CHAPITRE 2

PROTOCOLES REPOSANT SUR LE PROBLÈME DE LA FACTORISATION

Ce chapitre est consacré à la description de quelques cryptosystèmes dont la sécurité se base sur la difficulté de factoriser un entier naturel qui est le produit de deux (grands) nombres premiers. L'***artihmétique modulaire***, c'est à dire l'étude des quotients de $\mathbb{Z}$ est au coeur de toutes les constructions, l'interprète théorique principal étant le ***théorème des restes chinois***. Le cryptosystème ***RSA*** est l'un des plus célèbres protocoles cryptographiques reposant sur le problème de la factorisation ; une section entière lui est dédiée. Des questions de factorisation effective se prêtant à des application cryptographiques apparaissent également lorsque l'on s'intéresse aux carrés dans les anneaux $\mathbb{Z}/n\mathbb{Z}$. Les cryptosystèmes de ***Rabin*** et de ***Goldwasser-Micali***, faisant intervenir le ***symbole de Legendre***, en sont des illustrations.

2.1. Arithmétique modulaire

2.1.1. Le groupe $\mathbb{Z}/n\mathbb{Z}$ — On commence à s'interesser à la structure des quotients du groupe $\mathbb{Z}$. D'après la remarque 1.1.6, si H est un sous-groupe de $\mathbb{Z}$, alors $H = n\mathbb{Z}$, où l'entier n est univoquement déterminé. Deux entiers a et b sont ***congrus modulo n*** s'ils défiissent le même élément de $\mathbb{Z}/n\mathbb{Z}$, ce qui se traduit par la relation $n|a-b$, ou encore $a - b \in n\mathbb{Z}$. On écrit alors

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

L'élément

$$\bar{a} = a + n\mathbb{Z} = \{a + nm \mid m \in \mathbb{Z}\} \in \mathbb{Z}/n\mathbb{Z}$$

associé à a, i.e. l'ensemble des entiers qui sont congrus à a modulo n, est la ***classe (de congruence) de a modulo n***.

Proposition 2.1.1 — *Soit $n > 0$ un entier. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique, d'ordre n et il existe une bijection entre l'ensemble de ses sous-groupes et l'ensemble des diviseurs (positifs) de n.*

Démonstration — D'après le théorème 1.1.1, un entier est congru modulo n à un unique élément de l'ensemble $\{0, \dots, n-1\}$ et deux éléments distincts de ce dernier ne sont jamais congrus modulo n, ce qui implique que $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n. Il est cyclique, engendré par l'élément $\bar{1}$ (en effet, pour tout $x = \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, on a l'identité $x = a \cdot \bar{1}$). On a un homomorphisme surjectif canonique de groupes $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ défini par $f(a) = \bar{a}$ et la proposition A.2.9 affirme que f définit une bijection entre les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Il suffit alors d'appliquer la proposition 1.1.8. □

2.1.2. Groupes cycliques, le problème du logarithme discret (à rédiger) — Le groupe $\mathbb{Z}$ des entiers relatifs vérifie la propriété universelle suivante : étant donné un groupe G (pas nécessairement abélien) et un élément $g \in G$, il existe un unique homomorphisme de groupes $\exp_g : \mathbb{Z} \to G$ tel que $\exp_g(1) = g$. D'un point de vue explicite, on a l'identité

$$\exp_g(n) = g^n$$

pour tout $n \in \mathbb{Z}$. On rappelle que tel qu'il a été défini dans l'appendice, l'ordre de g est le cardinal du sous-groupe $\langle g \rangle$ de G qu'il engendre.

Proposition 2.1.2 — *Soient G un groupe et $g \in G$ un élément d'ordre fini n. Le groupe $\langle g \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, on a $g^m = 1$ si et seulement si n divise m.*

Démonstration — L'image de l'homomorphisme $\exp_g$ coïncide avec le sous-groupe $\langle g \rangle$ et le thórème d'isomorphisme pour les groupes affirme que ce dernier est isomorphe à $\mathbb{Z}/\ker(\exp_g)$. On a donc $\ker(\exp_g) = d\mathbb{Z}$, avec $d > 0$ univoquement déterminé (on ne peut avoir $d = 0$, sinon le groupe $\mathbb{Z}/\ker(\exp_g)$ serait d'ordre infini). En comparant les ordres, on obtient alors $d = n$. Finalement, on a l'identité $g^m = 1$ si et seulement si $m \in \ker(\exp_g) = n\mathbb{Z}$, ce qui se traduit par la relation $n|m$. □

Corollaire 2.1.3 — *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration — C'est un cas particulier du résultat précédent. □

2.1.3. L'anneau $\mathbb{Z}/n\mathbb{Z}$ — Dans ce chapitre, on s'intéresse au quotient de $\mathbb{Z}$ par rapport à un idéal $\mathfrak{a}$. L'anneau $\mathbb{Z}/0$ s'identifiant canoniquement avec $\mathbb{Z}$, on suppose $\mathfrak{a}$ non nul. D'après la proposition 1.1.5, on a alors $\mathfrak{a} = n\mathbb{Z}$, où l'entier $n > 0$ est univoquement déterminé.

Proposition 2.1.4 — *Soit $n > 0$ un entier. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n et il existe une bijection entre l'ensemble de ses idéaux et l'ensemble des diviseurs (positifs) de n.*

Démonstration — D'après le théorème 1.1.1, un entier est congru modulo n à un unique élément de l'ensemble $\{0,\dots,n-1\}$, d'où la première assertion. On a un homomorphisme surjectif canonique d'anneaux $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ défini par $f(a) = \bar{a}$ et la proposition A.3.4 affirme que f définit une bijection entre les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et les idéaux de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Il suffit alors d'appliquer la proposition 1.1.8. □

Dans la pratique, étant donné un élément de $\mathbb{Z}/n\mathbb{Z}$, on considère toujours son unique représentant dans l'ensemble $\{0,\dots,n-1\}$. Les opérations algébriques dans $\mathbb{Z}/n\mathbb{Z}$ (somme et produit) sont alors effectuées sur des entiers naturels inférieurs ou égaux à n. Au vu des résultats du chapitre précédent, la proposition ci-dessous est immédiate (l'élévation à la puissance m étant effectuée par exponentiation rapide, cf. le praragraphe 1.3.1).

Proposition 2.1.5 — *Les opérations de somme, de produit et d'élévation à la puissance $m > 0$ dans $\mathbb{Z}/n\mathbb{Z}$ sont de complexités respectives $O(\log(n)), O(\log^2(n))$ et $O(\log(m)\log^2(n))$.*

2.1.4. Le théorème des restes chinois — Le célèbre ***théorème des restes chinois*** est à la base de la conception pratique des cryptosystèmes présentés dans ce chapitre. Nous en présentons ici une version très générale. Étant donnés trois anneaux X, Y et S ainsi que deux homomorphismes d'anneaux $f : X \to S$ et $g : Y \to S$, l'ensemble

$$X \times_S Y = \{(x,y) \in X \times Y \mid f(x) = g(y)\}$$

est un sous-anneau de $X \times Y$ appelé ***produit fibré*** de X et Y au dessus de S.

Proposition 2.1.6 — *Étant donnés deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A, posons $\mathfrak{c} = \mathfrak{a} + \mathfrak{b}$ et considérons les anneaux $X = A/\mathfrak{a}$, $Y = A/\mathfrak{b}$ et $S = A/\mathfrak{c}$. On a alors des homomorphismes canoniques d'anneaux $f : X \to S$ et $g : Y \to S$. Avec ces hypothèses, l'anneau $X \times_S Y$ est isomorphe à $A/\mathfrak{a}\cap\mathfrak{b}$.*

Démonstration — On a un homomorphisme naturel d'anneaux $h : A \to X \times Y$ défini par $h(a) = (a+\mathfrak{a}, a+\mathfrak{b})$. Son image est contenue dans $X \times_S Y$. Étant donné $(x,y) \in X \times_S Y$, on a $x = a + \mathfrak{a}$ et $y = b + \mathfrak{b}$, avec $a, b \in A$. Par hypothèse, on a $a + \mathfrak{c} = b + \mathfrak{c}$, d'où l'existence de $a' \in \mathfrak{a}$ et $b' \in \mathfrak{b}$ tels que $a - b = a' - b'$. En posant $x = a - a' = b - b'$, on a alors les identités

$$h(x) = (x+\mathfrak{a}, x+\mathfrak{b}) = (a - a' + \mathfrak{a}, b - b' + \mathfrak{b}) = (a+\mathfrak{a}, b+\mathfrak{b}) = (x,y),$$

d'où l'inclusion $X \times_S Y \subset \mathrm{Im}(h)$, qui est alors une égalité. Le noyau de h coïncidant avec $\mathfrak{a}\cap\mathfrak{b}$, le théorème d'isomorphisme pour les anneaux permet de conclure. □

En généralisant la notion définie précédemment, nous dirons que deux éléments x et y de A sont ***congrus modulo*** un ideal $\mathfrak{a}$ s'ils définissent le même élément de $A/\mathfrak{a}$,

ce qui se traduit per la relation $x - y \in \mathfrak{a}$. On écrit alors

$$x \equiv y \pmod{\mathfrak{a}}.$$

De manière pratique, la démonstration du résultat ci dessus affirme qu'étant donnés deux éléments $a, b \in A$, le système de congruences

$$\begin{cases} x \equiv a \pmod{\mathfrak{a}}, \\ x \equiv b \pmod{\mathfrak{b}}, \end{cases}$$

admet une solution si et seulement si $a \equiv b \pmod{c}$, auquel cas elle est unique modulo $\mathfrak{a} \cap \mathfrak{c}$.

Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A sont ***étrangers*** si $\mathfrak{a} + \mathfrak{b} = A$, ce qui se traduit l'existence de deux éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$. On généralise ici la notion de coprimalité introduite dans le chapitre précédent pour $\mathbb{Z}$ et l'identité ci-dessus est l'analogue de l'identité de Bézout.

Lemme 2.1.7 — *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux étranger d'un anneau A alors on a l'identité $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.*

Démonstration — L'inclusion $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ étant immédiate, soit c un élément de $\mathfrak{a} \cap \mathfrak{b}$. Ayant fixé deux éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$, on obtient alors l'identité $c = ac + bc$. Les éléments ac et bc appartenant à l'idéal $\mathfrak{ab}$, il en est alors de même pour c, d'où l'inclusion $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$, qui est donc une egalité. □

Théorème 2.1.8 **(Théorème des restes chinois)** — *Étant donnés deux idéaux étrangers $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A, les anneaux $A/\mathfrak{ab}$ et $A/\mathfrak{a} \times A/\mathfrak{b}$ sont isomorphes.*

Démonstration — On reprend les notations de la proposition ci-dessus. Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ étant étrangers, l'anneau S est nul, ce qui implique que $X \times_S Y$ coïncide avec $X \times Y$, d'où un isomorphisme d'anneaux entre $A/\mathfrak{a} \cap \mathfrak{b}$ et $X \times Y$. Le dernier lemme permet de conclure. □

Ce dernier résultat affirme que le système de congruences présenté précédemment admet toujours une solution, qui est unique modulo $\mathfrak{ab}$. Cette dernière peut être explicitée de la manière suivante : étant donnés $a' \in \mathfrak{a}$ et $b' \in \mathfrak{b}$ tels que $a' + b' = 1$, il suffit de poser $x = ab' + a'b$.

Corollaire 2.1.9 — *Si n et m sont deux entiers premiers entre eux alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.*

Démonstration — C'est un cas particulier du dernier résultat, en remrquant que les idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$ sont étrangers si et seulement si les entiers n et m sont premiers entre eux □

2.1.5. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et la fonction indicatrice d'Euler — Commençons ce paragraphe en remarquant que le pgcd de deux entiers a et n ne dépend que de la classe de congruence de a modulo n. En particulier, nous pouvons écrire sans ambiguïté $x \wedge n$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 2.1.10 — *Étant donné un élément $x \in \mathbb{Z}/n\mathbb{Z}$, les conditions suivantes sont équivalente :*

1. *On a $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.*
2. *L'élément x est un générateur du groupe (additif) $\mathbb{Z}/n\mathbb{Z}$.*
3. *On a l'identité $x \wedge n = 1$.*

Démonstration — Montrons les implications (1)⇒(2)⇒(3)⇒(1).
(1)⇒(2) Tout d'abord, le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par la classe $\bar{1}$. Par hypothèse, il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy = \bar{1}$. En posant $y = \bar{u}$, avec $u \in \mathbb{N}$, on obtient les identités

$$ux = x + \cdots (u) \cdots + x = \bar{1}.$$

En particulier, l'élément $\bar{1}$ appartient au sous-groupe $\langle x \rangle$ de $\mathbb{Z}/n\mathbb{Z}$ engendré par x, d'où $\langle x \rangle = \mathbb{Z}/n\mathbb{Z}$.
(2)⇒(3) Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant engendré par x, il existe un entier (naturel) u tel que $ux = \bar{1}$. En posant $x = \bar{a}$, avec $a \in \mathbb{Z}$, on obtient la congruence $ua \equiv 1 \pmod{n}$, ce qui se traduit par l'existence d'un entier v tel que $ua + vn = 1$, d'où les identités $(x, n) = (a, n) = 1$.
(3)⇒(1) En posant $x = \bar{a}$, avec $a \in \mathbb{Z}$, il existe un couple d'entiers u et v tels que $au + nv = 1$, d'où l'identité $xy = 1$, avec $y = \bar{u}$ et, par suite, la relation $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Proposition 2.1.11 — *Le calcul de l'inverse d'un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est de complexité $O(\log^2(n))$.*

Démonstration — Un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est représenté par un entier $a \in \{0, \ldots, n-1\}$ tel que $(a, n) = 1$. La détermination de son inverse se réduit à l'explicitation d'une identité de Bézout $au + nv = 1$, ce qui peur être fait via l'algorithme d'Euclide étendu, avec une complexité de $O(\log^2(n))$.

□

La ***fonction indicatrice d'Euler*** est l'application φ qui associe à un entier $n > 0$ le nombre d'entiers $m \in \{0, \ldots, n-1\}$ premiers avec n. Les premières valeurs de φ sont reportées dans le tableau ci-dessous.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Proposition 2.1.12 — *La fonction indicatrice d'Euler vérifie les propriétés suivantes :*

1. *Pour tout entier $n > 0$, le groupe $(Z/n\mathbb{Z})^\times$ est d'ordre $\varphi(n)$.*
2. *Étant donnés deux enties naturels $n, m > 0$ premiers entre eux, on a l'identité*
$$\varphi(nm) = \varphi(n)\varphi(m).$$
3. *Pour tout nombre premier p et tout entier $e > 0$, on a la relation*
$$\varphi(p^e) = p^{e-1}(p-1).$$

Démonstration — La première assertion découle directement de la proposition 2.1.10 et du fait que tout élément de $\mathbb{Z}/n\mathbb{Z}$ possède un unique représentant dans l'ensemble $\{0, \ldots, n-1\}$. Le théorème des restes chinois affirme que les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes, ce qui implique que les groupes $(\mathbb{Z}/nm\mathbb{Z})^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ sont isomorphes et en comparant leurs ordres on obtient le deuxième point. Finalement, les entiers de l'ensemble $\{0, \ldots, p^e - 1\}$ qui ne sont pas premiers avec p^e sont ceux qui sont divisibles par p ; ils s'écrivent alors comme pa, avec $a \in \{0, \ldots, p^{e-1} - 1\}$ et il en existe donc p^{e-1}, d'où la troisième affirmation. □

Ce dernier résultat permet de calculer explicitement $\varphi(n)$ lorsque l'on connaît la factorisation de n .

Corollaire 2.1.13 — *Pour tout entier n, on a l'identité*
$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$
où p parcourt l'ensemble des nombres premiers divisant n.

Démonstration — En remarquant que l'identité 3 de la proposition précédente peut s'écrire comme
$$\varphi\left(p^e\right) = p^e \left(1 - \frac{1}{p}\right),$$
il suffit d'utiliser la multiplicativité de la fonction indicatrice d'Euler. □

Exercice 2.1.14 — Notons $\omega(n)$ le nombre de diviseurs premiers d'un entier $n > 0$ (comptés sans multiplicité). Montrer que l'on a les inégalités
$$\varphi(n) \geq \frac{n}{\omega(n)+1} \geq \frac{n}{\log_2(n)+1}.$$

Tel qu'il a été défini dans l'appendice, l'ordre d'un élément g d'un groupe fini G est le cardinal du sous-groupe $\langle g \rangle$ qu'il engendre.

