

Pour la réciproque, on procède par récurrence sur m. Si $m = 0$, alors $P(\alpha) = 0$ et la multiplicité de α comme racine de P est au moins 1. Si le résultat est satisfait pour $m-1$, l'est-il encore pour m ? Supposons que

$$P(\alpha) = (\mathrm{D}P)(\alpha) = \cdots = (\mathrm{D}^mP)(\alpha) = 0.$$

Par hypothèse de récurrence, puisque toutes les dérivées jusqu'à l'ordre $m-1$ évaluées en α sont nulles, on en déduit que α est racine de multiplicité au moins m. Ainsi,

$$P(X) = (X-\alpha)^m Q(X)$$

et

$$\mathrm{D}^m P = \sum_{k=0}^{m} \mathrm{C}_m^k \underbrace{\mathrm{D}^k (X-\alpha)^m}_{\frac{m!}{(m-k)!}(X-\alpha)^{m-k}} \mathrm{D}^{m-k} Q.$$

Si on évalue cette dérivée en α, on obtient

$$0 = (\mathrm{D}^m P)(\alpha) = m!\, Q(\alpha).$$

Puisque A est intègre, cela entraîne que $m! = 0$ ou $Q(\alpha) = 0$. Nous utilisons à présent le fait que m est strictement inférieur à la caractéristique de A. Cela signifie que dans le développement de $m! = 1.2.\cdots .m$, tous les facteurs sont non nuls. Pour que $m!$ soit nul, il faudrait alors que $m!$ soit un multiple de la caractéristique de A. Or nous avons vu que cette caractéristique est un nombre premier, cf. la section 6.1 du premier chapitre. Par conséquent, $m! \neq 0$ et $Q(\alpha) = 0$. De là, Q est divisible par $X-\alpha$ et α est donc racine de P de multiplicité au moins $m+1$.

■

Nous pouvons à présent démontrer le théorème IV.3.1.

Démonstration. Nous devons montrer que

$$(n+k)^t \alpha_j^{n+k} = \sum_{i=0}^{k-1} a_i\, (n+i)^t \alpha_j^{n+i}.$$

Soit $s \in \mathbb{N}$. On pose[5]

$$P_s(X) = X(X-1)\cdots(X-s+1).$$

Il s'agit d'un polynôme de degré s s'annulant en $0, 1, \ldots, s-1$. Il est clair que $P_0 = 1, P_1, \ldots, P_t$ forment une base de l'ensemble des polynômes de degré au plus t. Ainsi, il existe des coefficients $c_0, \ldots, c_t$ tels que

$$(X+n)^t = \sum_{\ell=0}^{t} c_\ell\, P_\ell(X). \tag{10}$$

Par hypothèse, α_j est racine de χ de multiplicité $m_j > t$. Par le lemme IV.3.2, $(\mathrm{D}^\ell \chi)(\alpha_j) = 0$ pour tout $\ell \in \{0, \ldots, t\}$. Rappelons que

$$\chi(X) = X^k - \sum_{i=0}^{k-1} a_i\, X^i.$$

Ainsi, pour $0 \leq \ell \leq t$, on a

$$\mathrm{D}^\ell \chi = \frac{k!}{(k-\ell)!} X^{k-\ell} - \sum_{i=\ell}^{k-1} a_i\, \frac{i!}{(i-\ell)!} X^{i-\ell}.$$

[5]Remarquons que si $k \geq s$, $P_s(k) := \frac{k!}{(k-s)!}$.

Evaluons à présent cette dérivée en α_j,

$$(\mathrm{D}^\ell\chi)(\alpha_j) = 0 = P_\ell(k)\,\alpha_j^{k-\ell} - \sum_{i=\ell}^{k-1} a_i\,P_\ell(i)\,\alpha_j^{i-\ell}.$$

En multipliant cette relation par α_j^ℓ et en remarquant que $P_\ell(i) = 0$ si $0 \leq i < \ell$, on obtient

$$P_\ell(k)\,\alpha_j^k = \sum_{i=0}^{k-1} a_i\,P_\ell(i)\,\alpha_j^i.$$

En utilisant (10) et la relation ci-dessus, il vient

$$\begin{aligned}(n+k)^t\alpha_j^{n+k} &= \sum_{\ell=0}^{t} c_\ell\,P_\ell(k)\,\alpha_j^{n+k} = \sum_{\ell=0}^{t} c_\ell\,\alpha_j^n\left(P_\ell(k)\,\alpha_j^k\right)\\ &= \sum_{\ell=0}^{t} c_\ell\,\alpha_j^n \sum_{i=0}^{k-1} a_i\,P_\ell(i)\,\alpha_j^i\end{aligned}$$

$$\begin{aligned}(n+k)^t\alpha_j^{n+k} &= \sum_{i=0}^{k-1} a_i\left(\sum_{\ell=0}^{t} c_\ell\,P_\ell(i)\right)\alpha_j^{n+i}\\ &= \sum_{i=0}^{k-1} a_i\,(n+i)^t\alpha_j^{n+i}.\end{aligned}$$

■

Remarque IV.3.4. Le théorème IV.3.1 nous donne des solutions de (8). Si $\chi(X) = \prod_{j=1}^{r}(X-\alpha_j)^{m_j}$, alors

$$\left\{\begin{array}{l}(\alpha_1^n)_{n\in\mathbb{N}}, (n\,\alpha_1^n)_{n\in\mathbb{N}}, \ldots, (n^{m_1-1}\,\alpha_1^n)_{n\in\mathbb{N}},\\ (\alpha_2^n)_{n\in\mathbb{N}}, (n\,\alpha_2^n)_{n\in\mathbb{N}}, \ldots, (n^{m_2-1}\alpha_2^n)_{n\in\mathbb{N}},\\ \qquad\qquad\vdots\\ (\alpha_r^n)_{n\in\mathbb{N}}, (n\,\alpha_r^n)_{n\in\mathbb{N}}, \ldots, (n^{m_r-1}\,\alpha_r^n)_{n\in\mathbb{N}}\end{array}\right.$$

sont $m_1 + m_2 + \cdots + m_r = k$ solutions[6] de (8). Il serait dès lors légitime d'espérer que ces éléments forment une base du A-sous-module de $A^{\mathbb{N}}$ de dimension k des solutions de (8). Il nous faut donc répondre à une telle question.

Remarque IV.3.5. Puisque l'ensemble des solutions de (8) est un A-sous-module, il est clair que la suite $(s_n)_{n\in\mathbb{N}}$ telle que

Principe de superposition

$$s_n = \sum_{i=1}^{r} T_i(n)\,\alpha_i^n \tag{11}$$

où T_i est un polynôme de degré strictement inférieur à m_i, est encore solution de (8).

[6]Puisque χ se factorise complètement, la somme des multiplicités est égale au degré du polynôme caractéristique de la récurrence.

Nous nous étions déjà convaincus lors de l'étude du chiffrement de Hill (proposition II.3.4) que les règles du calcul matriciel sur $\mathbb{R}$ sont encore, à quelques adaptations près, d'application sur un anneau quelconque. En particulier, rappelons qu'une matrice carrée $B \in A_n^n$ est inversible si et seulement si son déterminant est un élément inversible de A.

Théorème IV.3.6. *Soit $\mathcal{M} = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$ une matrice de A_n^n où A est un anneau commutatif intègre. Les conditions suivantes sont équivalentes :*

i) *les colonnes $C_1, \ldots, C_n$ de $\mathcal{M}$ engendrent A^n,*
ii) *les colonnes $C_1, \ldots, C_n$ de $\mathcal{M}$ forment une base de A^n,*
iii) *la matrice $\mathcal{M}$ est inversible.*

Si de plus A est fini, ces conditions sont encore équivalentes à

iv) *les colonnes $C_1, \ldots, C_n$ de $\mathcal{M}$ sont linéairement indépendantes.*

Démonstration. Il est clair que ii) entraîne i).

Montrons que iii) entraîne ii). Si $\mathcal{M}$ est inversible, il existe $\mathcal{N}$ tel que $\mathcal{M}\mathcal{N} = I$, autrement dit, pour tous $i, j \in \{1, \ldots, n\}$,

$$\sum_{k=1}^{n} [C_k]_i \, \mathcal{N}_{k,j} = \delta_{i,j} \text{ ou encore, } \sum_{k=1}^{n} \mathcal{N}_{k,j} \, [C_k]_i = [e_j]_i.$$

Par conséquent,

$$\sum_{k=1}^{n} \mathcal{N}_{k,j} \, C_k = e_j$$

et les vecteurs unitaires $e_1, \ldots, e_n$ engendrent A^n donc $C_1, \ldots, C_n$ aussi. Il faut encore montrer que les colonnes de $\mathcal{M}$ sont linéairement indépendantes. Supposons que[7]

$$\sum_{i=1}^{n} \lambda_i \, C_i = 0, \quad \lambda_i \in A.$$

Procédons par l'absurde et supposons qu'un des λ_i est non nul. Quitte à renuméroter les indices, on peut supposer $\lambda_1 \neq 0$. Ainsi,

$$\lambda_1 C_1 = -\sum_{i=2}^{n} \lambda_i \, C_i$$

et, le déterminant étant multilinéaire et alterné sur les colonnes,

$$\det \begin{pmatrix} \lambda_1 C_1 & C_2 & \cdots & C_n \end{pmatrix} = 0 = \lambda_1 \det \mathcal{M}$$

car la première colonne du déterminant est combinaison linéaire des autres. Puisque $\mathcal{M}$ est inversible, son déterminant l'est aussi et on en déduit que λ_1 est nul.

Il nous reste à montrer que i) entraîne iii). Puisque les colonnes de A engendrent A^n, les vecteurs unitaires $e_1, \ldots, e_n$ sont combinaisons linéaires

[7] Ici, A est un anneau quelconque. On ne peut donc pas supposer les λ_i inversibles.

de $C_1, \ldots, C_n$. Il existe des coefficients $\mathcal{N}_{k,j}$ tels que pour tout $j \in \{1, \ldots, n\}$,

$$\sum_{k=1}^{n} \mathcal{N}_{k,j}\, C_k = e_j.$$

De là,

$$\sum_{k=1}^{n} \mathcal{N}_{k,j}\, [C_k]_i = [e_j]_i = \delta_{i,j} \text{ ou } \sum_{k=1}^{n} \mathcal{M}_{i,k}\, \mathcal{N}_{k,j} = \delta_{i,j}.$$

Supposons à présent que A est un anneau fini. Il est clair que iii) implique iv) car nous avons déjà montré que iii) entraînait ii). Il nous reste à vérifier que iv) entraîne i). Il est clair que $\rangle C_1, \ldots, C_n \langle \subseteq A^n$. Deux combinaisons linéaires distinctes des colonnes de $\mathcal{M}$,

$$\sum_{i=1}^{n} \lambda_i\, C_i \text{ et } \sum_{i=1}^{n} \lambda'_i\, C_i \text{ , avec } (\lambda_1, \ldots, \lambda_n) \neq (\lambda'_1, \ldots, \lambda'_n),$$

donnent des éléments distincts de A^n. En effet, sinon, on en déduirait que les colonnes sont linéairement dépendantes. Ainsi, l'application

$$f : A^n \to \rangle C_1, \ldots, C_n \langle : (\lambda_1, \ldots, \lambda_n) \mapsto \sum_{i=1}^{n} \lambda_i\, C_i$$

est une bijection. Puisque A est fini[8], on en conclut que A^n et $\rangle C_1, \ldots, C_n \langle$ contiennent le même nombre d'éléments et vu l'inclusion donnée ci-dessus, les deux ensembles sont égaux.

■

On exploite l'isomorphisme entre l'ensemble A^k des conditions initiales et l'ensemble des solutions.

Au vu des remarques IV.2.4 et IV.3.4, la suite $(s_n)_{n\in\mathbb{N}}$ de terme général (11) donne la solution générale de l'équation linéaire récurrente homogène (8) si et seulement si

$$\begin{pmatrix} 1 \\ \alpha_1 \\ \alpha_1^2 \\ \vdots \\ \alpha_1^{k-1} \end{pmatrix}, \begin{pmatrix} 0 \\ \alpha_1 \\ 2\alpha_1^2 \\ \vdots \\ (k-1)\alpha_1^{k-1} \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \alpha_1 \\ 2^{m_1-1}\alpha_1^2 \\ \vdots \\ (k-1)^{m_1-1}\alpha_1^{k-1} \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ \alpha_r \\ \alpha_r^2 \\ \vdots \\ \alpha_r^{k-1} \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \alpha_r \\ 2^{m_r-1}\alpha_r^2 \\ \vdots \\ (k-1)^{m_r-1}\alpha_r^{k-1} \end{pmatrix}$$

forment une base de A^k. Au vu du théorème précédent, ceci a lieu si et seulement si

$$\det \left(n^t\, \alpha_i^n\right)_{\substack{n=0,\ldots,k-1;\\ i=1,\ldots,r;\, t=0,\ldots,m_i-1}}$$

est inversible dans A. Nous admettrons le résultat suivant.

