Nombres Premiers, Applications

Valentin KILIAN
Ecole Normale Supérieure de Rennes,

Mémoire sous la direction de Lionel FOURQUAUX (IRMAR)

26 février 2022

Table des matières

Introduction

Connus depuis l'antique Babylone, les nombres premiers n'ont pourtant pas encore révélé tous leurs mystères. Ces nombres qui n'ont pas d'autres facteurs qu'un et eux-mêmes semblent être les nombres les plus simples possibles et pourtant on échoue encore à trouver une régularité dans leur succession. Le grand L. EULER jugeait ce problème inaccessible à l'esprit humain, bien que nombre de ses successeurs soit parvenu à des résultats partiels, l'histoire lui donne pour le moment raison. L'Institut de mathématiques Clay offre d'ailleurs un prix de 1 million de dollars pour la résolution de conjecture de Riemann dont l'un des corolaires est la compréhension de répartition des nombres premiers. Les nombres premiers sont au coeur de la théorie des nombres puisque tout entier peut s'écrire de manière unique sous la forme d'un produit de nombres premiers, c'est ce qui faisait dire à l'immense C.GAUSS

> "Le problème de la distinction entre nombres premiers et nombres composés, et celui de la décomposition d'un nombre en produit de facteurs premiers sont les plus importants et les plus utiles de toute l'arithmétique. [...] L'honneur de la science semble exiger qu'on cultive avec zèle tout progrès dans la solution de ces élégantes et célèbres questions."

C.GAUSS ne pouvait pas avoir plus raison puisque les nombres premiers se sont révélés avoir des applications dans des domaines bien plus divers que la simple arithmétique. Ainsi la conjecture de Riemann relève du domaine de l'analyse complexe, nous verrons également des applications en théorie des groupes et en théorie des corps.

Cependant l'usage peut être le plus commun des nombres premiers reste la cryptographie. En effet la difficulté à décomposer de très grands nombres en facteurs premiers est à la base de cryptosystèmes que nous utilisons quotidiennement. C'est ainsi que des milliards de personnes utilisent sans cesse les nombres premiers sans même avoir conscience de l'incroyable complexité qu'ils renferment. [1]

Dans ce rapport nous allons nous efforcer de présenter de façon clair et concise certains des résultats les plus importants sur les nombres premiers ainsi que quelques applications. Dans un premier temps nous nous intéresserons à la factorialité de l'anneau des entiers $\mathbb{Z}$ (1) puis nous introduirons quelques unes des fonctions liées aux nombres premiers (2). Nous partirons alors à la recherche des nombres premiers en s'efforçant d'une part de comprendre leur répartition et d'autre part d'établir des critères de primalité (3). Tout au long de ce rapport nous nous efforcerons de donner des exemples d'applications à la fois abstraits et concrets.

L'ensemble de ce qui suit est très fortement inspiré (voire recopié) de plusieurs livres d'algèbre connus :

- *Mathématiques pour l'agrégation : Algèbre et géométrie* de Jean-Etienne ROMBALDI [2]
- *Cours d'Algèbre* de Daniel PERRIN [3].
- *Algèbre : le grand combat* de Grégory BERHUY [4]
- *Les Maths en Tête : Algèbre* de Xavier GOURDON [5]
- *Cours d'Algèbre* de Michel DEMAZURE [6]
- *Histoires Hédonistes de Groupes et de Géométrie* de Philippe CALDERO et Jérôme GERMONI [7]

D'autres ouvrages ont été utilisés pour certains résultats précis, ils seront systématiquement cités.

Chapitre 1

Factorialité de l'anneau $\mathbb{Z}$

Sources : *Mathématiques pour l'agrégation : Algèbre et géométrie*, J.E. ROMBALDI, chapitre 11 [2] et *Cours d'Algèbre*, D. PERRIN, chapitre I.5 [3]

Les nombres premiers apparaissent en premier lieu en arithmétique des entiers. En effet ils y jouent un rôle de briques élèmentaires dans un sens que l'on précisera plus loin.

1.1 L'ensemble des nombres premiers

Commençons par donner une définition rigoureuse

Définition 1.1.1. *On dit qu'un entier naturel p est* premier *si $p \neq 1$ et si ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.*

Exemple : les entiers 2, 3, 5, 7, 11 ou 13 sont premiers tandis que 14, 28 ou 33 ne le sont pas.
Les nombres premiers sont donc des nombres irréductibles

Théorème 1.1.2. *Tout entier $n \in \mathbb{Z} \setminus \{\pm 1\}$ a au moins un diviseur premier.*

Exemple : l'entier 7 est un diviseur premier de 14. Tout nombre premier est un diviseur premier de 0.

Théorème 1.1.3 (Euclide)**.** *L'ensemble $\mathcal{P}$ des nombres premiers est infini*

Démonstration. On sait déjà que $\mathcal{P}$ est non vide (il contient 2). Supposons par l'absurde que $\mathcal{P}$ soit fini et notons $\mathcal{P} = \{p_1, ..., p_r\}$. L'entier $n = p_1...p_r + 1$ qui est supérieur à 2 admet un diviseur premier $p_k \in \mathcal{P}$. Cet entier p_k divisant $n = p_1...p_r + 1$ et $p_1...p_r$, il divise la différence qui est égale à 1, ce qui est absurde. Ainsi $\mathcal{P}$ est infini. ■

Remarque : On note alors $(p_n)_{n\in\mathbb{N}^*}$ la suite ordonnée des nombres premiers ?

1.2 Théorème fondamental de l'arithmétique

Théorème 1.2.1 (Théorème fondamental de l'arithmétique)**.** *Tout entier naturel $n \geq 0$ se décompose de manière unique sous la forme*

$$n = q_1^{\alpha_1}...q_d^{\alpha_d} \qquad (\star)$$

où $d \in \mathbb{N}$ (avec la convention que si $d = 0$ alors le produit est vide), où les q_k sont des nombres premiers tel que $2 \leq q_1 < ... < q_d$ et les α_k sont des entiers naturels non nuls.

Démonstration.
Existence On procède par récurrence sur n.

- Pour $n = 1$ et $n = 2$ on a déjà la décomposition.
- Soit $n \geq 2$. Supposons le résultat acquis pour tout entier $k \in [\![2, n]\!]$. Si $n + 1$ est premier on a déjà la décomposition, sinon on écrit $n + 1 = ab$ avec $a, b \in [\![2, n]\!]$ et il suffit d'appliquer l'hypothèse de récurrence pour a et b.

Unicité on procède encore une fois par récurrence sur n

- Pour $n = 1$ et $n = 2$ c'est évident.
- Soit $n \geq 2$. Supposons le résultat acquis pour tout entier $k \in [\![2, n]\!]$. Supposons que l'on ait deux décompositions pour $n + 1$:

$$n + 1 = q_1^{\alpha_1} ... q_r^{\alpha_r} = m_1^{\beta_1} ... q_s^{\beta_s}$$

où les q_k [resp. les m_l] sont des nombres premiers deux à deux distincts et les α_k [resp. les β_l] sont des entiers naturels non nuls. L'entier q_1 est premier et divise $m_1^{\beta_1} ... q_s^{\beta_s}$, donc, d'après le lemme d'Euclide, il divise l'un des m_k, notons le m_{k_1}. L'entier m_{k_1} étant également premier on a nécessairement $q_1 = m_{k_1}$. On peut alors simplifier par q_1 pour se ramener à un entier inférieur où égal à n auquel on peut appliquer l'hypothèse de récurrence.