Lemme 2.1.15 — *Soit G un groupe fini. L'ordre d'un élément $g \in G$ est le plus petit entier $d > 0$ tel que $g^d = 1$. En particulier, on a l'identité $g^{|G|} = 1$.*

Démonstration — L'application $f : \mathbb{Z} \to G$ définie par $f(n) = g^n$ est un homomorphisme de groupes. Son image coïncidant avec $\langle g \rangle$, on en déduit un isomorphisme entre les groupes $\mathbb{Z}/\ker(f)$ et $\langle g \rangle$. Le sous-groupe

$$\ker(f) = \{n \in \mathbb{Z} \mid g^n = 1\}$$

n'est pas trivial (sinon f serait injectif, ce qui est exclu, car G est fini). On remarquera que dans $\mathbb{Z}$, la notion d'idéal et de sous-groupe (par rapport à la somme) coïncident. D'après la démonstration du théorème 1.1.1, on a alors $\ker(f) = d\mathbb{Z}$, où d est le plus petit élément strictement positif de $\ker(f)$, i.e. le plus petit entier naturel non d nul tel que $g^d = 1$. La dernière assertion découle du théorème de Lagrange : en effet, l'ordre d du sous-groupe $\langle g \rangle$ divise $|G|$ et, en posant $|G| = dn$, on obtient les identités

$$g^{|G|} = g^{dn} = (g^d)^n = 1^n = 1.$$

□

Remarque 2.1.16 — Lorsque G est abélien, la dernière identité du lemme peut être obtenue de manière directe : en effet, le groupe G étant abélien, l'élément $x = \prod_{h \in G} h$ est bien défini. Pour tout $g \in G$, l'application $f : G \to G$ définie par $f(h) = gh$ est bijective. On a alors les identités

$$1 = xx^{-1} = x^{-1} \prod_{h \in G} h = x^{-1} \prod_{h \in G} gh = x^{-1} g^{|G|} \prod_{h \in G} h = g^{|G|} x x^{-1} = g^{|G|}.$$

Exercice 2.1.17 — Montrer qu'un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et possède $\varphi(n)$ générateurs.

Le résultat suivant est un ingrédient fondamental dans la conception du cryptosystème RSA.

***Théorème 2.1.18* (Euler)** — *Soit $n > 0$ un entier. Pour tout entier a premier avec n, on a la congruence*

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

Démonstration — En posant $x = \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, la congruence de l'énoncé se traduit par l'identité $x^{\varphi(n)} = 1$ et découle directement du lemme 2.1.15 appliqué au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Exercice 2.1.19 — Soient $a > 1$ et $n > 0$ deux entiers. Montrer que n divise $\varphi(a^n - 1)$.

Proposition 2.1.20 — *Pour tout nombre entier $n > 1$, on a l'inégalité $\varphi(n) \leq n-1$ et les conditions suivantes sont équivalentes :*

1. *On a l'égalité $\varphi(n) = n - 1$.*
2. *L'entier n est un nombre premier.*
3. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Démonstration — Pour $n > 1$, les entiers 0 et n ne sont pas premiers entre eux, ce qui implique qu'il existe au plus $n-1$ éléments de l'ensemble $\{0, \ldots, n-1\}$ premiers avec n.

Montrons les implications (1)⇒(2)⇒(3)⇒(1). Si $\varphi(n) = n-1$, tout entier non nul $1 < m < n$ est premier avec n (et, en particulier, $m \not| n$), d'où la primalité de n. Si l'entier n est premier, la proposition 1.1.16 affirme que l'idéal $n\mathbb{Z}$ est maximal, ou encore que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps (cf. l'appendice). Finalement, si cette dernière condition est remplie, d'après le premier point de la proposition 2.1.12, l'entier $\varphi(n)$ est l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} - \{0\}$, d'où $\varphi(n) = n-1$. □

Dans la suite, adoptant une convention usuelle, étant donné un nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$.

Corollaire 2.1.21 **(Petit théorème de Fermat)** — *Pour tout $x \in \mathbb{F}_p$, on a l'identité $x^p = x$.*

Démonstration — L'assertion est immédiate pour $x = 0$. Pour $x \neq 0$, on a $x \in \mathbb{F}_p^\times$ (car $\mathbb{F}_p$ est un corps). D'après le théorème 2.1.18 et le lemme ci-dessus, on a l'identité $x^{p-1} = 1$, d'où la relation $x^p = x$. □

Remarque 2.1.22 — Ayant déterminé $\varphi(n)$ (ce qui est immédiat lorsque n est premier), le calcul de l'inverse d'un élémet de $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ peut être calculé en utilisant le théorème 2.1.18, qui amène à l'identité

$$x^{-1} = x^{\varphi(n)-1}.$$

La multiplication dans $\mathbb{Z}/n\mathbb{Z}$ étant de complexité $O(\log^2(n))$, par exponentiation rapide, on obtient un algorithme de calcul de l'inverse de complexité $O(\log^3(n))$.

2.2. Le cryptosystème RSA

2.2.1. Cryptosystèmes à clé publique — La cryptographie à clé publique est apparue en 1976 avec les travaux de Withfield Diffie et Martin Hellman. Un ***cryptosystème à clé publique***, également appelé ***cryptosystème asymétrique***, repose sur l'existence d'une ***clé publique*** pour le chiffrement, et d'une ***clé secrète*** pour le déchiffrement. Ces deux clés sont distinctes. Un utilisateur A qui souhaite envoyer un message à un utilisateur B, chiffre son message au moyen de la clé publique de B, et ce dernier au moyen de sa clé secrète, qu'il est seul à connaître, est alors en mesure de déchiffrer le message envoyé. Deux utilisateurs d'un cryptosystème à clé publique peuvent donc s'échanger des messages chiffrés, via un canal non sécurisé, et sans posséder de secret en commun. Son efficacité est basée sur le fait qu'il est impossible en un temps raisonnable de déterminer la clé secrète à partir de la clé publique.

2.2.2. Principe du protocole — Le protocole RSA est un cryptosystème à clé publique introduit en 1977 par Leonardo Adleman, Ronald Rivest et Adi Shamir. Sa sécurité repose sur le fait que connaissant un entier n, qui est le produit de deux grands nombre premiers p et q distincts, il est généralement très difficile, voire impossible pratiquement, de déterminer p et q, i.e. la factorisation de n. D'un point de vue théorique, le protocole repose sur le résultat suivant, qui est une conséquence du petit théorème de Fermat (cf. corollaire 2.1.21).

Proposition 2.2.1 — *Soient p et q deux nombres premiers distincts et posons $n = pq$. Pour tout entier naturel t congru à 1 modulo $\varphi(n)$ et tout élément $x \in \mathbb{Z}/n\mathbb{Z}$, on a l'identité $x^t = x$.*

Démonstration — D'après le théorème des restes chinois, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_q$. Il suffit donc de vérifier l'identité $x^t = x$ pour tout $x \in \mathbb{F}_p$ et tout $x \in \mathbb{F}_q$. L'assertion étant immédiate pour $x = 0$, supposons $x \in \mathbb{F}_p$ non nul. Par hypothèse, on a $t = k\varphi(n) + 1$, avec $k \in \mathbb{N}$, et la multiplicativité de la fonction indicatrice d'Euler amène à l'expression $\varphi(n) = (p-1)(q-1)$, d'où les identités

$$x^t = x^{1+k\varphi(n)} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{p-1})^{k(q-1)} = x,$$

la dernière égalité découlant du théorème 2.1.18 ou du corollaire 2.1.21. □

Nous pouvons maintenant décrire le protocole. Chaque utilisateur procède de la façon suivante :

- Il choisit deux nombres premiers p et q et determine ensuite les entier $n = pq$ et $\varphi(n) = (p-1)(q-1)$.
- Il choisit un entier e premier avec $\varphi(n)$ tel que $1 < e < \varphi(n)$. La classe de e modulo $\varphi(n)$ est donc inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$.
- Il détermine l'entier d tel que $1 < d < \varphi(n)$ et $ed \equiv 1 \mod \varphi(n)$. La classe de d modulo $\varphi(n)$ est donc l'inverse de la classe de e dans $\big(\mathbb{Z}/\varphi(n)\mathbb{Z}\big)^\times$.
- Il publie ensuite le couple (e, n), qui est sa ***clé publique***, et il conserve secret l'élément d, qui est sa ***clé secrète*** ou ***privée***.