Proposition IV.3.7. *La valeur du déterminant*

$$\det \left(n^t\, \alpha_i^n\right)_{\substack{n=0,\ldots,k-1;\\ i=1,\ldots,r;\, t=0,\ldots,m_i-1}}$$

est donnée par

$$\prod_{i=1}^{r} 0!\, 1! \cdots (m_i-1)!\ \alpha_i^{m_i(m_i-1)/2} \prod_{i<j} (\alpha_i - \alpha_j)^{m_i m_j}.$$

[8] Si A est infini, on ne peut pas faire de tels raisonnements. Par exemple, $2\mathbb{N} \subset \mathbb{N}$ et $\mathbb{N}$ et $2\mathbb{N}$ sont en bijection, sans pour autant que $\mathbb{N} = 2\mathbb{N}$!

Un produit d'éléments de A étant inversible si et seulement si chaque facteur est inversible[9], on en tire le résultat suivant.

Corollaire IV.3.8. *La suite $(s_n)_{n\in\mathbb{N}}$ de terme général* (11) *donne la solution générale de l'équation linéaire récurrente homogène* (8) *si et seulement si les conditions suivantes sont simultanément satisfaites :*

i) *les nombres $1, 2, \ldots, (\sup_{1\leq i\leq r} m_i) - 1$ sont premiers avec la caractéristique de A,*
ii) *pour toute racine α_i de χ de multiplicité $m_i \geq 2$, α_i est inversible dans A,*
iii) *pour tous $i < j$, $\alpha_i - \alpha_j$ est inversible dans A.*

Démonstration. C'est immédiat.

■

Sur un champ de caractéristique nulle comme $\mathbb{R}$ ou $\mathbb{C}$, les conditions du corollaire précédent sont trivialement satisfaites (c'est en particulier pour cette raison que nous avons imposé $a_0 \neq 0$ dans (8), car sinon 0 serait racine du polynôme caractéristique). Ainsi, nous avons le résultat suivant.

Théorème IV.3.9. *Avec nos notations habituelles, si $A = \mathbb{R}$, la solution générale de l'équation linéaire récurrente homogène* (8) *est donnée par la suite $(s_n)_{n\in\mathbb{N}}$ de terme général*

$$s_n = \sum_{i=1}^{r} T_i(n)\, \alpha_i^n$$

où T_i est un polynôme de degré strictement inférieur à m_i. Les coefficients des polynômes T_i sont déterminés par les conditions initiales.

Démonstration. C'est immédiat.

■

Remarque IV.3.10. Travaillant sur le corps de rupture de χ, il se peut que certaines racines α_i soient des nombres complexes.

Exemple IV.3.11. Considérons la suite satisfaisant pour tout $n \geq 0$, l'équation linéaire récurrente suivante

$$x_{n+4} = 6x_{n+3} - 13x_{n+2} + 24x_{n+1} - 36x_n$$

avec $x_0 = 0, x_1 = 2, x_2 = 1, x_3 = 1$. Le polynôme caractéristique est donné par

$$\chi(X) = X^4 - 6X^3 + 13X^2 - 24X + 36 = (X-3)^2(X-2i)(X+2i).$$

Ainsi, la solution générale de la récurrence est de la forme

$$x_n = (c_1 n + c_2)\, 3^n + c_3\, (2i)^n + c_4(-2i)^n.$$

[9]Soient $a, b \in A$. Si a et b sont inversibles, alors $b^{-1}a^{-1}$ est l'inverse de ab. Réciproquement, si ab est inversible, alors $ab(ab)^{-1} = 1$ et a a pour inverse $b(ab)^{-1}$. De même, $(ab)^{-1}ab = 1$ et b possède $(ab)^{-1}a$ pour inverse.

On détermine c_1, c_2, c_3, c_4 grâce aux conditions initiales. On résout le système

$$\begin{cases} x_0 = 0 &= c_2 + c_3 + c_4 \\ x_1 = 2 &= 3c_1 + 3c_2 + 2ic_3 - 2ic_4 \\ x_2 = 1 &= 18c_1 + 9c_2 - 4c_3 - 4c_4 \\ x_3 = 1 &= 81c_1 + 27c_2 - 8ic_3 + 8ic_4 \end{cases}$$

pour trouver

$$c_1 = \frac{2}{13},\ c_2 = -\frac{23}{169},\ c_3 = \frac{23}{338} - \frac{329}{676}i,\ c_4 = \overline{c_3}.$$

Remarquons que

$$c_3(2i)^n + c_4(-2i)^n = c_3\,(2i)^n + \overline{c_3\,(2i)^n} = 2\,\mathfrak{Re}(c_3\,(2i)^n).$$

De là, on obtient la forme close pour tout $n \geq 0$,

$$x_n = \frac{2}{13}\,n\,3^n - \frac{23}{169}\,3^n + \frac{23}{338}\,2^{n+1}\,\cos\left(n\frac{\pi}{2}\right) - \frac{329}{676}\,2^{n+1}\,\cos\left((n+1)\frac{\pi}{2}\right).$$

Les premiers termes de la suite sont

$$0, 2, 1, 1, 41, 185, 565, 1933, 7217, 25073, 82669, 273685, 909353, 2979641, \ldots.$$

Au vu de cette section, on peut affirmer qu'une des difficultés majeures pour obtenir une forme close est de rechercher les racines du polynôme caractéristique χ de la récurrence[10]. En utilisant la matrice compagnon comme dans l'exemple IV.2.10, la difficulté est analogue (puisqu'on se ramène au polynôme caractéristique de la matrice). Pour cette raison, on a souvent recours à d'autres techniques pour rechercher une forme close pour le terme général de la solution d'une équation linéaire homogène, comme par exemple, les séries formelles.

4. Suites linéaires récurrentes et déterminants de Hankel

Dans cette section, nous considérons uniquement des suites définies sur un champ arbitraire $\mathbb{K}$.

Remarque IV.4.1. Si la $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire d'ordre k, alors la suite translatée $(x_{n+k})_{n\geq 0}$ est une combinaison linéaire des suites $(x_n)_{n\geq 0}, \ldots, (x_{n+k-1})_{n\geq 0}$.

Remarque IV.4.2. Si les suites $\mathbf{x}_0 = (x_n)_{n\geq 0}, \ldots, \mathbf{x}_k = (x_{n+k})_{n\geq 0}$ sont linéairement dépendantes (l'ensemble $\mathbb{K}^{\mathbb{N}}$ étant un $\mathbb{K}$-vectoriel), alors la suite $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire d'ordre au plus k. En effet, il existe des coefficients $\lambda_0, \ldots, \lambda_k \in \mathbb{K}$ non tous nuls tels que

$$\lambda_0\mathbf{x}_0 + \cdots + \lambda_k\mathbf{x}_k = 0.$$

Soit $i \geq 0$ le plus grand indice tel que $\lambda_i \neq 0$. Si $i = 0$, cela signifie que $(x_n)_{n\geq 0}$ est la suite nulle. Sinon, on a

$$\mathbf{x}_i = \lambda_i^{-1}\lambda_0\mathbf{x}_0 + \cdots + \lambda_i^{-1}\lambda_{i-1}\mathbf{x}_{i-1}$$

[10]Pensez à la théorie de Galois. Il n'existe de méthode générale pour rechercher les racines d'un polynôme de degré 5 ou plus.

et la suite $(x_n)_{n\geq 0}$ satisfait une relation d'ordre $i \leq k$.

Définition IV.4.3. Soit $(x_n)_{n\geq 0}$ une suite. On pose

$$D_n^{(k+1)} := \det \begin{pmatrix} x_n & x_{n+1} & \cdots & x_{n+k} \\ x_{n+1} & x_{n+2} & \cdots & x_{n+k+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n+k} & x_{n+k+1} & \cdots & x_{n+2k} \end{pmatrix}.$$

Lemme IV.4.4. *Soit $(x_n)_{n\geq 0}$ une suite. Si $D_n^{(k)} = D_n^{(k+1)} = 0$, alors $D_{n+1}^{(k)} = 0$.*

Démonstration. Considérons les vecteurs $\overrightarrow{x}_i = (x_i, \ldots, x_{i+k-1})$, $i \geq$

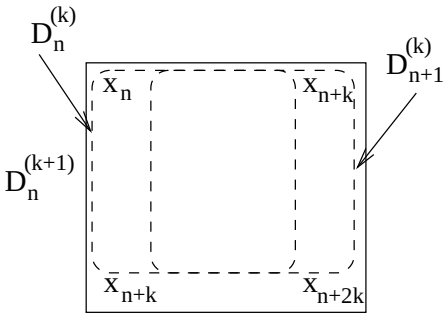


FIGURE IV.1. Les différents déterminants.

0. Par hypothèse, puisque $D_n^{(k)} = 0$, les vecteurs $\overrightarrow{x}_n, \ldots, \overrightarrow{x}_{n+k-1}$ sont linéairement dépendants. Si $\overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$ sont linéairement dépendants, alors $D_{n+1}^{(k)} = 0$ et la preuve est terminée.

Supposons donc $\overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$ linéairement indépendants. Dans ce dernier cas, $\overrightarrow{x}_n$ est combinaison linéaire[11] de $\overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$. Considérons à présent les vecteurs $\overrightarrow{x}'_i = (x_i, \ldots, x_{i+k})$, $i \geq 0$. Par hypothèse, puisque $D_n^{(k+1)} = 0$, les vecteurs $\overrightarrow{x}'_n, \ldots, \overrightarrow{x}'_{n+k}$ sont linéairement dépendants. Si $\overrightarrow{x}'_n, \ldots, \overrightarrow{x}'_{n+k-1}$ sont linéairement dépendants, alors $D_{n+1}^{(k)} = 0$ et la preuve est terminée.

Supposons donc que ces derniers vecteurs sont linéairement indépendants. Par conséquent, $\overrightarrow{x}'_{n+k}$ est combinaison linéaire de $\overrightarrow{x}'_n, \ldots, \overrightarrow{x}'_{n+k-1}$,

$$\overrightarrow{x}'_{n+k} = \sum_{j=0}^{k-1} \beta_j \overrightarrow{x}'_{n+j}.$$

Considérons l'application linéaire

$$T : (x_i, \ldots, x_{i+k-1}, x_{i+k}) \mapsto (x_i, \ldots, x_{i+k-1}).$$

[11]Par hypothèse, $\overrightarrow{x}_n, \ldots, \overrightarrow{x}_{n+k-1}$ sont linéairement dépendants donc $\overrightarrow{x}_n, \overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$ aussi. Mais $\overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$ sont linéairement indépendants. Donc le vecteur ajouté $\overrightarrow{x}_n$ est combinaison linéaire des autres.

$$\overrightarrow{x}_{n+k} = T(\overrightarrow{x}'_{n+k}) = \sum_{j=0}^{k-1} \beta_j T(\overrightarrow{x}'_{n+j}) = \sum_{j=0}^{k-1} \beta_j \overrightarrow{x}_{n+j} = \beta_0 \overrightarrow{x}_n + \sum_{j=1}^{k-1} \beta_j \overrightarrow{x}_{n+j}.$$

Rappelons que dans la situation considérée, $\overrightarrow{x}_n$ est combinaison linéaire de $\overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$. Par conséquent, nous avons obtenu une relation linéaire liant $\overrightarrow{x}_{n+1}, \ldots, \overrightarrow{x}_{n+k}$ et donc $D_{n+1}^{(k)} = 0$.

■

Proposition IV.4.5. *Une suite $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire si et seulement si il existe $k, N \geq 0$ tels que, pour tout $n \geq N$, $D_n^{(k+1)} = 0$.*

Démonstration. Au vu des deux remarques ci-dessus, $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire d'ordre au plus k si et seulement si les suites $\mathbf{x}_0 = (x_n)_{n\geq 0}, \ldots, \mathbf{x}_k = (x_{n+k})_{n\geq 0}$ sont linéairement dépendantes. Il est clair que si $\mathbf{x}_0 = (x_n)_{n\geq 0}, \ldots, \mathbf{x}_k = (x_{n+k})_{n\geq 0}$ sont linéairement dépendants, alors $D_n^{(k+1)} = 0$ pour tout $n \geq 0$.