■

Définition 1.2.2. *L'écriture (⋆) est la* décomposition en facteurs premiers *de n.*

Définition 1.2.3. *Soient $n \in \mathbb{N}, p \in \mathcal{P}$. La* valuation p-adique *de n est l'entier*

$$v_p(n) = \max \left\{ k \in \mathbb{N}, p^k | n \right\}.$$

Par convention $v_p(0) = -\infty$ pour tout $p \in \mathcal{P}$.

Remarques :

1. Avec les notations précédentes on a bien sûr $v_{q_k}(n) = \alpha_k$, on peut alors écrire la décomposition en facteurs premiers de n sous la forme $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.
2. Du théorème précédent on déduit que tout entier relatif non nul $n \in \mathbb{Z}$ s'écrit de manière unique $n = \pm q_1^{\alpha_1} ... q_r^{\alpha_r}$. On dit que l'anneau $\mathbb{Z}$ est un anneau *factoriel*.

Exemple : L'entier 60 se décompose en $60 = 2^2.3.5$ on a donc $v_5(60) = 1, v_2(60) = 2$ et $v_7(60) = 0$.

Nous allons voir que la décomposition en facteur premier des entiers permets de réduire l'étude des propriétés des entiers à l'étude des seuls nombres premiers. On comprends alors le caractère « fondamental » du théorème ainsi que la volonté de généraliser cette notion au travers des anneaux factoriels.

Exemples :

1. Soit $n \geq 2$ un entier, notons m le nombre de zéros qui terminent son écriture décimale. Alors n est divisible par 10^m et pas par 10^{m+1}, donc $m = \min\{v_2(n), v_5(n)\}$. On peut adapter cette méthode pour compter le nombre de zéros qui terminent l'écriture de n dans n'importe quelle base.
2. Si $n = \prod_{k=1}^{r} q_k^{\alpha_k}$ est un entier décomposé en produit de facteurs premiers, les diviseurs de n sont alors de la forme $d = \prod_{k=1}^{r} q_k^{\gamma_k}$ où $\gamma_k \in [\![0, \alpha_k]\!]$. On peut donc compter les diviseurs positifs de n, il y en a $\prod_{k=1}^{r} (\alpha_k + 1)$.
3. la décomposition en facteurs premiers peut également être utilisée pour calculer le pgcd et le ppcm de deux entiers, c'est l'objet de la proposition suivante :

Proposition 1.2.4. *Soient n, m deux entiers strictement positifs. On a :*

$$pgcd(n, m) = \prod_{p \in \mathcal{P}} p^{\min(v_p(n), v_p(m))}, \quad \textit{et} \quad ppcm(n, m) = \prod_{p \in \mathcal{P}} p^{\max(v_p(n), v_p(m))}$$

1.3 Utilisation en théorie des groupes : les théorèmes de Sylow

On comprend aisément que le théorème précédent n'est pas fondamental qu'en arithmétique des entiers mais qu'il a son importance dans tous les domaines où les entiers interviennent. Nous allons, par exemple, voir en quoi il est important en théorie des groupes.

Le théorème de Lagrange affirme que si H est un sous-groupe du groupe fini G alors son cardinal divise le cardinal de G. On peut se demander, à l'inverse, si dans un groupe de cardinal n il existe, pour tout diviseur d de n, un (ou plusieurs) sous-groupe d'ordre d. En général ce n'est pas vrai et on peut trouver des contre-exemples. Cependant cela reste vrai pour certains des diviseurs de n, la condition sur ces diviseurs s'exprimant en fonction de la décomposition en produit de facteurs premiers de l'ordre n du groupe.

On commence par rappeler un théorème important en théorie des groupes :

> **Théorème 1.3.1** (Théorème de Cayley)**.** *Si G est un groupe fini de cardinal n alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$*

Démonstration. Voir [2] 2.8 ■

On peut maintenant s'intéresser aux groupes de Sylow.

> **Définition 1.3.2.** *Soit G un groupe fini de cardinal n et p un diviseur premier de n. Notons $\alpha = v_p(n)$. On a donc $n = p^\alpha m$ avec $m \nmid p$. On appelle* p-sous groupe de Sylow *de G un sous-groupe d'ordre p^α.*

Exemple Soient $p \in \mathcal{P}$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments. Soit $G = GL_n(\mathbb{F}_p)$ où $n \in \mathbb{N}^*$. Alors en comptant les bases de $\mathbb{F}_p^n$ on montre que G est un groupe fini de cardinal :

$$\#G = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$$

d'où on peut déduire la valuation p-adique $v_p(\#G) = \frac{n(n-1)}{2}$. On exhibe alors un p-sous groupe de Sylow de G : l'ensemble des matrices triangulaires supérieures strictes :

$$P = \left\{A = (a_{ij})_{i,j\in[\![1,n]\!]} | a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\right\}$$

qui est clairement un groupe de cardinal $p^{\frac{n(n-1)}{2}}$.

En fait on peut toujours trouver un p-sous groupe de Sylow, c'est l'objet du théorème suivant :

> **Théorème 1.3.3** (Théorème de Sylow I)**.** *Soit G un groupe fini et p un diviseur premier de $\#G$, alors G contient au moins un p-sous groupe de Sylow.*

Démonstration. La preuve que l'on présente est fortement inspirée de [3], elle repose sur le lemme suivant qui permet, connaissant un p-sous groupe de Sylow d'un groupe G d'en trouver un pour un sous-groupe H.

> **Lemme 1.3.4.** *Soit G un groupe avec $\#G = n = p^\alpha m$ où $p \nmid m$ et soit H un sous groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. (du lemme) : Le groupe G agit sur G/S par translation à gauche et pour tout $a \in G$ le stabilisateur de aS est aSa^{-1}. Mais H agit lui aussi sur G/S (par restriction de l'action de G) avec comme stabilisateur de aS le sous-groupe $H_a := aSa^{-1} \cap H$.

Reste à voir que l'un de ces groupes est un p-sous groupe de Sylow de H. Par le théorème de Lagrange on sait que leur cardinal est une puissance entière de p (H_a est un sous groupe de aSa^{-1} qui a le même cardinal que le groupe S), il suffit donc de montrer qu'il existe un $a \in G$ tel que l'indice $[H : H_a]$ soit premier à p.