Soit A un utilisateur dont la clé publique est (e, n) et la clé secrète est d. L'***algorithme de chiffrement*** de A est l'application $f_A : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie pour tout $x \in \mathbb{Z}/n\mathbb{Z}$ par $f_A(x) = x^e$. C'est une bijection de $\mathbb{Z}/n\mathbb{Z}$ et d'après la proposition 2.2.1, on a $f_A^{-1}(x) = x^d$. On dit que f_A^{-1} est l'***algorithme de déchiffrement*** de A et l'élément x^e est appelé ***cryptogramme***. Si une personne B souhaite envoyer un message secret à A sous la forme d'un élément $x_0 \in \mathbb{Z}/n\mathbb{Z}$, il utilise la clé publique de A en lui envoyant l'élément $f_A(x_0)$. Afin d'obtenir x_0, il suffit alors pour A d'utiliser sa clé secrète en calculant $f_A^{-1}(x_0^e)$.

Exemple 2.2.2 — Prenons $(e, n) = (239, 406121)$ comme clé publique. On a $n = pq$ avec $p = 101$ et $q = 4021$. Il est facile de vérifier que p et q sont premiers (si q n'était

pas premier il devrait posséder un diviseur premier plus petit que $63 = \lfloor\sqrt{4021}\rfloor$, et ce n'est pas le cas). On obtient

$$\varphi(n) = 100 \cdot 4020 = 402000.$$

Afin de déterminer la clé secrète, il s'agit de calculer l'inverse de 239 modulo 402000. On utilise l'algorithme d'Euclide. Avec la présentation adoptée de cet algorithme, on obtient le tableau suivant :

	1682	119	2	
402000	239	2	1	0
1	0	1	-119	
0	1	-1682	200159	

La clé secrète est donc $d = 200159$.

2.2.3. Signature — L'algorithme RSA fournit un moyen de signer, ou d'authentifier, les messages. Soit A un utilisateur ayant pour clé publique (e, n) et pour clé secrète d. Supposons que A souhaite envoyer à B un message $x \in \mathbb{Z}/n\mathbb{Z}$, sans se préoccuper de sa confidentialité, mais de sorte que B soit certain que c'est bien A qui lui a transmis x. Pour cela, A envoie à B le couple

$$(x, x^d) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Avec la clé publique (e, n), B calcule alors

$$(x^d)^e = x^{de} = x.$$

Puisque A est seul à connaître d, B peut être a priori certain que c'est bien A l'expéditeur du message.

2.2.4. Cryptanalyse — Pour qu'un cryptosystème soit utilisable dans la pratique, il est nécessaire que le chiffrement et de déchiffrement (connaissant la clé secrète) puissent être effectués en un temps raisonnable. Idéalement, on souhaite que ces algorithmes soient en temps polynomial par rapport à la taille des clés. Dans la suite de se paragraphe, on fixe deux nombres premiers distincts p et q et l'on pose $n = pq$.

Proposition 2.2.3 — *Les algorithmes de chiffrement et de déchiffrement du protocole RSA utilisant un entier $n = pq$ sont de complexité $O(\log^3(n))$.*

Démonstration — Le chiffrement, ainsi que le déchiffrement sont juste des calculs de puissances dans $\mathbb{Z}/n\mathbb{Z}$. L'exposant étant inférieur à n, la proposition 2.1.5 affirme que la complexité est $O(\log^3(n))$. □

Remarque 2.2.4 — Il est également important de s'intéresser à la complexité de la mise en place du protocole lui-même. La clé publique est généralement choisie par un processus aléatoire. La détermination de la clé privée, qui se réduit au calcul de l'inverse de la clé publlique nodulo $\varphi(n)$, est de complexité $O(\log^2(n))$ (la complexité

est en fait dominée par la fonction $\log^2(\varphi(n)$, cette dernièrer étant elle-même dominée par $\log^2(n)$). Il ne reste qu'à déterminer une méthode efficace et rapide de construction des nombres premiers p et q. Cette question est cruciale en cryptographie, que ce soit d'un point de vue thérique ou pratique. Les contraintes de temps imposées à ce cours ne nous permettent malheureusement pas d'aborder ce sujet.

Considérons et une clé publique (e, n) utilisée lors d'un protocole RSA et notons d la cé secrète correspondante. Une personne souhaitant retrouver le message initial à partir de son cryptogramme peut commencer par essayer d'évaluer $\varphi(n)$, la clé secrète étant alors obtenue rapidement via l'algotithme d'Euclide. Cette démarche n'est pas très efficace. Le résultat suivant montre en effet que la connaissance de $\varphi(n)$ permet d'obtenir la factorisation de n par un algorithme de complexité polynomiale, là où le cryptosystème RSA repose justement sur la difficulté d'obtenir une telle factorisation (en un temps raisonnable).

Lemme 2.2.5 — *Connaisant n et $\varphi(n)$, il existe un algorithme de complexité $O(\log^3(n))$ permettant de déterminer p et q.*

Démonstration — Quitte à permuter p et q, on se réduit au cas $q < p$. Connaissant n et $\varphi(n)$, les entiers naturels

$$m = n - \varphi(n) + 1 = p + q \quad \text{et} \quad \Delta = m^2 - 4n = (p - q)^2$$

sont déterminés avec des algorithmes de complexités respectives $O(\log(n))$ (deux sommes) et $O(\log^2(n))$. En utilisant l'algorithme présenté dans le chapitre précédent, l'extraction de la racine carrée de Δ est de complexité $O(\log^3(n))$. L'identité

$$2p = m + \sqrt{\Delta}$$

Permet d'obtenir p en effectuant une somme et une division par 2 (un décalage à droite, en termes d'opérations sur les bits), pour une complexité de $O(\log(n))$. Globalement, cet algorithme de factorisation est donc de complexité $O(\log^3(n))$. □

Remarque 2.2.6 — Lors d'un protocole RSA, il est primordial de vérifier que le message x à envoyer soit premier avec n. En effet, dans la pratique, x ainsi que le cryptogramme $z = x^e$ sont représentés par des entiers naturels non nuls et strictement inférieurs à n. Si x et n n'étaient pas premiers entre eux, il en serait de même pour z et n. Leur pgcd, déterminé rapidement par l'algorithme d'Euclide, fournirait alors un diviseur non trivial de n, ce qui permettrait d'obtenir la factorisation de n et de déchiffrer ainsi tout cryptogramme. Ceci étant, lors d'une implémentation effective du protocole, la probabilité de tomber sur un élément x qui ne soit pas premier avec n est pratiquement nulle. En effet, en posant $n = pq$, avec $p < q$, on a les relations

$$\frac{\varphi(n)}{n} = 1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{n} > 1 - \frac{2}{p}.$$

En particulier, si p est un nombre premier de 1024 bits, la probabilité qu'un entier $m < n$ pris au hasard ne soit pas premier avec n est inférieure à 2^{-1023}.

Il faut remarquer que, bien que suffisante, la connaissance de $\varphi(n)$ n'est pas vraiment indispensable pour pouvoir déchiffrer un message. Il est en fait suffisant de déterminer un entier r tel que $x^{er} = x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 2.2.7 — *Posons $m = (p-1) \vee (q-1)$. Pour tout entier $u > 0$, les conditions suivantes sont équivalentes :*

1. *$x^u = x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.*
2. *$u \equiv 1 \pmod{m}$.*

Démonstration — D'après le théorème des restes chinois, le groupe $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_q$. La première condition est donc équivalente à $x^u = x$ pour tout $x \in \mathbb{F}_p$ et tout $x \in \mathbb{F}_q$. Soit $x \in \mathbb{F}_q$. Pour $x = 0$ on a toujours $x^u = x$. On peut donc se réduire au cas $x \in \mathbb{F}_p^\times$. La condition $x^u = x$ est alors équivalente à $x^{u-1} = 1$. Nous admettons ici le fait que le groupe $\mathbb{F}_p^\times$ est cyclique, d'ordre $p-1$ (ce résulat sera démontré dans le chapitre 3). Dans cette dernière condition, on peut alors se restreindre au cas où x est un générateur du groupe, auquel cas elle est vérifiée si et seulement si $p-1$ divise $u-1$. En procédant de manière analogue pour $\mathbb{F}_q$ on en déduit que la première condition de la proposition est équivalente à $p-1|u-1$ et $q-1|u-1$, ce qui se traduit par $m|u-1$. □

Corollaire 2.2.8 — *En posant $t = (p-1) \wedge (q-1)$, il existe t entiers r dans l'intervalle $[1, \varphi(n)[$ tels que $x^{er} = x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.*

Démonstration — D'après la proposition 2.2.7, la condition du corollaire est équivalente à $er \equiv 1 \pmod{m}$, qui admet une unique solution $r_0 \in \{1, \ldots, m-1\}$. On en déduit que r appartient à l'ensemble $\{r_0, r_0 + m, \ldots, r_0 + (t-1)m\}$, qui est de cardinal t. □

Un entier $r \in \{1, \ldots, \varphi(n) - 1\}$ vérifiant la condition du lemme est appelé ***clé de déchiffrement***. Lors du choix des nombres premiers p et q il est préférable de vérifier que le pgcd de $p-1$ et $q-1$ est petit, afin d'éviter l'existence de nombreuses clés de déchiffrement. L'existence de plusieurs clés de déchiffrement constitue également une faille dans la procédure de signature d'un message. En effet, elle permet juste d'affirmer que l'expéditeur possède une clé de déchiffrement, qui peut être différente de la clé secrète. Ceci dit, le nombre de clés de déchiffrement est majoré par $\sqrt{n} - 1$, et la probabilité d'en obtenir une de manière aléatoire est pratiquement nulle lorsque n est grand.