Supposons que k est le *plus petit* entier tel qu'il existe $N \geq 0$ satisfaisant

$$\forall n \geq N,\ D_n^{(k+1)} = 0.$$

Si $k = 0$, alors, $x_n = 0$ pour tout $n \geq N$. Dans la suite, on peut donc supposer $k \geq 1$. S'il existe $m \geq N$ tel que $D_m^{(k)} = 0$, alors $D_m^{(k)} = D_m^{(k+1)} = 0$ et par le lemme précédent, $D_{m+1}^{(k)} = 0$. On peut alors appliquer à nouveau le lemme avec $D_{m+1}^{(k)} = D_{m+1}^{(k+1)} = 0$ et donc $D_{m+2}^{(k)} = 0$, etc. On conclut que $D_n^{(k)} = 0$ pour tout $n \geq m$. Ceci contredit la minimalité de k. Par conséquent, on a

$$\forall n \geq N,\ D_n^{(k)} \neq 0.$$

Notons les lignes de $D_n^{(k+1)}$ par

$$\overrightarrow{x_i} = (x_i, \ldots, x_{i+k}).$$

Soit $n \geq N$. Par hypothèse, $D_n^{(k+1)} = 0$ et donc $\overrightarrow{x}_n, \ldots, \overrightarrow{x}_{n+k}$ sont des vecteurs linéairement dépendants. Puisque $D_n^{(k)} \neq 0$, $\overrightarrow{x}_n, \ldots, \overrightarrow{x}_{n+k-1}$ sont linéairement indépendants et donc $\overrightarrow{x}_{n+k}$ est combinaison linéaire de $\overrightarrow{x}_n, \ldots, \overrightarrow{x}_{n+k-1}$. D'où, de proche en proche, tout vecteur $\overrightarrow{x}_n$ avec $n \geq N$ est combinaison linéaire de $\overrightarrow{x}_N, \ldots, \overrightarrow{x}_{N+k-1}$: il existe $\alpha_{n,i}$ tels que

$$\overrightarrow{x}_n = \sum_{i=0}^{k-1} \alpha_{n,i}\, \overrightarrow{x}_{N+i}$$

ou encore, pour tout $n \geq N$,

$$\forall j \in \{0, \ldots, k\},\ x_{n+j} = \sum_{i=0}^{k-1} \alpha_{n,i}\, x_{N+i+j}. \tag{12}$$

Le système homogène de k équations et à $k+1$ inconnues $\lambda_0, \dots, \lambda_k$

$$\lambda_0 \begin{pmatrix} x_N \\ x_{N+1} \\ \vdots \\ x_{N+k-1} \end{pmatrix} + \lambda_1 \begin{pmatrix} x_{N+1} \\ x_{N+2} \\ \vdots \\ x_{N+k} \end{pmatrix} + \cdots + \lambda_k \begin{pmatrix} x_{N+k} \\ x_{N+k+1} \\ \vdots \\ x_{N+2k-1} \end{pmatrix} = 0$$

possède une solution non nulle $(a_0, \dots, a_k)$ car son rang est au plus k. Donc,

$$\forall n \in \{N, \dots, N+k-1\},\ a_0 x_n + a_1 x_{n+1} + \cdots + a_k x_{n+k} = 0.$$

Pour tout $n \geq N$, au vu de (12),

$$\sum_{j=0}^{k} a_j x_{n+j} = \sum_{j=0}^{k} a_j \sum_{i=0}^{k-1} \alpha_{n,i}\, x_{N+i+j} = \sum_{i=0}^{k-1} \alpha_{n,i} \underbrace{\sum_{j=0}^{k} a_j\, x_{N+i+j}}_{=0} = 0.$$

Ceci signifie que la suite $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire de degré au plus $N+k$.

■

Proposition IV.4.6. *Une suite non nulle $(x_n)_{n\geq 0} \in \mathbb{K}^{\mathbb{N}}$ satisfait une relation de récurrence linéaire à coefficients dans $\mathbb{K}$ d'ordre minimal k si et seulement si $D_0^{(k)} \neq 0$ et pour tout $n \geq k+1$, $D_0^{(n)} = 0$.*

Démonstration. Si $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire à coefficients dans $\mathbb{K}$ d'ordre k, alors il est clair que $D_0^{(n)} = 0$, pour tout $n \geq k+1$, la dernière colonne/ligne de la matrice étant combinaison linéaire des k précédentes.

Si k est l'ordre minimal de la récurrence, i.e., si la suite ne satisfait aucune relation à coefficients dans $\mathbb{K}$ d'ordre inférieur, alors les vecteurs $\overrightarrow{x}_0, \dots, \overrightarrow{x}_{k-1}$ sont linéairement indépendants où l'on a posé

$$\overrightarrow{x}_i = (x_i, \dots, x_{i+k-1}).$$

En effet, si tel n'est pas le cas, il existe des coefficients λ_i non tous nuls tels que $\lambda_0 \overrightarrow{x}_0 + \cdots + \lambda_{k-1} \overrightarrow{x}_{k-1} = 0$. Soit $\mathcal{M}$ la matrice compagnon $k \times k$ associée à la récurrence d'ordre k. Soit j, le plus grand indice tel que $\lambda_j \neq 0$. En multipliant à gauche par $\mathcal{M}^n$, il vient $\lambda_0 \mathcal{M}^n \overrightarrow{x}_0 + \cdots + \lambda_j \mathcal{M}^n \overrightarrow{x}_j = 0$ et donc

$$\forall n \geq 0,\ x_{n+j} = -\lambda_j^{-1}\lambda_{j-1} x_{n+j-1} - \cdots - \lambda_j^{-1}\lambda_0 x_n.$$

Cela signifie que la suite satisfait une relation d'ordre $j < k$ ce qui est impossible. On en conclut donc que $\overrightarrow{x}_0, \dots, \overrightarrow{x}_{k-1}$ sont linéairement indépendants et $D_0^{(k)} \neq 0$. Autrement dit, k est le plus petit entier tel que pour tout $n \geq k+1$, $D_0^{(n)} = 0$.

Pour la réciproque, puisque $D_0^{(k+1)} = D_0^{(k+2)} = 0$, le lemme IV.4.4 entraîne $D_1^{(k+1)} = 0$. De même, pour tout $n \geq k+1$, puisque $D_0^{(n)} = D_0^{(n+1)} =$

0, on obtient pour tout $n \geq k+1$, $D_1^{(n)} = 0$. Et de proche en proche,

$$\forall i \geq 0, \forall n \geq k+1,\ D_i^{(n)} = 0.$$

En particulier, pour tout $i \geq 0$, $D_i^{(k+1)} = 0$ et par la proposition précédente, la suite $(x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire. De plus, $D_0^{(k)} \neq 0$. Nous avons montré au paragraphe précédent que l'ordre minimal de la récurrence est le plus petit entier tel que pour tout $n \geq k+1$, $D_0^{(n)} = 0$. Ceci suffit.

■

Exemple IV.4.7. Reprenons l'exemple de la remarque IV.2.3 et la suite $100, 200, 1, 1, 2, 3, 5, 8, \ldots$. On a

$$\det\begin{pmatrix} 100 & 200 \\ 200 & 1 \end{pmatrix} = 39900, \quad \det\begin{pmatrix} 100 & 200 & 1 \\ 200 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix} = -79501$$

$$\det\begin{pmatrix} 100 & 200 & 1 & 1 \\ 200 & 1 & 1 & 2 \\ 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 5 \end{pmatrix} = -40000, \quad \det\begin{pmatrix} 100 & 200 & 1 & 1 & 2 \\ 200 & 1 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 5 \\ 1 & 2 & 3 & 5 & 8 \end{pmatrix} = 0.$$

Ceci montre qu'*a priori*, la suite en question peut satisfaire une relation d'ordre 4, mais aucune relation d'ordre inférieur.

5. Suites linéaires récurrentes sur un champ fini

Proposition IV.5.1. *Soient k, ℓ tels que $0 \leq \ell < k$. Soit $\mathbf{x} = (x_n)_{n\in\mathbb{N}}$ une suite du champ fini $\mathbb{F}_q$ satisfaisant une relation de récurrence linéaire*[12]

$$x_{n+k} = a_{k-1}\, x_{n+k-1} + \cdots + a_\ell\, x_{n+\ell}, \quad a_\ell \neq 0. \tag{13}$$

- *La suite est périodique à partir de ℓ, i.e., il existe une (plus petite) période $p > 0$ telle que pour tout $n \geq \ell$, $x_n = x_{n+p}$.*
- *Cette période est telle que $p \leq q^{k-\ell}$.*
- *Pour l'équation (13), la période est maximale pour les conditions initiales $x_0 = \cdots = x_{k-2} = 0$ et $x_{k-1} = 1$.*
- *Cette période maximale est égale à l'ordre de la matrice compagnon $\mathcal{M}$ dans le groupe multiplicatif $\mathrm{GL}_k(\mathbb{F}_q)$ des matrices $k \times k$ inversibles sur $\mathbb{F}_q$.*

Démonstration. Nous nous intéressons tout d'abord aux deux premiers points. Dénotons par $\overrightarrow{x_n}$ le vecteur

$$\overrightarrow{x_n} := \begin{pmatrix} x_{n+k-1} \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{F}_q^k.$$

[12] Il s'agit de l'équation (8) dans laquelle $a_0 = \cdots = a_{\ell-1} = 0$.

Ainsi, on a $\overrightarrow{x_n} = \mathcal{M}^n \overrightarrow{x_0}$, pour tout $n \geq 0$. Il est clair que parmi les $q^k + 1$ éléments

$$\overrightarrow{x_0}, \ldots, \overrightarrow{x_{q^k}},$$

au moins deux éléments $\overrightarrow{x_m}$ et $\overrightarrow{x_n}$ sont égaux ($0 \leq m < n \leq q^k$). Par conséquent,

$$\overrightarrow{x_m} = \overrightarrow{x_n} = \mathcal{M}^{n-m}\overrightarrow{x_m}.$$

On a donc périodicité de la suite à partir de x_m et la période trouvée est $n - m \leq q^k$. Il nous reste à montrer qu'on a périodicité à partir de x_ℓ. Pour ce faire, envisageons deux cas.

Premier cas : $a_0 \neq 0$. Par définition de la matrice compagnon, il est clair que $\det \mathcal{M} = a_0 \neq 0$. Puisque nous sommes sur un champ, cela signifie que $\mathcal{M}$ est inversible. De là,

$$\overrightarrow{x_m} = \mathcal{M}^m \overrightarrow{x_0} = \mathcal{M}^n \overrightarrow{x_0} = \overrightarrow{x_n}$$

d'où, en multipliant les deux membres par $\mathcal{M}^{-m}$, on obtient $\overrightarrow{x_0} = \mathcal{M}^{n-m} \overrightarrow{x_0}$ et on a donc périodicité depuis x_0.

Second cas : $a_0 = \cdots = a_{\ell-1} = 0$ et $a_\ell \neq 0$. On considère la suite $\mathbf{y} = (y_n)_{n\in\mathbb{N}}$ définie par $y_n = x_{n+\ell}$ pour tout $n \geq 0$. Il est clair que $\mathbf{y}$ satisfait encore la relation

$$y_{n-\ell+k} = \sum_{i=\ell}^{k-1} a_i \, y_{n-\ell+i}$$

qui se réécrit aussi

$$y_{n+(k-\ell)} = \sum_{i=0}^{k-\ell-1} a_{i+\ell} \, y_{n+i}.$$

On s'est donc ramené au premier cas. La suite $\mathbf{y}$ est périodique à partir de y_0 et sa période est inférieure ou égale à $q^{k-\ell}$. De là, la suite $\mathbf{x}$ a la même période et est périodique à partir de $x_\ell = y_0$.

Passons aux derniers points. Soit e l'ordre de $\mathcal{M}$ dans $\mathrm{GL}_k(\mathbb{F}_q)$, i.e., e est le plus petit entier tel que $\mathcal{M}^e = I$. En particulier,

$$\mathcal{M}^e \overrightarrow{x_0} = \overrightarrow{x_0}$$

et par conséquent, la période p de la solution est inférieure ou égale à e (et ce, quel que soit le choix de la condition initiale $\overrightarrow{x_0}$). Il nous suffit alors de prouver que la (plus petite) période correspondant aux conditions initiales $0, \ldots, 0, 1$ est supérieure ou égale à e. Vu la forme de la matrice compagnon, il existe des coefficients $\alpha_{i,j}$ ($1 \leq i < k$, $1 \leq j \leq i$) tels que, si on choisit comme conditions initiales $\overrightarrow{x_0} = e_1$, alors

$$\overrightarrow{x_1} = \mathcal{M}\overrightarrow{x_0} = e_2 + \alpha_{1,1}e_1, \ \overrightarrow{x_2} = \mathcal{M}\overrightarrow{x_1} = e_3 + \alpha_{2,2}e_2 + \alpha_{2,1}e_1, \ldots$$

$$\overrightarrow{x_{k-1}} = \mathcal{M}\overrightarrow{x_{k-2}} = e_k + \alpha_{k-1,k-1}e_{k-1} + \cdots + \alpha_{k-1,1}e_1.$$

Autrement dit, la matrice $\mathcal{A} = \begin{pmatrix} \overrightarrow{x_0} & \cdots & \overrightarrow{x_{k-1}} \end{pmatrix}$ est de la forme

$$\begin{pmatrix} 1 & \alpha_{1,1} & \alpha_{2,1} & \cdots & \alpha_{k-1,1} \\ 0 & 1 & \alpha_{2,2} & \cdots & \alpha_{k-1,2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & \alpha_{k-1,k-1} \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

et $\det \mathcal{A} = 1$. Il est clair que

$$\mathcal{M}^n \begin{pmatrix} \overrightarrow{x_0} & \cdots & \overrightarrow{x_{k-1}} \end{pmatrix} = \begin{pmatrix} \overrightarrow{x_n} & \cdots & \overrightarrow{x_{n+k-1}} \end{pmatrix}.$$

Supposons que n soit une période. Il nous suffit, pour conclure, de montrer que n est un multiple de e. Dans ce cas, par définition même d'une période, on a

$$\mathcal{M}^n \mathcal{A} = \mathcal{A}.$$

Or $\mathcal{A}$ est inversible donc

$$\mathcal{M}^n = I$$

ce qui montre que n est un multiple de e.

■

Remarque IV.5.2. Dans la proposition précédente, on peut même supposer que la période est inférieure ou égale à $q^{k-\ell} - 1$ car le k-uple $(0, \ldots, 0)$ fournirait la suite nulle et on peut donc considérer $\mathbb{F}_q^k$ privé de cet élément.

