Numéro d'ordre : 634

THÈSE

pour l'obtention du Grade de

Docteur de l'Université de POITIERS

(Faculté des Sciences Fondamentales et Appliquées)

(Diplôme national — Arrêté du 30 mars 1992)

SPÉCIALITÉ : MATHÉMATIQUES

Présentée par : François Arnault

-=-=-=-=-=-=-=-

Sur quelques tests probabilistes de primalité

-=-=-=-=-=-=-=-

Soutenue le 7 décembre 1993

Commission d'Examen :

P. Torasso,	Professeur à l'Université de Poitiers	Président
H. Cohen,	Professeur à l'Université de Bordeaux	Rapporteurs
J.H. Davenport,	Professeur à l'Université de Bath	Rapporteurs
G. Robin,	Professeur à l'Université de Limoges	Rapporteurs
J.M. Goursaud,	Professeur à l'Université de Poitiers	Directeur de thèse
F. Morain,	Ingénieur de l'Armement à l'Ecole Polytechnique	Examinateurs
C. Quitté,	Maître de Conférences à l'Université de Poitiers	Examinateurs

François ARNAULT
Université de Poitiers, Département de Mathématiques
40, av du Recteur Pineau, 86022 Poitiers Cedex FRANCE
E-Mail : arnault@knuth.univ-poitiers.fr

Résumé

Nous étudions dans cette thèse quelques tests probabilistes de primalité, en particulier ceux qui, vraisemblablement à cause de leur simplicité et de leur rapidité d'éxécution, sont implantés dans les systèmes de calcul formel usuels.

Nous commençons par présenter dans le chapitre 1 le test probabiliste de primalité le plus connu : le test de Rabin. Nous rappelons entre autres le théorème de Rabin, qui permet de majorer la probabilité d'echec de ce test.

Nous donnons dans les chapitres 3 et 6 deux méthodes permettant de construire des nombres composés déclarés premiers par le test de Rabin des systèmes de calcul formel comme Axiom et Maple. Quelques rappels sur les lois de réciprocité, utiles pour la première de ces méthodes sont rassemblés dans le chapitre 2.

Nous étudions aussi le test de Lucas (chapitre 4), d'un point de vue aussi algébrique que possible, en mettant en valeur l'analogie avec les pseudo-premiers classiques. Nous démontrons un analogue, pour les pseudo-premiers de Lucas, du théorème de Rabin. Précisément, nous montrons que, mises à part quelques rares exceptions bien cernées, le nombre de couples (P, Q) pour lesquels un nombre composé n est pseudo-premier de Lucas est majoré par $4n/15$. Nous montrons aussi dans le chapitre 6 que l'une des méthodes proposées pour construire des pseudo-premiers forts classiques s'adapte pour produire des pseudo-premiers forts de Lucas.

Nous étudions dans le chapitre 5 une fonction introduite dans le chapitre précédent et qui décrit le nombre d'éléments de norme 1 dans l'anneau des entiers d'un corps quadratique quotienté par un entier rationnel.

Enfin, nous terminons par un aperçu de quelques autres tests probabilistes de primalité, et utilisons dans quelques cas particuliers, des variantes de la méthode du chapitre 6 pour produire des nombres admissibles pour un test dû à Adams, Kurtz, Schanks et Williams, et pour produire des pseudo-premiers elliptiques forts.

Mots-clé

Tests probabilistes de primalité, Nombres pseudo-premiers, Pseudo-premiers de Lucas, Suite de Perrin, Courbes elliptiques, Systèmes de calcul formel, Entiers quadratiques, Lois de réciprocité.

Abstract

In this work, we study some probabilistic primality tests. We emphasize those which, because of their simplicity and running time, are implemented in most computer algebra packages.

In chapter 1, we describe the most known probabilistic primality test : the Rabin test. We recall the Rabin's theorem, which bounds the probability this test fails showing a number to be composite.

We give, in chapters 3 and 6, two ways for building composite numbers, which are found to be prime by the Rabin test of packages as Axiom or Maple. Before, we recall in chapter 2, some results about reciprocity which are useful for the first way.

We also study the Lucas test (chapter 4), in a point of view as algebraic as possible, bringing the connections with the Rabin test to light. We prove a similar result to the Rabin theorem for the Lucas test. We also show in chapter 6 that we can build Lucas strong pseudoprimes, using a variation of one of the two preceeding ways.

The chapter 5 is devoted to the analysis of a number theoretic function, introduced in the previous chapter. This function describes the number of norm 1 elements in the ring of integers of a quadratic field modulo a rational integer.

We conclude by an overview of other probabilistic primality tests. We use variations of the chapter 6 method to build composite numbers, which pass a primality test involving cubic fields, and some strong elliptic pseudoprimes.

Key-words

Probabilistic primality tests, pseudoprimes, Lucas pseudoprimes, Perrin sequence, Elliptic curves, Computer algebra systems, Quadratic integers, Reciprocity laws.

Remerciements

Je remercie tout d'abord Jean-Marie Goursaud, qui a bien voulu me donner la possibilité de préparer une thèse et faire ainsi mes premiers pas dans la recherche.

Je voudrais aussi exprimer ma reconnaissance aux nombreux membres ou responsables du Laboratoire de Mathématiques de Poitiers, et en particulier à Pierre Torasso, qui a bien voulu m'accueillir au sein de l'URA et accepter de présider la commission d'examen.

J'ai eu le grand plaisir de rencontrer plusieurs fois les membres du Département de Mathématiques de Limoges. Je leur exprime ma sympathie et je remercie en particulier Guy Robin, pour avoir accepté de rapporter sur ce mémoire, d'avoir corrigé quelques erreurs et de m'avoir suggéré de nouvelles idées. Je lui dois en particulier celles du chapitre 5.

Je remercie James H. Davenport qui, malgré son emploi du temps chargé, a pris le temps de rapporter sur cette thèse, ainsi que pour sa participation au grand projet Axiom.

Je remercie Henri Cohen, dont les écrits m'ont souvent inspiré, et qui a bien voulu, lui aussi, accepter la tâche de rapporteur.

Merci à François Morain, qui s'est intéressé de très près à ce travail, qui a eu la gentillesse de m'inviter quelques jours à l'INRIA Rocquencourt et qui a attiré mon attention sur les pseudo-premiers de Lucas.

Je dois à Patrice Naudin le système XWEB de documentation de programmes "*Literate Programming*" dont je suis un utilisateur privilégié. Grâce à lui, j'ai pu rédiger l'appendice de ce mémoire. Je dois aussi à Patrice de précieux conseils pour l'usage de TEX.

J'exprime aussi mes remerciements à toutes les personnes du Laboratoire de Mathématiques, qui ont pu contribuer à ce travail durant ces trois dernières années. Je pense en particulier aux tâches administratives, de documentation, ou de reprographie.

Enfin et surtout, en quelques lignes bien trop courtes, je tiens le plus sincèrement à remercier Claude Quitté. Avec le plus grand désintérêt, il m'a guidé et encouragé tout au long de ce travail.

Table des matières

Chapitre 0

■ **Introduction** — **1**

1. — Tests de primalité — 1
2. — Bibliographie — 3

Chapitre 1

■ **Nombres pseudo-premiers et test de Rabin** — **5**

1. — Nombres pseudo-premiers, fortement pseudo-premiers... — 5
2. — Le test de Rabin — 8
3. — Démonstration du théorème de Rabin — 9
4. — Bibliographie — 12

Chapitre 2

■ **Réciprocité** — **15**

1. — Symbole de restes de puissances $m^{\text{ièmes}}$ — 15
2. — Le cas des puissances quatrièmes — 17
3. — Réciprocité — 17
4. — Réciprocité biquadratique — 18
5. — Bibliographie — 19

Chapitre 3

■ **Nombres composés pseudo-premiers forts dans plusieurs bases** — **21**

1. — Nombres fortement pseudo-premiers dans une base — 21
2. — L'intervention des lois de réciprocité — 24
3. — Plusieurs bases — 26
4. — Quelques exemples — 27
5. — Bibliographie — 30

Chapitre 4

■ **Suites de Lucas et pseudo-premiers de Lucas** — **31**
1. — Suites de Lucas — 31
2. — Structure modulaire de l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ — 34
3. — Eléments de norme 1 — 35
4. — Liens entre les paramètres P et Q et l'élément τ — 38
5. — Formules de dénombrement — 40
6. — Analogues du théorème de Rabin — 43
7. — Analogues des nombres de Carmichael — 48
8. — Bibliographie — 49

Chapitre 5

■ **Estimations de la fonction ϕ_D** — **51**
1. — Rappels — 51
2. — Préliminaires — 53
3. — La fonction ψ — 54
4. — Progressions arithmétiques — 55
5. — Produits partiels — 55
6. — La fonction ϕ_D — 57
7. — Bibliographie — 59

Chapitre 6

■ **Nombres de Carmichael fortement pseudo-premiers, pseudo-premiers forts de Lucas, dans plusieurs bases** — **61**
1. — Motivations — 61
2. — Préliminaires — 62
3. — Nombres de Carmichael fortement pseudo-premiers — 63
4. — Théorèmes d'extension — 64
5. — Application aux tests de primalité de Maple et d'Axiom — 66
6. — Construire des pseudo-premiers de Lucas — 69
7. — Exemple — 71
8. — Problème ouvert — 72
9. — Bibliographie — 73

Chapitre 7

■ **D'autres tests probabilistes de primalité** **75**
1. — Généralisations des suites de Lucas 75
2. — La suite de Perrin 75
3. — Corps de degré quelconque 81
4. — Pseudo-premiers elliptiques 82
5. — Bibliographie 88

Chapitre 0

Introduction

Le développement des ordinateurs a profondément bouleversé de nombreuses branches des mathématiques.* Parmi les domaines qui ont subi la plus grande révolution, il y a l'un des plus anciens et des plus riches : la *Théorie des Nombres*. Au cœur même de cette théorie, on trouve bien sûr le théorème fondamental de l'arithmétique :

0.1. — Théorème. *Tout entier naturel supérieur à 1 se décompose en un produit de facteurs premiers. De plus, cette décomposition est unique à l'ordre près des facteurs.*

L'importance de ce théorème est cruciale : calculer le cardinal du groupe des inversibles modulo un entier revient en fait à factoriser cet entier. De même, le fait qu'un entier soit somme de deux carrés est étroitement lié à sa factorisation. Plus généralement, la plupart des fonctions importantes en arithmétique s'expriment naturellement à partir de la factorisation de leurs arguments.

Or, ce théorème, si important soit-il, n'est pas (encore ?) totalement effectif. En effet, s'il est facile de trouver la décomposition de petits nombres n, nous verrons qu'il devient très difficile de faire de même au fur et à mesure que la taille de n augmente. En fait, le théorème fondamental fait apparaître deux problèmes distincts du point de vue effectif. Premièrement celui de factoriser les entiers (i.e. en trouver des facteurs propres). Deuxièmement, celui de déterminer si ces facteurs peuvent eux-mêmes être factorisés ou bien s'ils sont premiers. L'objet de ce travail concerne principalement le second problème.

1. Tests de primalité

Test naïf

Bien sûr, il est clair qu'il existe un algorithme qui permet de résoudre à la fois les deux problèmes de la factorisation et de la primalité (c'est-à-dire une procédure qui permet de déterminer, en un nombre fini d'opérations, la décomposition d'un entier quelconque en facteurs premiers). En voici un connu de tous : essayer successivement de diviser (i.e. vérifier si le reste de la division euclidienne est nul) le nombre n à tester par les entiers 1, 2, ..., jusqu'à la partie entière de $\sqrt{n}$. Si aucune de ces divisions entières ne se révèle exacte, alors n est premier. Sinon, on trouve ainsi le plus petit diviseur non trivial d de n et il suffit de réappliquer la même procédure à n/d pour compléter la décomposition de n.

Même si cette méthode peut être accélérée d'un facteur constant important si l'on remarque que les divisions par les nombres pairs (sauf 2) sont inutiles, voire que les divisions par les multiples de 3, 5, ..., sont aussi inutiles (factorisation "à la roue"), elle reste de

* En fait, les mathématiques effectives sont nées bien avant les ordinateurs : l'algorithme d'Euclide, méthode efficace du calcul de pgcd, est vieux de 22 siècles.

complexité bien trop grande ($O(\sqrt{n}\log n)$). Elle est par exemple tout à fait inutilisable pour des nombres dont la taille est de l'ordre de quelques centaines de chiffres dont les méthodes modernes de cryptographie font grand usage.

Tests déterministes

Fort heureusement, il existe d'autres méthodes bien plus efficaces pour tester et prouver qu'un nombre est premier. Les plus performantes à l'heure actuelle sont celle de Cohen et Lenstra, qui fait usage de sommes de Gauss et de Jacobi [1] [3] et, plus récemment, celle due à Atkin et Morain, utilisant des courbes elliptiques [6] [8]. Ce dernier test a d'ailleurs été le premier capable de prouver la primalité de n'importe quel nombre (premier !) de mille chiffres. Il a même été utilisé avec succès pour des nombres de 1500 chiffres environ [7].

Tests adaptés à une certaine classe de nombres

Pour certaines classes de nombres bien précises, on dispose de tests de primalité spécifiques, bien plus rapides que les méthodes "tous usages". C'est le cas des nombres de Fermat, nombres de la forme $F_n = 2^{2^n} + 1$, et du test de Pépin :

1.1. — Test de Pépin. *Soit $b = 3$, 5 ou 10. Le nombre de Fermat F_n, pour $n \geq 2$, est premier si et seulement si la relation suivante est vérifiée :*

$$b^{(F_n-1)/2} \equiv -1 \text{ modulo } F_n.$$

C'est aussi le cas des nombres de Mersenne, nombres de la forme $M_q = 2^q - 1$, et du test de Lucas-Lehmer qui est un cas particulier des tests étudiés dans le chapitre 4 :

1.2. — Test de Lucas-Lehmer. *Soit $q \geq 3$ un entier impair et soit $(L_i)_{i\in\mathbb{N}}$ la suite de Lucas-Lehmer définie modulo M_q par*

$$L_0 = 4, \qquad L_{i+1} = L_i^2 - 2 \text{ modulo } M_q \quad \textit{pour } i \geq 0.$$

Alors le nombre M_q est premier si et seulement si $L_{q-2} \equiv 0$ modulo M_q.

C'est principalement grâce à ce test que l'on a pu établir la liste des 31 premiers nombres de Mersenne premiers. Ce sont les M_q pour q appartenant à la liste

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607,$$
$$1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937,$$
$$21701, 23209, 44497, 86243, 110503, 132049, 216091.$$

Pour les curieux, notons que le nombre M_{216091} possède 65050 chiffres décimaux et que le plus grand nombre premier connu à ce jour est M_{756839}, qui possède 227832 chiffres décimaux. Sa découverte, en mars 92, est due à Slowinsky et Gage (et bien sûr, au test de Lucas-Lehmer). Elle a nécessité 19 heures de calculs sur un Cray II.

Tests probabilistes

Même si des tests comme celui d'Atkin et Morain permettent de prouver la primalité de nombres de plus de mille chiffres, cette opération n'est pas devenue des plus banales car elle demande une puissance de calcul énorme : pour prouver la primalité de

$$N_{3539} = \frac{2^{3539}+1}{3},$$

il a fallu à ce test un mois et demi et douze stations SUN, pour un total cumulé de 319 jours de temps CPU !

Or, il se trouve qu'il existe une autre classe de tests de primalité, dits tests probabilistes par opposition aux tests précédents qui sont dits déterministes*. Ici, l'adjectif probabiliste* signifie que le test donne une réponse à la question "le nombre n est-il premier ?" sans avoir une **preuve** que la réponse est juste mais seulement une quasi-certitude. Plus précisément, tous les tests probabilistes que nous rencontrerons recherchent par différents moyens une preuve que leur argument est composé. Si une telle preuve est trouvée, le test déclare que le nombre est composé. Si au contraire aucune telle preuve n'est trouvée après des efforts jugés suffisants, le test déclare que le nombre est "très probablement premier", avec une probabilité d'erreur infime, inférieure à une constante connue.

Les tests probabilistes nous font perdre des certitudes mais nous font gagner beaucoup de temps : il faut moins de deux heures aux systèmes de calcul formel comme `ScratchPad` ou `Maple` pour montrer qu'un nombre de la taille de N_{3539} est probablement premier. Il faut seulement quelques secondes à ces tests pour traiter des nombres de cent ou deux cents chiffres, ce qui les rend extrèmement attrayants pour des applications courantes.

Soulignons aussi le fait suivant : même si la possibilité existe que de tels tests probabilistes répondent qu'un nombre composé est "probablement premier", la probabilité qu'un tel événement arrive est si faible qu'il n'est pas à redouter en pratique. Il est par exemple raisonnable de penser qu'un tel événement n'est jamais arrivé depuis la naissance de ces systèmes de calcul formel, hormis dans les occasions où, comme c'est le cas dans ce mémoire, quelqu'un déploie une volonté certaine à les tromper. En tout cas la sécurité des tests probabilistes que nous étudierons reste en particulier très largement suffisante pour des applications courantes ou commerciales (vente de clés pour RSA, par exemple).