Exemples 2.2.9 —

1. Reprenons les valeurs $p = 101$ et $q = 4021$ de l'exemple précédent. Un simple calcul montre que $100 \wedge 4020 = 20$. Il existe donc 20 clés de déchiffrement, données explicitement par la formule $19259 + 20100k$, avec $k \in \{0, \ldots, 19\}$. La clé secrète est obtenue pour $k = 9$.
2. Si les nombres premiers p et q sont impairs (ce qui est toujours le cas dans la pratique), il existe toujours au moins deux clés de déchiffrement. Il en existe exactement deux si et seulement si $\frac{p-1}{2}$ et $\frac{q-1}{2}$ sont premiers entre eux. Tel est le cas par exemple si $p = 2p' + 1$ et $q = 2q' + 1$ avec p' et q' premiers. En supposant $p < q$, le nombre de clés de déchiffrement est maximal lorsque $p - 1$ divise $q - 1$, auquel cas il en existe exactement $p - 1$.

Exercice 2.2.10 — Afin d'utiliser le protocole RSA, Alice choisit les nombres premiers $p = 101$ et $q = 131$. Elle transmet ensuite la clé publique $(3901, 13231)$. Elle réalise assez vite que son choix était très mauvais. Pourquoi ?

2.3. Symbole de Legendre et carrés dans $\mathbb{Z}/n\mathbb{Z}$

2.3.1. Le symbole de Legendre — Dans la suite $p > 2$ désigne un nombre premier. Étant donné un entier n, le ***symbole de Legendre*** $(\frac{n}{p})$ est l'entier défini par la relation

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } p|n, \\ 1 \text{ si } p\not|n \text{ et n est un carré modulo } p, \\ -1 \text{ sinon.} \end{cases}$$

Un entier n tel que $(\frac{n}{p}) = 1$ est appelé ***résidu quadratique***. Si $(\frac{n}{p}) = -1$, on parle de ***non-résidu quadratique***. Par définition, le symbole de Legendre $(\frac{n}{p})$ ne dépend que de la classe de n modulo p. En effectuant une division euclidienne, on peut donc toujours se réduire au cas $0 \leq n < p$. De plus, étant donné $x \in \mathbb{F}_p$, on peut écrire $(\frac{x}{p})$ sans ambiguité. Notons $(\mathbb{F}_p^\times)^2$ le sous-groupe des carrés de $\mathbb{F}_p^\times$, i.e. l'image de l'homomorphisme $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ d'élévation au carré. On a alors $(\frac{x}{p}) = 1$ si et seulement si $x \in (\mathbb{F}_p^\times)^2$. Avec un légér abus de langage, les éléments de $(\mathbb{F}_p^\times)^2$ seront également appelés résidus quadratiques. Le résultat ci-dessous affirme que la moitié des éléments de $\mathbb{F}_p^\times$ sont des résidus quadratiques.

Lemme 2.3.1 — *Le groupe $(\mathbb{F}_p^\times)^2$ est d'ordre $(p-1)/2$.*

Démonstration — Le noyau de l'homomorphisme $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ d'élévation au carré étant le sous-groupe $\mu_2 = \{\pm 1\}$, le théorème d'isomorphisme pour les groupes affirme que son image, qui n'est autre que $(\mathbb{F}_p^\times)^2$, est d'ordre $(p-1)/2$. □

Théorème 2.3.2 **(Euler)** — *On a la congruence*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

Démonstration — L'assertion étant claire pour $x = 0$, supposons x non nul. Considérons l'homomorphisme de groupes $g : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ défini par $g(x) = x^{(p-1)/2}$. On doit montrer que pour tout $x \in \mathbb{F}_p$, on a l'identité $g(x) = \left(\frac{x}{p}\right)$. Les relations $g(x)^2 = x^{p-1} = 1$ impliquent que l'image de g est contenue dans le sous-groupe $\mu_2 = \{\pm 1\}$ de $\mathbb{F}_p^\times$. En admettant une fois encore que le groupe $\mathbb{F}_p^\times$ est cyclique et en fixant un de ses générateurs t, on a nécessairement $g(t) \neq 1$, ce qui implique que l'image de g coïncide avec μ_2 et, par suite, que $\ker(g)$ est d'ordre $(p-1)/2$. Par ailleurs le lemme 2.1.15 amène à l'inclusion $(\mathbb{F}_p^\times)^2 \subset \ker(g)$, qui est alors une égalité (il suffit de comparer les ordres). On a donc $(\frac{x}{p}) = 1$ (resp. $(\frac{x}{p}) = -1$) si et seulement si $g(x) = 1$ (resp. $g(x) = -1$), d'où $g(x) = (\frac{x}{p})$ pour tout $x \in \mathbb{F}_p^\times$. □

Remarque 2.3.3 — Les classes des entiers $0, 1$ et -1 modulo p étant deux à deux distinctes, le symbole de Legendre est univoquement déterminé par sa classe modulo p. En particulier, le théorème 2.3.2 fournit une méthode de calcul effectif de $(\frac{n}{p})$.

Corollaire 2.3.4 — *Étant donnés un nombre premier $p > 2$ et deux entiers n et m, on a l'identité*

$$\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right).$$

Démonstration — D'après le théorème 2.3.2, on a les congruences

$$\left(\frac{nm}{p}\right) \equiv (nm)^{\frac{p-1}{2}} \equiv n^{\frac{p-1}{2}} m^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \pmod{p},$$

ce qui implique que l'entier $a = (\frac{nm}{p}) - (\frac{n}{p})(\frac{m}{p})$ est divisible par p. Les inégalité $|a| \leq 2 < p$ amènent alors à l'identité $a = 0$. □

Corollaire 2.3.5 — *Pour tout nombre premier $p > 2$, on a l'identité*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

En particulier, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p est congru à 1 modulo 4.

Démonstration — On procède exactement comme dans la démonstration du corollaire 2.3.4. □

Proposition 2.3.6 — *Étant donnés un nombre premier $p > 2$ et un entier naturel $n < p$, le calcul du symbole de Legendre $(\frac{n}{p})$ est de complexité $O(\log^3(p))$.*

Démonstration — D'après la remarque 2.3.3, il suffit de déterminer la classe de $(\frac{n}{p})$ modulo p. Le théorème 2.3.2 affirme que ceci revient à calculer $\bar{n}^{(p-1)/2}$ dans $\mathbb{F}_p$. La multiplication dans $\mathbb{F}_p$ étant de complexité $O(\log^2(p))$, en utilisant l'algorithme d'exponentiation rapide, on obtient une méthode de calcul du symbole de Legendre de complexité de $O(\log^3(p))$. □

Remarque 2.3.7 — En utilisant la ***loi de réciprocité quadratique*** pour le le ***symbole de Jacobi***, on obtient un algorithme de calcul de $(\frac{n}{p})$ de complexité $O(\log^2(p))$ (cf. le complément à ce chapitre).

2.3.2. Extraction de racines carrées dans $\mathbb{F}_p$ — Soit $p > 2$ un nombre premier. Du moment où l'on sait qu'un élément $x \in \mathbb{F}_p^\times$ est un carré, il est nécessaire de déterminer un algorithme de calcul de ses (deux) racines carrées. Dans ce cours, nous ne traiterons explicitement que le cas où p est congru à 3 modulo 4, qui est particulièrement simple. Dans le cas général, on dispose de méthodes efficaces, telles que l'algorithme de ***Cipolla***, ou celui de ***Tonelli-Shanks***, qui nécessitent néanmoins la connaissance d'un non-résidu quadratique de $\mathbb{F}_p^\times$.