5.1. Retour sur le chiffrement par flot. On peut utiliser les suites linéaires récurrentes pour réaliser un chiffrement par flot (cf. section 3.5 du deuxième chapitre). En effet, ces suites se prètent bien aux applications informatiques car il est possible de les implémenter facilement grâce à un *registre à décalage linéaire* (*linear feedback shift register*). Expliquons le fonctionnement d'un tel registre sur un exemple.

Exemple IV.5.3. Soit l'équation linéaire récurrente sur $\mathbb{Z}_2$

$$x_{n+4} = x_{n+1} + x_n \pmod 2$$

et les conditions initiales $x_0 = x_1 = x_2 = 0$ et $x_3 = 1$. Les premiers termes de la suite sont

$$0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, \ldots$$

Ainsi, on s'aperçoit que la suite est périodique de période 15,

$$(x_n)_{n \in \mathbb{N}} = (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)^\omega.$$

Cette suite peut être produite à l'aide du registre représenté à la figure IV.2. Ce registre contient 4 cases t_1, t_2, t_3, t_4. Au départ, les cases sont initialisées avec les conditions initiales de la récurrence : $t_i \leftarrow x_{i-1}$, $i = 1, 2, 3, 4$. A chaque unité $n \in \mathbb{N}$ de temps, le contenu de t_1 est produit par le registre et constitue l'élément x_n de la suite. Le contenu des cases t_2, t_3, t_4 est déplacé d'une case vers la gauche et enfin, on effectue le calcul du terme

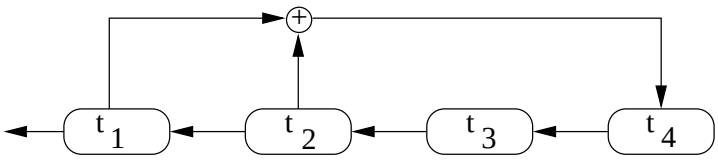


FIGURE IV.2. Registre à décalage linéaire.

suivant de la suite qui est stocké dans t_4. Toutes ces opérations sont réalisées simultanément.

n	production	t_1	t_2	t_3	t_4
	—	x_0	x_1	x_2	x_3
0	x_0	x_1	x_2	x_3	$x_4 = x_0 + x_1$
1	x_1	x_2	x_3	x_4	$x_5 = x_1 + x_2$
2	x_2	x_3	x_4	x_5	$x_6 = x_2 + x_3$
⋮	⋮				

Voici une réalisation sous Mathematica (pour les détails, se référer à l'aide en ligne). Chaque lettre de l'alphabet correspond, comme de coutûme, à un entier $x < 32$ qui est représenté en base 2 par un mot de longueur 5 (on place éventuellement des zéros de tête pour obtenir une telle représentation).

```
:> codetxt = Flatten[Map[IntegerDigits[#,2,5] &, code["bonjour"]]]
Out[]= {00010011110111001010011111010110010}

:> Length[%]
Out[]= 35

:> x0 = {0,0,0,1};
:> f[x_] := Append[x, Mod[ x[[Length[x]-3]]+x[[Length[x]-2]],2]]
:> cle = Nest[f,x0,31]
Out[]= {00010011010111100010011010111100010}

:> txtchiffre = Mod[codetxt+cle, 2]
Out[]= {00000000100000101000000101101010000}
```

Pour retrouver le texte clair, il suffit de réappliquer la clé,

```
:> Mod[txtchiffre+cle, 2]
Out[]= {00010011110111001010011111010110010}
```

Remarque IV.5.4. Nous voudrions attirer l'attention du lecteur sur le caractère "prédictible" des suites linéaires récurrentes. En effet, pour une relation linéaire récurrente d'ordre k,

$$x_{n+k} = \sum_{i=0}^{k-1} a_i \, x_{n+i},$$

il suffit à Oscar de connaître $2k+1$ termes consécutifs $x_\ell, \ldots, x_{\ell+2k}$ de la suite pour retrouver les k coefficients $a_0, \ldots, a_{k-1}$ de l'équation de récurrence que la suite satisfait. Connaissant ces coefficients, il peut alors reconstruire la suite à partir du ℓ-ième terme. En effet, pour tout $j = 1, \ldots, k$, on a

$$x_{\ell+k+j} - x_{\ell+k+j-1} = \sum_{i=0}^{k-1} a_i\, x_{\ell+j+i} - \sum_{i=0}^{k-1} a_i\, x_{\ell+j+i-1} = \sum_{i=0}^{k-1} a_i\, (x_{\ell+j+i} - x_{\ell+j+i-1}).$$

Puisque $x_\ell, \ldots, x_{\ell+2k}$ sont connus, on est en présence de k équations linéaires à k inconnues.

$$\begin{cases} x_{\ell+k+1} - x_{\ell+k} = a_0\,(x_{\ell+1} - x_\ell) + \cdots + a_{k-1}\,(x_{\ell+k} - x_{\ell+k-1}) \\ \vdots \\ x_{\ell+2k} - x_{\ell+2k-1} = a_0\,(x_{\ell+k} - x_{\ell+k-1}) + \cdots + a_i\,(x_{\ell+2k-1} - x_{\ell+2k-2}) \end{cases}$$

Cette remarque montre que les suites linéaires récurrentes ne peuvent être considérées comme des suites pseudo-aléatoires. On appelle *suite pseudo-aléatoire* toute suite qui passe avec succès toute une série de tests statistiques pour vérifier la distribution uniforme de la suite, sa non-prédictibilité, etc.

Remarque IV.5.5. Un autre générateur de suites pseudo-aléatoires peut être construit sur le logarithme discret. On se place sur $\mathbb{Z}_p^*$ avec γ, un générateur. Pour une condition initiale $x_0 \in \mathbb{Z}_p^*$, on considère la suite définie par

$$x_{n+1} = \gamma^{x_n} \mod p.$$

Enfin, on engendre la suite de bits $(z_n)_{n\in\mathbb{N}}$ par

$$z_n := \begin{cases} 1 \text{ si } x_n > p/2, \\ 0 \text{ sinon.} \end{cases}$$

Connaissant p et γ (qui peuvent être considérés comme publiques), si le problème du logarithme discret est difficile, il est alors inconcevable pour Oscar de prédire les éléments de la suite $(z_n)_{n\in\mathbb{N}}$ s'il ne connaît pas un terme de la suite $(x_n)_{n\in\mathbb{N}}$. La suite $(z_n)_{n\in\mathbb{N}}$ peut donc être utilisée comme clé dans un chiffrement par flot.

6. Séries formelles et fonctions génératrices

Dans cette section, nous nous contenterons d'étudier quelques aspects purement formels des séries génératrices. Il faut néanmoins savoir que des outils classiques d'analyse complexe peuvent se révéler très utiles pour, par exemple, obtenir des renseignements asymptotiques sur les suites étudiées. Un ouvrage très intéressant et abordable consacré entièrement aux séries et fonctions génératrices sous ses divers aspects est [**25**], voir aussi [**5**].

Définition IV.6.1. Soit A un anneau commutatif. On introduit l'anneau $A[[z]]$ des séries formelles sur A comme suit. Une *série formelle* à coefficients

dans A est simplement une suite $\mathbf{a} = (a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ que l'on notera symboliquement

$$s_{\mathbf{a}}(z) = \sum_{n=0}^{\infty} a_n\, z^n.$$

On dit que z est l'*indéterminée* de la série. Pour faire de $A[[z]]$ un anneau commutatif, on définit la *somme* de deux séries formelles par

$$\left(\sum_{n=0}^{\infty} a_n\, z^n\right) + \left(\sum_{n=0}^{\infty} b_n\, z^n\right) = \sum_{n=0}^{\infty} (a_n + b_n)\, z^n.$$

Autrement dit, aux séries formelles associées aux suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, on fait correspondre la série formelle de la suite $(a_n + b_n)_{n\in\mathbb{N}}$. On définit comme seconde opération, le *produit de Cauchy*[13]de deux séries formelles par

$$\left(\sum_{n=0}^{\infty} a_n\, z^n\right) . \left(\sum_{n=0}^{\infty} b_n\, z^n\right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j\right)\, z^n.$$

Cette opération étend naturellement l'opération de produit de deux polynômes de $A[z]$. On vérifie aisément que, muni de ces deux opérations, $A[[z]]$ jouit d'une structure d'anneau commutatif. On peut bien évidemment plonger A (resp. l'anneau des polynômes $A[z]$) dans $A[[z]]$ en identifiant $a \in A$ à la suite $(a, 0, 0, \ldots)$, i.e., à la série formelle $\sum_{n=0}^{\infty} a\, \delta_{n,0}\, z^n$ (resp. en identifiant le polynôme $a_0 + a_1 z + \cdots + a_d z^d$ à la suite $(a_0, \ldots, a_d, 0, 0, \ldots)$).

Remarque IV.6.2. Nous prenons la convention suivante. Dans cette section, nous considérons uniquement des suites numériques, i.e., l'anneau A est le champ $\mathbb{R}$ des nombres réels. Lorsqu'on considère une série de puissances comme ci-dessus, on peut soit la voir comme une fonction de la variable complexe z et dès lors, s'intéresser à sa convergence, à son rayon de convergence, etc... ou bien, comme ce sera le cas ici, la série est simplement considérée comme un objet combinatoire codant, au moyen de certaines conventions, les éléments de $\mathbf{a}$.

Définition IV.6.3. Soit $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ une suite. La *fonction génératrice* (ou *série génératrice*) de $\mathbf{a}$ est la série formelle

$$s_{\mathbf{a}}(z) = \sum_{n=0}^{\infty} a_n\, z^n.$$

Rappelons une fois encore, que les fonctions génératrices sont des objets algébriques pouvant être manipulés comme tels, sans se préoccuper d'une hypothétique convergence[14].

[13]Certains auteurs parlent parfois du *produit de convolution* de deux séries formelles.

[14]En fait, les notions de convergence peuvent s'avérer utiles lorsqu'on désire, par exemple, estimer le comportement asymptotique d'une suite.

Remarque IV.6.4. Une fraction rationnelle (i.e., le quotient de deux polynômes) est considérée comme une expression compacte pour une fonction génératrice. Etant donné la fraction rationnelle P/Q, $P, Q \in \mathbb{R}[z]$, on obtient la série correspondante en effectuant la (longue[15]) division euclidienne de P par Q. On peut remarquer que si Q est le polnôme réciproque d'une suite linéaire récurrente, une telle division est toujours possible et ce, même dans un anneau quelconque. En effet, le coefficient du terme indépendant vaut 1.

Exemple IV.6.5. Soit la fraction rationnelle propre $\frac{1}{1-z}$. Si on effectue l'algorithme de la longue division, on obtient

$$\begin{array}{rrrrr|l}
1 & & & & & 1-z \\
\cline{6-6}
-(1 & -z) & & & & 1+z+z^2+\cdots \\
\cline{1-2}
 & z & & & & \\
 & -(z & -z^2) & & & \\
\cline{2-3}
 & & z^2 & & & \\
 & & -(z^2 & -z^3) & & \\
\cline{3-4}
 & & & z^3 & & \\
 & & & & \ddots &
\end{array}$$

Ainsi,

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$$

est la fonction génératrice de la suite constante $\mathbf{1} = (1)_{n\in\mathbb{N}}$.

Exemple IV.6.6. La suite des carrés parfaits $(n^2)_{n\in\mathbb{N}} = 0, 1, 4, 9, 16, \ldots$ a pour fonction génératrice

$$\frac{z+z^2}{1-3z+3z^2-z^3}.$$

En effet,

$$\begin{array}{rrrrrr|l}
z & +z^2 & & & & & 1-3z+3z^2-z^3 \\
\cline{6-6}
-(z & -3z^2 & +3z^3 & -z^4) & & & z+4z^2+9z^3+\cdots \\
\cline{1-4}
 & 4z^2 & -3z^3 & +z^4 & & & \\
 & -(4z^2 & -12z^3 & +12z^4 & -4z^5) & & \\
\cline{2-5}
 & & 9z^3 & -11z^4 & +4z^5 & & \\
 & & -(9z^3 & -27z^4 & +27z^5 & -9z^6) & \\
\cline{3-6}
 & & & 16z^4 & -23z^5 & 9z^6 & \\
 & & & & & \ddots &
\end{array}$$

La justification précise sera donnée dans l'exemple IV.6.8. En effet, à ce stade, il serait fastidieux de vérifier qu'à l'étape n de la longue division, le coefficient obtenu pour z^n est n^2. Très bientôt, nous aurons à notre

[15]Contrairement à la division euclidienne classique, on commence avec les termes de plus petit degré.

disposition d'autres outils permettant des manipulations aisées de telles expressions. On peut aussi lire l'exemple IV.6.11 où est fourni une relation de récurrence linéaire pour cette suite.