2. Bibliographie

[1] L.M. Adleman, C. Pomerance, R.S. Rumely : *On distinguishing prime numbers from composite numbers.* Annals of Mathematics, n° 117, 1983, pp. 173–206.

[2] H. Cohen : *Cryptographie, factorisation et primalité : l'utilisation des courbes elliptiques.* Journée annuelle de la Société Mathématique Française, 1987.

[3] H. Cohen, H.W. Lenstra, Jr. : *Primality testing and Jacobi sums.* Mathematics of Computation, vol. 42, N° 165, janvier 1984, pp. 297–330.

* On utilise souvent les adjectifs probabiliste et déterministe avec une toute autre signification qu'il faut se garder de confondre avec celle qui est entendue ici.

[4] J.D. Dixon : *Factorization and primality tests.* American Mathematical Monthly, vol. 91, 1974, pp. 333-352.

[5] D.E. Knuth : *The Art of Computer Programming. Tome 2 : Semi-numerical algorithms.* Addison-Wesley, 1973.

[6] F. Morain : *Courbes elliptiques et tests de primalité.* Thèse, Université Lyon I, septembre 1990.

[7] F. Morain : *Prime values of partition numbers and the primality of* $p(1840926)$. Rapport de recherche LIX/92/RR/11, Laboratoire d'informatique de l'Ecole Polytechnique.

[8] F. Morain : *Elliptic curves and primality proving.* Mathematics of computation, vol. 61, n$^\circ$ 203, juil. 1993, pp. 29–68.

[9] P. Naudin, C. Quitté : *Algorithmique Algébrique.* Masson, 1992.

[10] V.R. Pratt : *Every prime has a succint certificate.* SIAM Journal of Computing, vol. 4, 1975, pp. 214–220.

[11] P. Ribenboim : *The Book of Prime Number Records.* Springer-Verlag, 1988.

[12] H. Riesel : *Prime Numbers and Computers Methods for Factorizations.* Birkaüser Boston Inc., 1985.

[13] H.W. Lenstra, Jr. : *Primality testing with Artin symbols.* dans : N. Koblitz (ed.), Number Theory related to Fermat's last theorem, Progress in Mathematics, vol. 28, Birkhäuser, Boston, 1982.

[14] A.K. Lenstra, H.W. Lenstra, Jr. : *Algorithms in Number Theory.* in : Hand Book of Theoretical Computer Science, Chap 12, J. van Leeuwen (ed.), 1990.

Chapitre 1

Nombres pseudo-premiers et test de Rabin

Le test de Rabin est certainement le test de primalité qui est le plus utilisé et le plus répandu dans les bibliothèques des systèmes de calcul formel (citons `Maple` [8], `Pari` [4], `Axiom` [2]). Les raisons de son succès sont liées à sa simplicité : ce test est extrêmement facile à programmer et très rapide d'exécution (sa complexité est en $O(\log n)^3$). Bref, ce test serait idéal et rendrait caduque toute recherche dans le domaine des tests de primalité s'il n'était pas "probabiliste" dans le sens que nous précisons maintenant.

Le test de Rabin accepte comme donnée un nombre entier positif n et fournit comme résultat l'une des deux réponses suivantes : (a) Le nombre n est composé, (b) Le nombre n est "presque certainement premier". Par la seconde réponse, on entend que n appartient à un sous-ensemble de $\mathbb{N}$ qui est constitué de tous les nombres premiers ainsi que de quelques exceptions. De telles exceptions sont en fait si rares que nous n'avons pas trouvé, dans la littérature sur le sujet, de nombres fortement pseudo-premiers dans suffisamment de bases pour être susceptibles d'être déclarés premiers par les implantations courantes du test de Rabin. Nous décrirons dans les chapitres 3 et 6 deux méthodes que nous avons conçues et qui nous ont permis d'exhiber de telles exceptions et d'en construire de nombreux exemples.

Notons que le test de Rabin est totalement rigoureux quand il déclare qu'un nombre est non premier. C'est pourquoi certains préfèrent l'appeler "test de non-primalité" plutôt que "test de primalité". La plupart des notions exposées dans ce chapitre sont extraites de nombreux articles ou ouvrages. Parmis eux, citons [3], [5], [7], [11] et [13]. Citons aussi [9] où l'on décrit une variante du test de Rabin, qui est déterministe si l'Hypothèse de Riemann Généralisée est vraie.

1. Nombres pseudo-premiers, fortement pseudo-premiers...

Avant de présenter en détail le test de Rabin, nous avons besoin de quelques définitions.

Nombres pseudo-premiers, probablement premiers

1.1. — **Définition.** *Soit $b \in \mathbb{N}^*$. Un entier composé $n \in \mathbb{N}^*$ est dit pseudo-premier de base b s'il vérifie la relation suivante (qui implique que n et b soient premiers entre eux) :*

$$b^{n-1} \equiv 1 \quad \text{modulo } n.$$

Remarques et exemples. D'après le petit théorème de Fermat, tout nombre premier ne divisant pas b vérifie la congruence ci-dessus. Un nombre n, composé ou non, qui vérifie

cette congruence (donc un nombre premier ou pseudo-premier) est parfois dit *probablement premier de base b*. Le nombre $341 = 11 \cdot 31$ est pseudo-premier de base 2, le nombre $91 = 7 \cdot 13$ est pseudo-premier de base 3, le nombre $105 = 3 \cdot 5 \cdot 7$ est pseudo-premier de base 13...

Pour tester si un nombre n est probablement premier dans une base donnée b, il suffit d'élever b à la puissance $n-1$ modulo n. C'est une opération qui ne nécessite pas, même si n a plusieurs dizaines de chiffres, des calculs gigantesques : elle peut être réalisée rapidement par un ordinateur à l'aide d'un algorithme d'exponentiation dichotomique. Ainsi ce test (test de Fermat) peut être un moyen efficace de prouver que n est composé (s'il l'est). Par exemple, pour

$$n = 2^{128} + 1 = 340282366920938463463374607431768211457,$$

il suffit de 128 élévations au carré modulo n pour se rendre compte que $3^{n-1} \not\equiv 1$ modulo n et donc que n n'est pas premier (notons tout de même que le nombre ci-dessus est un nombre de Fermat et que, pour ceux-ci, on dispose d'un test déterministe spécifique, le test de Pépin — cf. théorème 0.1.1 ou bien [16]). Inversement, on apprend en lisant [14] que, pour b fixé, il y a "très peu" de nombres pseudo-premiers de base b. Par exemple, il y a "seulement" 21853 nombres composés et pseudo-premiers de base 2 inférieurs à $25 \cdot 10^9$ et le plus petit d'entre eux est 341. On apprend aussi, en lisant [3], que si l'on pose

$$\beta(n) = \text{nombre de } b \text{ tels que } 1 < b < n-1 \text{ et } n \text{ pseudo-premier de base } b,$$

alors parmi les 421502 nombres n composés impairs inférieurs à 10^6, le rapport $\beta(n)/n$ est inférieur à 10^{-4} pour 292440 d'entre eux (près de 70%). Notons que l'on a la formule exacte suivante pour $\beta(n)$:

1.2. — **Théorème.** *Pour $n = p_1^{r_1} \cdots p_s^{r_s}$ entier positif, le nombre $\beta(n)$ de bases b telles que $1 < b < n-1$ et que n soit probablement premier de base b est égal à*

$$\beta(n) = \prod_{i=1}^{s} \operatorname{pgcd}(n-1, p_i - 1).$$

Nombres de Carmichael

Cependant il existe des nombres composés qui mettent totalement en défaut le test de Fermat : ce sont les *nombres de Carmichael*, dont le plus petit est 561, et qui ont la propriété d'être pseudo-premiers de base b pour tout entier b premier avec eux. Plus précisément :

1.3. — **Définition.** *Un nombre n est dit de Carmichael s'il est composé et s'il est pseudo-premier de base b pour chaque b premier avec n.*

1.4. — **Définition.** *On appelle indicateur de Carmichael la fonction qui, à tout entier naturel $n \geq 2$, associe le plus petit exposant $\lambda(n)$ du groupe des inversibles modulo n, c'est-à-dire le plus petit entier m tel que l'on ait*

$$x^m \equiv 1 \text{ modulo } n \qquad \textit{pour tout } x \textit{ premier avec } n.$$

Parallèlement à l'indicateur d'Euler, l'indicateur de Carmichael se calcule de la manière suivante :

$$\lambda(2) = 1, \qquad \lambda(4) = 2, \qquad \lambda(2^r) = 2^{r-2} \quad \text{pour } r \geq 3,$$
$$\lambda(p^r) = p^{r-1}(p-1) \qquad \text{pour } p \text{ premier impair et } r \geq 1,$$
$$\lambda(n_1 n_2) = \text{ppcm}(\lambda(n_1), \lambda(n_2)) \qquad \text{pour } n_1 \text{ et } n_2 \text{ premiers entre eux.}$$

Un nombre composé est de Carmichael si et seulement si $\lambda(n)$ divise $n-1$.

C'est encore [14] qui nous apprend qu'il existe 2163 nombres de Carmichael inférieurs à $25 \cdot 10^9$ (voir aussi [12]) et c'est seulement très récemment que W.R. Alford, A. Granville et C. Pomerance [1] ont montré que l'ensemble des nombres de Carmichael est infini. C'est en grande partie l'existence de tels nombres qui fait l'intérêt de la définition suivante.

Nombres fortement pseudo-premiers, fortement probablement premiers

1.5. — Définitions. *Soit $b \in \mathbb{N}^*$. Un entier impair $n \in \mathbb{N}^*$ est dit fortement probablement premier de base b s'il vérifie l'une des conditions suivantes, en posant $n-1 = 2^k q$ avec q impair,*

$$b^q \equiv 1 \quad \text{modulo } n$$

ou bien

$$\text{il existe un entier } i \text{ tel que } 0 \leq i < k \text{ et } b^{2^i q} \equiv -1 \text{ modulo } n.$$

Un entier composé fortement probablement premier de base b est dit fortement pseudo-premier de base b.

1.6. — Propriétés. (a) *(Critère de Miller) Si p est un nombre premier et si b n'est pas un multiple de p alors p est fortement probablement premier de base b.* **(b)** *Tout nombre fortement pseudo-premier de base b est pseudo-premier de base b.*

Démonstration — La deuxième affirmation est évidente. Avec les notations de la définition, la première peut se démontrer en considérant le plus petit entier i tel que $b^{2^i q} \equiv 1$ modulo p (il existe, d'après le petit théorème de Fermat). Si $i > 0$ alors $b^{2^{i-1} q} \equiv -1$ modulo p puisque 1 n'admet que deux racines carrées modulo p. Elle peut aussi se démontrer à l'aide de la formule

$$a^{p-1} - 1 = (a^q - 1)(a^q + 1)(a^{2q} + 1) \cdots (a^{2^{k-1} q} + 1)$$

et en utilisant le fait que l'anneau des entiers modulo p est intègre. □

Exemples. Citons $2047 = 23 \cdot 89$, $121 = 11^2$, et $781 = 11 \cdot 71$ qui sont respectivement les plus petits entiers fortement pseudo-premiers dans les bases respectives 2, 3 et 5, et le nombre $3\,215\,031\,751 = 151 \cdot 751 \cdot 28351$ (c'est un nombre de Carmichael) qui est fortement pseudo-premier dans les quatre bases 2, 3, 5 et 7. Cependant, les nombres fortement pseudo-premiers dans plusieurs bases sont rares : dans [14], on apprend que le seul qui

soit inférieur à $25 \cdot 10^9$ et qui soit fortement pseudo-premier dans les bases 2, 3, 5 et 7 est l'exemple ci-dessus. De plus, il n'y a pas d'équivalents forts aux nombres de Carmichael, on a même le théorème suivant :

1.7. — Théorème (Rabin [15]). *Pour n entier impair supérieur à 2, on note*

$$B(n) = \{b \in (\mathbb{Z}/n\mathbb{Z})^* \mid n \text{ est fortement probablement premier de base } b\}.$$

Si n est composé et distinct de 9 alors on a l'inégalité

$$|B(n)| \leq \phi(n)/4$$

où ϕ désigne la fonction indicatrice d'Euler.

Démonstration — Elle fait l'objet de la section 3. □

2. Le test de Rabin

Nous pouvons maintenant décrire le test de Rabin de façon précise. Etant donné un ensemble d'entiers positifs B de cardinal k fini, le test consiste, pour un entier impair n, à déterminer si n est fortement probablement premier de base b pour chacune des bases b éléments de B. Si n est non fortement probablement premier pour une des bases considérées, n est prouvé composé. Si n est fortement probablement premier pour toutes les bases de B, n est "presque certainement premier". Dans ce cas, la probabilité ρ qu'il y ait erreur (i.e. que n soit composé) peut être rendue arbitrairement petite, pourvu que k soit assez grand.

Attention aux probabilités !

Il n'est pas inutile de préciser les différentes probabilités qui interviennent et de rappeler ici l'erreur commune signalée dans [5]. Nous supposerons que le paramètre n est fourni par une fonction de choix et, par abus de langage, on appelera "probabilité que n soit composé" la probabilité que le résultat de la fonction de choix soit composé. Etant donnés deux événements X et Y, notons $\text{prob}(X|Y)$ la probabilité de X relativement à Y, c'est-à-dire la probabilité, lorsque l'événement Y survient, qu'il soit accompagné de l'événement X. La probabilité ρ dont il est question dans le paragraphe précédent est

$$\rho = \text{prob}(n \text{ est composé} \mid n \text{ est déclaré premier}).$$

Or, on déduit du théorème de Rabin la relation

$$\text{prob}(n \text{ est déclaré premier} \mid n \text{ est composé}) \leq 1/4^k.$$

La théorie élémentaire des probabilités indique que

$$\begin{aligned}&\text{prob}(n \text{ est composé} \mid n \text{ est déclaré premier}) \times \text{prob}(n \text{ est déclaré premier}) \\ &= \text{prob}(n \text{ est déclaré premier} \mid n \text{ est composé}) \times \text{prob}(n \text{ est composé})\end{aligned}$$

justifiant ainsi, puisque la probabilité que n soit déclaré premier est minorée par la probabilité que n soit premier, que la probabilité ρ puisse être rendue arbitrairement petite pourvu que k soit choisi suffisamment grand. De plus, les auteurs de [5] montrent que, même si cela ne résulte pas uniquement du théorème de Rabin, on a aussi l'inégalité $\rho \leq 1/4^k$, au moins pour n assez grand.

Implantations

L'ensemble B cité précédemment diffère suivant l'implémentation choisie du test de Rabin et on peut atteindre avec ce test une fiabilité aussi grande que l'on veut en choisissant un ensemble B assez grand. Les implémentations courantes du test utilisent généralement de 5 à 10 bases qui sont choisies ou bien une fois pour toutes ou bien au hasard à chaque utilisation. De plus, le test de Rabin proprement dit est généralement précédé par une recherche systématique de petits facteurs.

Par exemple, le test implanté dans le système de calcul formel `Axiom` est constitué essentiellement de deux phases. Dans la première, le test détermine (par un simple calcul de pgcd), si l'entier passé en paramètre admet un facteur premier compris entre 2 et 313 (le dernier premier dont le carré est inférieur à 10^5). La deuxième phase est un test de Rabin (auquel J. Davenport a apporté quelques améliorations décrites au chapitre 6) qui utilise comme bases l'ensemble des dix premiers nombres premiers impairs $\{3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$. Quand le test d'`Axiom` indique qu'un nombre n est "presque certainement premier", la probabilité qu'il soit réellement premier est, d'après le théorème 1.7 de Rabin et les précisions de [5], supérieure à $1 - 1/4^{10} > 0.99999904$.

3. Démonstration du théorème de Rabin

Racines dans un groupe cyclique

3.1. — **Lemme.** *Soit G un groupe cyclique et q un entier. (a) Le nombre de racines $q^{\text{ièmes}}$ de 1 dans G est* $\operatorname{pgcd}(q, |G|)$. *(b) Un élément x est une puissance $q^{\text{ième}}$ dans G si et seulement si on a*

$$x^{|G|/\operatorname{pgcd}(q,|G|)} = 1.$$

Dans ce cas, le nombre de racines $q^{\text{ièmes}}$ de x dans G est $\operatorname{pgcd}(q, |G|)$.

Démonstration — Posons $d = \operatorname{pgcd}(q, |G|)$. La démonstration de (a) est facile si l'on remarque (grâce aux relations de Bezout) que

$$x^q = 1 \quad \Longleftrightarrow \quad x^d = 1.$$

De même, les puissances $q^{\text{ièmes}}$ de G sont les puissances $d^{\text{ièmes}}$. Il est alors clair que y est une puissance $d^{\text{ième}}$ si et seulement si $y^{|G|/d} = 1$. De plus, si une racine $q^{\text{ième}}$ de x existe, on obtient les autres en la multipliant par les d racines $q^{\text{ièmes}}$ de 1. □

Une formule de dénombrement

3.2. — **Théorème (Monier [10]).** *Soit $p_1^{r_1} \cdots p_s^{r_s}$ la décomposition primaire d'un entier $n > 2$ impair. Posons*

$$\begin{cases} n - 1 = 2^k q \\ p_i - 1 = 2^{k_i} q_i \quad \textit{pour } 0 \le i \le s, \end{cases} \qquad \textit{avec } q,\ q_i \textit{ impairs}$$

en ordonnant les p_i de telle manière que $k_1 \leq \cdots \leq k_s$. Le nombre de bases dans lesquelles n est fortement probablement premier est donné par la formule

$$|B(n)| = \left(1 + \sum_{j=0}^{k_1-1} 2^{js}\right) \prod_{i=1}^{s} \operatorname{pgcd}(q, q_i).$$

Démonstration — L'ensemble $B(n)$ est réunion disjointe des ensembles

$$P(n) = \{b \in (\mathbb{Z}/n\mathbb{Z})^* \mid b^q = 1\},$$
$$Q_j(n) = \{b \in (\mathbb{Z}/n\mathbb{Z})^* \mid b^{2^j q} = -1\}, \quad \text{pour } 0 \leq j \leq k-1$$

que nous allons dénombrer séparément.