L'application $\bar{h} \in H/H_a \mapsto (ha)S \in Orb(aS)$ (l'orbite de aS dans G/S sous l'action de H) est clairement une . On a donc $\#(H/H_a) = \#Orb(aS)$. Ecrivons l'équation au classe :

$$\#(G/S) = \sum_{a\in G} \#(H/H_a) = \sum_{a\in G} \#Orb(aS).$$

Si tous les $\#Orb(aS)$ étaient divisibles par p, il en serait donc de même pour $\#(G/S)$ Mais ceci contredit le fait que S soit un p-sous groupe de Sylow de G. ■

On continue la preuve du théorème de Sylow. Soit G un groupe de p un diviseur de $\#G := n$. On plonge d'abord G dans $\mathfrak{S}_n$ par le théorème de Cayley (1.3.1), puis on plonge $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ en envoyant une permutation sur la matrice de permutation associé (i.e. $\sigma \in \mathfrak{S}_n$ s'envoie sur l'endomorphisme u_σ défini dans la base canonique par $u(e_i) = e_{\sigma(i)}$).

On vient donc de réaliser G comme un sous groupe de $GL_n(\mathbb{F}_p)$ qui possède un p-sous groupe de Sylow d'après l'exemple ci-dessus, on conclut alors grâce au lemme (1.3.4) que G possède également un p-sous groupe de Sylow. ■

Le second théorème de Sylow étudie la conjugaison des p-sous groupe de Sylow.

Théorème 1.3.5 (Théorème de Sylow II)**.** *Soit G un groupe fini de cardinal n et p un diviseur premier de n. Notons $\alpha = v_p(n)$ on a donc $n = p^\alpha m$ avec $p \nmid m$*

1. *Si H est un sous groupe de G et que le cardinal de H est une puissance de p alors il existe un p-Sylow S avec $H \subset S$.*
2. *les p-Sylow sont tous conjugués (en donc leur nombre s_p divise n)*
3. *On a $s_p \equiv 1[p]$ (donc s_p divise m)*

Démonstration. On prouve 1. et 2. ensemble. Si H est un sous groupe de G de cardinal une puissance de p et S un p-Sylow de G, il existe en vertu du lemme 1.3.4 un élément $a \in G$ tel que $H_a := aSa^{-1} \cap H$ soit un p-Sylow de H. Mais comme $\#H$ est une puissance de p on a nécessairement $H_a = H$, donc H est inclus dans aSa^{-1} qui est un Sylow. Si de plus H est un Sylow alors on a exactement $H = aSa^{-1}$. Ainsi les p-Sylow forment un orbite sous l'action de G par conjugaison et donc $s_p | n$.

Pour 3. on fait opérer G par conjugaison sur l'ensemble X des p-Sylow. Soit S un p-Sylow, par restriction S agit lui aussi par conjugaison du X. L'équation au classe nous permet alors d'écrire que

$$\#X \equiv \#X^S[p]$$

où X^S est l'ensemble des points fixes de X sous l'action de S. Reste à voir que $\#X^S$=1. Bien sur si $s \in S$ alors $sSs^{-1} = S$ autrement dit $S \in X^S$, on doit donc montrer que c'est le seul.

Soit donc T un p-Sylow et supposons que $T \in X^S$ i.e. $\forall s \in S,\ sTs^{-1} = T$. Soit $N =< S, T >$ le sous-groupe de G engendré par S et T. On a $S \subset N$ et $T \subset N$ et ce sont donc a fortiori des p-Sylow de N. Mais comme $T \in X^S$ on a T sous groupe distingué de N. Or d'après le point 2. qu'on vient de démontrer les p-Sylow de N sont tous conjugués. Soit donc $n \in N$ tel que $nTn^{-1} = S$ alors puisque T est distingué dans N on vient d'écrire $T = S$ ce qui conclut la preuve. ■

Au passage on A démontr2 le résultats suivant :

Porisme 1.3.6. *Si S est un p-Sylow de G, on a*
S distingué dans G $\Leftrightarrow$ S est l'unique p-Sylow de G $\Leftrightarrow$ $s_p = 1$

Exemple : Un groupe d'ordre $63 = 3^2 \times 7$ n'est pas simple. En effet on a $s_7 \equiv 1[7]$ et $s_7 | 9$ donc $s_7 = 1$ et l'unique 7-Sylow est un sous groupe distingué non trivial.

Chapitre 2

Fonctions arithmétiques liées aux nombres premiers

Sources : *Mathématiques pour l'agrégation : Algèbre et géométrie*, J.E. ROMBALDI, chapitre 10, 11 et 13 [2] et *Algèbre : le grand combat*, G.BERHUY, chapitre XVI [4]

En théorie des nombres on appelle *fonction arithmétique* toute fonction définie de $\mathbb{N}^*$ dans un sous ensemble de $\mathbb{C}$, on peut également les voir comme des suites de nombres complexes indexées par $\mathbb{N}^*$. Lorsque qu'une fonction arithmétique est multiplicative, la décomposition en produit de facteurs premiers permet de calculer sa valeur en n'importe quel entier en connaissant uniquement sa valeur en les nombres premiers. Nous allons voir plusieurs exemples de fonctions arithmétiques multiplicatives. Certaines de ces fonctions interviennent dans l'élaboration de critères de primalité comme nous le verrons dans la partie suivante (3) mais aussi dans d'autres domaines plus exotiques notamment en analyse complexe et en physique.

2.1 La fonction indicatrice d'Euler

Soit $n \geq 2$ entier, on note $\bar{a}$ la classe de $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, et $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe mutiplicatif des éléments inversibles de $Z/n\mathbb{Z}$. Du théorème de Bézout on déduit le théorème suivant

Théorème 2.1.1. *Soit $a \in \mathbb{Z}$, les affirmations suivantes sont équivalentes :*

1. *$\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$*
2. *a est premier avec n*
3. *$\bar{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$*

Définition 2.1.2. *On appelle* fonction indicatrice d'Euler *la fonction φ qui à $n \in \mathbb{N}^*$ associe le nombre $\#(\mathbb{Z}/n\mathbb{Z})^\times$. Par convention $\varphi(1) = 1$.*

Exemple : Si p est premier alors tous les entiers compris entre 1 et $p-1$ sont premiers avec p ainsi $\varphi(p) = p - 1$.

Du théorème de Lagrange on déduit :

Théorème 2.1.3 (Euler)**.** *Pour tout $a \in \mathbb{Z}$ premier avec n, on a $a^{\varphi(n)} \equiv 1[n]$.*

Pour p premier le théorème d'Euler devient le « petit » théorème de Fermat :

Corollaire 2.1.4 (Fermat)**.** *Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ premier avec p. Alors on a $a^{p-1} \equiv 1[p]$ donc pour tout $a \in \mathbb{Z}$ on a $a^p \equiv a[p]$.*

Théorème 2.1.5. *Soit $n \geq 2$ entier, on a* $n = \sum_{d|n} \varphi(d)$

La décomposition en produit de facteur premier permet de calculer la fonction indicatrice d'Euler. On a d'abord le lemme

Lemme 2.1.6. *Si $p \in \mathcal{P}$, et $\alpha \in \mathbb{N}^*$ on a* $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

d'où on peut déduire

Théorème 2.1.7. *Soit $n = \prod_{k=1}^{r} q_k^{\alpha_k}$ un entier (plus grand que 2) décomposé en produit de facteurs premiers, alors*

$$\varphi(n) = \prod_{k=1}^{r} (q_k^{\alpha_k} - q_k^{\alpha_k - 1}) = n \prod_{k=1}^{r} (1 - \frac{1}{q_k})$$

2.2 La fonction de Möbius

Définition 2.2.1. *On définie la fonction de Möbius par*

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

pour tout $n \in \mathbb{N}^*$. En particulier $\mu(n)$ est non nul si et seulement si n est sans facteur carré.