En plus de la somme et du produit (de Cauchy), on dispose d'autres opérations dans $\mathbb{R}[[z]]$ pour manipuler les séries formelles. Bien sûr, on peut tout d'abord considérer des combinaisons linéaires de séries formelles. Si $s_{\mathbf{a}}(z)$ et $s_{\mathbf{b}}(z)$ sont deux séries de $\mathbb{R}[[z]]$ et $\alpha, \beta \in \mathbb{R}$, alors on considère

$$\alpha\, s_{\mathbf{a}}(z) + \beta\, s_{\mathbf{b}}(z) = \sum_{n=0}^{\infty} (\alpha\, a_n + \beta\, b_n)\, z^n.$$

La multiplication de la série génératrice de la suite $(a_n)_{n\in\mathbb{N}}$ par z^m permet d'obtenir la série génératrice de la suite translatée

$$\underbrace{0, \ldots, 0}_{m \text{ fois}}, a_0, a_1, a_2, \ldots,$$

$$z^m\, s_{\mathbf{a}}(z) = \sum_{n=0}^{\infty} a_n\, z^{n+m} = \sum_{n=m}^{\infty} a_{n-m} z^n.$$

Pour passer de la série génératrice de $(a_n)_{n\in\mathbb{N}}$, à la série translatée de k termes vers la droite $(a_{n+k})_{n\in\mathbb{N}}$, il suffit de considérer la série formelle

$$\frac{s_{\mathbf{a}}(z) - a_0 - a_1 z - \cdots - a_{k-1} z^{k-1}}{z^k} = \frac{1}{z^k} \sum_{n=k}^{\infty} a_n z^n = \sum_{n=k}^{\infty} a_n z^{n-k} = \sum_{n=0}^{\infty} a_{n+k} z^n.$$

Si, dans $s_{\mathbf{a}}(z)$, on remplace l'indéterminée z par cz, on obtient la série génératrice de la suite $(c^n a_n)_{n\in\mathbb{N}}$,

$$s_{\mathbf{a}}(cz) = \sum_{n=0}^{\infty} c^n a_n\, z^n.$$

On peut introduire un opérateur $\mathrm{D} : \mathbb{R}[[z]] \to \mathbb{R}[[z]]$, appelé *dérivée formelle*, défini par

$$\mathrm{D}\left(\sum_{n=0}^{\infty} a_n\, z^n \right) = \sum_{n=0}^{\infty} (n+1)\, a_{n+1}\, z^n.$$

Insistons encore sur le fait qu'on ne donne aucun sens topologique à cet opérateur et il n'y a donc aucun problème, ni aucune objection à lever, pour "dériver" une série. Ainsi, $\mathrm{D}s_{\mathbf{a}}(z)$ est la série génératrice de la suite $((n+1)a_{n+1})_{n\in\mathbb{N}}$. En combinant dérivation formelle et multiplication par z, il vient

$$z\mathrm{D}s_{\mathbf{a}}(z) = \sum_{n=1}^{\infty} n a_n\, z^n.$$

Par analogie avec l'opérateur de dérivation formelle, on introduit également un opérateur d'*intégration formelle*,

$$\int_0^z s_{\mathbf{a}}(t)\, dt = a_0 z + \frac{1}{2} a_1 z^2 + \frac{1}{3} a_2 z^3 + \cdots = \sum_{n=1}^{\infty} \frac{1}{n} a_{n-1} z^n.$$

Proposition IV.6.7. *Si $s_{\mathbf{a}}(z)$ est la série génératrice de $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$, alors*

$$\frac{1}{1-z}\, s_{\mathbf{a}}(z)$$

est la série génératrice de la suite $(\sum_{k=0}^{n} a_k)_{n\in\mathbb{N}}$ des sommes partielles de $\mathbf{a}$.

Démonstration. Il s'agit d'une simple vérification. On sait que $\frac{1}{1-z}$ est une forme close pour la série génératrice de la suite constante $\mathbf{1} = (1)_{n\in\mathbb{N}}$ (cf. exemple IV.6.5). Par définition du produit (de Cauchy) de deux séries, le coefficient de z^n du produit proposé est égal à

$$\sum_{k=0}^{n} a_k \mathbf{1}_{n-k}.$$

Ceci conclut la preuve.

■

Exemple IV.6.8. Au vu de l'exemple IV.6.5, la série génératrice de la suite $\mathbf{1} = (1)_{n\in\mathbb{N}}$ est $1/1-z$. En la dérivant (formellement), on obtient[16]

$$\mathrm{D}\frac{1}{1-z} = \frac{1}{(1-z)^2} = \sum_{n=1}^{\infty} n\, z^{n-1} = \sum_{n=0}^{\infty} (n+1)\, z^n$$

et dès lors,

$$\frac{z}{(1-z)^2} = \sum_{n=0}^{\infty} n\, z^n.$$

En dérivant (formellement) une seconde fois la relation obtenue, il vient alors

$$\mathrm{D}\frac{z}{(1-z)^2} = \frac{1+z}{(1-z)^3} = \sum_{n=0}^{\infty} (n+1)^2\, z^n.$$

Enfin, en multipliant par z, on retrouve la forme close de l'exemple IV.6.6,

$$\frac{z+z^2}{(1-z)^3} = \sum_{n=0}^{\infty} n^2\, z^n$$

qui est la série génératrice de la suite des carrés parfaits.

Nous présentons une méthode immédiate pour obtenir les séries génératrices de $(a_{2n})_{n\in\mathbb{N}}$ et de $(a_{2n+1})_{n\in\mathbb{N}}$ à partir de la série génératrice $s_{\mathbf{a}}(z)$ de $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$.

Proposition IV.6.9. *La série formelle*

$$\frac{s_{\mathbf{a}}(z) + s_{\mathbf{a}}(-z)}{2} = \sum_{n=0}^{\infty} a_{2n}\, z^{2n} \text{ (resp. } \frac{s_{\mathbf{a}}(z) - s_{\mathbf{a}}(-z)}{2} = \sum_{n=0}^{\infty} a_{2n+1}\, z^{2n+1} \text{)}$$

est la série génératrice de la suite $(a_0, 0, a_2, 0, a_4, 0, \ldots)$ des termes d'indice pair de $\mathbf{a}$ (resp. de la suite $(0, a_1, 0, a_3, 0, a_5, 0, \ldots)$ des termes d'indice impair de $\mathbf{a}$).

[16] On peut vérifier que la dérivation formelle d'une forme close suit les règles de dérivation usuelles de l'analyse. Ces vérifications n'apportent rien à notre exposé et sont laissées au lecteur.

Démonstration. C'est immédiat.

■

6.1. Résolution d'équations linéaires grâce aux séries formelles. Nous avons introduit les séries formelles dans le but principal de résoudre des équations de récurrence linéaires. On procède alors par "*identification des coefficients*". On recherche tout d'abord, par un procédé purement mécanique, une forme close (sous forme d'une fraction rationnelle) pour la série génératrice de la suite et ensuite, on développe cette fraction en série de puissances. Etant en présence de deux expressions représentant la même série, il suffit alors de remarquer que

Ce sont ici des séries formelles !

$$\sum_{n=0}^{\infty} a_n\, z^n = \sum_{n=0}^{\infty} b_n\, z^n$$

si et seulement si $a_n = b_n$, pour tout $n \geq 0$. Nous décrivons la marche à suivre sur un exemple.

Soit la suite de Fibonacci satisfaisant la relation

$$\begin{cases} x_{n+2} = x_{n+1} + x_n, \\ x_0 = 1,\, x_1 = 1. \end{cases}$$

(Nous avons choisi ces conditions initiales particulières pour simplifier un rien les calculs.) Soit s la série génératrice de la suite $(x_n)_{n\in\mathbb{N}}$,

$$s(z) = \sum_{n=0}^{\infty} x_n\, z^n.$$

Etape 1. Par de simples manipulations algébriques faisant bien évidemment intervenir l'équation de récurrence, on peut exprimer s sous forme d'une fraction rationnelle. Il vient

$$\begin{aligned} s(z) &= x_0 + x_1\, z + \sum_{n=0}^{\infty} x_{n+2}\, z^{n+2} \\ &= 1 + z + \sum_{n=0}^{\infty} (x_{n+1} + x_n) z^{n+2} \\ &= 1 + z + z \sum_{n=0}^{\infty} x_{n+1}\, z^{n+1} + z^2 \sum_{n=0}^{\infty} x_n\, z^n \\ &= 1 + z + z\,[s(z) - x_0] + z^2\, s(z). \end{aligned}$$

De là, on en tire que

$$s(z) = \frac{1}{1 - z - z^2}.$$

En fait, on peut sans grande difficulté obtenir le résultat général suivant.

Théorème IV.6.10. *La suite* $\mathbf{x} = (x_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ *est une suite linéaire récurrente satisfaisant l'équation* (8) *à coefficients dans* A *si et seulement*

si la série génératrice $s_{\mathbf{x}}(z)$ est une fraction rationnelle ayant pour dénominateur le polynôme réciproque[17] $1-a_{k-1}z-\cdots-a_0z^k$. *De plus, le numérateur de la fraction dépend uniquement des conditions initiales* $x_0,\ldots,x_{k-1}$.

Avant de procéder à la preuve, utilisons ce dernier résultat pour obtenir une relation de récurrence linéaire pour la suite des carrés.

Exemple IV.6.11. Si nous admettons que la série de l'exemple IV.6.6 est bien la série génératrice de la suite des carrés, puisque cette série est une fraction rationnelle de la forme

$$\frac{z+z^2}{1-3z+3z^2-z^3},$$

alors, le théorème ci-dessus stipule que la suite des carrés satisfait la relation de récurrence

$$x_{n+3}=3x_{n+2}-3x_{n+1}+x_n.$$

Ceci se vérifie aisément.

Démonstration. La condition est nécessaire. Elle a déjà été discutée ci-dessus et devrait paraître claire au le lecteur. Voici les détails.

$$\begin{aligned} s_{\mathbf{x}}(z) &= \sum_{i=0}^{k-1} x_i\,z^i+\sum_{n=0}^{\infty} x_{n+k}\,z^{n+k} \\ &= \sum_{i=0}^{k-1} x_i\,z^i+\sum_{n=0}^{\infty} \left(a_{k-1}\,x_{n+k-1}+\cdots+a_0\,x_n\right)\,z^{n+k} \\ &= \sum_{i=0}^{k-1} x_i\,z^i+\sum_{i=0}^{k-1} a_i\,z^{k-i}\,(s_{\mathbf{x}}(z)-x_0-\cdots-x_{i-1}z^{i-1}) \end{aligned}$$

De là, on trouve

$$\left(1-\sum_{i=0}^{k-1} a_i\,z^{k-i}\right)\,s_{\mathbf{a}}(z)=\sum_{i=0}^{k-1} x_i\,z^i-\underbrace{\sum_{i=1}^{k-1} a_i\,z^{k-i}\sum_{j=0}^{i-1} x_j\,z^j}_{=\sum_{t=1}^{k-1}\sum_{i=0}^{t-1} a_{k-t+i}x_i\,z^t}$$

où le coefficient du membre de gauche est exactement le polynôme réciproque annoncé et le membre de droite est un polynôme en z de degré $<k$. Ce dernier dépend uniquement des conditions initiales $x_0,\ldots,x_{k-1}$ et des coefficients $a_1,\ldots,a_{k-1}$.

Réciproquement, si on considère un polynôme $P(z)=\sum_{i=0}^{k-1} b_i\,z^i$ de degré au plus $k-1$, alors par longue division (ou par développement de Taylor), on obtient le développement

$$\frac{P(z)}{1-a_{k-1}\,z-\cdots-a_0\,z^k}=\sum_{n=0}^{\infty} x_n z^n.$$

[17] En anglais, l'inverse d'un nombre se dit "reciprocal". Par contre, l'inverse d'une fonction se traduit par "inverse".

De là, on trouve

$$\begin{aligned} P(z) &= (1 - a_{k-1}\, z - \cdots - a_0\, z^k) \sum_{n=0}^{\infty} x_n z^n \\ &= \sum_{n=0}^{\infty} x_n z^n - a_{k-1} \sum_{n=1}^{\infty} x_{n-1} z^n - \cdots - a_0 \sum_{n=k}^{\infty} x_{n-k} z^n \\ &= \sum_{i=0}^{k-1} x_i\, z^i - \sum_{i=1}^{k-1} a_i\, z^{k-i} \sum_{j=0}^{i-1} x_j\, z^j \\ &\quad + \sum_{n=k}^{\infty} (x_n - a_{k-1}\, x_{n-1} - \cdots - a_0\, x_{n-k}) z^n. \end{aligned}$$

Ceci montre que pour tout $n \geq k$, la suite $(x_n)_{n\geq 0}$ satisfait la relation $x_n - a_{k-1}\, x_{n-1} - \cdots - a_0\, x_{n-k} = 0$. De plus, en identifiant les coefficients dans

$$P(z) = \sum_{i=0}^{k-1} b_i\, z^i = \sum_{i=0}^{k-1} x_i\, z^i - \sum_{i=1}^{k-1} a_i\, z^{k-i} \sum_{j=0}^{i-1} x_j\, z^j$$

on retrouve les conditions initiales $x_0, \ldots, x_{k-1}$ en fonction des a_i et des b_i.

■

Remarque IV.6.12. Si le polynôme caractéristique de la relation

$$\chi(X) = X^k - a_{k-1} X^{k-1} - \cdots - a_0$$

ne s'annule pas en zéro (autrement dit, si $a_0 \neq 0$) et possède $\alpha_1, \ldots, \alpha_t$ comme zéros de multiplicité respective $m_1, \ldots, m_t$, alors le polynôme réciproque $1 - a_{k-1} X - \cdots - a_0 X^k = X^k\, \chi(\frac{1}{X})$ possède évidemment les inverses $1/\alpha_1, \ldots, 1/\alpha_t$ des zéros de $\chi(X)$ comme zéros avec les mêmes multiplicité $m_1, \ldots, m_t$.