• Dénombrons d'abord $P(n)$. Le théorème chinois fournit l'égalité

$$|P(n)| = \prod_{i=1}^{s} |P(p_i^{r_i})|.$$

Mais le lemme 3.1 indique que

$$\begin{aligned} |P(p_i^{r_i})| &= \operatorname{pgcd}(q, \phi(p_i^{r_i})) \\ &= \operatorname{pgcd}(q, p_i - 1) \qquad \text{car } q \text{ est premier avec } n \\ &= \operatorname{pgcd}(q, q_i) \qquad \text{car } q \text{ est impair.} \end{aligned}$$

Donc on a

$$|P(n)| = \prod_{i=1}^{s} \operatorname{pgcd}(q, q_i).$$

• Dénombrons maintenant $Q_j(n)$. Nous avons là aussi

$$|Q_j(n)| = \prod_{i=1}^{s} |Q_j(p_i^{r_i})|. \tag{1}$$

D'après le lemme 3.1, on a

$$\begin{aligned} Q_j(p_i^{r_i}) \neq \emptyset &\iff (-1)^{\phi(p_i^{r_i})/\operatorname{pgcd}(2^j q, \phi(p_i^{r_i}))} = 1 \\ &\iff \frac{2^{k_i} q_i}{2^{\inf(j,k_i)} \operatorname{pgcd}(q, q_i)} \quad \text{est pair.} \end{aligned}$$

Ces conditions sont vérifiées si et seulement si $j < k_i$ et, dans ce cas (toujours d'après le lemme 3.1),

$$|Q_j(p_i^{r_i})| = \operatorname{pgcd}(2^j q, \phi(p_i^{r_i})) = 2^j \operatorname{pgcd}(q, q_i).$$

Donc, d'après (1),

$$|Q_j(n)| = \begin{cases} 0 & \text{si } j \geq k_1, \\ 2^{js} \prod_{i=1}^{s} \operatorname{pgcd}(q, q_i) & \text{si } j < k_1. \end{cases}$$

• Enfin, l'égalité

$$|B(n)| = |P(n)| + \sum_{j=0}^{k-1} |Q_j(n)|$$

permet de conclure en remarquant que, puisque $n \equiv 1$ modulo 2^{k_1} (car $p_i \equiv 1$ modulo 2^{k_1} quel que soit i), on a $k_1 \leq k$. □

Majorations

3.3. — Lemme. *Avec les notations de la proposition 3.2, on a l'inégalité*

$$\frac{|B(n)|}{\phi(n)} \leq \frac{1}{2^{s-1}} \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}}.$$

De plus, si les k_i ne sont pas tous égaux, on a même

$$\frac{|B(n)|}{\phi(n)} \leq \frac{1}{2^s} \prod_{i=1}^{s} \frac{\operatorname{pgcd}(q, q_i)}{q_i} \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}} \leq \frac{1}{2^s} \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}}.$$

Démonstration — D'après 3.2 et puisque $\phi(n) = 2^{k_1+\cdots+k_s} \cdot \prod q_i \cdot \prod p_i^{r_i-1}$, on a

$$\frac{|B(n)|}{\phi(n)} = \frac{1 + \sum_{j=0}^{k_1-1} 2^{js}}{2^{k_1+\cdots+k_s}} \prod_{i=1}^{s} \frac{\operatorname{pgcd}(q, q_i)}{q_i} \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}}. \tag{2}$$

Il est clair que l'on peut minorer le premier facteur du membre de droite de (2) par

$$\begin{aligned} \frac{1 + \sum_{j=0}^{k_1-1} 2^{js}}{2^{sk_1}} &= \frac{1 + (2^{sk_1} - 1)/(2^s - 1)}{2^{sk_1}} \\ &= \left(1 + \frac{2^{sk_1}}{2^s - 1} - \frac{1}{2^s - 1}\right) \Big/ 2^{sk_1} \\ &= \left(1 - \frac{1}{2^s - 1}\right) \Big/ 2^{sk_1} + \frac{1}{2^s - 1}. \end{aligned}$$

Comme le montre la dernière expression, cette quantité est une fonction décroissante de k_1. On peut donc la majorer en remplaçant k_1 par 1 :

$$\frac{1 + \sum_{j=0}^{k_1-1} 2^{js}}{2^{sk_1}} \leq \frac{1}{2^{s-1}}.$$

La démonstration de la première assertion du lemme se termine en remarquant que le deuxième facteur du membre de droite de (2) peut être majoré par 1. La démonstration de la seconde assertion s'obtient de la même façon en remarquant que l'on peut alors minorer $2^{k_1+\cdots+k_s}$ par 2^{sk_1+1}. □

Démonstration du théorème 1.7

On utilise à nouveau les notations de 3.2.

• Supposons d'abord que $s = 1$. Le lemme 3.3 indique que

$$\frac{|B(n)|}{\phi(n)} \leq \frac{1}{p_1^{r_1-1}}.$$

Si $p_1 \geq 5$, le théorème est démontré (car $r_1 > 1$). De même si $p_1 = 3$ et $r_1 \geq 3$. Reste le cas exceptionnel $n = 9$ (pour lequel le rapport vaut $1/3$).

• Supposons maintenant que $s = 2$. Si on a $k_1 < k_2$, le résultat s'obtient par la deuxième assertion du lemme 3.3. Notons que l'on peut obtenir de cette manière une majoration plus forte que $1/4$, sauf dans le cas des nombres de la forme

$$n = (2q_1 + 1)(4q_1 + 1) \qquad (q_1 \text{ impair}),$$

pour lesquels la proposition 3.2 montre que le rapport est exactement $1/4$. Si $k_1 = k_2$ on a, par la première assertion de 3.3,

$$\frac{|B(n)|}{\phi(n)} \leq \frac{1}{2} \frac{\operatorname{pgcd}(q, q_1)}{q_1} \frac{\operatorname{pgcd}(q, q_2)}{q_2}.$$

Mais on montre que l'un au moins des rapports $\operatorname{pgcd}(q, q_i)/q_i$ est majoré par $1/3$ car sinon, on aurait $q_1 \mid q$ et $q_2 \mid q$ ce qui entraînerait que q_1 et q_2 diviseraient

$$\begin{aligned} 2^k q &= p_1 p_2 - 1 = (2^{k_1} q_1 + 1)(2^{k_1} q_2 + 1) - 1 \\ &= 2^{k_1}(q_1 + q_2) + 2^{2k_1} q_1 q_2, \end{aligned}$$

d'où $q_1 = q_2$ ce qui est exclu. On obtient donc $|B(n)|/\phi(n) \leq 1/6$.

• Supposons maintenant que $s \geq 3$. Le résultat est clair par la première assertion du lemme 3.3. Notons là aussi que la majoration obtenue est exactement $1/4$ seulement pour les nombres de la forme

$$n = (2q_1 + 1)(2q_2 + 1)(2q_3 + 1) \qquad \text{avec } q_1,\, q_2,\, q_3 \text{ impairs et divisant } n - 1,$$

pour lesquels la proposition 3.2 montre que le rapport est exactement $1/4$. □

4. Bibliographie

[1] W.R. Alford, A. Granville, C. Pomerance : *There are infinitely many Carmichael numbers.* To appear, 1992.

[2] R. Jenks, R. Sutor : *Axiom, The Scientific Computation System.* Springer-Verlag 1992.

[3] R. Baillie, S. Wagstaff Jr : *Lucas pseudoprimes.* Mathematics of Computation, vol. 35, n° 152, oct. 1980, pp. 1391–1417.

[4] C. Batut : *Aspects algorithmiques du système de calcul arithmétique en multi-précision PARI.* Thèse, Université Bordeaux I, 1989.

[5] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, C. Pomerance : *The generation of random numbers that are probably prime.* Journal of Cryptology, vol 1, 1988, pp. 53–64.

[6] G. Jaeschke : *The Carmichael numbers to* 10^{12}. Mathematics of Computation, vol. 55, n° 191, 1990, pp. 383–389.

[7] H.W. Lenstra, Jr. : *Primality testing.* Proceedings of the CWI symposium, novembre 1983.

[8] B. Char, K. Geddes, G. Gonnet, B. Leong, M. Monagan, S. Watt : *Maple V Library Reference Manual.* Springer-Verlag and Waterloo Maple Publishing, 1991.

[9] G.L. Miller : *Riemann's Hypothesis and tests for primality.* Proceedings of the Seventh Annual ACM Symposium on the Theory of Computing, 4–7 mai 1975, Albuquerque, New Mexico, pp. 234–239.

[10] L. Monier : *Evaluation and comparison of two efficient primality testing algorithms.* Theoretical Computer Science, vol. 11, pp. 97–108, 1980.

[11] P. Naudin, C. Quitté : *Algorithmique Algébrique.* Masson, 1992.

[12] R.G.E. Pinch : *The Carmichael numbers up to* 10^{15}. Mathematics of Computation, vol. 61, n° 203, juil. 1993, pp. 381–391.

[13] J.M. Pollard : *Theorems on factorization and primality testing.* Proceedings of Cambridge Philosophical Society, vol. 76, 1974, pp. 521–528.

[14] C. Pomerance, J.L. Selfridge, S.S. Wagstaff : *The pseudoprimes to* $25 \cdot 10^9$. Mathematics of Computation, vol. 35, n° 151, 1980, pp. 1003–1026.

[15] M.O. Rabin : *Probabilistic algorithms for testing primality.* Journal of Number Theory, vol. 12, 1980, pp. 128–138.

[16] P. Ribenboim : *The Book of Prime Number Records.* Springer-Verlag, 1988.

Chapitre 2

Réciprocité

L'objet de ce chapitre est de présenter le symbole de résidus de puissances quatrièmes et la loi de réciprocité biquadratique qui nous sera utile dans le chapitre 3. Il est essentiellement extrait de [5], qui est l'ouvrage de référence. Pour une présentation attractive, on peut aussi consulter [1]. Pour un traitement particulièrement efficace des notions de bases, il faut bien sûr se référer à [8].

1. Symbole de restes de puissances $m^{\text{ièmes}}$

Pour p premier de $\mathbb{Z}$, le symbole de Legendre induit un caractère multiplicatif

$$\mathbb{Z}/p \ni [a]_p \longmapsto \left(\frac{a}{p}\right)$$

d'ordre 2 du corps $\mathbb{Z}/p$. Le symbole de Legendre est un "symbole de restes de carrés". Pour tout entier $k \geq 2$, on définit de manière analogue un symbole de restes de puissances $m^{\text{ièmes}}$ mais le cadre naturel de cette définition est le corps cyclotomique $\mathbb{Q}(\sqrt[m]{1})$.

Rappels sur les racines $m^{\text{ièmes}}$

Soit ζ une racine primitive $m^{\text{ième}}$ de l'unité. Nous notons $\mathcal{O} = \mathbb{Z}[\zeta]$ l'anneau des entiers de $\mathbb{Q}(\zeta)$.

1.1. — **Proposition.** *Soit p un nombre premier ne divisant pas m et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$ contenant p. Alors les éléments $\zeta, \zeta^2, \ldots, \zeta^{m-1}$ sont tous distincts modulo $\mathfrak{p}$. D'autre part, si $N(\mathfrak{p})$ désigne la norme de $\mathfrak{p}$, alors $N(\mathfrak{p}) \equiv 1$ modulo m.*

Démonstration — Pour montrer la première assertion, il suffit de montrer que

$$\zeta^i \not\equiv 1 \text{ modulo } \mathfrak{p} \qquad \text{pour tout } i \text{ tel que } 1 \leq i \leq m-1.$$

En évaluant l'identité

$$1 + X + X^2 + \cdots + X^{m-1} = \prod_{i=1}^{m-1} (X - \zeta^i)$$

pour $X = 1$, on obtient $m = \prod(1 - \zeta^i)$. Puisque $m \notin \mathfrak{p}$, on en déduit le résultat. Les m classes modulo $\mathfrak{p}$ des racines $m^{\text{ièmes}}$ de l'unité forment un sous-groupe du groupe $(\mathcal{O}/\mathfrak{p})^*$, ce dernier étant d'ordre $N(\mathfrak{p}) - 1$. Cela démontre la fin de la proposition. □

Définition

A tout idéal premier $\mathfrak{p}$ de $\mathcal{O}$ ne contenant pas m on va associer de manière naturelle un caractère multiplicatif d'ordre m du corps $\mathcal{O}/\mathfrak{p}$, appelé le caractère des restes de puissances $m^{\text{ièmes}}$ modulo $\mathfrak{p}$. Pour $\alpha \in \mathcal{O} \setminus \mathfrak{p}$, on a

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \text{ modulo } \mathfrak{p}.$$

D'après la proposition 1.1, il existe une unique racine $m^{\text{ième}}$ ζ^i de l'unité telle que

$$\alpha^{(N(\mathfrak{p})-1)/m} \equiv \zeta^i \text{ modulo } \mathfrak{p}. \tag{1}$$

D'où la définition suivante :

1.2. — Définition. *Pour $\mathfrak{p}$ idéal premier de $\mathcal{O}$ ne contenant pas m et pour $\alpha \in \mathcal{O}$, on appelle symbole de reste de puissance $m^{\text{ième}}$ de α modulo $\mathfrak{p}$ et on note $(\alpha/\mathfrak{p})_m$ l'élément suivant de $\mathcal{O}$:*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m = \begin{cases} 0 & \text{si } \alpha \in \mathfrak{p}, \\ \zeta^i & \text{si } \alpha \notin \mathfrak{p}, \end{cases}$$

où ζ^i est la racine $m^{\text{ième}}$ de l'unité définie par l'équation (1).

On démontre facilement (voir par exemple [5]) les propriétés suivantes :

1.3. — Proposition. *Soient $\alpha, \beta \in \mathcal{O}$ et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$ ne contenant pas m.*

- *Le symbole $(\alpha/\mathfrak{p})_m$ vaut 1 si et seulement si α est une puissance $m^{\text{ième}}$ dans $\mathcal{O}/\mathfrak{p}$.*
- *On a la congruence*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m \equiv \alpha^{(N(\mathfrak{p})-1)/m} \text{ modulo } \mathfrak{p}.$$

- *On a la relation de multiplicativité*

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_m = \left(\frac{\alpha}{\mathfrak{p}}\right)_m \left(\frac{\beta}{\mathfrak{p}}\right)_m.$$

- *Si $\alpha \equiv \beta$ modulo $\mathfrak{p}$, alors*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m = \left(\frac{\beta}{\mathfrak{p}}\right)_m.$$

- *On a l'égalité*

$$\left(\frac{\zeta}{\mathfrak{p}}\right)_m = \zeta^{(N(\mathfrak{p})-1)/m}.$$

- *Pour σ élément du groupe de Galois de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$, on a l'identité*

$$\sigma\left(\frac{\alpha}{\mathfrak{p}}\right)_m = \left(\frac{\sigma(\alpha)}{\sigma(\mathfrak{p})}\right)_m.$$

Notation. Si $\mathfrak{p}$ est un idéal principal $\pi\mathcal{O}$, alors on note indifféremment $(\alpha/\pi)_m$ à la place de $(\alpha/\mathfrak{p})_m$.

2. Le cas des puissances quatrièmes

L'anneau $\mathbb{Z}[i]$

On rappelle que l'anneau $\mathbb{Z}[i]$ est principal (même euclidien), que ses éléments inversibles sont $\pm 1, \pm i$ et que ses irréductibles se répartissent en trois catégories :

- L'élément $1+i$ et ses associés.
- Les premiers rationnels congrus à 3 modulo 4 et leurs associés.
- les éléments $r+is$ dont la norme r^2+s^2 est un premier rationnel congru à 1 modulo 4.

Symbole des restes de puissances quatrièmes

Puisque tout idéal de $\mathbb{Z}[i]$ est principal, nous utiliserons souvent la notation $(\alpha/\pi)_4$ au lieu de $(\alpha/\pi\mathcal{O})_4$. Pour tout irréductible π non associé à $1+i$, et pour tout α tel que $\pi \nmid \alpha$, ce symbole est égal à ± 1 ou à $\pm i$.

En plus des propriétés énoncées par la proposition 1.3, il est clair que le symbole $(\alpha/\pi)_4$ vaut -1 si et seulement si α est un carré mais pas une puissance quatrième dans l'anneau $\mathbb{Z}[i]/(\pi)$.

3. Réciprocité

Réciprocité quadratique

L'un des théorèmes les plus célèbres et importants de l'arithmétique est la *Loi de Réciprocité Quadratique* dont la première démonstration complète et totalement rigoureuse est due à Gauss [3].