Lemme 2.2.2. *Soit $n \in \mathbb{N}^*$ alors on a* $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si n=1} \\ 0 & \text{sinon} \end{cases}$

Théorème 2.2.3 (Formule d'inversion de Möbius)**.** *Soit $u, v \in \mathbb{R}^{\mathbb{N}^*}$ deux suites réelles, alors s'équivalent :*

1. $\forall n \in \mathbb{N}^* \quad u(n) = \sum_{d|n} v(d)$
2. $\forall n \in \mathbb{N}^* \quad v(n) = \sum_{d|n} \mu(d) u(\frac{n}{d})$

On peut alors faire le lien avec la fonction indicatrice d'Euler :

Proposition 2.2.4. *Si $n \in \mathbb{N}^*$ on a* $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$

2.3 Le symbole de Legendre

Dans ce paragraphe on se donne un nombre premier impair $p \in \mathcal{P}$ et pour tout $k \in \mathbb{Z}$ on note $\bar{k}$ la classe de k modulo p dans $\mathbb{F}_p$. On note $\mathfrak{F}_p^{\times 2}$ l'ensemble des carrés de $\mathbb{F}_p^\times$ i.e.

$$\mathfrak{F}_p^{\times 2} = \left\{ (\bar{k})^2 \mid \bar{k} \in \mathbb{F}_p^\times \right\}$$

Considérons l'équation arithmétique $aX^2 + bX + c \equiv 0 \ [p]$ où p est un nombre premier impair tel que $p \nmid a$. Puisque $p \nmid 4a$ cela équivaut à

$$\begin{aligned} 4a^2X^2 + 4abX + 4ac &\equiv 0 && [p] \\ (2aX + b)^2 &\equiv b^2 - 4ac && [p] \\ Y^2 &\equiv d && [p] \end{aligned}$$

où on a posé $Y = 2aX + b$ et $d = b^2 - 4ac$. Ainsi la résolution des équations arithmétiques quadratiques dans $\mathbb{F}_p$ se réduit à la résolution des équations du type $X^2 \equiv k \ [p]$ et c'est ce qui motive l'étude que nous nous apprêtons à faire.

Définition 2.3.1. *On dit qu'un entier k non multiple de p est un* résidu quadratique modulo p *si $\bar{k}$ est un carré dans $\mathbb{F}_p^*$.*

Lemme 2.3.2. *On a $\#\mathfrak{F}_p^{\times 2} = \frac{p-1}{2}$.*

Lemme 2.3.3. *Soit $\bar{x} \in \mathbb{F}_p^\times$ alors on a $(\bar{x})^{\frac{p-1}{2}} = \pm\bar{1}$. De plus, $(\bar{x})^{\frac{p-1}{2}} = \bar{1}$ si, et seulement si, $\bar{x} \in \mathfrak{F}_p^{\times 2}$.*

Notons $\mathcal{L}_p : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ le morphisme de groupes obtenu par composition du morphisme $\bar{x} \in \mathbb{F}_p^\times \mapsto (\bar{x})^{\frac{p-1}{2}} \in \{\pm\bar{1}\}$ et de l'isomorphisme évident $\{\pm\bar{1}\} \simeq \{\pm 1\}$. Ainsi, d'après le lemme précédent, pour tout $\bar{x} \in \mathbb{F}_p^\times$ on a $\mathcal{L}_p(\bar{x}) = 1$ si, et seulement si, $\bar{x} \in \mathfrak{F}_p^{\times 2}$. On peut alors poser pour tout $a \in \mathbb{Z}$:

$$\left(\frac{a}{p}\right) = \begin{cases} \mathcal{L}_p(\bar{a}) & \text{si } p \nmid a \\ 0 & \text{si } p \mid a \end{cases}$$

Définition 2.3.4. *On appelle* symbole de Legendre (modulo p) *la fonction arithmétique $\left(\frac{\cdot}{p}\right)$.*

Proposition 2.3.5. *Soit $a \in \mathbb{Z}$, le nombre a est un résidu quadratique modulo p si, et seulement si, $\left(\frac{a}{p}\right) = 1$.*

Proposition 2.3.6. *On a les règles de calculs suivantes*

1. *Le symbole de Legendre est une fonction multiplicative i.e. pour tous $a, b \in \mathbb{Z}$ on a*
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$
2. *Pour tous $a, b \in \mathbb{Z}$ tels que $a \equiv b\ [p]$, on a*
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$
3. *On a $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ autrement dit $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1\ [4] \\ -1 & \text{si } p \equiv 3\ [4] \end{cases}$*
4. *On a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ autrement dit $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1\ [8] \\ -1 & \text{si } p \equiv \pm 3\ [8] \end{cases}$*

Nous allons maintenant établir la loi de la réciprocité quadratique qui nous permettra de calculer le symbole de Legendre de manière (presque) algorithmique à condition de savoir factoriser en produit de facteurs premiers.

Théorème 2.3.7 (Loi de réciprocité quadratique)**.** *Soient p, q deux nombres premiers impairs distincts. Alors on a :*
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Remarque : Autrement dit on a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ si p et $q \equiv 3\ [4]$ et $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sinon.

Démonstration.
On reproduit ici une preuve que l'on peut trouver dans [7] il existe au moins plusieurs dizaines de preuves

différentes de ce résultat. L'idée est de calculer de deux façons différentes le cardinal modulo p de la "sphère" définie sur $\mathbb{F}_q$ par :

$$\mathcal{B} = \left\{ (x_1, ..., x_p) \in \mathbb{F}_q^p,\ \sum_{i=1}^{p} x_i^2 = 1 \right\}$$

D'une part, on fait agir le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ sur X, d'autre part on utilise les formes quadratiques.

Etape 1 : Action de groupe. On a

$$(\spadesuit) \quad \#\mathcal{B} \equiv \left(\frac{p}{q}\right) + 1 \ [p]$$

En effet, faisons agir $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique sur $\mathbb{F}_q^p$:

$$\forall k \in \mathbb{Z}/p\mathbb{Z},\ \forall (x_1, ..., x_p) \in \mathbb{F}_q^p \quad k \cdot (x_1, ..., x_p) = (x_{1+k}, ..., x_{n+k})$$

où les indices sont vus modulo p dans le sens où $\forall l \in \mathbb{N}\ x_{l+p} = x_l$.