Exemple IV.6.13. Considérons la suite $(x_n)_{n\geq 0}$ satisfaisant, pour tout $n \geq 0$, $x_{n+3} = a x_{n+2} + b x_{n+1} + c x_n$. Sa série génératrice est de la forme

$$s(z) = \frac{d + ez + fz^2}{1 - az - bz^2 - cz^3}.$$

Dès lors, $(1 - az - bz^2 - cz^3)(\sum_{n=0}^{\infty} x_n\, z^n) = d + ez + fz^2$ et, en identifiant les coefficients, on obtient le système

$$\begin{cases} d = x_0 \\ e = x_1 - a x_0 \\ f = x_2 - a x_1 - b x_0 \end{cases}$$

et bien sûr, pour tout $n \geq 3$, $0 = x_n - a x_{n-1} - b x_{n-2} - c x_{n-3}$. Ainsi, les conditions initiales déterminent les coefficients du numérateur de la fraction rationnelle et inversement.

Etape 2. La deuxième partie de la méthode consiste à développer la fraction rationnelle en série de puissances. Si on décompose $\frac{1}{1-z-z^2}$ en fractions simples, on obtient

Dans cette méthode, une telle décomposition constitue en pratique le point délicat!

$$\frac{1}{1-z-z^2} = \frac{\sqrt{5}}{5\,(z+\tau)} - \frac{\sqrt{5}}{5\,(z+\tau')}$$

où on emploie les mêmes notations qu'à l'exemple IV.2.10. Le résultat suivant est alors fort utile.

Proposition IV.6.14. *On a*

$$\boxed{\frac{1}{(1-\rho z)^{t+1}} = \sum_{n=0}^{\infty} \mathrm{C}_{n+t}^{t}\ \rho^n\, z^n.}$$

Démonstration. Nous savons que

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n.$$

En dérivant t fois cette relation, on obtient

$$\mathrm{D}^t \frac{1}{1-z} = t! \frac{1}{(1-z)^{t+1}} = \sum_{n=t}^{\infty} n(n-1)\cdots(n-t+1)\, z^{n-t}.$$

De là,

$$\frac{1}{(1-z)^{t+1}} = \frac{1}{t!} \sum_{n=t}^{\infty} \frac{n!}{(n-t)!}\, z^{n-t} = \frac{1}{t!} \sum_{n=0}^{\infty} \frac{(n+t)!}{n!}\, z^n.$$

D'où la conclusion, en remplaçant l'indéterminée z par ρz.

■

Nous pouvons utiliser ce résultat pour obtenir le développement recherché. Il vient[18]

$$\frac{1}{z+\tau} = \frac{1}{\tau\,(1+\frac{1}{\tau}z)} = \frac{-\tau'}{1-\tau' z} = -\tau' \sum_{n=0}^{\infty} \tau'^n\, z^n$$

de même que

$$\frac{1}{z+\tau'} = -\sum_{n=0}^{\infty} \tau^{n+1}\, z^n.$$

D'où, on obtient

$$\begin{aligned} s(z) &= \sum_{n=0}^{\infty} x_n\, z^n = \frac{1}{1-z-z^2} = -\frac{\sqrt{5}}{5} \sum_{n=0}^{\infty} \tau'^{n+1}\, z^n + \frac{\sqrt{5}}{5} \sum_{n=0}^{\infty} \tau^{n+1}\, z^n \\ &= \sum_{n=0}^{\infty} \frac{\sqrt{5}}{5} (\tau^{n+1} - \tau'^{n+1})\, z^n \end{aligned}$$

[18] Puisque τ et τ' sont les racines de $X^2 - X - 1$, on a $\tau^2 = \tau + 1$ et donc $\tau = 1 + \frac{1}{\tau}$. De plus, il est clair que $\tau - 1 = -\tau'$ et donc $-\tau' = 1/\tau$.

et par identification des coefficients, pour tout $n \geq 0$,

$$x_n = \frac{\sqrt{5}}{5}(\tau^{n+1} - \tau'^{n+1}).$$

Exemple IV.6.15. Si nous désirons obtenir la fonction génératrice des nombres de Fibonacci d'indice pair, on peut procéder comme suit. On vient de montrer que la suite

$$(x_n)_{n\in\mathbb{N}} = 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

a $s(z) = \frac{1}{1-z-z^2}$ pour fonction génératrice. Ainsi, au vu de la proposition IV.6.9, la fonction génératrice de la suite

$$1, 0, 2, 0, 5, 0, 13, 0, 34, 0, 89, 0, \ldots$$

est donnée par

$$\begin{aligned} t(z) &= \frac{s(z) + s(-z)}{2} = \sum_{n=0}^{\infty} x_{2n}\, z^{2n} \\ &= \frac{1}{2}\left(\frac{1}{1-z-z^2} + \frac{1}{1+z-z^2}\right) = \frac{1-z^2}{1-3z^2+z^4}. \end{aligned}$$

Ce que nous désirons obtenir, c'est la fonction génératrice

$$u(z) = \sum_{n=0}^{\infty} x_{2n}\, z^n$$

de la suite $1, 2, 5, 13, 34, 89, \ldots$. Or, on remarque que $u(z^2) = t(z)$. Par conséquent, on a

$$u(z) = \frac{1-z}{1-3z+z^2}.$$

En particulier, la suite $1, 2, 5, 13, 34, 89, \ldots$ satisfait la relation $y_{n+2} = 3y_{n+1} - y_n$. Si on développait la fraction ci-dessus en série de puissances, on pourrait obtenir une formule close pour la suite de termes pairs de la suite de Fibonacci. En guise d'exercice, on trouve[19]

$$\frac{1-z}{1-3z+z^2} = -\frac{5+\sqrt{5}}{10\,(z-\tau^2)} + \frac{\sqrt{5}-5}{10\,(z-\tau'^2)},$$

$$\frac{1}{z-\tau^2} = -\frac{\tau'^2}{1-\tau'^2 z} = -\sum_{n=0}^{\infty} \tau'^{2(n+1)}\, z^n \text{ et } \frac{1}{z-\tau'^2} = -\sum_{n=0}^{\infty} \tau^{2(n+1)}\, z^n.$$

De là, une formule close pour la suite des termes pairs est donnée par

$$\frac{5-\sqrt{5}}{10}\tau^{2(n+1)} + \frac{5+\sqrt{5}}{10}\tau'^{2(n+1)}.$$

[19] On utilise le fait que $1/\tau^2 = \tau'^2$.

6.2. A propos de la sous-suite $(x_{pn+\ell})_{n\geq 0}$. La construction décrite ci-dessus se généralise aisément. On considère une fois encore des suites numériques. Soit $\mathbf{x} = (x_n)_{n\geq 0}$ une suite linéaire récurrente satisfaisant (8) avec $s_{\mathbf{x}}(z) = P(z)/Q(z)$. Tout d'abord, si ω est une racine p-ième primitive de l'unité, on a

$$\frac{1}{p}\sum_{t=0}^{p-1} s_{\mathbf{x}}(\omega^t z) = \sum_{n=0}^{\infty} x_{pn}\, z^{pn}.$$

En effet, on a

$$\frac{1}{p}\sum_{t=0}^{p-1} s_{\mathbf{x}}(\omega^t z) = \sum_{i=0}^{\infty} x_i \left(1+\omega^i+\omega^{2i}+\cdots+\omega^{(p-1)i}\right) z^i$$

et si i est multiple de p, $(1+\omega^i+\omega^{2i}+\cdots+\omega^{(p-1)i}) = p$, sinon

$$1+\omega^i+\omega^{2i}+\cdots+\omega^{(p-1)i} = \frac{(\omega^i)^p-1}{\omega^i-1} = 0.$$

D'autre part, on a la fraction rationnelle suivante

$$\frac{1}{p}\sum_{t=0}^{p-1} s_{\mathbf{x}}(\omega^t z) = \frac{1}{p}\sum_{t=0}^{p-1} \frac{P(\omega^t z)}{Q(\omega^t z)} =: \frac{A(z)}{B(z)}.$$

En réduisant au même dénominateur, on doit considérer l'expression

$$B(z) = \prod_{t=0}^{p-1} Q(\omega^t z).$$

Si $Q(z) = a_0(z-\alpha_1)\cdots(z-\alpha_k)$ où les zéros de Q sont répétés selon leur multiplicité, alors

$$\prod_{t=0}^{p-1} Q(\omega^t z) = a_0^p \prod_{i=1}^{k}\prod_{t=0}^{p-1}(\omega^t z-\alpha_i) = a_0^p \prod_{i=1}^{k} \omega^{p(p-1)/2} \prod_{t=0}^{p-1}(z-\frac{\alpha_i}{\omega^t}).$$

Notez que $\omega^{p(p-1)/2} = \pm 1$ suivant la parité de p. Si on remarque que

$$\{1, 1/\omega, \ldots, 1/\omega^{p-1}\} = \{1, \omega, \ldots, \omega^{p-1}\},$$

on peut encore écrire

$$B(z) = a_0^p \prod_{i=1}^{k} \omega^{p(p-1)/2} \prod_{t=0}^{p-1}(z-\omega^t\alpha_i) = a_0^p \prod_{i=1}^{k} \omega^{p(p-1)/2}\,(z^p-\alpha_i^p).$$

En effet, les p racines p-ièmes de α_i^p sont exactement $\alpha_i, \omega\alpha_i, \ldots, \omega^{p-1}\alpha_i$. Ceci montre que le polynôme $B(z)$ a tous ses termes de degré multiple de p. Or, nous avons

$$\frac{1}{p}\sum_{t=0}^{p-1} s_{\mathbf{x}}(\omega^t z) = \sum_{n=0}^{\infty} x_{pn}\, z^{pn} = \frac{A(z)}{B(z)}.$$

Donc le polynôme $A(z) = B(z)\sum_{n=0}^{\infty} x_{pn}\, z^{pn}$ a également tous ses termes de degré multiple de p. Il est donc licite de considérer la fraction rationnelle

$$\frac{A(z^{1/p})}{B(z^{1/p})}$$

où $A(z^{1/p})$ et $B(z^{1/p})$ sont des polynômes en z. Cette fraction rationnelle est évidemment égale à la série génératrice de la suite $(x_{pn})_{n\geq 0}$,

$$\frac{A(z^{1/p})}{B(z^{1/p})} = \sum_{n=0}^{\infty} x_{pn}\, z^n.$$

Autrement dit, par le théorème IV.6.10, la suite $(x_{pn})_{n\geq 0}$ satisfait une relation de récurrence linéaire.

Corollaire IV.6.16. *Soient $p \geq 1$, $\ell \geq 0$. Si $\mathbf{x} = (x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire, il en est de même pour la sous-suite $(x_{pn+\ell})_{n\geq 0}$.*

Démonstration. Au vu du développement ci-dessus, si $\mathbf{x} = (x_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire, alors $s_{\mathbf{x}}$ est une fraction rationnelle et il en est de même pour la série génératrice de la suite $(x_{pn})_{n\geq 0}$. Enfin, si $\mathbf{y} = (y_n)_{n\geq 0}$ satisfait une relation de récurrence linéaire, la suite $(y_{n+\ell})_{n\geq 0}$ satisfait exactement la même relation (seules les conditions initiales changent).

■

On peut même aller encore un peu plus loin. Dans ce qui suit, on suppose $a_0 \neq 0$. En effet, si la relation de récurrence (8) est à coefficients entiers, il est légitime d'espérer que la suite $(x_{pn+\ell})_{n\geq 0}$ satisfasse également une relation de récurrence à coefficients entiers. Montrons que si le polynôme caractéristique $\chi_{\mathbf{x}}$ de la suite $\mathbf{x} = (x_n)_{n\geq 0}$ est à coefficients entiers, il en est de même pour celui de la suite $(x_{pn+\ell})_{n\geq 0}$.

Au vu de la remarque IV.6.12, en conservant les notations introduites précédemment, si le polynôme réciproque $Q(z) = a_0(z-\alpha_1)\cdots(z-\alpha_k)$, en posant pour tout i, $\beta_i = 1/\alpha_i$, alors $\chi_{\mathbf{x}}(z) = (z-\beta_1)\cdots(z-\beta_k)$. En développant, on obtient

$$\chi_{\mathbf{x}}(z) = z^k - e_1(\beta_1,\ldots,\beta_k)z^{k-1} + e_2(\beta_1,\ldots,\beta_k)z^{k-2} + \cdots + (-1)^k e_k(\beta_1,\ldots,\beta_k)$$

où

$$\left\{\begin{array}{rcl} e_1(\beta_1,\ldots,\beta_k) & = & \sum_{1\leq i\leq k}\beta_i \\ e_2(\beta_1,\ldots,\beta_k) & = & \sum_{1\leq i_1<i_2\leq k}\beta_{i_1}\beta_{i_2} \\ e_3(\beta_1,\ldots,\beta_k) & = & \sum_{1\leq i_1<i_2<i_3\leq k}\beta_{i_1}\beta_{i_2}\beta_{i_3} \\ & \vdots & \\ e_{k-1}(\beta_1,\ldots,\beta_k) & = & \sum_{1\leq i_1<\cdots<i_{k-1}\leq k}\beta_{i_1}\cdots\beta_{i_{k-1}} \\ e_k(\beta_1,\ldots,\beta_k) & = & \beta_1\cdots\beta_k \end{array}\right.$$

et puisque $\chi_{\mathbf{x}}(z) \in \mathbb{Z}[z]$, alors pour tout i, $e_i(\beta_1,\ldots,\beta_k) \in \mathbb{Z}$.