3.1. — Théorème (Loi de Réciprocité Quadratique). *Soient p et q deux nombres premiers impairs. On a la relation :*

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

Remarquons que les entiers $-p$ et $-q$ sont des irréductibles de l'anneau $\mathbb{Z}$ mais que l'énoncé ci-dessus n'est plus valable si on les substitue à p ou à q. Cet énoncé de la loi de réciprocité quadratique fait donc jouer aux irréductibles positifs de $\mathbb{Z}$ un rôle privilégié. Pour énoncer la loi de réciprocité biquadratique, nous devons aussi privilégier certains irréductibles de $\mathbb{Z}[i]$ et définir la notion d'élément normalisé, de telle manière que tout irréductible de $\mathbb{Z}[i]$ non associé à $1+i$ sera associé à un unique irréductible normalisé.

Eléments normalisés

3.2. — Définition. *Un entier de Gauss non inversible est dit normalisé s'il est congru à 1 modulo $2+2i$, autrement dit, s'il est congru à 1 ou à $3+2i$ modulo 4, ou encore s'il s'écrit sous la forme $r+is$ avec s pair et $r+s \equiv 1$ modulo 4.*

On vérifie aisément que le groupe des inversibles de $\mathbb{Z}[i]/(4)$ se décompose sous la forme

$$(\mathbb{Z}[i]/4)^\times = \{1, 3+2i\} \times \{1, i, -1, -i\}.$$

Donc, tout élément de $\mathbb{Z}[i]$ inversible modulo 4 (i.e. non divisible par $1+i$) est associé à un et un seul élément normalisé. D'autre part, tout élément normalisé de $\mathbb{Z}[i]$ se décompose en un produit d'irréductibles normalisés.

4. Réciprocité biquadratique

Pour b entier premier fixé, il est aisé de caractériser (en termes de congruences modulo $4b$) les nombres premiers p tels que b soit un carré, respectivement un non carré, en utilisant la loi de réciprocité quadratique. De manière analogue, nous aurons besoin dans le chapitre 3 de déterminer des conditions suffisantes pour qu'un premier p soit une puissance quatrième modulo un premier fixé b. Nous allons pour cela utiliser la loi de réciprocité biquadratique, que nous rappelons dans ce chapitre. Elle est l'analogue pour les restes de puissances quatrièmes de la loi de réciprocité quadratique mais s'énonce de façon naturelle dans l'anneau $\mathbb{Z}[i]$.

4.1. — Théorème (Loi de Réciprocité Biquadratique). *Soient π et ρ deux irréductibles distincts et normalisés de $\mathbb{Z}[i]$. On a la relation suivante :*

$$\left(\frac{\pi}{\rho}\right)_4 = (-1)^{((N(\pi)-1)/4)\,((N(\rho)-1)/4)} \left(\frac{\rho}{\pi}\right)_4.$$

Elle s'accompagne de lois complémentaires :

4.2. — Proposition. *Soit $\pi = r+is$ un irréductible normalisé de $\mathbb{Z}[i]$. On a les relations*

$$\left(\frac{i}{\pi}\right)_4 = i^{-(r-1)/2} \qquad \text{et} \qquad \left(\frac{1+i}{\pi}\right)_4 = i^{(r-s-1-s^2)/4}.$$

De ces lois complémentaires, on déduit facilement la proposition suivante :

4.3. — Proposition. *Soit $\pi = r+is$ un irréductible normalisé de $\mathbb{Z}[i]$. On a*

$$\left(\frac{-1}{\pi}\right)_4 = (-1)^{(r-1)/2}, \qquad \text{et} \qquad \left(\frac{2}{\pi}\right)_4 = i^{\,rs/2}.$$

La loi de réciprocité biquadratique a été énoncée pour la première fois par Gauss [3] et [4]. Sa démonstration et celles des lois complémentaires sont exposées dans [5] et reprennent celles de Eisenstein [2]. Elles figurent aussi dans [7] et, celles de leurs analogues cubiques figurent dans [5] et [6]. Notons que l'on doit aussi à Eisenstein une loi de réciprocité générale, entre les symboles des restes de puissances $k^{\text{ièmes}}$ pour k premier. Enfin, citons l'exposé [9] qui donne un aperçu historique intéressant sur toutes ces notions.

5. Bibliographie

[1] D.A. Cox : *Primes of the Form $x^2 + ny^2$.* Wiley-Interscience, John Wiley & Sons, 1989.

[2] G. Eisenstein : *Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste.* Mathematische Werke, Band 1, pp. 223–245, New-York, Chelsea, 1975.

[3] C.F. Gauss : *Disquisitiones Arithmeticae.* Leipzig 1801. Traduction : *Recherches Arithmétiques*, Paris 1807.

[4] C.F. Gauss : *Werke, vol. II.* Gottingen et Leipzig, 1863–1927.

[5] K. Ireland, M. Rosen : *A Classical Introduction to Modern Number Theory.* Springer-Verlag, 1982.

[6] J.R. Joly : *Démonstration cyclotomique de la loi de réciprocité cubique.* Bulletin des Sciences Mathématiques, 2° série, vol. 96, pp. 273–278, 1972.

[7] P. Kaplan : *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique.* Journal of Mathematical Society of Japan, vol 25, N° 4, 1973.

[8] P. Samuel : *Théorie Algébrique des Nombres.* Hermann, Collection Méthodes, Paris 1967.

[9] A. Weil : *La cyclotomie jadis et naguère.* L'Enseignement Mathématique, vol. 20, 1974, pp. 247–263.

Chapitre 3

Nombres composés pseudo-premiers forts dans plusieurs bases

Comme nous l'avons vu dans le chapitre 1, le test de Rabin est un test probabiliste de primalité, qui est aujourd'hui utilisé par de nombreux systèmes de calcul formel comme, par exemple, `GP-Pari` [3], `Maple` [4] et `Axiom` [2]. Ce choix est justifié par la grande simplicité de ce test et sa rapidité d'éxécution. De plus, la fiabilité du test semblait suffisante, comme le montraient les expériences numériques de [6] ainsi que le théorème de Rabin 1.1.7. A tel point que l'on trouve dans le code de `Maple` version V.2, le commentaire suivant : *Presently, there are no composite numbers known to us that will make* `isprime()` *return* `true`.

A l'époque où la méthode exposée dans ce chapitre a été mise au point, nous utilisions le système de calcul formel `ScratchPad` [5], ancêtre d'`Axiom`. Nous avons été saisis par le contraste provoqué par l'absence, dans la littérature, d'exemples explicites de nombres composés passant ce test, joint au sentiment commun que de tels nombres se devaient d'exister. Ce fut donc avant tout un jeu de trouver le premier nombre composé déclaré premier par `ScratchPad`. Ensuite, et pour démontrer la puissance de la méthode, nous l'avons appliquée à d'autres ensembles de bases. Notons aussi que nous avons effectivement programmé cette méthode dans le langage `ScratchPad`, avec en particulier une fonction qui accepte en entrée une liste quelconque de bases premières et qui fournit en sortie, sauf pour certaines données initiales exceptionnelles décrites dans ce chapitre, un nombre composé et fortement pseudo-premier simultanément dans chacune des bases fournies.

Notons aussi que la méthode présentée dans ce chapitre a déjà été exposée dans [1].

1. Nombres fortement pseudo-premiers dans une base

Forme générale

Nous nous devions de construire des nombres composés pseudo-premiers dans les dix bases 2, 3, 5, 7, 11, 13, 17, 19, 23 et 29 utilisées par `ScratchPad`. Notre première idée a naturellement été de chercher ces nombres sous la forme d'un produit $n = p_1 p_2$ de deux nombres premiers. La première remarque que nous pouvions faire s'exprime alors par le lemme suivant

1.1. — Lemme. *Soit $n = p_1 p_2$ le produit de deux nombres premiers. On a l'équivalence*

$$p_1 - 1 \text{ divise } n - 1 \qquad \Longleftrightarrow \qquad p_1 - 1 \text{ divise } p_2 - 1.$$

Démonstration — Elle est évidente dès que l'on a écrit la condition de gauche sous la forme $n \equiv 1$ modulo $p_1 - 1$ et celle de droite sous la forme $p_2 \equiv 1$ modulo $p_1 - 1$. □

Pseudo-primalité

Si les conditions de ce lemme sont vérifiées alors, d'après le petit théorème de Fermat, on a $b^{n-1} \equiv 1$ modulo p_1 pour tout entier b premier avec p_1. C'est un premier pas vers la réalisation de la congruence $b^{n-1} \equiv 1 \bmod n$ qui exprime — si elle est vraie — que n est pseudo-premier de base b. Nous avons donc choisi d'imposer aux nombres que nous recherchions de vérifier les conditions du lemme 1.1. En fait, c'est l'examen des tables de [6] qui nous a guidés dans cette voie, puisqu'elles révèlent que parmi les treize nombres composés inférieurs à $25 \cdot 10^9$ et simultanément pseudo-premiers dans les trois bases 2, 3 et 5, onze sont du type décrit par le lemme 1.1.

Arbitrairement, nous avons imposé au rapport $(p_2 - 1)/(p_1 - 1)$ d'être égal à 2. Autrement dit, les facteurs p_1 et p_2 sont liés l'un à l'autre par les relations suivantes :

$$\begin{cases} p_1 = 2q + 1 \\ p_2 = 4q + 1 \end{cases} \qquad \text{avec } q \in \mathbb{N}.$$

Le deuxième et dernier pas que nous devons franchir pour que le nombre n soit pseudo-premier de base b est de réaliser la congruence $b^{n-1} \equiv 1$ modulo p_2. Mais nous pouvons écrire

$$n - 1 = p_1(p_2 - 1) + \frac{p_2 - 1}{2}.$$

Nous avons donc la relation

$$\begin{aligned} b^{n-1} &\equiv b^{(p_2-1)/2} \qquad \text{d'après le petit théorème de Fermat,} \\ &\equiv \left(\frac{b}{p_2}\right) \text{ modulo } p_2. \end{aligned}$$

D'où le lemme suivant :

1.2. — Lemme. *Soit $n = p_1 p_2$ le produit de deux nombres premiers tels que*

$$(p_2 - 1) = 2(p_1 - 1).$$

Pour $b \in \mathbb{N}^*$, le nombre n est pseudo-premier de base b si et seulement si b est un carré modulo p_2. □

Pseudo-primalité forte

En supposant que les conditions du lemme 1.2 soient vérifiées, cherchons d'autres conditions suffisantes pour que n soit un pseudo-premier **fort** de base b. Un examen attentif de la valeur de $b^{(n-1)/2}$ modulo n va nous donner une réponse satisfaisante :

1.3. — Lemme. *Soient n, p_1, p_2 et b vérifiant les conditions du lemme 1.2 et soit $\pi \in \mathbb{Z}[i]$ tel que $p_2 = N(\pi)$. Alors n est fortement pseudo-premier de base b dès que les conditions suivantes sont vérifiées :*

$$\left(\frac{b}{p_1}\right) = -1 \qquad \textit{et} \qquad \left(\frac{b}{\pi}\right)_4 = -1$$

c'est-à-dire dès que b est un non carré dans $\mathbb{Z}$ modulo p_1, et un carré sans être une puissance quatrième dans $\mathbb{Z}[i]$ modulo π.

Démonstration — Notons d'abord que, pour que n soit fortement pseudo-premier de base b, il suffit que la congruence

$$b^{(n-1)/2} \equiv -1 \text{ modulo } n \tag{1}$$

soit vérifiée. Or, nous avons la relation

$$\begin{aligned}\frac{n-1}{2} &= \frac{p_1(p_2-1)+(p_1-1)}{2} \\ &= \frac{2p_1(p_1-1)+(p_1-1)}{2} \\ &= (2p_1+1)\frac{p_1-1}{2},\end{aligned}$$

et donc, puisque $2p_1+1$ est impair,

$$\begin{aligned}b^{(n-1)/2} &= \left(b^{(p_1-1)/2}\right)^{2p_1+1} \\ &\equiv \left(\frac{b}{p_1}\right)^{2p_1+1} \quad \text{modulo } p_1. \\ &= \left(\frac{b}{p_1}\right)\end{aligned}$$

Ainsi, la première égalité de l'énoncé indique que

$$b^{(n-1)/2} \equiv -1 \text{ modulo } p_1. \tag{2}$$

D'autre part, nous avons aussi

$$\frac{n-1}{2} = p_1\frac{p_2-1}{2} + \frac{p_2-1}{4}$$

et cela montre (rappelons que l'on suppose que les conditions du lemme 1.2 sont vérifiées) :

$$b^{(n-1)/2} \equiv \left(\frac{b}{p_2}\right)^{p_1} b^{(p_2-1)/4} = b^{(p_2-1)/4} \quad \text{modulo } p_2.$$

Ainsi, la deuxième égalité de l'énoncé signifie $b^{\frac{n-1}{2}} \equiv -1$ modulo π. Mais, puisque π et $\overline{\pi}$ sont premiers entre eux,

$$b^{(n-1)/2} \equiv -1 \text{ modulo } \pi \quad \Longleftrightarrow \quad b^{(n-1)/2} \equiv -1 \text{ modulo } p_2.$$

Donc, la deuxième égalité de l'énoncé s'écrit

$$b^{(n-1)/2} \equiv -1 \quad \text{modulo } p_2. \tag{3}$$

Finalement, les deux congruences (2) et (3) donnent la relation (1) qui était notre objectif. □

2. L'intervention des lois de réciprocité

Nous allons utiliser la loi de réciprocité quadratique afin de déterminer des conditions (en termes de congruences sur p_1 et sur p_2) nécessaires et suffisantes pour que b soit un carré modulo p_2 et ne soit pas un carré modulo p_1 ; ainsi que la loi de réciprocité biquadratique afin de déterminer des conditions nécessaires et suffisantes (en termes de congruences sur un facteur irréductible π de p_2 dans $\mathbb{Z}[i]$) pour que b soit un carré non bicarré modulo p_2. Puis, nous exprimerons l'ensemble des conditions du lemme 1.3 sous forme de congruences sur π dans $\mathbb{Z}[i]$.

Le cas de la base 2

Considérons d'abord le cas de la base 2. D'après la loi complémentaire 2.4.3, la seconde égalité de 1.3 s'écrit $i^{\frac{rs}{2}} = -1$ (avec $\pi = r + is$). Si l'on suppose que π est normalisé (définition 2.3.2), cela est équivalent à

$$\pi \equiv 1 + 4i \quad \text{ou} \quad 5 + 4i \quad \text{modulo } 8.$$

Remarquons que $\pi \equiv 1 + 4i$ modulo 8 implique $p_2 \equiv 1$ modulo 16, tandis que $\pi \equiv 5 + 4i$ modulo 8 implique que $p_2 \equiv 9$ modulo 16. Cependant, puisque l'on veut que la première condition du lemme 1.3 soit aussi satisfaite, nous devons avoir $p_1 \equiv 3$ ou 5 modulo 8. A cause des relations liant p_1 et p_2 entre eux, nous devons choisir $\pi \equiv 1 + 4i$ modulo 8 et éliminer l'autre alternative. Résumons tout cela dans un lemme :

2.1. — Lemme. *Soit $n = p_1p_2$ le produit de deux nombres premiers et π un irréductible normalisé de $\mathbb{Z}[i]$ tels que*

$$(p_2 - 1) = 2(p_1 - 1) \qquad \text{et} \qquad p_2 = N(\pi).$$

Le nombre n est fortement pseudo-premier de base 2 dès que π est congru à $5+4i$ modulo 8.
□

Cas d'une base b congrue à 3 modulo 4

Maintenant, expliquons comment produire des irréductibles π de $\mathbb{Z}[i]$ vérifiant la deuxième condition du lemme 1.3. Considérons d'abord le cas où b est congru à 3 modulo 4. Puisque π et $-b$ sont des irréductibles normalisés de $\mathbb{Z}[i]$, la loi de réciprocité biquadratique montre que

$$\left(\frac{-b}{\pi}\right)_4 = (-1)^{((b^2-1)/4)((p_2-1)/4)} \left(\frac{\pi}{b}\right)_4,$$

c'est-à-dire

$$\left(\frac{-b}{\pi}\right)_4 = \left(\frac{\pi}{b}\right)_4,$$

puisque $b^2 \equiv 1$ modulo 8. Donc, et d'après la définition 2.1.2,

$$\begin{aligned}\left(\frac{b}{\pi}\right)_4 &= \left(\frac{-1}{\pi}\right)_4 \left(\frac{-b}{\pi}\right)_4 \\ &= (-1)^{(p_2-1)/4} \left(\frac{\pi}{b}\right)_4.\end{aligned}$$

Il nous suffit alors de trouver une solution z de l'équation

$$(-1)^{(N(z)-1)/4}\left(\frac{z}{b}\right)_4 = -1, \tag{A_3}$$

(Remarquons que le premier facteur du membre de gauche dans cette égalité est ± 1 selon que z est congru à 1 ou bien à $3+2i$ modulo 4.) et ensuite de trouver des irréductibles congrus à z modulo $4b$. En effet, ces irréductibles π seront alors eux aussi solutions de (A_3) et satisfairont donc la deuxième égalité du lemme 1.3.