Proposition 2.3.8 — *Soit $x \in \mathbb{F}_p^\times$ un résidu quadratique. Si p est congru à 3 modulo 4 alors l'élément*

$$y = x^{\frac{p+1}{4}}$$

est une racine carrée de x (l'autre étant égale à $-x$).

Démonstration — En s'appuyant sur le corollaire 2.3.2, on a les identités

$$y^2 = x^{\frac{p+1}{2}} = x \cdot x^{\frac{p-1}{2}} = x\left(\frac{x}{p}\right) = x.$$

□

Corollaire 2.3.9 — *Pour p congru à 3 modulo 4, l'extraction de racines carrées dans $\mathbb{F}_p$ est de complexité $O(\log^3(p))$.*

Démonstration — Il suffit d'appliquer la proposition précédente en utilisant l'algorithme d'exponentiation rapide. □

2.3.3. Carrés dans $\mathbb{Z}/n\mathbb{Z}$ — Au vu des applications en cryptographie, nous n'étudierons les carrés et les méthodes d'extraction de racines carrés dans $\mathbb{Z}/n\mathbb{Z}$ que dans le cas particulier où $n = pq$ est le produit de deux nombres premiers impairs $p \neq q$, qui sont fixés une fois pour toutes. Comme pour $\mathbb{F}_p$, un carré de $(\mathbb{Z}/n\mathbb{Z})^\times$ est appelé résidu quadratique. Étant donné un groupe abélien G, on note $G[2]$ le ***sous-groupe de 2-torsion***, formé par les éléments $g \in G$ tels que $g^2 = 1$.

Lemme 2.3.10 — *Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times[2]$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Démonstration — Étant donnés deux groupes G et H, on montre facilement que l'identité $(G \times H)[2] = G[2] \times H[2]$. Le lemme découle alors du théorème des restes chinois, qui affirme que $(\mathbb{Z}/n\mathbb{Z})^\times$ est isomorphe à $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$, et du fait que les groupes $\mathbb{F}_p^\times[2]$ et $\mathbb{F}_q^\times[2]$ sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$. □

Corollaire 2.3.11 — *Un résidu quadratique de $(\mathbb{Z}/n\mathbb{Z})^\times$ possède 4 racines carrées.*

Démonstration — Soit $x = y^2$ un carré de $(\mathbb{Z}/n\mathbb{Z})^\times$. Un élément $z \in (\mathbb{Z}/n\mathbb{Z})^\times$ est une racine carrée de x si et seulement si $z^{-1}y$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times[2]$. Il suffit alors d'appliquer le lemme ci-dessus. □

Proposition 2.3.12 — *On a les propriétés suivantes :*

1. *Le sous-groupe des carrés de $(\mathbb{Z}/n\mathbb{Z})^\times$ est d'ordre $\frac{1}{4}\varphi(n)$.*
2. *Un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est un carré si et seulement si $(\frac{x}{p}) = (\frac{x}{q}) = 1$.*

Démonstration — L'élévation au carré définit un endomorphisme $(\mathbb{Z}/n\mathbb{Z})^\times$ ayant pour image le sous-groupe des carrés et pour noyau le groupe $(\mathbb{Z}/n\mathbb{Z})^\times[2]$. Le point 1 découle alors du théorème d'isomorphisme pour les groupes et du lemme 2.3.10. Le théorème des restes chinois implique que l'homomorphisme canonique $f : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ est un isomorphisme. Un élément $(x, y) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ étant un carré si et seulement s'il en est de même pour x et y, on obtient le point 2. □

Le ***problème de la résidualité quadratique***[1] consiste à déterminer si un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est un résidu quadratique. Si l'on connaît la factorisation de n, le point 2 de la proposition 2.3.12 réduit la question au simple calcul de deux symboles de Legendre, ce qui peut être effectué par un algorithme de complexité $O(\log^3(n))$. Par contre, lorsque la factorisation de n n'est pas connue, on ne dispose pas d'algorithme de complexité polynomiale permettant de résoudre le problème. De nombreux protocoles cryptographiques se basent sur cette dichotomie. On retrouve une situation analogue lorsque l'on s'intéresse au problème d'extraction de racines carrées d'un résidu quadratique x de $\mathbb{Z}/n\mathbb{Z}$: si l'on connaît p et q, en appliquant les méthodes décrites dans les paragraphes précédents, on détermine facilement les racines carrées de x dans $\mathbb{F}_p$ et $\mathbb{F}_q$. Une identité de Bézout permet alors d'en déduire ses racines carrées dans $\mathbb{Z}/n\mathbb{Z}$. Si, par contre, on ne connaît pas la factorisation de n, la détermination des racines carrées de x est un problème difficile, équivalent à la factorisation de n, comme le montre le résultat ci-dessous.

Proposition 2.3.13 — *La connaissance de* 3 *racines carrées d'un résidu quadratique de $(\mathbb{Z}/n\mathbb{Z})^\times$ permet d'obtenir la factorisation de n par un algorithme de complexité $O(\log^2(n))$.*

Démonstration — Si $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est une racine carrée d'un résidu quadratique, il en est de même pour $-x$. Soit $y \neq \pm x$ une troisième racine carrée. On obtient alors l'identité $(x - y)(x + y) = 0$. L'entier $d = (x - y, n)$ est différent de 1 (dans le cas contraire, on aurait $y = -x$) et de n (autrement, on obtiendrait $y = x$). On a donc $d = p$ ou $d = q$. En utilisant l'algorithme d'Euclide, la détermination de d est de complexité $O(\log^2(n))$, d'où le résultat. □

1. Dans la littérature, on retrouve également le terme résiduosité, un néologisme qui nous parraît plus que dissonant.

2.4. Applications cryptographiques

2.4.1. Le cryptosystème de Rabin — Le ***cryptosystème de Rabin*** est un protocole d'échange à clé publique basé sur la difficulté d'extraire des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$ lorsque l'on ne connaît pas la factorisation de n. Voulant communiquer de manière confidentielle en utilisant un réseau non sécurisé, deux utilisateurs, Alice et Bob, procèdent de la manière suivante :

- Alice choisit deux nombres premiers distincts p et q congrus à 3 modulo 4, qui constituent sa clé secrète, et publie leur produit $n = pq$, qui est la clé publique.
- Afin d'envoyer un message $u \in \mathbb{Z}/n\mathbb{Z}$, Bob transmet à Alice l'élément $v = u^2$.
- Alice détermine les quatre racines carrées de u dans $\mathbb{Z}/n\mathbb{Z}$. L'une d'entre elles est le message original.

La phase de chiffrement se réduisant à une simple élévation au carré dans $\mathbb{Z}/n\mathbb{Z}$, elle est de complexité $O(\log^2(n))$. Connaissant la factorisation de n, la phase de déchiffrement nécessite l'extraction de racines carrées dans $\mathbb{F}_p$ et $\mathbb{F}_q$, qui peut être effectuée en appliquant la proposition 2.3.8. Elle est donc de complexité $O(\log^3(n))$. Si une tierce personne récupère le cryptogramme u, elle ne peut le déchiffrer, à moins connaître la factorisation de n.

2.4.2. Le protocole de Goldwasser-Micali — Ce cryptosystème se base sur le problème de la résiduosité quadratique (cf. la fin du paragraphe 2.3.3). C'est une fois encore un protocole à clé publique, qui se déroule de la manière suivante :

- Alice choisit deux nombres premiers impairs $p < q$ et calcule l'entier $n = pq$. Elle choisit ensuite un entier n tel que $(\frac{x}{p}) = (\frac{x}{q}) = -1$. Sa clé privée est le couple (p, q), la clé publique est le couple (x, n).
- Bob veut transmettre à Alice une suite de bits $(a_1, \dots, a_r)$. Pour chaque $i \in \{1, \dots, r\}$, il choisit un élément $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ au hasard et calcule $y_i = x_i^2 x^{a_i}$. Il envoie ensuite à Alice la suite $(y_1, \dots, y_r)$.
- Afin de déchiffrer le cryptogramme $(y_1, \dots, y_r)$, en calculant $(\frac{y_i}{p})$ et $(\frac{y_i}{q})$, Alice détermine si y_i est un carré dans $\mathbb{Z}/n\mathbb{Z}$. Si c'est le cas, elle en déduit que $a_i = 0$, sinon, $a_i = 1$.