On souhaite maintenant étudier les orbites de cette action : pour $x \in \mathcal{B}$ le stabilisateur $Stab(x)$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ donc il est de cardinal 1 ou p. Puisque $\#Orb(x) = \#(\mathbb{Z}/p\mathbb{Z}) \div \#Stab(x)$ alors $Orb(x)$ est de taille 1 ou p. Si $\#Orb(x)$=1 alors $x_i = x_j$ pour tout $i, j \in [\![1, p]\!]$ et donc $x = (y, ..., y)$ pour un $y \in \mathbb{F}_p$. On a donc en particulier que $py^2 = 1$. Il y a donc autant de $x \in \mathcal{B}$ tel que $\#Orb(x) = 1$ que d'éléments dans $\left\{ y \in \mathbb{F}_p,\ py^2 = 1 \right\}$ dont on étudie maintenant le cardinal.

> **Lemme 2.3.8.** *Soit q premier impair : Pour $a \in \mathrm{F}_q^\times$, on note $R(a)$ l'ensemble des solutions de l'equation $ax^2 = 1$, avec $x \in \mathbb{F}_q$. On a $|R(a)| = 1 + \left(\frac{a}{q}\right)$.*

Démonstration. Par disjonction de cas sur $\left(\frac{a}{q}\right)$:

- Si $\left(\frac{a}{q}\right) = 1$ alors a est un carré, $a = b^2$, on trouve deux solutions $x = b^{-1}$ et $x = -b^{-1}$. Comme F_q est un corps, le polynôme $aX^2 - 1 \in \mathbb{F}_q[X]$ a au plus deux racines, donc $|R(a)| = 2 = 1 + \left(\frac{a}{q}\right)$. -
- Si $\left(\frac{a}{q}\right) = -1$, a n'est pas un carré, a^{-1} non plus (car $\left(b^{-1}\right)^2 = \left(b^2\right)^{-1}$), et donc l'équation $x^2 = a^{-1}$ n'a pas de solution, d'où $|R(a)| = 0 = 1 + \left(\frac{a}{q}\right)$

Dans tous les cas, on a bien $\left|\left\{x \in \mathbb{F}_q : ax^2 = 1\right\}\right| = 1 + \left(\frac{a}{q}\right)$. ■

Pour conclure l'étape 1, on utilise l'équation aux classes : soit Ω une famille de représentants des classes de B sous l'action de $\mathbb{Z}/p\mathbb{Z}$. On a alors

$$|\mathcal{B}| \equiv \sum_{x \in \Omega} |\operatorname{Orb}(x)| \equiv \left|\left\{y : py^2 = 1\right\}\right| \ [p]$$

D'après le lemme on retrouve alors bien ($\spadesuit$).

Etape 2 : Forme quadratique. On commence par admettre les deux théorèmes suivants qui découle de la théorie des formes quadratiques :

> **Théorème 2.3.9.** *Soit V un $\mathbb{F}_p$ espace vectoriel de dimension fini. Soit $a \in \mathbb{F}_p^\times$ qui n'est pas un résidu quadratique de p. Soit f une forme quadratique non dégénérée sur V. Il existe une base de V dans laquelle la matrice de f est soit I_n soit* $\operatorname{Diag}(1, \ldots, 1, a)$

Démonstration. Voir [2] 15.6 ■

> **Corollaire 2.3.10.** *Soient q_1, q_2 deux formes quadratiques non dégénérées sur V qui ont même discriminant (i.e. même déterminant modulo les carrés du corps de base). Alors elles sont congruentes i.e il existe $\phi \in GL(V)$ tel que $q_1 = q_2 \circ \phi$.*

Comme p est impair, on peut poser $d := \frac{p-1}{2} \in \mathbb{N}$ puis $a := (-1)^d$. On note également $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

On définit q_1, q_2 deux formes quadratiques sur $\mathbb{F}_q^p$ de la manière suivante :

$$q_1(x_1, \ldots, x_p) = \sum_{i=1}^{p} x_i^2, \quad q_2(y_1, z_1, \ldots, y_d, z_d, t) = 2\sum_{i=1}^{d} y_i z_i + at^2$$

Les matrices associées dans la base canonique sont :

$$I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \quad \text{et} \quad A = \begin{pmatrix} J & & & \\ & \ddots & & \\ & & J & \\ & & & a \end{pmatrix}$$

ou A est une matrice diagonale par blocs (avec d blocs J), d'où $\det(A) = \det(J)^d \cdot a = 1$ car $\det(J) = -1$. Les formes quadratiques q_1 et q_2 sont non-dégénérées et de même discriminant, elles sont donc congruentes d'après le théorème 2.3.9. Ainsi, le cardinal de l'ensemble $\mathcal{B} = \{x \in \mathbb{F}_q^p : q_1(x) = 1\}$ est égal au cardinal de l'ensemble $B' = \{x \in \mathbb{F}_q^p : q_2(x) = 1\}$. On dénombre maintenant les eléments de B' : soit $(y_1, z_1, \ldots, y_d, z_d, t) \in \mathcal{B}'$

- Si $y_1 = \cdots = y_d = 0$: on doit avoir $at^2 = 1$, ce qui laisse $1 + \left(\frac{a}{q}\right)$ possibilités pour t d'apres le lemme 2.3.8. On est libre de choisir les z_i, donc il y a q^d possibilités pour les z_i, soit un total de $q^d\left(1 + \left(\frac{a}{q}\right)\right)$ éléments de cette forme.
- Si au moins un y_i est non-nul : une fois $y_1, \ldots, y_d$ et t fixés, les z_i doivent satisfaire l'équation

  $$q_2(y_1, z_1, \ldots, y_d, z_d, t) = 1$$

  qui est l'équation d'un hyperplan affine de $\mathbb{F}_q^d$, qui est done de cardinal q^{d-1}. Il y a donc $q^d - 1$ choix possibles pour les y_i, q possibilités pour t, et q^{d-1} possibilités pour les z_i, soit un total de $\left(q^d - 1\right) qq^{d-1}$ éléments de cette forme.

Ainsi, on obtient $\#\mathcal{B}' = q^d\left(1 + \left(\frac{a}{q}\right)\right) + \left(q^d - 1\right) qq^{d-1} = \#\mathcal{B}$ d'où

$$(\heartsuit) \quad \#\mathcal{B} = q^d\left(\left(\frac{a}{q}\right) + q^d\right)$$

Etape 3 : Conclusion D'après le point 3. des règles de calcul 2.3.6 on a $\left(\frac{a}{q}\right) = \left((-1)^d\right)^{\frac{q-1}{2}}$

Ainsi en combinant ($\spadesuit$) et ($\heartsuit$) et en remarquant que par définition $q^d \equiv \left(\frac{q}{p}\right)$ on obtient :

$$\begin{aligned} q^d\left(\left((-1)^d\right)^{\frac{q-1}{2}} + q^d\right) &\equiv 1 + \left(\frac{p}{q}\right) \quad [p] \\ \left(\frac{q}{p}\right)\left((-1)^{\frac{p-1}{2}\frac{q-1}{2}} + \left(\frac{q}{p}\right)\right) &\equiv 1 + \left(\frac{p}{q}\right) \quad [p] \\ \left(\frac{q}{p}\right) \times (-1)^{\frac{p-1}{2}\frac{q-1}{2}} + \cancel{\left(\frac{q}{p}\right)^2} &\equiv \cancel{1} + \left(\frac{p}{q}\right) \quad [p] \end{aligned}$$

Finalement comme les symboles de Legendre $\left(\frac{q}{p}\right)$ et $\left(\frac{p}{q}\right)$ valent plus ou moins 1 et comme $p \neq 2$, cette égalité est aussi vrai dans $\mathbb{Z}$, ce qui prouve le résultat. ■

Exemple : Le symbole de Legendre nous permet de savoir si une équation arithmétique quadratique modulo p admet des solutions. Par exemple : $X^2 = 219$ admet-elle une solution modulo 383 ? On calcule le

symbole de Legendre :

$$\begin{aligned}\left(\frac{219}{383}\right) &= \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)\\ &= -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right)\\ &= -\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right)\\ &= \left(\frac{2}{73}\right) \qquad\qquad = 1\end{aligned}$$

La réponse est donc oui.