Cas d'une base b congrue à 1 modulo 4

Examinons maintenant le cas où b est congru à 1 modulo 4. L'entier b se décompose dans $\mathbb{Z}[i]$ en un produit $b = \omega\overline{\omega}$ de deux irréductibles normalisés. La loi de réciprocité biquadratique énonce alors que

$$\begin{cases} \left(\dfrac{\omega}{\pi}\right)_4 = (-1)^{(b-1)/4\cdot(p_2-1)/4}\left(\dfrac{\pi}{\omega}\right)_4 \\ \left(\dfrac{\overline{\omega}}{\pi}\right)_4 = (-1)^{(b-1)/4\cdot(p_2-1)/4}\left(\dfrac{\pi}{\overline{\omega}}\right)_4. \end{cases}$$

Faisons le produit de ces deux égalités, on obtient

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{\pi}{\omega}\right)_4\left(\frac{\pi}{\overline{\omega}}\right)_4.$$

Mais, d'après la proposition 2.1.3, les symboles $(\pi/\overline{\omega})_4$ et $(\overline{\pi}/\omega)_4$ sont inverses l'un de l'autre. L'équation ci-dessus devient donc

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{\pi\overline{\pi}^{-1}}{\omega}\right)_4$$

où $\overline{\pi}^{-1}$ désigne l'inverse de $\overline{\pi}$ modulo b. Il ne reste plus qu'à trouver une solution normalisée z de l'équation

$$\left(\frac{z\overline{z}^{-1}}{\omega}\right)_4 = -1. \tag{A_1}$$

Ainsi, tout irréductible π congru modulo $4b$ à une telle solution z sera aussi une solution de (A_1) et donc satisfera la deuxième égalité du lemme 1.3.

Rôle de la réciprocité quadratique

Les deux sections précédentes vont nous aider à réaliser la deuxième égalité du lemme 1.3. De manière semblable, il nous faut examiner la première égalité de ce lemme. Elle est équivalente à

$$(-1)^{\frac{p_1-1}{2}\frac{b-1}{2}}\left(\frac{p_1}{b}\right) = -1.$$

En utilisant l'égalité $p_1 = (N(\pi)+1)/2$, cela devient

$$(-1)^{\frac{N(\pi)-1}{4}\frac{b-1}{2}}\left(\frac{(N(\pi)+1)/2}{b}\right) = -1.$$

Ainsi, pour tout irréductible π congru modulo $4b$ à une solution fixée z de l'équation

$$(-1)^{\frac{N(z)-1}{4}\frac{b-1}{2}}\left(\frac{(N(z)+1)/2}{b}\right) = -1, \qquad \text{(B)}$$

nous aurons $N(\pi) \equiv N(z)$ modulo $8b$ et $(N(\pi)+1)/2 \equiv (N(z)+1)/2$ modulo $4b$. Ainsi, π sera aussi une solution de (B) et la première égalité de 1.3 sera satisfaite.

Un exemple

Ainsi, si z est une solution commune à (A_3) et (B) (resp. à (A_1) et (B)) alors tout irréductible normalisé π congru à z modulo $4b$ sera aussi solution de ces mêmes équations et les conditions du lemme 1.3 seront vérifiées. Par exemple, considérons le cas $b = 7$. Il est facile de trouver un entier de Gauss τ vérifiant $(\tau/7)_4 = -1$. Par exemple, nous pouvons prendre $\tau = 1 + i$. De là nous trouvons l'entier de Gauss $z_1 = 1 + 8i$ qui est congru à 1 modulo 4 et à τ modulo 7. Le nombre z_1 est donc solution de (A_3) et, de plus, il est aussi solution de (B). Donc, avec les notations du lemme 1.3, le nombre n est fortement pseudo-premier de base 7 dès que π est congru à $1 + 8i$ modulo 28. Un raisonnement semblable s'applique à $z_2 = 7 + 6i$, qui vérifie les deux équations (A_3) et (B).

3. Plusieurs bases

Ici, précisons les conséquences, dans le choix de z, de sa classe modulo 4. Le lemme 2.1 montre que, si l'on veut que n soit pseudo-premier à la fois dans la base 2 et dans une autre base b, nous devons choisir des solutions z de (A_3) et (B) (resp. de (A_1) et (B)) telles que $z \equiv 1$ modulo 4 (comme z_1 dans l'exemple ci-dessus). Si, au contraire nous choisissons un $z \equiv 3 + 2i$ modulo 4 (comme z_2), les conditions de 2.1 ne sont plus satisfaites. Pire, on a dans ce cas $p_2 \equiv 5$ modulo 8, de telle sorte que 2 est un non carré modulo p_2 et, par le lemme 1.2, le nombre n n'a plus aucune chance d'être pseudo-premier de base 2.

Le cas des bases de `ScratchPad`

Nous donnons dans la table 1, pour différentes bases b, **des** conditions suffisantes pour que n soit fortement pseudo-premier de base b. Elles ont été déterminées en suivant l'exemple ci-dessus de la base 7.

Cette table montre, quand cela est possible, deux solutions aux équations (A_3) et (B) (resp. (A_1) et (B)). Les solutions de la colonne de gauche sont congrues à 1 modulo 4 et donc sont compatibles avec les conditions du lemme 2.1. Au contraire, celles de la colonne de droite sont congrues à $3 + 2i$ modulo 4 et donc mènent à des entiers n qui ne sont pas pseudo-premiers de base 2.

pour $b = 2$:	$\pi \equiv 5 + 4i$			modulo 8
pour $b = 3$:	$\pi \equiv$		$7 + 6i$	modulo 12
pour $b = 7$:	$\pi \equiv 1 + 8i$	ou	$7 + 6i$	modulo 28
pour $b = 11$:	$\pi \equiv 5 + 12i$	ou	$3 + 22i$	modulo 44
pour $b = 13$:	$\pi \equiv 5 + 24i$	ou	$7 + 18i$	modulo 52
pour $b = 17$:	$\pi \equiv 1 + 12i$	ou	$3 + 2i$	modulo 68
pour $b = 19$:	$\pi \equiv 1 + 28i$	ou	$3 + 6i$	modulo 76
pour $b = 23$:	$\pi \equiv 1 + 32i$	ou	$3 + 30i$	modulo 92
pour $b = 29$:	$\pi \equiv 1 + 56i$	ou	$3 + 10i$	modulo 116

Table 1

Les bases récalcitrantes

Malheureusement, les bases 3 et 5 présentent quelques difficultés particulières. En effet, pour $b = 5$, le facteur p_2 doit être congru à 1 ou à 9 modulo 10 afin que 5 soit un carré modulo p_2. Cela force p_1 à être congru à 1, 5, 6 ou 0 modulo 10. Puisque p_1 est premier, seule la congruence $p_1 \equiv 1$ modulo 10 est possible (hormis le cas $p_1 = 5$ qui est sans intérêt). Alors, 5 est un carré modulo p_1, ce qui est contraire à ce que l'on désire.

Le cas $b = 3$ est un peu moins récalcitrant. On peut vérifier qu'une solution de (A_3) doit nécessairement appartenir à l'une des quatre classes $9 + 4i$, $9 + 8i$, $7 + 6i$, $11 + 6i$ modulo 12. Si π appartient à l'une des deux premières, alors on a $p_1 \equiv 1$ modulo 12 et donc l'équation (B) ne peut être satisfaite. Si π appartient à l'une des deux dernières classes, on a $p_1 \equiv 7$ modulo 12. Dans ce cas, l'équation (B) est bien satisfaite mais cela n'est plus compatible avec les conditions du lemme 2.1. Cela explique pourquoi la colonne de gauche de la ligne $b = 3$ est restée vide dans la table 1.

En conclusion, cette méthode ne permet pas de trouver des pseudo-premiers forts dans la base 5, ni non plus dans les deux bases 2 et 3 simultanément.

Nous nous contentons donc, pour ces deux bases exceptionnelles, d'une méthode palliative : les relations de la table 2 assurent que 3 et 5 sont des puissances quatrièmes modulo p_2 et des carrés modulo p_1, de telle manière que

$$\begin{cases} 3^{\frac{n-1}{2}} \equiv 1 \\ 5^{\frac{n-1}{2}} \equiv 1 \end{cases} \quad \text{modulo } n$$

ce qui, en particulier, fait que n est pseudo-premier dans les bases 3 et 5.

$\pi \equiv 1$ modulo 12
$\pi \equiv 1$ modulo 20

Table 2

4. Quelques exemples

Ici, nous construisons explicitement des nombres composés passant le test de Rabin de `ScratchPad`.

Application au test de `ScratchPad`

Les huit conditions de la colonne de gauche de la table 1 et les deux de la table 2 sont compatibles entre elles et, en appliquant l'algorithme d'Euclide étendu, on voit qu'elles sont toutes satisfaites dès que $\pi = r + is$ est tel que

$$\begin{cases} r \equiv r_0 = 11310652501 \\ s \equiv s_0 = 8996896140 \end{cases} \qquad \text{modulo } m = 25878772920.$$

Par exemple, prenons $r = r_0 + 8m$ et $s = s_0 + m$. Dans ce cas, p_1 et p_2 sont des nombres premiers, donc

$$p_1 p_2 = 11950687687952657925183613157251163518982455 81 \tag{4}$$

est fortement pseudo-premier dans les bases 2, 7, 11, 13, 17, 19, 23, 29, et pseudo-premier dans les bases 3 et 5. De plus, un peu de chance aidant, ce nombre est aussi fortement pseudo-premier dans les bases 3 et 5 (même dans la base 31). Il passe le test de `ScratchPad`.

Les congruences des tables 1 et 2 permettent en fait de trouver bien d'autres nombres composés déclarés premiers par `ScratchPad` (en une nuit de calcul, un petit programme `ScratchPad` sur un PC/RT en a trouvé un peu plus de 150). La table 3 en liste quelques-uns avec, dans la colonne de droite, un facteur de chacun d'eux.

Puissance de la méthode

Comme nous l'avons dit au début du chapitre, cette méthode s'applique aussi pour trouver des pseudo-premiers forts dans d'autres ensembles de bases. Nous l'avons appliquée avec succès pour trouver le nombre suivant (337 chiffres) :

$$\begin{aligned} &80383745745363949125707961434194210813883768828755814583748891752229 \\ &\quad 74273765333652186502336163960045457915042023603208766569966760987284 \\ &\quad\quad 04396540823292873879185086916685732826776177102938969773947016708 23 \\ &\quad\quad\quad 04286871099974399765441448453411558724506334092790222752962294149 84 \\ &\quad\quad\quad\quad 23068816854043264575340183297861112989606448452161916528725975349 01 \end{aligned}$$

qui admet le facteur p_2 suivant

$$\begin{aligned} &400958216639499605418306452084546853005188166041132508774 \\ &\quad 50620473800321707011962427162231915972197335821631650853 \\ &\quad\quad 58166969145233813917169287527980445796800452592031836601 \end{aligned}$$

et qui est fortement pseudo-premier pour chacune des quarante-six bases premières inférieures à 200. Nous pensons que, pour toutes les bases premières supérieures ou égales à 7, les conditions du lemme 1.3 admettent des solutions et nous l'avons vérifié jusqu'à $2 \cdot 10^5$. La seule limitation au nombre de bases que l'on pourrait traiter simultanément semble être la croissance de la taille des nombres ainsi calculés.

119506876879526579251836131572511635189824558 1	48889032896862784894921
16290257385019777169358274185401920652803366770 1	570793436980835952031801
13455873872920516973871865505439376466822062427 41	16404800439457053617079 61
7692791161358542966875525622841704601525549750 41	12403863238006571125881 61
14283914342789550577664802151675635270642549955 81	16902020200431397293949 21
31108983027998663437247701521425492603923813241 41	24943529432700041792715 61
29946171637073368700289177774170097699534730138 21	24472912224364867647670 81
82187761223124145892594538152848801947915561367 81	40543251281347465681717 21
34844078171499455841671710708580565849571676715 61	26398514417102889633458 41
75421233600088636633377126002982879491057298387 61	38838443223200550069026 41
21725013656018763076105459253647137482758798581 781	65916634707816756194017 21
65133961998738965332758869580009452514988654652 701	11413497448086538678021 801
19840288923887081357309700907668002023719213638 581	62992521657554051845969 21
47541247850812051206127444470777277816562180694 361	97510253666793474510890 41
39779522428648597279007990324893075438060056256 981	89195877066878598274945 21
47824338726623806233423439382232910557660981544 141	97800141847160739415515 61
43874569201307542082066453928189683393299200908 581	93674510088185187243769 21
48778780261654321019168500503289058505676861834 261	98771230894075954123796 41
40731291916337435991504960386523783671925548224 861	90256625148891353826560 41
41469711110447105472587285165731839878829067531 321	91071083347511690257120 81
65670822302684064701133181659108281791806006666 541	11460438237928256877809 161
63252554105207970448541699928950793646076357042 101	11247448964561517000041 401
59721204718706216859042583248556917834479829851 881	10928971106074552785723 121
12708934672239958035306348345985729847442997507 6021	15942982576820410008125 881
85843893295239595189377466133361685127561783678 341	13102968617472881300862 361
11196823175883688386525941436964392696229387458 3421	14964506791661186176245 481
16948438352603469842848316749901279455443655446 381	18411104449545372041946 121
96336211523909469613388058773005046560271648037 061	13880649230054728936002 841
10347858370635239843589943948557310341225515747 4061	14386005957620926721280 841
31999871092526644183748897214642264532551028931 0641	25298170326142815415222 561
34077061965855429957951411995479272410173459995 5221	26106344809588120491442 681
14536650723692750553871771641409802516236184541 6421	17050894829124218461227 481
13538627805738708354326871845603232170937034430 7421	16455168067047330133341 481
10195337925068795136860068937272027477220050576 4461	14279592378684200477698 441
10837410651003240128705693079891864175551134571 3841	14722371175189980332739 361
23336070740784143394274219759365091590914873033 3041	21603736130949268467680 161
32294425422346007951334031494981908612905171349 4961	25414336671393179586865 441
21988820882856349079636738037485610843153044625 7261	20970846851215307599541 641
13526914767421499642115692915362104354547562140 9861	16448048375063528881046 041
12796144310841725738448720435402091603722792086 6941	15997590012774877797398 761
40257829612533603308418078172268444362199177829 2701	28375281359850373581781 801
31039006876770320461489181986008188328672956180 3401	24915459809833058933415 601
13286652432299987225948032569644540685391539948 3421	16301320457128610920845 481
32289806317723776673702052887461086929017262972 4401	25412519087144342634429 601
13557083110800840338711587450932433808251923477 6781	16466379754397042533131 721
13923343685400374952057888667330274592716687863 6861	16687326739415378842184 041
33329367678644745560312444548558564495403277468 0001	25818353037575710383120 001

Table 3

5. Bibliographie

[1] F. Arnault : *Test de Rabin-Miller : Nombres composés qui le "passent".* Département de mathématiques de l'Université de Poitiers, prépublication n° 61, nov. 1991.

[2] R. Jenks, R. Sutor : *Axiom, The Scientific Computation System.* Springer-Verlag 1992.

[3] C. Batut : *Aspects algorithmiques du système de calcul arithmétique en multi-précision PARI.* Thèse, Université Bordeaux I, 1989.

[4] B. Char, K. Geddes, G. Gonnet, B. Leong, M. Monagan, S. Watt : *Maple V Library Reference Manual.* Springer-Verlag and Waterloo Maple Publishing, 1991.

[5] IBM Computer Algebra Group : *The Scratchpad Computer Algebra System Interactive Environment Users Guide.* Edited by R. Sutor, 1989.

[6] C. Pomerance, J.L. Selfridge, S.S. Wagstaff : *The pseudoprimes to* $25 \cdot 10^9$. Mathematics of Computation, vol. 35, n° 151, 1980, pp. 1003–1026.

Chapitre 4

Suites de Lucas et pseudo-premiers de Lucas

Dans [1], on définit un nouveau type de pseudo-premiers, dont les propriétés sont parallèles à celles des pseudo-premiers classiques. Le langage utilisé est celui des suites de Lucas, dont les propriétés sont riches et à première vue mystérieuses. Ce langage est repris par la (quasi-?)totalité des nombreux articles et ouvrages sur le sujet (citons [4], [6], [5], [7], [8], [9], [11]). Le but de ce chapitre est de donner une autre présentation des pseudo-premiers de Lucas, plus conceptuelle et mettant mieux en valeur l'analogie avec les pseudo-premiers classiques.

Rappelons que l'intérêt des suites de Lucas ne se limite pas aux tests probabilistes de primalité mais, que l'on peut en déduire des conditions nécessaires et suffisantes pour la primalité d'un entier n tel que la factorisation de $n+1$ soit connue, et qu'il existe des critères de primalité puissants, développés dans [3], exploitant au maximum les connaissances partielles que l'on peut avoir sur les factorisations des deux entiers $n \pm 1$. D'autre part, les suites de Lucas ont donné naissance à un algorithme de factorisation : la "méthode $p+1$" de Williams [11], efficace si l'entier n à factoriser est tel que les facteurs premiers de $n+1$ soient petits. L'analogie avec la méthode $p-1$ de Pollard s'éclaircit si l'on adopte le point de vue algébrique développé dans ce chapitre.