La phase de chiffrement est de complexité $O(r \log^2(n))$, car elle se réduit à r élévations au carré et à r multiplications (au plus) dans $\mathbb{Z}/n\mathbb{Z}$. Le déchiffrement ne nécessite que le calcul de deux symboles de Legendre. Il est donc de complexité $O(r \log^2(n))$. On remarquera que lors de la phase de déchiffrement, seul le calcul de $(\frac{y_i}{p})$ est nécessaire. On a en effet les identités

$$\left(\frac{y_i}{q}\right) = \left(\frac{x_i^2}{q}\right)\left(\frac{x}{q}\right)^{a_i} = \left(\frac{x}{q}\right)^{a_i} = \left(\frac{x}{p}\right)^{a_i} = \left(\frac{x_i^2}{p}\right)\left(\frac{x}{p}\right)^{a_i} = \left(\frac{y_i}{p}\right).$$

2.4.3. Alice et Bob jouent à pile ou face — Afin de jouer à pile ou face à distance, Alice et Bob procèdent de la manière suivante :

- Alice choisit deux nombres premiers distincts p et q et elle transmet leur produit $n = pq$ à Bob.
- Bob choisit au hasard un entier strictement positif $a < \frac{n}{2}$ (lancer de la pièce) et envoie à Alice son carré b modulo n.
- Alice détermine les quatre racines carrées de b modulo n. Seules deux d'entre elles sont représentées par des entiers positifs a et c inférieurs à $\frac{n}{2}$. Elle en choisit une, et l'envoie à Bob (elle parie que c'est l'entier a choisi par Bob).
- Si Bob n'est pas en mesure d'exhiber c, c'est que l'entier envoyé par Alice coïncide avec a ; elle a donc remporté son pari. En effet, ne connaissant pas la factorisation de n, Bob n'est pas en mesure d'extraire des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$ (en un temps raisonnable) et ne peut donc pas tricher.

Si Alice et Bob veulent réitérer le pari, il est nécessaire de changer les valeurs de p et q. Dans le cas contaire, dès qu'Alice perd le pari, Bob est en mesure de factoriser n, car il connait toutes les racines carrées d'un élément de $\mathbb{Z}/n\mathbb{Z}$ (cf. la proposition 2.3.13), et peut donc tricher.

2.5. Complément : réciprocité quadratique et symbole de Jacobi

2.5.1. La loi de réciprocité quadratique — Nous allons commencer avec un résultat classique en théorie élémentaire des nombres.

***Théorème 2.5.1* (Wilson)** — *Pour tout nombre premier p, on a la congruence*

$$(p-1)! \equiv -1 \pmod{p}$$

Démonstration — La classe de $(p-1)!$ modulo p n'est autre que le produit des éléments de $\mathbb{F}_p^\times$. Étant donné un élément $x \in \mathbb{F}_p^\times$, si $x \neq x^{-1}$, les éléments x et x^{-1} apparaissent dans un tel produit et s'éliminent donc. On en déduit que la classe de $(p-1)!$ modulo p est le produit des éléments $x \in \mathbb{F}_p^\times$ tels que $x = x^{-1}$, ce qui se traduit par $x = \pm 1$. □

Corollaire 2.5.2 — *Soit $p > 2$ un nombre premier. En posant $m = (p-1)/2$, on a la congruence*

$$m!^2 \equiv (-1)^{m+1} \pmod{p}.$$

Démonstration — Le théorème de Wilson amène aux congruences

$$-1 \equiv (p-1)! \equiv \prod_{k=1}^{m} k(p-k) \equiv (-1)^m m!^2 \pmod{p},$$

d'où le résultat. □

Nous pouvons à présent énoncer et démontrer la ***loi de réciprocité quadratique***. Il existe à ce jour plus de 300 démonstrations différentes de ce résultat fondamental. Celle que nous proposons ici repose sur le théorème des restes chinois.

Théorème 2.5.3 — *Étant donnés deux nombres premiers impairs p et q, on a l'identité*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Démonstration — L'assertion étant immédiate lorsque $p = q$, supposons p et q distincts. Posons $n = pq$ et considérons le groupe $G = (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$. On s'intéresse à l'élément

$$x = \prod_{g\in G} g.$$

Dans la suite, on note $[a]$ l'image canonique dans G d'un entier a premier à n. Un élément $g \in G$ possède un unique représentant $a \in \mathbb{Z}$ tel que $0 < a < n/2$ et $(a, n) = 1$. En posant $p' = (p-1)/2, q' = (q-1)/2$ et $n' = (n-1)/2$, les entiers a de l'intervalle $]0, n/2[$ qui ne sont pas premiers avec n sont du type $a = up$, avec $u \in \{1, \dots, q'\}$, ou $a = vq$, avec $v \in \{1, \dots, p'\}$. On en déduit l'identité $x = [N]$, avec

$$N = \prod_{\substack{0<a<n/2\\(a,n)=1}} a = \frac{\prod_{0<a<n/2} a}{\prod_{\substack{0<a<n/2\\(a,n)=p}} a \prod_{\substack{0<a<n/2\\(a,n)=q}} a} = \frac{n'!}{p^{q'}q'!q^{p'}p'!}.$$

L'entier $M = q^{p'}p'!N$ est le produit des entiers inférieurs à $n/2$ qui ne sont pas divisibles par p. Tenant compte du théorème de Wilson, on obtient alors les relations

$$M \equiv \prod_{0<a<p,0<b<q'} (a+bp) \prod_{0<a\le p'} (a+q'p) \equiv p'! \prod_{0<a<p} a^{q'} \equiv (p-1)!^{q'} \equiv (-1)^{q'}p'! \pmod p,$$

d'où les congruences

$$(-1)^{q'}p'! \equiv M \equiv q^{p'}p'!N \equiv \left(\frac{q}{p}\right) p'!N \pmod p,$$

et, finalement,

$$N \equiv (-1)^{q'} \left(\frac{q}{p}\right) \pmod p.$$

En procédant de manière analogue, on obtient la congruence

$$N \equiv (-1)^{p'} \left(\frac{p}{q}\right) \pmod q.$$

Le théorème des restes chinois induit un isomorphisme entre les groupes $(\mathbb{Z}/n\mathbb{Z})^\times$ et $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$. Un élément de G possède alors un unique représentant $(u, v) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$, avec $u = \bar{a}, v = \bar{b}$, les entiers a et b vérifiant les relations $0 < a < p$ et $0 < b \le q'$. On en déduit que l'élément x est représenté par le couple

$$\prod_{0<a<p,0<b\le q'} (\bar{a}, \bar{b}) = \prod_{0<a<p} (\bar{a}^{q'}, \overline{q'!}) = (\overline{(p-1)!}^{q'}, \overline{q'!}^{p-1}) =$$
$$= ((-1)^{q'}, (-1)^{(p'+1)p'}) = ((-1)^{q'}, (-1)^{p'q'+p'}).$$

Dans ce cas, l'élément

$$\zeta = ((-1)^{p'+q'+p'q'}, 1) = \pm((-1)^{q'}, (-1)^{p'q'+q'}) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$$

est également un représentant de x. Par ailleurs, d'après ce qui précède, x est représenté par l'élément

$$(\bar{N}, \bar{N}) = \left((-1)^{q'} \left(\frac{q}{p}\right), (-1)^{p'} \left(\frac{p}{q}\right)\right) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times.$$

Comme précédemment, l'élément

$$\eta = \left((-1)^{q+q'} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right), 1\right) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$$

est aussi un représentant de x, d'où $\eta = \pm\zeta$, puis $\eta = \zeta$ (car $q > 2$) et, finalement, l'identité

$$(-1)^{p'q'} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1$$

dans $\mathbb{F}_p$, qui est alors également une identité dans $\mathbb{Z}$ (car $p > 2$). □

Remarque 2.5.4 — La loi de réciprocité quadratique affirme que si p et q sont congrus à 3 modulo 4 alors $(\frac{p}{q}) = -(\frac{q}{p})$, sinon $(\frac{p}{q}) = (\frac{q}{p})$.