Remarque : Symbole de Jacobi et test de primalité de Solovay-Strassen : Comme on l'a déjà vu le symbole de Legendre est multiplicatif par rapport à la variable du haut. On peut forcer la multiplicativité par rapport à la variable du bas en définissant le *symbole de Jacobi* : soit $N = \prod_{k=1}^{r} q_k^{\alpha_k}$ un entier impair ≥ 2 décomposé en facteurs premiers, pour tout $a \in \mathbb{Z}$ on pose :

$$\left(\frac{a}{N}\right) = \left(\frac{a}{q_1}\right)^{\alpha_1} \ldots \left(\frac{a}{q_k}\right)^{\alpha_k}$$

Le symbole de Jacobi ne permet plus de tester si x est un résidu quadratique modulo n. En revanche, on peut toujours le calculer en utilisant la loi de réciprocité quadratique, valable pour tous entiers impairs premiers entre eux. Le symbole de Jacobi est à la base du test de primalité de Solovay-Strassen : on choisit un entier premier avec n. On calcule $a^{(n-1)/2} \bmod n$, puis le symbole de Jacobi $\left(\frac{a}{n}\right)$. L'entier n satisfait au test si :

$$a^{\frac{a-1}{2}} \equiv \left(\frac{a}{n}\right) \ [n]$$

D'après un théorème d'Euler, si n est premier, il satisfait au test de Solovay-Strassen pour tout entier a. S'il n'est pas premier, on prouve qu'il existe au moins un entier premier avec n sur deux pour lequel n ne satisfait pas le test. Si on effectue k tests successifs, avec des entiers a différents chaque fois choisis au hasard, la probabilité pour que n soit premier s'il satisfait à chacun des tests est de l'ordre de $1 - 1/2^{\mathrm{k}}$.

Algorithm 1: Test de Solovay-Strassen

Data: n un entier impair dont on veut connaître la primalité ;
k le nombre maximum de fois où le symbole de Jacobi va être calculé.
for $i = 0$ *to* $k - 1$ **do**
  choisir a au hasard entre 2 et n–1
  $x \leftarrow \left(\frac{a}{n}\right)$
  if $x = 0$ *ou* $x \not\equiv a^{\frac{a-1}{2}}\ [n]$ **then**
    return Composé
  end
end
return Probablement premier

Source : https://www.bibmath.net/crypto/index.php?action=affiche&quoi=complements/symblegendre

Chapitre 3

A la recherche des nombres premiers

Sources : *Mathématiques pour l'agrégation : Algèbre et géométrie*, J.E. ROMBALDI chapitre 11 [2], *Cours d'Algèbre* M.DEMAZURE chapitre 2 et 5 [6] et Les Maths en Tête : Algébre de Xavier GOURDON chapitre 1 [5]

On sait désormais ce que sont les nombres premiers et pourquoi ils sont importants en arithmétique. Nous avons également démontré qu'il y avait un nombre infini de nombres premiers. Il est alors naturel de se demander comment sont répartis les nombres premiers. Cette question qui peut sembler simple est en réalité extrêmement complexe, à vrai dire le problème est à l'heure actuelle toujours ouvert. On dispose cependant de quelques résultats positifs (dont certains très compliqués) qui viennent nous informer sur cette répartition sans pour autant la décrire totalement. Il est en fait plus que probable que la résolution de ce problème nécessite l'intervention de domaines des mathématiques très différents de l'arithmétique mais cela nous amènerait bien au delà du propos de ce mémoire.

Si le problème de la répartition des nombres premiers n'est pas encore résolu, disposons-nous tout de même d'un moyen simple d'identifier les nombres premiers, ou de calculer la décomposition d'un entier en produit de facteurs premiers ? Là encore la question a beau être simple la réponse est nettement plus complexe. On dispose en effet de certains critères mais ils ne sont pas parfaits. En un sens heureusement puisque c'est cette difficulté à identifier les nombres premiers qui permet de créer certains des cryptosystèmes qui protègent notre vie numérique.

3.1 Répartition asymptotique des nombres premiers

Si $n \in \mathbb{N}^*$ on note $\mathcal{P}_n = \mathcal{P} \cap [\![1, n]\!]$ et $\pi(n) = \#\mathcal{P}_n$. On remarque que, d'après le théorème d'Euclide que nous avons démontré au premier chapitre on a $\pi(n) \underset{n\to+\infty}{\longrightarrow} +\infty$. On souhaite maintenant estimer plus précisément le comportement de $\pi(n)$ quand n tend vers $+\infty$.

On dispose d'un résultat précis sous la forme d'un équivalent pour $\pi(n)$. Ce résultat est connu sous le nom de *théorème des nombres premiers*, sa démonstration fait appel à de l'analyse complexe et dépasse le cadre de ce mémoire, nous nous contenterons donc d'admettre ce théorème.

Théorème 3.1.1 (Théorème des nombres premiers)**.** $\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln(n)}$

Démonstration. Voir [8] Annexe C ou [9] Chapitre XII ■

On en déduit

Corollaire 3.1.2 (Théorème de raréfaction de Legendre)**.** $\frac{\pi(n)}{n} \underset{n\to+\infty}{\longrightarrow} 0$

On dispose cependant d'un résultat sur la répartition asymptotique des nombres premiers qui ne fait appel qu'à des raisonnements arithmétiques.

Théorème 3.1.3 (Inégalité de Tchebychev)**.** *Pour tout entier $n \neq 3$ on l'encadrement suivant*

$$\ln(2)\frac{n}{\ln(n)} \leq \pi(n) \leq e\frac{n}{\ln(n)}$$

Corollaire 3.1.4. *Soit $n \geq 2$ un entier, on rappelle qu'on a noté p_n le n-ième nombre premier. On a alors l'encadrement*

$$\frac{1}{e} n \ln(n) \leq p_n \leq \frac{2}{\ln(2)} n \ln(n)$$

Application : On en déduit par exemple que $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$

3.2 Critères de primalité

Désormais nous savons que plus un nombre est grand moins il a de chance qu'il soit premier, on peut alors se demander comment savoir si un nombre est premier ou pas.