Nous commençons par rappeler les définitions et premières propriétés des suites de Lucas sous leur forme usuelle.

1. Suites de Lucas

Notations

Soient P et Q deux entiers tels que $D = P^2 - 4Q$ ne soit pas un carré parfait. Considérons les suites $(X_n)_{n\in\mathbb{N}}$ définies par la récurrence linéaire :

$$X_{n+1} = PX_n - QX_{n-1} \qquad \text{pour } n \geq 1.$$

Si l'on désigne par α et β les racines du polynôme $X^2 - PX + Q$, les suites (X_n) sont les combinaisons linéaires des suites (α^n) et (β^n) et sont entièrement déterminées par leurs coefficients initiaux X_0 et X_1.

Les suites de Lucas sont de telles suites, généralement notées (U_n) et (V_n), déterminées par leurs deux premiers termes :

$$U_0 = 0, \quad U_1 = 1 \quad \text{et} \quad V_0 = 2, \quad V_1 = P.$$

On voit aisément que ce sont des suites d'entiers et que leurs termes généraux s'expriment alors sous la forme :

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n. \tag{1}$$

Propriétés

Les deux théorèmes suivants sont respectivement présentés comme les analogues du petit théorème de Fermat et du critère de Miller 1.1.6 par les auteurs de [1]. Pourtant, le langage des suites de Lucas qu'ils utilisent pour les démontrer peut laisser perplexe sur la nature du lien entre ces résultats. Les démonstrations que nous en donnons ici mettent en valeur cette analogie grâce à l'apparition d'un groupe cyclique qui joue le même rôle que le groupe des inversibles modulo p dans le chapitre 1. L'analogie deviendra encore plus flagrante dans les sections ultérieures.

1.1. — Théorème. *Soit p un nombre premier impair ne divisant pas D et désignons par $\varepsilon(p)$ le symbole de Legendre (D/p). Si $\varepsilon(p) = 1$, supposons de plus que p ne divise pas Q. On a la relation :*

$$p \mid U_{p-\varepsilon(p)}.$$

Démonstration — Nous notons $\mathcal{O}$ l'anneau des entiers du corps $\mathbb{Q}(\sqrt{D})$. Suivant le signe de $\varepsilon(p)$, l'anneau quotient $\mathcal{O}/p$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$ ou à $\mathbb{F}_{p^2}$. On a donc respectivement les relations

$$\begin{cases} \alpha^p \equiv \alpha \\ \beta^p \equiv \beta \end{cases} \quad \text{ou bien} \quad \begin{cases} \alpha^p \equiv \beta \\ \beta^p \equiv \alpha \end{cases} \quad \text{modulo } p.$$

Dans les deux cas, on a

$$\alpha^{p-\varepsilon(p)} \equiv \beta^{p-\varepsilon(p)}$$

et le théorème résulte de (1). □

1.2. — Remarque. Sous les mêmes conditions, les arguments ci-dessus démontrent que l'on a aussi

$$\begin{aligned} V_{p-1} &\equiv 2 \quad \text{modulo } p, \quad && \text{si } \varepsilon(p) = 1 \text{ et } p \nmid Q, \\ V_{p+1} &\equiv 2Q \quad \text{modulo } p, \quad && \text{si } \varepsilon(p) = -1, \\ U_p &\equiv \varepsilon(p) \quad \text{modulo } p, \\ V_p &\equiv P \quad \text{modulo } p. \end{aligned}$$

1.3. — Théorème. *Soit p un premier ne divisant pas $2QD$ et posons $\varepsilon(p) = (D/p)$ et $p - \varepsilon(p) = 2^k q$ avec q impair. Alors l'une ou l'autre des conditions suivantes est vérifiée :*

$$p \mid U_q \qquad \textit{ou} \qquad \textit{il existe un } i \textit{ tel que } 0 \leq i < k \textit{ et } p \mid V_{2^i q}$$

Démonstration — Posons $\tau = \alpha\beta^{-1}$ modulo p. On voit, pour $k \in \mathbb{N}$, que

$$\begin{aligned} p \mid U_k &\iff \tau^k \equiv 1 \quad \text{modulo } p, \\ p \mid V_k &\iff \tau^k \equiv -1 \quad \text{modulo } p. \end{aligned}$$

les conditions de l'énoncé se reformulent donc ainsi :

$$\tau^q = 1 \qquad \text{ou} \qquad \text{il existe un } i \text{ tel que } 0 \leq i < k \text{ et } \tau^{2^i q} = -1.$$

Par construction, l'élément τ est de norme 1 dans $\mathcal{O}/(p)$. Nous allons montrer que le sous-groupe des éléments de norme 1 dans $\mathcal{O}/(p)$ est cyclique d'ordre $p - \varepsilon(p)$.

• Si $\varepsilon = -1$, alors $\mathcal{O}/(p)$ est un corps fini de cardinal p^2. Son groupe multiplicatif est cyclique donc le sous-groupe des éléments de norme 1 est aussi cyclique. De plus la norme d'un élément x de $\mathcal{O}/(p)$ est x^{p+1}. Les éléments de norme 1 sont donc les racines $(p+1)^{\text{ièmes}}$ de l'unité dans un groupe cyclique d'ordre $p^2 - 1$. Il y en a donc $p + 1$.

• Si $\varepsilon = 1$, alors $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ est scindé dans $\mathcal{O}$. On a un isomorphisme

$$\begin{array}{ccccc} \mathcal{O}/(p) & \simeq & \mathcal{O}/\mathfrak{p} \times \mathcal{O}/\overline{\mathfrak{p}} & \simeq & \mathcal{O}/\mathfrak{p} \times \mathcal{O}/\mathfrak{p} \\ [x]_p & \leftrightarrow & ([x]_{\mathfrak{p}}, [x]_{\overline{\mathfrak{p}}}) & \leftrightarrow & ([x]_{\mathfrak{p}}, [\overline{x}]_{\mathfrak{p}}). \end{array}$$

Or, le conjugué d'un élément (x, y) de $\mathcal{O}/\mathfrak{p} \times \mathcal{O}/\mathfrak{p}$ est (y, x). Les éléments de norme 1 sont donc ceux de la forme $(x, 1/x)$ avec $0 \neq x \in \mathcal{O}/\mathfrak{p}$. Il est alors clair qu'ils forment un groupe cyclique d'ordre $p - 1$.

La fin de la démonstration est alors identique à celle du critère de Miller 1.1.6 : considérons le plus petit entier i tel que $b^{2^i q} \equiv 1$ modulo p (il existe, d'après 1.1). Si $i > 0$ alors $b^{2^{i-1} q} \equiv -1$ modulo p puisque 1 n'admet que deux racines carrées dans le groupe cyclique des éléments de norme 1. □

Pseudo-premiers (forts) de Lucas, probablement premiers de Lucas

Ces deux théorèmes ont naturellement amené les auteurs de [1] à poser les définitions suivantes, par analogie avec les notions classiques de probablement premiers, de pseudo-premiers et de pseudo-premiers forts (définitions 1.1.1 et 1.1.5) :

1.4. — Définitions. On appelle *probablement premier de Lucas de paramètres P et Q* tout entier $n > 1$, impair, premier avec Q et tel que

$$n \mid U_{n-\varepsilon(n)}$$

où l'on désigne par $\varepsilon(n)$ le symbole de Jacobi (D/n). Si de plus n est composé, il est dit *pseudo-premier de Lucas de paramètres P et Q.*

1.5. — Définitions. On appelle *probablement premier fort de Lucas de paramètres P et Q* tout entier $n > 1$ premier avec $2QD$ et tel que

$$n \mid U_q \qquad \text{ou} \qquad \text{il existe un entier } i \text{ tel que } 0 \leq i < k \text{ et } n \mid V_{2^i q}$$

où l'on a posé $\varepsilon(n) = (D/n)$ et $n - \varepsilon(n) = 2^k q$ avec q impair. Si de plus n est composé, il est dit *pseudo-premier fort de Lucas pour les paramètres P et Q.*

Dans [1], on étudie la distribution des pseudo-premiers de Lucas et on en déduit plusieurs tests probabilistes de primalité analogues aux tests de Fermat et de Rabin. On y montre aussi qu'un algorithme testant à la fois des propriétés de pseudo-primalité au sens classique et au sens de Lucas constitue un test probabiliste de primalité particulièrement sûr. Plus précisément, Baillie et Wagstaff soulignent le fait que les nombres n qui sont simultanément pseudo-premiers dans une ou plusieurs bases données et pseudo-premiers de Lucas pour des paramètres P et Q donnés avec $\varepsilon(n) = -1$ sont particulièrement rares (voir la section 6.8).

2. Structure modulaire de l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$

Soit D un entier qui ne soit pas un carré parfait. La clef de l'étude des suites de Lucas de paramètres P et Q avec $P^2 - 4Q = D$ réside dans l'examen de la structure de l'anneau $\mathcal{O}$ modulo un entier rationnel. Pour un anneau A, nous notons $A^\times$ le groupe des inversibles de A. Le but de cette section est de démontrer la proposition suivante, qui sera utilisée dans la prochaine section :

2.1. — Proposition. *Soit $\mathcal{O}$ l'anneau des entiers d'un corps de nombres et soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$. Pour tout entier $r \geq 1$, on a la décomposition*

$$(\mathcal{O}/\mathfrak{p}^r)^\times = \{[1+\gamma] \in (\mathcal{O}/\mathfrak{p}^r)^\times \mid \gamma \in \mathfrak{p}\} \times \{x^{N(\mathfrak{p})^{r-1}} \mid x \in (\mathcal{O}/\mathfrak{p}^r)^\times\} \tag{2}$$

en produit direct de sous-groupes.

Lemmes préliminaires

2.2. — Lemme. *Pour $\alpha, \beta \in \mathcal{O}$, pour $r \geq 1$ entier et pour $k \in \mathfrak{p} \cap \mathbb{Z}$, on a l'implication*

$$\alpha \equiv \beta \text{ modulo } \mathfrak{p} \quad \Rightarrow \quad \alpha^{k^{r-1}} \equiv \beta^{k^{r-1}} \text{ modulo } \mathfrak{p}^r.$$

Démonstration — Pour $\alpha - \beta \in \mathfrak{p}$, on a

$$\begin{aligned} \alpha^k - \beta^k &= (\alpha-\beta)(\alpha^{k-1} + \alpha^{k-2}\beta + \cdots + \beta^{k-1}) \\ &\equiv (\alpha-\beta)(\alpha^{k-1} + \alpha^{k-1} + \cdots + \alpha^{k-1}) \quad \text{modulo } \mathfrak{p} \\ &= (\alpha-\beta)k\alpha^{k-1} \in \mathfrak{p}^2, \end{aligned}$$

ce qui démontre le résultat pour $r = 2$. Une récurrence facile laissée au lecteur démontrerait le résultat pour r quelconque. □

2.3. — Lemme. *Il existe une injection naturelle*

$$(\mathcal{O}/\mathfrak{p})^\times \ni [\alpha] \longmapsto [\alpha^{N(\mathfrak{p})^{r-1}}] \in (\mathcal{O}/\mathfrak{p}^r)^\times.$$

Son image est donc un groupe cyclique.

Démonstration — Comme $N(\mathfrak{p}) \in \mathfrak{p}$, le lemme 2.2 montre que le morphisme ci-dessus est bien défini. De plus, si l'on a une congruence

$$\alpha^{N(\mathfrak{p})^{r-1}} \equiv \beta^{N(\mathfrak{p})^{r-1}} \quad \text{modulo } \mathfrak{p}^r,$$

alors on a la même congruence modulo $\mathfrak{p}$. Donc, puisque $\alpha^{N(\mathfrak{p})} \equiv \alpha$ et $\beta^{N(\mathfrak{p})} \equiv \beta$ modulo $\mathfrak{p}$, on a alors

$$\alpha \equiv \alpha^{N(\mathfrak{p})^{r-1}} \equiv \beta^{N(\mathfrak{p})^{r-1}} \equiv \beta \quad \text{modulo } \mathfrak{p},$$

ce qui montre que le morphisme est injectif. Son image est donc isomorphe à $(\mathcal{O}/\mathfrak{p})^\times$ qui est cyclique puisque $\mathcal{O}/\mathfrak{p}$ est un corps fini. □

Démonstration de la proposition 2.1

Pour $\alpha \in \mathcal{O}$ on a la congruence $\alpha^{N(\mathfrak{p})} \equiv \alpha$ modulo $\mathfrak{p}$ et donc, par récurrence, $\alpha^{N(\mathfrak{p})^{r-1}} \equiv \alpha$ modulo $\mathfrak{p}$. On a donc, si $\alpha \notin \mathfrak{p}$,

$$\alpha^{N(\mathfrak{p})^{r-1}-1} \equiv 1 \quad \text{modulo } \mathfrak{p}.$$

Ainsi, l'égalité

$$\alpha = (\alpha^{N(\mathfrak{p})^{r-1}-1})^{-1}\, \alpha^{N(\mathfrak{p})^{r-1}} \tag{3}$$

montre que $(\mathcal{O}/\mathfrak{p}^r)^\times$ est bien le produit des deux sous-groupes. Montrons que ce produit est direct. Supposons que l'on ait une congruence

$$1+\gamma \equiv \alpha^{N(\mathfrak{p})^{r-1}} \quad \text{modulo } \mathfrak{p}^r \qquad \text{avec } \gamma \in \mathfrak{p},\ \alpha \in \mathcal{O}.$$

De $\alpha^{N(\mathfrak{p})} \equiv \alpha$ modulo $\mathfrak{p}$ on tire, par récurrence,

$$\alpha \equiv \alpha^{N(\mathfrak{p})^{r-1}} \equiv 1+\gamma \equiv 1 \text{ modulo } \mathfrak{p}.$$

Puis, d'après le lemme 2.2, on obtient

$$\alpha^{N(\mathfrak{p})^{r-1}} \equiv 1 \quad \text{modulo } \mathfrak{p}^r$$

ce qui montre bien que l'intersection des deux sous-groupes est réduite à l'unité. □

3. Eléments de norme 1

La structure de l'anneau des entiers inversibles modulo n a été d'une grande importance dans l'étude des pseudo-premiers et pseudo-premiers forts (chapitre 1). En particulier, l'ingrédient principal de la démonstration du théorème de Rabin 1.1.7 est le fait que le groupe des inversibles modulo p^r avec p premier impair est cyclique. Le résultat qui suit est l'une des clefs de la profonde analogie entre les pseudo-premiers classiques et les pseudo-premiers de Lucas. Sa démonstration fait l'objet de la présente section.

Pour l'anneau $\mathcal{O}$ des d'entiers d'un corps de nombres et pour $a \in \mathbb{Z}$, le quotient $\mathcal{O}/(a)$ est une algèbre et un module libre de rang fini sur l'anneau $\mathbb{Z}/a\mathbb{Z}$. Nous notons $(\mathcal{O}/(a))^\wedge$ le groupe des éléments de norme 1 dans $\mathcal{O}/(a)$. Par définition, c'est l'ensemble des éléments $[x]$ de $\mathcal{O}/(a)$ tels que le déterminant de l'application

$$\mathcal{O}/(a) \ni [y] \longmapsto [x][y] \in \mathcal{O}/(a)$$

soit égal à 1. Autrement dit, $(\mathcal{O}/(a))^\wedge$ est l'image de l'ensemble

$$\{x \in \mathcal{O} \mid N(x) \equiv 1 \text{ modulo } a\}$$

par la surjection canonique $\mathcal{O} \to \mathcal{O}/(a)$.

3.1. — Théorème. *Soit $\mathcal{O}$ l'anneau des entiers d'un corps quadratique $\mathbb{Q}(\sqrt{D})$. Soient p un nombre premier rationnel ne divisant pas $2D$ et $r \geq 1$ un entier. Le groupe $(\mathcal{O}/p^r)^\wedge$ est* **cyclique** *d'ordre $p^{r-1}\big(p-(D/p)\big)$.*

Lemme préliminaire

3.2. — **Lemme.** *Avec les notations du théorème 3.1 et en supposant que $r \geq 2$, le morphisme canonique*

$$(\mathcal{O}/p^r)^\wedge \longrightarrow (\mathcal{O}/p^{r-1})^\wedge$$

est surjectif et son noyau est de cardinal p.

Démonstration — Soit α élément de $(\mathcal{O}/p^{r-1})^\wedge$ et soient $u, v \in \mathbb{Z}/p^r\mathbb{Z}$ tels que $u + v\sqrt{D} \bmod p^{r-1} = \alpha$. Nous devons montrer qu'il existe exactement p couples d'entiers (k, l) tels que $0 \leq k, l < p$ et

$$N\big((u + kp^{r-1}) + (v + lp^{r-1})\sqrt{D}\big) \equiv 1 \text{ modulo } p^r.$$

Cela s'écrit

$$u^2 - Dv^2 + 2p^{r-1}(uk - vld) + p^{2(r-1)}(k^2 + Dl^2) \equiv 1 \text{ modulo } p^r,$$

ou encore, puisque $r \geq 2$,

$$u^2 - Dv^2 + 2p^{r-1}(uk - vld) \equiv 1 \text{ modulo } p^r.$$

Finalement, cela revient à compter les couples (k, l) solutions de

$$uk \equiv \frac{1 - (u^2 - Dv^2)}{2p^{r-1}} + vlD \text{ modulo } p.$$

Or, cette équation admet exactement p solutions (une pour chaque valeur fixée de l), ce qui termine la démonstration. □

Décomposition en produit direct

3.3. — **Proposition.** *Avec les notations du théorème 3.1, si p est inerte dans $\mathcal{O}$, on a la décomposition*

$$(\mathcal{O}/p^r)^\wedge = \{[1 + \gamma] \in (\mathcal{O}/p^r)^\wedge \mid \gamma \in p\} \times \{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\wedge\} \tag{4}$$

en produit direct de sous-groupes.