2.5.2. Le symbole de Jacobi — Soit n un entier naturel impair et considérons sa factorisation $n = \prod_{p|n} p^{e_p}$. Pour tout entier m, le ***symbole de Jacobi*** $\left(\frac{m}{n}\right)$ est l'entier défini par la relation

$$\left(\frac{m}{n}\right) = \prod_{p|n} \left(\frac{m}{p}\right)^{e_p}.$$

Si n est premier, on retrouve le symbole de Legendre usuel.

Proposition 2.5.5 — *Le symbole de Jacobi vérifie les propriétés suivantes :*

1. *On a* $(\frac{m}{n}) \in \{0, 1, -1\}$ *et* $(\frac{m}{n}) \neq 0$ *si et seulement si* n *et* m *sont premiers entre eux.*
2. *Le symbole de Jacobi* $(\frac{m}{n})$ *ne dépend que de la classe de* m *modulo* n*.*
3. *Quels que soient les entiers* u *et* v*, on a la relation*
$$\left(\frac{uv}{n}\right) = \left(\frac{u}{n}\right)\left(\frac{v}{n}\right).$$
4. *Quels que soient les entiers impairs* u *et* v*, on a la relation*
$$\left(\frac{m}{uv}\right) = \left(\frac{m}{u}\right)\left(\frac{m}{v}\right).$$

Démonstration — Ce sont toutes des conséquences directes de la définition du symbole de Jacobi et des propriétés du symbole de Legendre. □

Lemme 2.5.6 — *Pour tout entier impair n, posons $\psi(n) = \frac{n-1}{2}$. On a alors la congruence*

$$\psi(nm) \equiv \psi(n) + \psi(m) \pmod 2.$$

Démonstration — En posant $n = 2u+1$ et $m = 2v+1$, on a les identités

$$\psi(nm) \equiv \frac{(2u+1)(2v+1)-1}{2} \equiv 2uv + u + v \equiv \psi(n) + \psi(m) \pmod 2.$$

□

Corollaire 2.5.7 — *Pour tout entier impair n, on a l'identité*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

Démonstration — Considérons la factorisation $n = \prod_{p|n} p^{e_p}$. En combinant le corollaire 2.3.5 et le lemme 2.5.6, on obtient

$$\left(\frac{-1}{n}\right) = \prod_{p|n} \left(\frac{-1}{p}\right)^{e_p} = (-1)^{\sum_{p|n} e_p \psi(p)} = (-1)^{\psi(n)}.$$

□

Théorème 2.5.8 — *Étant donnés deux entiers naturels impairs n et m, on a l'identité*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \left(\frac{n}{m}\right).$$

Démonstration — L'assertion étant trivialement vérifiée si n et m ne sont pas premiers entre eux, supposons que $(n,m) = 1$. Pour tout entier impair r, posons une fois de plus $\psi(r) = \frac{r-1}{2}$. On procède comme dans la démonstration du corollaire 2.5.7 : en posant $n = \prod_i p_i^{a_i}$ et $m = \prod_i q_i^{b_i}$, la loi de réciprocité quadratique pour le symbole de Legendre amène aux identités

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{q_i}{p_j}\right)^{a_i b_j} = \prod_{i,j} (-1)^{a_i b_j \psi(p_i)\psi(q_j)} \left(\frac{p_i}{q_j}\right)^{a_i b_j} = (-1)^{\sum_{i,j} a_i b_j \psi(p_i)\psi(q_j)} \left(\frac{n}{m}\right).$$

Finalement, en appliquant le lemme 2.5.6, on obtient les congruences

$$\sum_{i,j} a_i b_j \psi(p_i)\psi(q_j) \equiv \sum_i a_i \psi(p_i) \sum_j b_j \psi(q_j) \equiv \sum_i a_i \psi(p_i)\psi(m) \equiv$$
$$\equiv \psi(n)\psi(m) \pmod 2.$$

□

Exercice 2.5.9 — Montrer que pour tout entier impair n, l'entier $n^2 - 1$ est divisible par 8.

Proposition 2.5.10 — *Pour tout entier impair $n \geq 3$, on a l'identité*

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

En d'autres termes, on a $(\frac{2}{n}) = 1$ si et seulement si n est congru à ± 1 modulo 8.

Démonstration — On procède par récurrence sur l'entier n : pour $n = 3$, on a les identités

$$\left(\frac{2}{3}\right) = -1 = (-1)^{\frac{3^2-1}{8}}.$$

Soit donc $n > 3$ un entier impair et supposons la propriété vérifiée pour $n-2$. On a alors les relations

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{-2}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n-2}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n}{n-2}\right) =$$
$$= (-1)^{\frac{n-1}{2}}\left(\frac{2}{n-2}\right) = (-1)^{\frac{n-1}{2}}(-1)^{\frac{(n-2)^2-1}{8}} = (-1)^{\frac{4n-4+(n-2)^2-1}{8}} = (-1)^{\frac{n^2-1}{8}},$$

ce qui permet de conclure. La dernière assertion est juste une vérification directe (on remarquera que la parité de $(n^2-1)/8$ ne dépend que de la classe de n modulo 8). □

2.5.3. Calcul explicite du symbole de Jacobi — Soient n et m deux entiers impairs, avec $1 < n < m$. Nous terminons cette section en décrivant un algorithme efficace de calcul du symbole de Jacobi $(\frac{m}{n})$ ne nécessitant pas la connaissance de la factorisation de n. Cette méthode repose essentiellement sur la loi de réciprocité quadratique pour le symbole de Jacobi et sur une version modifiée de l'algorithme d'Euclide étendu.

- Pour $m = 1$, on obtient $(\frac{m}{n}) = 1$ et l'algorithme s'arrête.
- Pour $m > 1$, la loi de réciprocité quadratique amène à l'identité $(\frac{m}{n}) = \pm(\frac{n}{m})$, le signe ne dépendant que de la classe de n et m modulo 4.
- En considérant la division euclidienne modifiée $n = mq + r$, avec $|r| < m/2$, on obtient la relation $(\frac{n}{m}) = \left(\frac{r}{m}\right)$.
- Pour $r = 0$, on obtient les identités
$$\left(\frac{m}{n}\right) = \pm\left(\frac{r}{m}\right) = 0$$
et l'algorithme s'arrête.
- Sinon, l'entier r possède une écriture unique du type $r = \pm 2^a b$, avec $b > 0$ impair. Par construction, on a l'inégalité $b < m/2$ et les identités
$$\left(\frac{r}{m}\right) = \left(\frac{\pm 1}{m}\right)\left(\frac{2}{m}\right)^a\left(\frac{b}{m}\right).$$
La détermination de $(\frac{-1}{m})$ ne dépend que de la classe de m modulo 4. De même, $(\frac{2}{m})$ ne dépend que de la classe de m modulo 8. De plus, l'entier $(\frac{2}{m})^a$ est égal à $(\frac{2}{m})$ si a est impair et à 1 sinon.
- On répète le procédé en remplaçant $(\frac{m}{n})$ par $(\frac{b}{m})$.

Chaque étape de l'algorithme est de complexité polynomiale par rapport à la taille des entiers considérés. De manière plus précise, l'opération la plus coûteuse (en temps) est la division eucllidienne modifiée de n par m (cf. le troisième point ci-dessus), qui est de complexité $O(\log^2(n))$. La factorisation de r se réduit à une suite de décalages sur la droite et ne pose pas de problème. Finalement, ayant utilisé la division euclidienne modifiée, le nombre de boucles nécessaires pour que l'algorithme aboutisse est majoré par $\log_2(n)$. On en déduit que cette méthode de calcul du symbole de Jacobi est de complexité globale $O(\log^2(n))$ améliorant ainsi l'algorithme de calcul du symbole de Legendre découlant du théorème 2.3.2 (qui était de complexité $O(\log^3(n))$.

Exemple 2.5.11 — Calculons le symbole de Jacobi $(\frac{43}{143})$ de deux manières différentes :

- Tout d'abord en considérant la factorisation $143 = 11{\cdot}13$, on obtient les identités
$$\left(\frac{43}{143}\right) = \left(\frac{43}{11}\right)\left(\frac{43}{13}\right) = \left(\frac{-1}{11}\right)\left(\frac{4}{13}\right) = -1.$$
- Sans avoir recours à la factorisation de 143, la loi de réciprocité quadratique pour le symbole de Jacobi amène aux relations
$$\left(\frac{43}{143}\right) = -\left(\frac{143}{43}\right) = -\left(\frac{14}{43}\right) = -\left(\frac{2}{43}\right)\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) =$$
$$= -\left(\frac{1}{7}\right) = -1.$$