3.2.1 Un premier critère naïf

Dans un premier temps, étant donné un entier n dont on veut savoir s'il est premier, on peut chercher a simplement appliquer la définition et a vérifier la divisibilité de n par tous les entiers entre 2 et n, si aucun d'eux ne divisent n alors n est premier. En fait on n'est pas obligé de vérifier pour tous les entiers inférieurs à n :

Proposition 3.2.1. *Soit $n \geq 2$ un entier non premier, alors n a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$*

Corollaire 3.2.2 (Critère de primalité naïf)**.** *Pour savoir si n est premier on peut tester sa divisibilité avec tous les entiers entre 2 et $m = \lfloor \sqrt{n} \rfloor$, si aucun ne parvient à le diviser alors n est premier.*

Application : Crible d'Eratosthéne Du critère de primalité naïf on déduit ce qui historiquement vu sûrement le premier algorithme d'énumération des nombres premiers : le crible d'Erastosthéne.

Soit N un entier, on veut énumérer tous les nombres premiers inférieurs à N. Pour ce faire on commence par placer dans une grille tous les entiers de 2 à N. On va procéder par élimination en supprimant de la grille tous les multiples d'un entier autre que lui-même. En premier on raye les multiples de 2, puis les multiples de 3 restants, puis les multiples de 5 restants, et ainsi de suite en rayant à chaque fois tous les multiples du plus petit entier restant.

Le corollaire ci dessus affirme que lorsque le carré du plus petit entier restant est supérieur à N alors on peut s'arrêter puisque dans ce cas, tous les non-premiers de la grille ont été rayés lors des étapes précédentes. Il ne reste alors plus que les entiers qui ne sont multiples que de 1 et d'eux-mêmes, autrement il reste exactement les nombres premiers. (Source : Wikipedia)

~~01~~	**02**	**03**	~~04~~	**05**	~~06~~	**07**	~~08~~	~~09~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

Exemple Crible d'Eratosthéne pour $N = 100$.

Algorithm 2: Crible d'Erastosthéne

Data: n un entier, la taille maximale du crible
$L =$ tableau de booléen de taille n, initialisé à Vrai
Mettre à Faux les cases d'indice pair > 2
$L[1] = Faux$
$i = 3$
while $i^2 \leq n$ **do**
  if $L[i]$ **then**
    for $j = i^2$ *to* n *par pas de* $2 \times i$ **do**
      $L[j] =$ *Faux*
    end
  end
  $i = i + 1$
end
return L

3.2.2 Un critère probabiliste : le test de Miller-Rabin

On s'intéresse maintenant à un test de primalité probabiliste : étant donné un entier n, il peut soit conclure de manière certaine que n est composé soit que n est probablement premier. La probabilité qu'un nombre déclaré premier soit en réalité composé pouvant être rendu aussi faible que souhaitée.

On déduit du petit théorème de Fermat que :

Proposition 3.2.3. *Soit $p > 2$ un nombre premier, on note $s = v_2(p-1)$ et d l'entier impair tel que $p - 1 = 2^s \times d$. Alors, pour tout entier a qui n'est pas divisible par p :*

$$a^d \equiv 1 \quad [p] \qquad ou \qquad \exists r \in [\![0, s-1]\!], \quad a^{2^r d} \equiv -1 \quad [p]$$

Démonstration. Remarquons tout d'abord que dans un corps, l'équation $X^2 = 1$ admet exactement deux solutions : 1 et -1. En particulier, si $p \in \mathcal{P}$ les seuls entiers dont le carré est congru à 1 modulo p sont congrus à 1 ou à -1 modulo p (en considérant le corps fini $\mathbb{F}_p$). Ensuite, d'après le petit théorème de Fermat,

$$a^{p-1} = \left(a^d\right)^{2^s} \equiv 1 \quad [p]$$

et en prenant de façon répétée des racines carrées (i.e. des solution des équations de la forme $x^2 = b) à partir de a^{p-1}$, on obtient soit toujours 1 modulo p, jusqu'à $a^d = 1[p]$, soit pour un certain $0 \leq r < s$, $a^{d2^r} = -1[p]$ (et $a^{d2^i} = 1[p]$ pour $r < i \leq s$), seule autre racine carrée possible de 1 modulo p. ■

Par contraposée, si :

$$a^d \not\equiv 1 \quad [n] \quad \text{et} \quad \forall r \in [\![0, s-1]\!] \quad a^{2^r d} \not\equiv -1 \quad [n] \qquad (\mathfrak{C})$$

alors n est composé, et a est appelé un *témoin de Miller* pour le fait que n est composé. En revanche, si la condition $(\mathfrak{C})$ est réalisée, n n'est pas nécessairement premier. On dit alors que n est *fortement probablement premier* (en base a). Lorsque n n'est pas premier mais pourtant fortement probablement premier en base a, on dit que a est un menteur fort (pour n premier), et que n est *fortement pseudo-premier* (en base a).

Le nombre a peut être choisi sans perte de généralité inférieur à n, plus précisément $1 < a < n$. L'efficacité du test de Miller-Rabin s'appuie sur le théorème (admis) suivant :

Théorème 3.2.4 (Théorème de Rabin)**.** *Soit n un entier impair à au moins deux chiffres et composé. Alors il existe au plus $\frac{\varphi(n)}{4}$ menteurs forts $a \in [\![1, n]\!]$.*

Corollaire 3.2.5. *Soit n un entier impair composé alors au moins $\frac{3}{4}$ des entiers $a \in [\![1, n]\!]$, sont des témoins de Miller pour n.*

Démonstration. Soit n entier impair, composé, à au moins 2 chiffres, alors d'après le théorème il existe au plus $\frac{\varphi(n)}{4}$ menteurs forts $a \in [\![1, n]\!]$ il y a donc au moins $n - \frac{\varphi(n)}{4}$ témoins de Miller pour n dans $[\![1, n]\!]$. Il suffit alors de majorer grossièrement $\varphi(n) \leq n$ pour obtenir le résultat.

Reste à traiter le cas $n = 9$ qui est le seul impair composé à un chiffre. On a $9 - 1 = 8 = 1.2^3$ donc $d = 1$ et $s = 3$. On peut alors faire les calculs à la main et on trouve que seul 1 et 8 ne sont pas témoins de Miller pour 9, il y a donc largement plus de $\frac{3}{4}$ des entiers entre 1 et 9 qui sont des témoins de Miller pour 9. ■

II suffit donc de répéter le test pour suffisamment d'entiers a choisis indépendamment, pour que la probabilité qu'un entier n composé soit déclarée à tort premier devienne très faible. Ainsi le test de Miller Rabin prend la forme suivante (Source : Wikipedia) :

Algorithm 3: Test de Miller-Rabin

Data: n un entier impair ≥ 3, k un entier ≥ 1
for $i = 0$ *to* k **do**
  Choisir a uniformément au hasard dans $[\![2, n–2]\!]$
  if a *est un témoin de Miller pour* n **then**
    return Composé
  end
end
return Probablement premier

où

Algorithm 4: Témoins de Miller-Rabin

Data: n un entier impair ≥ 3, a un entier ≥ 1
Calculer s et d tels que $n - 1 = 2s \times d$ avec d impair et $s > 0$ car n impair
$x := a \times d[n]$
if $x = 1$ *ou* $x = n - 1$ **then**
  return Faux
end
for $i = 0$ *to* $s - 1$ **do**
  $x := x^2[n]$
  if $x = n - 1$ **then**
    return Faux
  end
end
return Vrai