Démonstration — Reprenons l'égalité (3) : elle s'écrit ici

$$\alpha = (\alpha^{p^{2(r-1)}-1})^{-1}\, \alpha^{p^{2(r-1)}}. \tag{5}$$

La norme étant multiplicative, si α est de norme 1 modulo p^r, il en est de même du facteur $\alpha^{p^{2(r-1)}}$ de l'égalité ci-dessus, et donc aussi de l'autre facteur. Ainsi, l'égalité (5) montre que $(\mathcal{O}/p^r)^\wedge$ est bien le produit (4) des deux sous-groupes. De plus, puisque l'on a les relations

$$\{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\wedge\} = \{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\times\} \cap (\mathcal{O}/p^r)^\wedge \tag{6}$$

et

$$\{[1 + \gamma] \in (\mathcal{O}/p^r)^\wedge \mid \gamma \in p\} = \{[1 + \gamma] \in (\mathcal{O}/p^r)^\times \mid \gamma \in p\} \cap (\mathcal{O}/p^r)^\wedge.$$

le fait que le produit (4) soit direct résulte du fait que le produit (2) le soit. □

Démonstration du théorème 3.1

• Supposons d'abord que p soit inerte dans $\mathcal{O}$. Le lemme 2.3 montre que le deuxième facteur de la décomposition (2) (pour $\mathfrak{p} = (p)$) est cyclique d'ordre $p^2 - 1$. Or, le deuxième facteur de la décomposition (4) est un sous-groupe de celui de (2) d'après (6). Il est donc, lui aussi, cyclique.

De plus, d'après 2.2, l'injection du lemme 2.3 induit une bijection

$$(\mathcal{O}/p)^\wedge \to \{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\wedge\}.$$

Puisque le conjugué d'un élément x de $\mathcal{O}/p$ est x^p, les éléments de norme 1 dans $\mathcal{O}/p$ y sont les racines $(p+1)^{\text{ièmes}}$ de l'unité, qui sont en nombre $p+1$. Donc, le facteur de droite de la décomposition (4) est d'ordre $p+1$.

Considérons maintenant le premier facteur de la décomposition (4). Le lemme 3.2 montre par récurrence qu'il est d'ordre p^{r-1}.

Pour montrer qu'il est lui-aussi cyclique, montrons d'abord par récurrence sur r qu'il existe $\gamma \in p\mathcal{O} \setminus p^2\mathcal{O}$ tel que $[1+\gamma]$ appartient à $(\mathcal{O}/p^r)^\wedge$. Pour $r = 1$ ou 2, il suffit de prendre $\gamma = p^2 + p\sqrt{D}$ puisque

$$\begin{aligned} N(1+\gamma) &= (1+p^2)^2 + p^2 D \\ &\equiv 1 \text{ modulo } p^r. \end{aligned}$$

Pour $r \geq 3$, l'hypothèse de récurrence affirme qu'il existe $\gamma \in p\mathcal{O} \setminus p^2\mathcal{O}$ avec $N(1+\gamma) \equiv 1$ modulo p^{r-1}. Mais le lemme 3.2 montre l'existence d'un élément $1+\gamma'$ tel que

$$\begin{cases} 1+\gamma' \equiv 1+\gamma \text{ modulo } p^{r-1} \\ [1+\gamma'] \in (\mathcal{O}/p^r)^\wedge. \end{cases}$$

Comme $\gamma \equiv \gamma'$ modulo p^2, on a bien $\gamma' \in p\mathcal{O} \setminus p^2\mathcal{O}$ ce qui termine la récurrence. On vérifie alors aisément que

$$(1+\gamma)^{p^{k-1}} \equiv 1 + p^{k-1}\gamma \quad \text{modulo } p^k \qquad \text{pour } k \geq 1.$$

Donc, $1+\gamma$ est d'ordre p^{r-1} dans le facteur de gauche de (4) et en est un générateur, ce qui prouve que ce facteur est cyclique.

Enfin, on a montré que $(\mathcal{O}/p^r)^\wedge$ est le produit d'un groupe cyclique d'ordre $p+1$ par un autre d'ordre p^{r-1}. Il est donc cyclique d'ordre $p^{r-1}(p+1)$.

• Supposons maintenant que $p = \mathfrak{p}\overline{\mathfrak{p}}$ soit scindé dans $\mathcal{O}$. Montrons grâce à la décomposition (2) que le groupe $(\mathcal{O}/\mathfrak{p}^r)^\times$ est cyclique. Nous savons grâce au lemme 2.3 que le facteur de droite est cyclique d'ordre $p-1$. Quant au facteur de gauche, il est d'ordre

$$N(\mathfrak{p}^r)/N(\mathfrak{p}) = N(\mathfrak{p})^{r-1} = p^{r-1}.$$

Il est facile de voir que, si γ est un élément de $\mathfrak{p} \setminus \mathfrak{p}^2$, alors on a

$$(1+\gamma)^{p^{k-1}} \equiv 1 \text{ modulo } \mathfrak{p}^k$$

mais

$$(1+\gamma)^{p^{k-1}} \not\equiv 1 \text{ modulo } \mathfrak{p}^{k-1} \qquad \text{pour } k \geq 1.$$

Donc $1+\gamma$ est d'ordre p^{r-1} et est un générateur du facteur de gauche qui est donc, lui-aussi, cyclique.

On a montré que $(\mathcal{O}/\mathfrak{p}^r)^\times$ est le produit d'un groupe cyclique d'ordre $p-1$ par un autre d'ordre p^{r-1}. Il est donc cyclique d'ordre $p^{r-1}(p-1)$. Enfin, on a un morphisme injectif

$$(\mathcal{O}/\mathfrak{p}^r)^\times \ni x \quad \longmapsto \quad (x, 1/x) \in (\mathcal{O}/\mathfrak{p}^r)^\times \times (\mathcal{O}/\overline{\mathfrak{p}}^r)^\times \simeq (\mathcal{O}/p^r)^\times$$

dont l'image est $(\mathcal{O}/p^r)^\wedge$. □

La fonction ϕ_D

Par analogie avec la fonction indicatrice d'Euler, le théorème 3.1 nous suggère de poser la définition suivante :

3.4. — Définition. Soit D un entier non nul. Pour $n > 0$ entier impair premier avec D on pose

$$\phi_D(n) = \prod_{i=1}^{s} p_i^{r_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right)$$

où $n = p_1^{r_1} \cdots p_s^{r_s}$ est la décomposition de n en facteurs premiers distincts.

Pour D non carré parfait, le groupe $(\mathcal{O}/n)^\wedge$ est donc d'ordre $\phi_D(n)$. Pour D carré parfait, ϕ_D est la fonction d'Euler usuelle.

4. Liens entre les paramètres P et Q et l'élément τ

Nous avons déjà remarqué, dans la démonstration du théorème 1.3, l'importance du groupe des éléments de norme 1 dans l'anneau $\mathcal{O}/p$ (p premier impair). Pour n composé, nous avons une situation analogue qui rappelle de très près celle du chapitre 1 et que nous décrivons maintenant. Bien sûr, nous désignons par P et Q des entiers tels que $D = P^2 - 4Q$ ne soit pas un carré parfait et notons $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$. Nous désignons aussi par α et $\beta \in \mathcal{O}$ les racines du polynôme $X^2 - PX + Q$ et par (U_n) et (V_n) les suites de Lucas définies dans la section 1. Enfin, pour $n \in \mathbb{N}$, on note $\varepsilon(n)$ le symbole de Jacobi (D/n).

4.1. — Lemme. *Soit $n > 1$ un entier impair premier avec QD et posons $\tau = \alpha\beta^{-1}$ dans l'anneau $\mathcal{O}/n$ (τ est bien défini puisque $Q = \alpha\beta$ est premier avec n). Pour $k \in \mathbb{N}$, on a les équivalences*

$$n \mid U_k \iff \tau^k = 1,$$
$$n \mid V_k \iff \tau^k = -1.$$

En particulier, le nombre n est probablement premier de Lucas pour les paramètres P et Q si et seulement si $\tau^{n-\varepsilon(n)} = 1$, et il est fortement probablement premier de Lucas pour les paramètres P et Q si et seulement si on a

$$\tau^q = 1 \qquad \textit{ou} \qquad \textit{s'il existe un } i \textit{ tel que } 0 \leq i < k \textit{ et } \tau^{2^i q} = -1,$$

où l'on a posé $n - \varepsilon(n) = 2^k q$, avec q impair.

Démonstration — Elle résulte de (1) puisque, par exemple, on a

$$\begin{aligned} n \mid V_k &\iff V_k \in n\mathcal{O} \quad \text{car } n\mathcal{O} \cap \mathbb{Z} = n\mathbb{Z} \text{ et } V_k \in \mathbb{Z}, \\ &\iff \alpha^k + \beta^k \in n\mathcal{O}, \\ &\iff \tau^k + 1 \in n\mathcal{O} \quad \text{car } \alpha\beta = Q \text{ et } \operatorname{pgcd}(Q, n) = 1. \end{aligned}$$

□

A tout couple de paramètres P et Q tels que $P^2 - 4Q = D$, nous avons vu que l'on pouvait associer un élément τ dans le groupe $(\mathcal{O}/n)^\wedge$. Inversement, la donnée de τ suffit à retrouver la classe modulo n des paramètres P et Q de départ. Plus précisément, on a la proposition :

4.2. — Proposition. *Soit D un entier qui ne soit pas un carré parfait et désignons par $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$. Soit $n > 1$ un entier impair premier avec D. Alors, pour tout P entier, il existe un entier Q unique modulo n et tel que $P^2 - 4Q \equiv D$ modulo n. De plus, l'ensemble des entiers P vérifiant*

$$\begin{cases} 0 \leq P < n \\ \operatorname{pgcd}(P^2 - D, n) = 1 \quad (\textit{i.e. } \operatorname{pgcd}(Q, n) = 1), \end{cases}$$

est en bijection avec l'ensemble des éléments τ du groupe $(\mathcal{O}/n)^\wedge$ tels que $\tau - 1$ soit inversible dans $\mathcal{O}/n$. Cette bijection est donnée par les formules explicites

$$\begin{cases} \tau \equiv (P + \sqrt{D})(P - \sqrt{D})^{-1} \\ P \equiv \sqrt{D}(\tau + 1)(\tau - 1)^{-1} \end{cases} \qquad \text{modulo } n\mathcal{O}. \tag{7}$$

Démonstration — La première assertion est claire, puisque n est impair. Remarquons ensuite que, puisque le conjugué de τ dans $\mathcal{O}/n$ est τ^{-1}, on a, en posant $u + \sqrt{D}v = \sqrt{D}(\tau + 1)(\tau - 1)^{-1}$,

$$\begin{aligned} u - v\sqrt{D} &= \overline{\sqrt{D}(\tau + 1)(\tau - 1)^{-1}} \\ &\equiv -\sqrt{D}(\tau^{-1} + 1)(\tau^{-1} - 1)^{-1} \qquad \text{modulo } n \\ &= -\sqrt{D}(1 + \tau)(1 - \tau)^{-1} \\ &= \sqrt{D}(\tau + 1)(\tau - 1)^{-1} = u + v\sqrt{D}. \end{aligned}$$

Puisque n est impair, on obtient $v \equiv 0$ modulo n, prouvant ainsi que la congruence exprimant P dans (7) est bien vérifiée par un entier rationnel. Il ne reste alors plus qu'à démontrer l'équivalence des égalités (7), ce qui ne présente pas de difficultés. □

5. Formules de dénombrement

Les techniques classiques employées dans le chapitre 1 pour dénombrer les bases dans lesquelles un entier donné est probablement premier (resp. fortement probablement premier) peuvent donc être reprises pour les probablement premiers de Lucas. C'est ce que nous faisons dans les deux théorèmes suivants. Le premier de ces théorèmes est un résultat bien connu qui figure dans [1] (avec toutefois une démonstration bien moins algébrique). Cependant, nous n'avons trouvé nulle part la démonstration du deuxième théorème (un résultat semblable est cependant énoncé dans [2]) ni non plus les résultats de la section 6, qui en sont des conséquences.

Pseudo-primalité

5.1. — Théorème. *Soit D un entier qui ne soit pas un carré parfait. Pour $n = p_1^{r_1} \cdots p_s^{r_s}$ entier positif impair et tel que* $\operatorname{pgcd}(D, n) = 1$, *nous désignons par $\varepsilon(n)$ et $\varepsilon(p_i)$ les symboles (D/n) et (D/p_i). Le nombre $\gamma(n)$ de couples (P, Q) vérifiant*

$$\begin{cases} P^2 - 4Q \equiv D \text{ modulo } n \\ \operatorname{pgcd}(Q, n) = 1 \end{cases} \qquad 0 \leq P, Q < n$$

et tels que n soit probablement premier de Lucas pour les paramètres P et Q est donné par :

$$\gamma(n) = \prod_{i=1}^{s} \Big(\operatorname{pgcd}\big(n - \varepsilon(n), p_i - \varepsilon(p_i)\big) - 1 \Big).$$

Démonstration — Soit $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$. D'après 4.2, nous devons compter les éléments τ de $(\mathcal{O}/n)^\wedge$ tels que

$$\tau - 1 \in (\mathcal{O}/n)^\times \quad \text{et} \quad \tau^{n-\varepsilon(n)} = 1.$$

Or, cela est équivalent à

$$\tau - 1 \in (\mathcal{O}/p_i^{r_i})^\times \qquad \text{et} \qquad \tau^{n-\varepsilon(n)} \equiv 1 \quad \text{modulo } p_i^{r_i}\mathcal{O} \qquad \text{pour } 1 \leq i \leq s. \tag{8}$$

D'après le théorème 3.1 et le lemme 1.3.1, la dernière congruence admet

$$\begin{aligned} d &= \operatorname{pgcd}\Big(n - \varepsilon(n), p_i^{r_i - 1}\big(p_i - \varepsilon(p_i)\big)\Big) \\ &= \operatorname{pgcd}\big(n - \varepsilon(n), p_i - \varepsilon(p_i)\big) \end{aligned}$$

solutions. Parmi ces solutions τ, il convient de retirer celles pour lesquelles $\tau - 1$ n'est pas inversible modulo p_i. Montrons que la seule solution concernée par ce retrait est 1. Notons d'abord que

$$\begin{cases} \tau^{n-\varepsilon(n)} \equiv 1 \\ \tau^{p_i^{r_i-1}\left(p_i - \varepsilon(p_i)\right)} \equiv 1 \end{cases} \implies \tau^d \equiv 1 \implies \tau^{p_i - \varepsilon(p_i)} \equiv 1 \quad \text{modulo } p_i^{r_i}\mathcal{O}.$$

Soit $\mathfrak{p}$ un idéal premier contenant $p_i\mathcal{O}$. Pour $k \geq 1$ entier, on a

$$\begin{aligned} \tau \equiv 1 \text{ modulo } \mathfrak{p}^k &\Longrightarrow \tau^{p_i} \equiv 1 \text{ modulo } \mathfrak{p}^{k+1} && \text{par le lemme 2.2,} \\ &\Longrightarrow 1 \equiv \tau^{p_i - \varepsilon(p_i)} \equiv \tau^{-\varepsilon(p_i)} && \text{modulo } \mathfrak{p}^{k+1} \\ &\Longrightarrow \tau \equiv 1 \text{ modulo } \mathfrak{p}^{k+1}. \end{aligned}$$

Donc, par récurrence, on a $\tau \equiv 1$ modulo $\mathfrak{p}^{r_i}$. Si p_i est scindé, cela implique $\tau \equiv 1$ modulo $\overline{\mathfrak{p}}^{r_i}$ (puisque $\overline{\tau} = \tau^{-1}$). Dans tous les cas (inerte ou scindé), on obtient bien $\tau \equiv 1$ modulo $p_i^{r_i}$. Le nombre de solutions de (8) est donc

$$\operatorname{pgcd}\big(n - \varepsilon(n), p_i - \varepsilon(p_i)\big) - 1.$$

Enfin, le théorème chinois permet de conclure. □

Pseudo-primalité forte

Pour n entier impair supérieur à 2, notons

$$C_D(n) = \left\{ (P,Q) \;\middle|\; \begin{array}{c} 0 \leq P, Q < n, \qquad P^2 - 4Q \equiv D \text{ modulo } n, \\ n \text{ est fortement probablement premier de Lucas pour } P \text{ et } Q \end{array} \right\}.$$

5.2. — **Théorème.** *Soit $p_1^{r_1} \cdots p_s^{r_s}$ la décomposition en facteurs premiers distincts d'un entier $n > 2$ tel que* $\operatorname{pgcd}(2D, n) = 1$. *Posons*

$$\begin{cases} n - \varepsilon(n) = 2^k q \\ p_i - \varepsilon(p_i) = 2^{k_i} q_i \quad \text{pour } 1 \leq i \leq s \end{cases} \qquad \text{avec } q,\ q_i \text{ impairs,}$$

en ordonnant les p_i de telle manière que $k_1 \leq \cdots \leq k_s$. Le nombre de couples (P,Q) pour lesquels n est fortement probablement premier de Lucas est donné par la formule

$$|C_D(n)| = \prod_{i=1}^{s} \big(\operatorname{pgcd}(q, q_i) - 1\big) + \sum_{j=0}^{k_1 - 1} 2^{j\,s} \prod_{i=1}^{s} \operatorname{pgcd}(q, q_i).$$

Démonstration — Elle est analogue à celle de 1.3.2. Il s'agit ici de dénombrer les ensembles

$$\begin{aligned} P'(n) &= \{\tau \in (\mathcal{O}/n)^\wedge \mid 1 - \tau \in (O/n)^\times, \tau^q = 1\}, \\ Q'_j(n) &= \{\tau \in (\mathcal{O}/n)^\wedge \mid 1 - \tau \in (O/n)^\times, \tau^{2^j q} = -1\}, \qquad \text{pour } 0 \leq j \leq k-1 \end{aligned}$$

dont $C_D(n)$ est la réunion disjointe.