Le polynôme $B(z^{1/p}) = a_0^p \prod_{i=1}^k \omega^{p(p-1)/2}(z-\alpha_i^p)$ est le polynôme réciproque du polynôme caractéristique $\xi(z)$ de la suite $(x_{pn+\ell})_{n\geq 0}$. Encore une fois, au vu de la remarque IV.6.12, on a

$$\xi(z) = \prod_{i=1}^{k}(z-\beta_i^p).$$

Ce polynôme peut être considéré comme un polynôme $S(\beta_1, \ldots, \beta_k)$ en les k variables[20] $\beta_1, \ldots, \beta_k$ dont les coefficients sont des polynômes de $\mathbb{Z}[z]$. Ce polynôme est symétrique : pour toute permutation ν de $\{1, \ldots, k\}$,

$$S(\beta_{\nu(1)}, \ldots, \beta_{\nu(k)}) = S(\beta_1, \ldots, \beta_k).$$

Par un résultat classique en algèbre commutative, tout polynôme symétrique s'exprime comme un polynôme en les polynômes symétriques élémentaires.

Théorème IV.6.17 (Théorème fondamental des polynômes symétriques). *Soit A un anneau commutatif. Tout polynôme symétrique $S(X_1, \ldots, X_k) \in A[X_1, \ldots, X_k]$ s'écrit (de manière unique) comme*

$$S(X_1, \ldots, X_k) = T(e_1(X_1, \ldots, X_k), \ldots, e_k(X_1, \ldots, X_k))$$

avec $T \in A[Y_1, \ldots, Y_k]$.

En appliquant ce résultat à $\xi(z) \in \mathbb{Z}[z][\beta_1, \ldots, \beta_k]$, il existe un polynôme $T \in \mathbb{Z}[z][Y_1, \ldots, Y_k]$ tel que

$$\xi(z) = T(e_1(\beta_1, \ldots, \beta_k), \ldots, e_k(\beta_1, \ldots, \beta_k))$$

Or nous savons déjà que pour tout i, $e_i(\beta_1, \ldots, \beta_k) \in \mathbb{Z}$. De là, $\xi(z) \in \mathbb{Z}[z]$. Par conséquent, la suite $(x_{pn+\ell})_{n \geq 0}$ satisfait une relation de récurrence à coefficients entiers.

7. Chemins de Dyck et nombres de Catalan

Cette section présente un exemple important d'utilisation des fonctions génératrices dans le but d'obtenir la solution d'une relation de récurrence particulière apparaissant dans divers problèmes de combinatoire et de dénombrement.

Considérons $n+1$ éléments $a_0, \ldots, a_n$ dont on désire réaliser le produit. Ne pouvant réaliser le produit que de deux facteurs à la fois, de combien de façons différentes peut-on calculer ce produit, en laissant l'ordre des facteurs inchangé ? Autrement dit, de combien de façons peut-on "parenthéser" une telle expression ?

$n = 0$	a_0	1
$n = 1$	$a_0 \cdot a_1$	1
$n = 2$	$a_0 \cdot (a_1 \cdot a_2)$ $\quad$ $(a_0 \cdot a_1) \cdot a_2$	2
$n = 3$	$(a_0 \cdot (a_1 \cdot a_2)) \cdot a_3$ $\quad$ $((a_0 \cdot a_1) \cdot a_2) \cdot a_3$ $\quad$ $(a_0 \cdot a_1) \cdot (a_2 \cdot a_3)$ $a_0 \cdot ((a_1 \cdot a_2) \cdot a_3)$ $\quad$ $a_0 \cdot (a_1 \cdot (a_2 \cdot a_3))$	5
$\vdots$		$\vdots$

Notons $\mathcal{C}_n$ la réponse recherchée pour le nombre de produits distincts de $n+1$ facteurs. Notre but est de déterminer une formule close pour $\mathcal{C}_n$. Avant d'y

[20] Une réflexion s'impose, maintenant z ne joue plus le rôle de la variable, on considère un polynôme à plusieurs variables $\beta_1, \ldots, \beta_k$. Il faut prendre le temps de faire le point ! Par exemple, $(z - \beta_1^p)(z - \beta_2^p) = \beta_1^p \beta_2^p - z\beta_1^p - z\beta_2^p + z^2 = S(\beta_1, \beta_2)$ et le coefficient du terme en β_1^p est $-z \in \mathbb{Z}[z]$.

parvenir, passons en revue quelques autres[21] situations où apparaissent ces nombres $\mathcal{C}_n$.

Exemple IV.7.1 (Langage de Dyck des mots bien parenthésés). Soit l'alphabet $\Sigma = \{a, b\}$. On considère l'ensemble $\mathfrak{D}$ des mots écrits sur Σ contenant le même nombre de a que de b et tels que pour tout préfixe d'un mot de $\mathfrak{D}$, le nombre de a apparaissant dans ce préfixe est supérieur ou égal au nombre de b. Par exemple,

$$aabb, abab, aababb, ababaababb, \ldots$$

appartiennent à $\mathfrak{D}$. On parle de langage bien parenthésé car il suffit de remplacer "a" par "(" et "b" par ")" pour obtenir des expressions bien parenthésées. Si pour un mot écrit sur Σ, on convient de représenter un a (resp. b) par un déplacement d'une unité vers la droite et vers le haut (resp. le bas), alors un mot du langage $\mathfrak{D}$ de longueur $2n$ représente un déplacement dans le plan (rapporté à un repère orthonormé) de l'origine au point de coordonnées $(2n, 0)$ sans jamais passer par un point d'ordonnée négative. Une

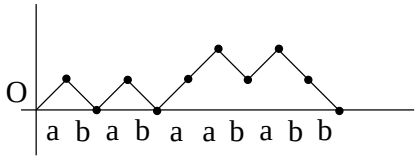


FIGURE IV.3. Un mot de Dyck de longueur 10.

représentation des mots de Dyck de longueur 6 est donnée à la figure IV.4. Il est clair que le nombre de mots de Dyck de longueur $2n$ est égal à $\mathcal{C}_n$.

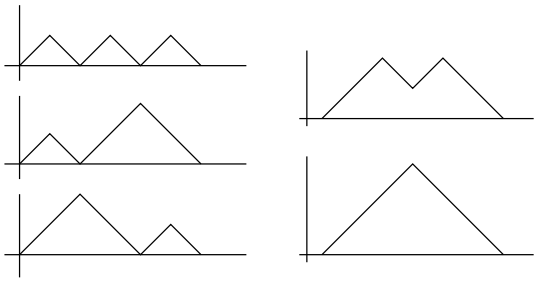


FIGURE IV.4. Les mots de Dyck de longueur 6.

Exemple IV.7.2. On peut désirer compter le nombre de triangulations de polygones convexes à $n \geq 3$ côtés. Comme il sera facile de le vérifier, le

[21] On peut trouver une liste de problèmes où apparaissent les nombres $\mathcal{C}_n$ dans W. G. Brown, *Historical note on a recurrent combinatorial problem*, American Math. Monthly **72**, 973–977, (1965). Ces nombres apparaissent également dans le dénombrement d'arbres binaires à n noeuds.

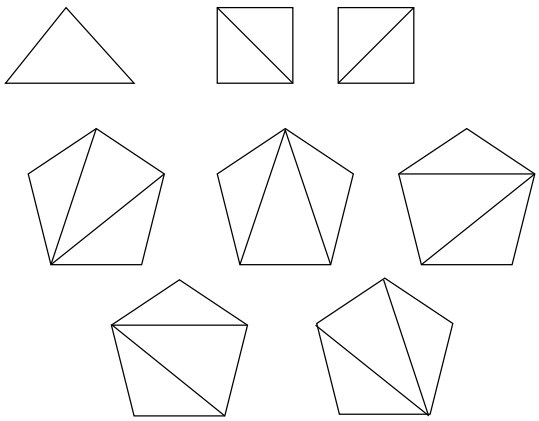


FIGURE IV.5. Nombre de triangulations d'un triangle, carré et pentagone.

nombre de triangulations distinctes d'un n-gone est égal à $\mathcal{C}_{n-2}$. En effet, l'argument de comptage développé pour le nombre de produits de $n+1$ facteurs s'adapte au cas des polygones[22]. Cet argument est détaillé à la remarque IV.7.3.

Revenons à notre problème initial. Pour compter le nombre de produits distincts des facteurs ordonnés $a_0, \ldots, a_n$, il faut s'apercevoir que dans la suite des produits partiels réalisés, on effectue un ultime produit se trouvant dès lors hors de toute parenthèse. Par exemple, si on entoure ce dernier produit, parmi les produits de 4 facteurs, on trouve

$$(a_0 \cdot a_1) \odot (a_2 \cdot a_3) \text{ ou } (a_0 \cdot (a_1 \cdot a_2)) \odot a_3.$$

Ainsi, cette dernière opération est le produit d'un facteur reprenant les $k+1$ premiers éléments $a_0, \ldots, a_k$ et d'un second facteur reprenant les $n-k$ autres éléments $a_{k+1}, \ldots, a_n$. Cet argument montre que, pour tout $n > 0$, $\mathcal{C}_n$ satisfait la relation non linéaire suivante

$$\mathcal{C}_n = \mathcal{C}_0\,\mathcal{C}_{n-1} + \mathcal{C}_1\,\mathcal{C}_{n-2} + \cdots + \mathcal{C}_{n-1}\,\mathcal{C}_0 = \sum_{k=0}^{n-1} \mathcal{C}_k\,\mathcal{C}_{n-1-k}.$$

Pour étendre cette définition à $n = 0$, puisque $\mathcal{C}_0 = 1$, on a

$$\boxed{\mathcal{C}_n = \sum_{k=0}^{n-1} \mathcal{C}_k\,\mathcal{C}_{n-1-k} + \delta_{n,0}}$$

(bien sûr, si $n = 0$, la somme ne contient aucun terme et vaut 0).

[22]Si un polygone a n côtés, lorsqu'on trace une quelconque diagonale, on se ramène à un polygone à k côtés et à un second polygone à $n-k+2$ côtés.

Remarque IV.7.3. [23] Soit T_n le nombre de triangulations d'un n-gone dont les sommets sont numérotés consécutivement de 1 à n. Si une triangulation ne contient aucune diagonale d'extrémité 1, alors elle contient nécessairement la diagonale joignant les sommets 2 et n. Ainsi, on se ramène à trianguler un polygône à $n-1$ sommets et le nombre de ces triangulations est T_{n-1}.

Sinon, la triangulation envisagée contient une diagonale joignant 1 à j avec $j \in \{3, \ldots, n-1\}$ minimal. Ainsi, on dispose d'un polygone P_1 à j sommets $\{1, \ldots, j\}$ et d'un polygone P_2 à $n-j+2$ sommets $\{j, j+1, \ldots, n, 1\}$. Vu la minimalité de j, la triangulation de P_1 ne contient pas de diagonale d'extrémité 1 (il y a donc T_{j-1} triangulations possibles car ces triangulations contiennent la diagonale joignant 2 à j, c'est le même argument que précédemment). Par contre, il n'y a aucune restriction sur P_2 et il peut être triangulé de T_{n-j+2} façons. Au total, le nombre de triangulations du n-gone pour lesquelles le sommet 1 est l'extrémité d'une diagonale de la triangulation vaut

$$\sum_{j=3}^{n-1} T_{j-1} T_{n-j+2}.$$

Si on pose $T_2 = 1$ et si on ajoute les triangulations du n-gone ne contenant aucune diagonale d'extrémité 1, on trouve

$$\forall n \geq 3, \quad T_n = T_{n-1} \underbrace{T_2}_{=1} + \sum_{j=3}^{n-1} T_{j-1} T_{n-j+2} = \sum_{j=3}^{n} T_{j-1} T_{n-j+2}.$$

En posant $S_n = T_{n+2}$, on trouve pour tout $n \geq 1$,

$$S_{n-2} = \sum_{j=3}^{n} S_{j-3} S_{n-j} = \sum_{j=0}^{n-3} S_j S_{n-j-3} = \mathcal{C}_{n-2}$$

et donc $T_n = \mathcal{C}_{n-2}$.

On peut reconnaître dans

$$\mathcal{C}_n = \sum_{k=0}^{n-1} \mathcal{C}_k \, \mathcal{C}_{n-1-k} + \delta_{n,0}$$

le terme général d'un produit de séries formelles. Ainsi, on introduit la série génératrice

Appeler "produit de convolution", le produit de Cauchy, est bien choisi, dans une situation comme celle-ci !

$$s_{\mathbf{C}}(z) = \sum_{n=0}^{\infty} \mathcal{C}_n \, z^n.$$

[23] Cette remarque judicieuse est dûe à L. Waxweiler. Merci Laurent !