On peut alors déduire de la discussion précédente le résultat suivant qui assure la qualité du test de Miller-Rabin :

> **Théorème 3.2.6** (Critère de Miller-Rabin)**.** *Soit n entier supérieur à 3 et soit $k \in \mathbb{N}^*$. On applique l'algorithme ci dessus avec l'entrée (n, k). Si la sortie du test est Faux alors n est composé de manière certaine, si la sortie du test est Vrai alors n est premier avec probabilité $1 - (\frac{1}{4})^k$.*

Le test de Miller-Rabin s'implémente avec une complexité temporelle en $O(k(\log(n)^3)$ la plupart des calculs étant effectués lors de la recherche d'un témoin de Miller (on procède alors à des exponentiations rapides). La test de Miller-Rabin est également efficace puisque pour k assez grand la probabilité qu'il se trompe est très proche de 0. L'ensemble de ces qualités explique pourquoi ce test est réellement utilisé notamment en informatique.

Application : On peut par exemple utiliser le test de Miller-Rabin pour générer des grands nombres premiers : on génère aléatoirement un grand nombre impair et on vérifie sa primilité avec Miller-Rabin, s'il est premier c'est bon, sinon on recommence. Le théorème des nombres premiers assure que l'on trouvera un nombre premier après un nombre d'essais raisonnablement petit. Bien sûr nous ne sommes pas certains que le nombre ainsi obtenu est premier mais il l'est très probablement. [10]

Remarque Il existe d'autres algorithmes probabilistes de primalité notamment le test de Solovay-Strassen qui utilise les résidus quadratiques et le symbole de Jacobi (voir 2). L'idée fondamentale est que lorsque p est premier la condition $\left(\frac{a}{p}\right) = l$ caractérise les résidus quadratiques, ainsi $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\ [p]$. Cela fournit alors une nouvelle condition nécessaire de primalité dont on peut déduire le test de Solovay-Strassen.

3.3 Utilisation en cryptographie : le cryptosystème RSA

Nous abordons à présent une utilisation des nombres premiers qui nous concerne tous, spécialistes comme béotiens : la cryptographie. En effet nous utilisons au quotidien (parfois sans même le savoir) des cryptosystémes basés sur les nombres premiers, c'est en particulier le cas à chaque fois que l'on utilise une carte bleue mais plus généralement dès que l'on souhaite échanger une information sécurisée sur internet. L'un des cryptosystèmes les plus utilisée est le chiffrement RSA dont nous allons expliquer le principe mathématique.

On commence par se donner deux grands nombres premiers distincts p et q (par exemple grâce à l'application précédente) et on pose $n = pq$. On se donne également c, d deux entiers tel que $cd \equiv 1[\varphi(n)]$ (dans les faits on choisit e premier avec $\varphi(n)$ puis on calcule son inverse modulo $\varphi(n)$ que l'on appelle d)

Définition 3.3.1. *On définit la* fonction de chiffrement $g : t \in \mathbb{Z}/n\mathbb{Z} \longmapsto t^c \in \mathbb{Z}/n\mathbb{Z}$ *et la* fonction de déchiffrement $f : t \in \mathbb{Z}/n\mathbb{Z} \longmapsto t^d \in \mathbb{Z}/n\mathbb{Z}$

Théorème 3.3.2. *On a* $f \circ g = Id$

Démonstration. Les nombres p et q étant premiers et distincts on a $\varphi(n) = (p-1)(q-1)$ d'après le théorème 2.1.7. On dispose de $k \in \mathbb{Z}$ tel que $cd = 1 + k\varphi(n)$. Soit $t \in \mathbb{Z}/n\mathbb{Z}$ on veut prouver que $t^{cd} \equiv t[n]$, il suffit pour cela de montrer que $t^{cd} \equiv t[p]$ et $t^{cd} \equiv t[q]$ (d'après le théorème chinois). Les nombres premiers p et q jouant des rôles en tout point similaires on se contente de démontrer que $t^{cd} \equiv t[p]$:

- si $pgcd(t, p) = 1$ alors par le théorème de Fermat (2.1.4) on a $t^{p-1} \equiv 1[p]$ donc $t^{cd} \equiv (t^{p-1})^{k(q-1)}t \equiv t\ [p]$.
- si $pgcd(t, p) \neq 1$ alors p divise t et donc $t^{cd} \equiv t \equiv 0\ [p]$.

Par suite comme ceci est vrai pour tout $t \in \mathbb{Z}$ alors $f \circ g = Id$ ■

On peut chiffrer un message (représenté par un élément $t \in \mathbb{Z}/n\mathbb{Z}$) avec la fonction g puis le déchiffrer avec la fonction f. Le couple (n, c) est appelé la *clef publique*, l'entier d la *clef secrète*. La connaissance de la clef publique permet de reconstruire facilement g et donc de chiffrer un message, si on connait en plus la clef secrète on peut reconstruire f et on est donc en mesure de déchiffrer le message. La sécurité de ce système repose sur le fait que connaissant seulement la clef publique il est très difficile de déterminer f. Bien sur si l'on parvenait à décomposer n en produit de facteurs premiers on casserait le chiffrement mais une telle opération est pour le moment impossible dés que les nombres premiers sont suffisamment grands et correctement choisis. En d'autres termes tout le monde peut chiffrer un message grâce à la clef publique mais seul les détenteurs de la clef privée sont en mesure de déchiffrer le message en un temps raisonnable.

La robustesse du chiffrement RSA en fait une méthode encore couramment utilisée aujourd'hui bien qu'il ait été inventé dans les années 1970. Son apparition à provoqué un regain d'intérêt pour les algorithmes de factorisation et de primalité.

Bibliographie

[1] J-P. Delahaye. *Merveilleux nombres premiers*. Belin, 2013.

[2] J.E. Rombaldi. *Mathématiques pour l'Agrégation : Algèbre & géométrie*. De Boeck Supérieur, 2017.

[3] D. Perrin. *Cours d'algèbre*. Ellipses, 1996.

[4] G. Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018.

[5] X. Gourdon. *Les Maths en Tête : Algèbre*. Ellipses, Paris, 2eme edition, 2009.

[6] M. Demazure. *Cours d'algèbre*. Nouvelle bibliothèque mathématique. Cassini, 2008.

[7] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries.* Calvage & Mounet, 2013.

[8] X. Gourdon. *Les Maths en Tête : Analyse*. Ellipses, Paris, 2eme edition, 2008.

[9] H. Queffélec and C. Zuily. *Analyse pour l'Agrégation*. Dunod, 5e edition, 2020.

[10] J. Buchmann. *Introduction la cryptographie*. Sciences sup. Dunod, Paris, 2006.