Dès lors, il vient

$$\begin{aligned} s_{\mathbf{C}}(z) &= \sum_{n=1}^{\infty} \left(\sum_{k=0}^{n-1} \mathcal{C}_k \, \mathcal{C}_{n-1-k} \right) z^n + z^0 \\ &= \underbrace{\sum_{k=0}^{\infty} \mathcal{C}_k \, z^k}_{s_{\mathbf{C}}(z)} \underbrace{\sum_{n=k+1}^{\infty} \mathcal{C}_{n-1-k} \, z^{n-k}}_{z \, s_{\mathbf{C}}(z)} + 1. \end{aligned}$$

De là, on trouve l'équation du second degré

$$z \, s_{\mathbf{C}}^2 - s_{\mathbf{C}} + 1 = 0$$

qui possède comme solutions

$$s_{\mathbf{C}}(z) = \frac{1 \pm \sqrt{1 - 4\,z}}{2\,z}.$$

Puisque $s_{\mathbf{C}}(0) = \mathcal{C}_0 = 1$, cela nous conduit à choisir

$$s_{\mathbf{C}}(z) = \frac{1 - \sqrt{1 - 4\,z}}{2\,z}.$$

Il ne reste plus qu'à développer cette fraction en série de puissances pour obtenir une formule close pour $\mathcal{C}_n$.

Proposition IV.7.4. *Pour tout $t \in \mathbb{R} \setminus \mathbb{N}$, on a*

$$(1+z)^t = \sum_{n=0}^{\infty} \mathrm{C}_t^n \, z^n$$

où pour $t \in \mathbb{R}$ et $n \in \mathbb{N}$, on définit le coefficient binomial "généralisé"

$$\mathrm{C}_t^n := \frac{t(t-1)\cdots(t-n+1)}{n!}.$$

Remarque IV.7.5. On trouve parfois la notation $t^{\underline{n}}$ pour

$$t(t-1)\cdots(t-n+1),$$

avec $t \in \mathbb{R}$ et $n \in \mathbb{N}$. Ainsi, $\mathrm{C}_t^n = t^{\underline{n}}/n!$.

"Falling power"
On aurait déjà pu introduire cette notation à la page 120.

Démonstration. C'est immédiat. Si z est un nombre complexe tel que $|z| < 1$, en utilisant le développement de Taylor en variables complexes, on a

$$F(z) = \sum_{n=0}^{\infty} \frac{(D_z^n F)(0)}{n!} \, z^n.$$

Ici, $F(z) = (1+z)^t$, $D_z^n F = t^{\underline{n}} (1+z)^{t-n}$ et $(D_z^n F)(0) = t^{\underline{n}}$. Cette identité est donc encore valable pour les séries formelles correspondantes.

∎

Au vu de cette proposition,

$$\sqrt{1+z} = \sum_{n=0}^{\infty} \mathrm{C}_{1/2}^n \, z^n$$

et

$$\sqrt{1-4z} = \sum_{n=0}^{\infty} \mathrm{C}_{1/2}^{n} (-4z)^n = 1 + \sum_{n=1}^{\infty} \frac{1}{2n} \mathrm{C}_{-1/2}^{n-1} (-4z)^n$$

car, pour $n \geq 1$,

$$\mathrm{C}_{1/2}^{n} = \frac{1}{n!}\left(\frac{1}{2}\right)^{\underline{n}} = \frac{1}{n!}\frac{1}{2}\left(-\frac{1}{2}\right)^{\underline{n-1}} = \frac{1}{2n}\frac{1}{(n-1)!}\left(-\frac{1}{2}\right)^{\underline{n-1}} = \frac{1}{2n}\mathrm{C}_{-1/2}^{n-1}.$$

Lemme IV.7.6. *Soient $k \in \mathbb{N}$, $r \in \mathbb{R}$. On dispose des identités suivantes,*

i)
$$\mathrm{C}_{r}^{k} = (-1)^k \mathrm{C}_{k-r-1}^{k},$$

ii)
$$\mathrm{C}_{-1/2}^{k} = \left(-\frac{1}{4}\right)^k \mathrm{C}_{2k}^{k}.$$

Démonstration. Pour la première, il vient

$$\begin{aligned} r^{\underline{k}} &= r(r-1)\cdots(r-k+1) \\ &= (-1)^k(-r)(1-r)\cdots(k-1-r) \\ &= (-1)^k(k-1-r)^{\underline{k}}. \end{aligned}$$

Pour la seconde, remarquons tout d'abord que

$$r^{\underline{k}}(r-\frac{1}{2})^{\underline{k}} = \frac{(2r)^{\underline{2k}}}{2^{2k}}. \tag{14}$$

Pour le voir, il suffit de développer le membre de gauche en intercalant les facteurs des deux expressions,

$$r(r-\frac{1}{2})(r-1)(r-\frac{3}{2})\cdots(r-k+1)(r-k+\frac{1}{2}) = \frac{(2r)}{2}\frac{(2r-1)}{2}\cdots\frac{(2r-2k+1)}{2}.$$

Divisons les deux membres de (14) par $k!^2$. On trouve

$$\frac{r^{\underline{k}}}{k!}\frac{(r-\frac{1}{2})^{\underline{k}}}{k!} = \frac{(2r)^{\underline{2k}}}{(2k)!}\frac{(2k)!}{k!k!}\frac{1}{2^{2k}}$$

c'est-à-dire,

$$\mathrm{C}_{r}^{k}\,\mathrm{C}_{r-1/2}^{k} = \frac{1}{2^{2k}}\mathrm{C}_{2r}^{2k}\mathrm{C}_{2k}^{k}.$$

Cette dernière identité étant satisfaite pour tout $r \in \mathbb{R}$ et tout $k \in \mathbb{N}$, elle est encore satisfaite pour $k = r = n \in \mathbb{N}$,

$$\mathrm{C}_{n-1/2}^{n} = \frac{1}{4^n}\mathrm{C}_{2n}^{n}.$$

Par le premier point, on a

$$\mathrm{C}_{n-1/2}^{n} = (-1)^n \mathrm{C}_{n-(n-1/2)-1}^{n} = (-1)^n \mathrm{C}_{-1/2}^{n}$$

d'où la conclusion.

■

Nous pouvons à présent conclure nos développements. On a

$$\sqrt{1-4z} = 1 + \sum_{n=1}^{\infty} \frac{1}{2n} \, \mathrm{C}_{-1/2}^{n-1} \, (-4z)^n$$

d'où

$$s_{\mathbf{C}}(z) = \frac{1-\sqrt{1-4\,z}}{2\,z} = -\frac{1}{2z} \sum_{n=1}^{\infty} \frac{1}{2n} \, \mathrm{C}_{-1/2}^{n-1} \, (-4z)^n = \sum_{n=1}^{\infty} \frac{1}{n} \, \mathrm{C}_{-1/2}^{n-1} \, (-4z)^{n-1}$$

et par le lemme précédent, il vient

$$s_{\mathbf{C}}(z) = \sum_{n=1}^{\infty} \frac{1}{n} \left(-\frac{1}{4}\right)^{n-1} \mathrm{C}_{2(n-1)}^{n-1} \, (-4z)^{n-1} = \sum_{n=0}^{\infty} \frac{1}{n+1} \, \mathrm{C}_{2n}^{n} \, z^n.$$

En conclusion,

$$\boxed{\mathcal{C}_n = \frac{1}{n+1} \, \mathrm{C}_{2n}^{n}.}$$

Remarque IV.7.7. Sachant que $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$, alors

Rappelez-vous la formule de Stirling.

$$\mathcal{C}_n = \frac{1}{n+1} \frac{(2n)!}{n!^2} \sim \frac{1}{n+1} 2\sqrt{\pi n} \left(\frac{2n}{e}\right)^{2n} \frac{1}{2\pi n} \left(\frac{e}{n}\right)^{2n} = \frac{2^{2n}}{(n+1)\sqrt{\pi n}}.$$

Exemple IV.7.8. Dans Mathematica, après avoir chargé (une fois pour toutes) le package approprié, on dispose d'une fonction calculant le n-ième nombre de Catalan.

```
:> << DiscreteMath‘Combinatorica‘
:> Table[CatalanNumber[i], {i,1,20}]
Out[]= {1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786,
       208012, 742900, 2674440, 9694845, 35357670, 129644790,
       477638700, 1767263190, 6564120420}
```

8. Systèmes d'équations linéaires récurrentes

Il arrive que dans certains problèmes apparaisse non pas une relation de récurrence linéaire mais bien un système de relations de récurrence. L'utilisation des séries génératrices permet dans bien des cas de résoudre un tel système. On peut remarquer que la méthode développée s'apparente aux méthodes employées en analyse pour résoudre un système d'équations différentielles où l'on utilise la transformée de Laplace. Nous considérons un simple exemple.

Soit le système

$$\begin{cases} u_{n+2} = 2v_{n+1} + u_n \\ v_{n+2} = u_{n+1} + v_n \end{cases}$$

avec les conditions initiales $u_0 = 1$, $u_1 = 0$, $v_0 = 0$ et $v_1 = 1$. Si on introduit les séries génératrices des deux suites, il vient

$$s_{\mathbf{u}}(z) = \sum_{n=0}^{\infty} u_n \, z^n = u_0 + u_1 \, z + \sum_{n=0}^{\infty} (2v_{n+1} + u_n) \, z^{n+2}$$

et

$$s_{\mathbf{v}}(z) = \sum_{n=0}^{\infty} v_n\, z^n = v_0 + v_1\, z + \sum_{n=0}^{\infty} (u_{n+1} + v_n)\, z^{n+2}.$$

Ainsi,

$$s_{\mathbf{u}} = 1 + 2z\,(s_{\mathbf{v}} - v_0) + z^2\, s_{\mathbf{u}} = 1 + 2z\, s_{\mathbf{v}} + z^2\, s_{\mathbf{u}}$$

et

$$s_{\mathbf{v}} = z + z\,(s_{\mathbf{u}} - u_0) + z^2\, s_{\mathbf{v}} = z\, s_{\mathbf{u}} + z^2\, s_{\mathbf{v}}.$$

Il suffit à présent de résoudre le système de deux équations à deux inconnues en $s_{\mathbf{u}}$ et $s_{\mathbf{v}}$ pour trouver

$$s_{\mathbf{u}}(z) = \frac{1 - z^2}{1 - 4z^2 + z^4} \quad \text{et} \quad s_{\mathbf{v}}(z) = \frac{z}{1 - 4z^2 + z^4}.$$

Nous nous sommes ramenés à devoir développer en série de puissances deux fractions rationnelles indépendantes.

Bibliographie

[1] E. Bach, J. Shallit, *Algorithmic Number Theory*, Vol. 1, Foundations of Computing Series, MIT Press, (1996).

[2] J. Buchmann, *Introduction to cryptography*, Second edition, Undergraduate Texts in Mathematics, Springer, (2002).

[3] J.-M. De Koninck, A. Mercier, *Introduction à la théorie des nombres*, Collection universitaire de mathématiques, Modulo, Québec, (1994).

[4] P. Flajolet, R. Sedgewick, *An Introduction to the Analysis of Algorithms*, Addison Wesley, (1996).

[5] P. Flajolet, R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, (2009).

[6] R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete Mathematics, A foundation for computer science*, Second edition, Addison Wesley, (1994).

[7] B. Green, T. Tao, The primes contain arbitrarily long arithmetic progressions, *Annals of Math.* (2008), 56 pages.

[8] L. S. Hill, Concerning certain linear transformation apparatus of cryptography, *Amer. Math. Monthly* **38** (1931), 135–154.

[9] D. Khan, *The Codebreakers, the Story of Secret Writing*, Macmillan, 1967.

[10] N. Koblitz, *A course in Number Theory and Cryptography*, Graduate Texts in Mathematics **114**, Second edition, Springer, (1994).

[11] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computations in Mathematics **3**, Second edition, Springer, (1999).

[12] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Annals of Math.* **126** (1987), 649–673.

[13] S. Ling, C. Xing, *Coding Theory, a first course*, Cambridge University Press, (2004).

[14] G.E. Martin, *Counting: the art of enumerative combinatorics*, Undergraduate Texts in Mathematics, Springer, (2001).

[15] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, (1996).

[16] M. Mignotte, *Algèbre concrète, cours et exercices*, Collection CAPES/Agrégation, Ellipses, Paris, (2003).

[17] M. Mignotte, *Mathématiques pour le calcul formel*, Presses Universitaires de France, Paris, (1989).

[18] O. Pretzel, *Error-Correcting Codes and Finite Fields*, Oxford Applied Math. and Computing Science Series, Oxford Univ. Press, reprint (2000).

[19] K. H. Rosen (Editor), *Handbook of Discrete and Combinatorial Mathematics*, CRC Press (2000).

[20] A. Salomaa, *Public-Key Cryptography*, Second edition, Texts in Theoretical Computer Science, An EATCS Series, Springer, (1996).

[21] B. Schneier, *Cryptographie appliquée*, deuxième édition, International Thomson publishing France, Paris, (1997).

[22] L. Schwartz, *Algèbre 3ème année*, deuxième édition, Dunod, Paris, (2003).

[23] D. Stinson, *Cryptographie, Théorie et pratique*, International Thomson Publishing France, Paris, (1996).

[24] J. Talbot, D. Welsh, *Complexity and Cryptography, An Introduction*, Cambridge Univ. Press (2006).
[25] H. Wilf, *Generatingfunctionology*, Academic Press (1994).

Liste des figures

Index