• Nous utilisons là-aussi le théorème chinois qui nous ramène au calcul de $|P'(p_i^{r_i})|$. Comme dans le théorème 5.1, la condition d'inversibilité de $1-\tau$ modulo p_i exclut la solution 1. Donc le lemme 1.3.1 indique que l'on a, comme dans le théorème 1.3.2,

$$\begin{aligned}|P'(p_i^{r_i})| &= \operatorname{pgcd}\bigl(q, \phi_D(p_i^{r_i})\bigr) - 1 \\ &= \operatorname{pgcd}\bigl(q, p_i - \varepsilon(p_i)\bigr) - 1 \qquad \text{car } q \text{ est premier avec } n, \\ &= \operatorname{pgcd}(q, q_i) - 1 \qquad \text{car } q \text{ est impair.}\end{aligned}$$

Donc on a

$$|P'(n)| = \prod_{i=1}^{s} \bigl(\operatorname{pgcd}(q, q_i) - 1\bigr).$$

• Dénombrons maintenant $Q'_j(p_i^{r_i})$. Ici, la condition d'inversibilité de $1-\tau$ modulo p_i n'exclut aucune solution. En effet, puisque p_i est impair on ne peut avoir, pour $\mathfrak{p}$ idéal premier contenant $p_i\mathcal{O}$,

$$1 = 1^{2^j q} \equiv \tau^{2^j q} \equiv -1 \qquad \text{modulo } \mathfrak{p}.$$

D'après le lemme 1.3.1, on a

$$|Q'_j(p_i^{r_i})| = \begin{cases} 0 & \text{si } j \geq k_i, \\ \operatorname{pgcd}(2^j q, \phi_D(p_i^{r_i})) = 2^j \operatorname{pgcd}(q, q_i) & \text{si } j < k_i. \end{cases}$$

• Enfin, l'égalité

$$|C_D(n)| = |P'(n)| + \sum_{j=0}^{k-1} |Q'_j(n)|$$

permet de conclure en remarquant que, puisque $n \equiv \varepsilon(n)$ modulo 2^{k_1} (car $p_i \equiv \varepsilon(p_i)$ modulo 2^{k_1} quel que soit i), on a $k_1 \leq k$. □

Exemple. Illustrons cela avec $n = 3569 = 43 \cdot 83$ et $D = 13$. On a

$$\varepsilon(43) = \left(\frac{13}{43}\right) = 1, \quad \varepsilon(83) = \left(\frac{13}{83}\right) = -1, \quad \varepsilon(3569) = \left(\frac{13}{3569}\right) = -1,$$
$$43 - 1 = 2 \cdot 21, \quad 83 + 1 = 2^2 \cdot 21, \quad 3569 + 1 = 2 \cdot 21 \cdot 85.$$

On a donc

$$|P| = \bigl(\operatorname{pgcd}(21 \cdot 85, 21) - 1\bigr)\bigl(\operatorname{pgcd}(21 \cdot 85, 21) - 1\bigr) = 20^2 = 400,$$
$$|Q_0| = \operatorname{pgcd}(21 \cdot 85, 21) \operatorname{pgcd}(21 \cdot 85, 21) = 21^2 = 441.$$

Donc $|C(3569)| = 841$.

6. Analogues du théorème de Rabin

Il est clair que le théorème 5.2 nous permettrait de prouver le résultat suivant, en reprenant mot à mot la démonstration du théorème de Rabin 1.1.7.

6.1. — Corollaire. *Si n est composé et impair alors*

$$|C_D(n)| \leq \phi_D(n)/4.$$

Mais puisque, contrairement à la fonction d'Euler usuelle, la fonction $\phi_D(n)$ n'est pas majorée par n et puisque sa valeur est inconnue tant que n n'est pas factorisé, nous avons jugé utile d'énoncer le résultat plus satisfaisant que voici :

6.2. — Théorème. *Si n est composé et impair et distinct de 9 alors*

$$|C_D(n)| \leq \frac{4}{15}n.$$

sauf si n est un produit de deux nombres premiers jumelés

$$n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$$

avec q_1 impair et $\varepsilon(2^{k_1}q_1 - 1) = -1$, $\varepsilon(2^{k_1}q_1 + 1) = 1$. De plus, dans tous les cas, on a

$$|C_D(n)| \leq n/2.$$

Démonstration — Elle fait l'objet de la fin de cette section. □

Lemmes auxiliaires

Le lemme suivant est simplement une adaptation de lemme 1.3.3. Nous n'en répéterons pas la démonstration, qui serait identique.

6.3. — Lemme. *Avec les notations de la proposition 5.2, on a les inégalités*

$$\frac{|C_D(n)|}{\phi_D(n)} \leq \begin{cases} \dfrac{1}{2^{s-1}} \displaystyle\prod_{i=1}^{s} \frac{\operatorname{pgcd}(q, q_i)}{q_i} \\ \dfrac{1}{2^{s-1}} \displaystyle\prod_{i=1}^{s} \frac{1}{p_i^{r_i - 1}} \\ 1/2^{s-1+\delta_2+\cdots+\delta_s} \quad \text{où } \delta_i = k_i - k_1. \end{cases}$$

Le lemme suivant fournit des majorations assez grossières. Il nous suffira pour l'instant.

6.4. — Lemme. *Soit D un entier non nul. Pour $n > 0$ entier impair et premier avec D on a*

$$\phi_D(n) \leq \left(\frac{4}{3}\right)^s n$$

où s est le nombre de facteurs premiers distincts, de n. De plus, on a les cas particuliers suivants :

$$\begin{aligned} s \geq 2 \quad &\Longrightarrow \quad \phi_D(n) \leq \frac{8}{5} n, \\ s \geq 3 \quad &\Longrightarrow \quad \phi_D(n) \leq \frac{64}{35} n. \\ s \geq 4 \quad &\Longrightarrow \quad \phi_D(n) \leq \frac{768}{385} \left(\frac{12}{11}\right)^{s-4} n. \end{aligned}$$

Démonstration — Pour $n_1, n_2 \in \mathbb{N}^*$ premiers entre eux et tels que $\operatorname{pgcd}(n_1 n_2, 2D) = 1$, on a la relation

$$\phi_D(n_1 n_2) = \phi_D(n_1)\phi_D(n_2).$$

Pour la première partie du lemme, il suffit donc de traiter le cas où $n = p^r$ est la puissance d'un nombre premier impair ne divisant pas D. On a alors

$$\frac{\phi_D(p^r)}{p^r} = \frac{p^{r-1}(p - \varepsilon(p))}{p^r} = 1 - \varepsilon(p)/p \leq 1 + 1/p \leq 4/3.$$

d'où le résultat. La seconde partie du lemme se démontre de la même façon en remarquant que $p_i \geq 5$ sauf pour au plus l'un des indices i, que $p_i \geq 7$ sauf pour au plus deux indices i et que $p_i \geq 11$ sauf pour au plus trois indices i. □

Démonstration du théorème 6.2

La démonstration est très longue et reprend en partie celle du théorème de Rabin 1.1.7. Cependant, nous devons examiner de plus près les cas limites que nous y avons rencontrés. Nous utilisons à nouveau les notations du théorème 5.2.

• Considérons d'abord le cas $s = 1$. La deuxième majoration du lemme 6.3 indique que

$$|C_D(n)| \leq \frac{1}{p_1^{r_1 - 1}} \phi_D(n).$$

Pour $p_1 \geq 5$, on obtient, puisque $r_1 \geq 2$,

$$|C_D(n)| \leq \phi_D(n)/5.$$

Le lemme 6.4 permet alors d'en déduire l'inégalité $|C_D(n)| \leq (4/15)n$.

Pour $p_1 = 3$, un raisonnement semblable s'applique, à condition toutefois que $r_1 \geq 3$. Notons que pour le cas $n = 9$, il est facile de vérifier que

$$\begin{aligned} &\text{pour } \varepsilon(3) = 1 : \quad C_D(n) = 1, \quad \phi_D(n) = 6, \\ &\text{pour } \varepsilon(3) = -1 : \quad C_D(n) = 3, \quad \phi_D(n) = 12. \end{aligned}$$

• Considérons maintenant le cas $s = 2$. D'après la deuxième partie du lemme 6.4, il suffit de montrer que l'on a l'inégalité

$$|C_D(n)| \leq \frac{1}{6}\phi_D(n). \tag{9}$$

Or le lemme 6.3 fournit les majorations

$$\frac{|C_D(n)|}{\phi_D(n)} \leq \begin{cases} 1/6 & \text{si } r_i \geq 2 \text{ pour au moins un } i \\ 1/8 & \text{si } \delta_2 = k_2 - k_1 \geq 2 \end{cases}$$

ce qui suffit pour conclure dans ces deux cas.

D'autre part, examinons le cas où $q_1 \neq q_2$. La première inégalité du lemme 6.3 indique que

$$\frac{|C_D(n)|}{\phi_D(n)} \leq \frac{1}{2}\frac{\operatorname{pgcd}(q, q_1)}{q_1}\frac{\operatorname{pgcd}(q, q_2)}{q_2}.$$

Montrons que l'un au moins des rapports $\operatorname{pgcd}(q, q_i)/q_i$ est majoré par $1/3$. Sinon, on aurait $q_1 \mid q$ et $q_2 \mid q$ ce qui entraînerait que q_1 et q_2 diviseraient

$$\begin{aligned} 2^k q &= p_1 p_2 - \varepsilon(p_1 p_2) \\ &= (2^{k_1} q_1 + \varepsilon(p_1))(2^{k_1+\delta_2} q_2 + \varepsilon(p_2)) - \varepsilon(p_1 p_2) \\ &= 2^{2k_1+\delta_2} q_1 q_2 \pm 2^{k_1}(q_1 \pm 2^{\delta_2} q_2). \end{aligned}$$

Nous aurions alors $q_1 \mid q_2$ et $q_2 \mid q_1$, contredisant l'hypothèse $q_1 \neq q_2$. On a donc

$$\frac{|C_D(n)|}{\phi_D(n)} \leq 1/6$$

et l'équation (9) est bien vérifiée.

Nous pouvons donc supposer que $r_1 = r_2 = 1$, que $\delta_2 = k_2 - k_1$ vaut 0 ou 1, et que $q_1 = q_2$. Pour $\delta_2 = 1$, l'entier n est de la forme

$$\begin{aligned} n &= (2^{k_1} q_1 \pm 1)(2^{k_1+1} q_1 \pm 1) \qquad \text{avec } q_1 \text{ impair.} \\ &\geq (2^{k_1} q_1 - 1)(2^{k_1+1} q_1 - 1) \\ &= 2(2^{k_1} q_1)^2 - 3(2^{k_1} q_1) + 1 \end{aligned}$$

et le théorème 5.2 donne

$$\begin{aligned} |C_D(n)| &= (q_1 - 1)^2 + (1 + 4 + \cdots + 4^{k_1-1}) q_1^2 \\ &= (q_1 - 1)^2 + \frac{4^{k_1} - 1}{3} q_1^2 \\ &\leq \frac{4^{k_1} + 2}{3} q_1^2. \end{aligned}$$

Nous séparons le cas où $k_1 = 1$ de celui où $k_1 \geq 2$. Pour $k_1 \geq 2$ on a

$$\begin{aligned} 4n - 15|C_D(n)| &\geq 3(2^{k_1}q_1)^2 - 10q_1^2 - 12(2^{k_1}q_1) + 4 \\ &> 2(2^{k_1}q_1)^2 - 12(2^{k_1}q_1) + 4 \qquad \text{car } k_1 \geq 2 \\ &= 2\big((2^{k_1}q_1)^2 - 6(2^{k_1}q_1) + 2\big). \end{aligned}$$

Les racines de ce trinôme sont inférieures à 6 ; il prend donc des valeurs positives pour $2^{k_1}q_1 \geq 6$. Comme $k_1 \geq 2$, il reste seulement le cas $2^{k_1}q_1 = 4$, ce qui implique $n = 21$ ou 35 et que $|C_D(n)| = 5$.

Pour $k_1 = 1$, on a

$$n \geq (2q_1 - 1)(4q_1 - 1) \qquad \text{avec } q_1 \text{ impair.}$$

donc

$$\begin{aligned} 4n - 15|C_D(n)| &\geq 2q_1 + 6q_1 - 11 \\ &> 0 \quad \text{si } q_1 \neq 1. \end{aligned}$$

Il reste le cas où $q_1 = 1$, ce qui implique que $n = 15$ et que $|C_D(n)| = 1$.

Enfin, pour $k_1 = k_2$, nous sommes en présence d'un nombre n de la forme

$$n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1) = 4^{k_1}q_1^2 - 1 \quad \text{avec } \varepsilon(n) = -1.$$

Puisque $n = 2^k q - 1$, nous avons aussi $q = q_1^2$. Ici, le théorème 5.2 donne

$$\begin{aligned} |C_D(n)| &= (q_1 - 1)^2 + \frac{4^{k_1} - 1}{3}q_1^2 \\ &= \frac{4^{k_1} + 2}{3}q_1^2 - 2q_1 + 1. \end{aligned}$$

Donc,

$$\begin{aligned} 3(n - 2|C_D(n)|) &= 4^{k_1}q_1^2 - 4q_1^2 + 12q_1 - 9 \\ &\geq 12q_1 - 9 > 0. \end{aligned}$$

• Maintenant, considérons le cas $s = 3$. D'après la deuxième partie du lemme 6.4, il suffit de montrer que l'on a l'inégalité

$$|C_D(n)| \leq \frac{7}{48}\phi_D(n). \tag{10}$$

Là encore, le lemme 6.3 permet de conclure dans les situations suivantes :

$$\frac{|C_D(n)|}{\phi_D(n)} \leq \begin{cases} 1/12 & \text{si } r_i \geq 2 \text{ pour au moins un } i \\ 1/8 & \text{si les } k_i \text{ ne sont pas tous égaux} \\ 1/12 & \text{si l'un des } q_i \text{ ne divise pas } q \end{cases}$$

puisqu'alors l'inégalité (10) est vérifiée.

Dans le cas restant

$$n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1}q_2 + \varepsilon_2)(2^{k_1}q_3 + \varepsilon_3)$$

avec q_1, q_2, q_3 impairs et divisant $n - \varepsilon(n) = 2q$, la formule 5.2 s'écrit

$$\begin{aligned}|C_D(n)| &= (q_1-1)(q_2-1)(q_3-1) + (1+8+\cdots+8^{k_1-1})q_1q_2q_3\\ &= (q_1-1)(q_2-1)(q_3-1) + \frac{8^{k_1}-1}{7}q_1q_2q_3\\ &= (q_1-1)(q_2-1)(q_3-1) + \phi_D(n)/7 - q_1q_2q_3/7.\end{aligned}$$

L'inégalité (10) que l'on veut montrer s'écrit

$$(q_1-1)(q_2-1)(q_3-1) + \phi_D(n)/7 - q_1q_2q_3/7 \leq \frac{7}{48}\phi_D(n)$$

ou encore

$$\phi_D(n)/336 \geq (q_1-1)(q_2-1)(q_3-1) - q_1q_2q_3/7,$$

ce qui est vérifié dès que

$$\phi_D(n) = 8^{k_1}q_1q_2q_3 \geq 336q_1q_2q_3$$

donc en particulier dès que $k_1 \geq 3$.

Traitons le cas où $k_1 = 2$, on vérifie alors que

$$\begin{aligned}4n - 15|C_D(n)| &\geq 106q_1q_2q_3 - 49(q_1q_2 + q_1q_3 + q_2q_3) + (q_1+q_2+q_3) + 11\\ &= 106(q_1-1)(q_2-1)(q_3-1)\\ &\quad + 269(q_1-1)(q_2-3) + 269(q_1-1)(q_3-3) + 57(q_2-3)(q_3-3)\\ &\quad + 661(q_1-1) + 123(q_2-3) + 123(q_3-3) + 237\end{aligned}$$

ce qui est visiblement positif puisqu'un seul au plus des q_i peut être égal à 1, et que l'on peut supposer que c'est q_1.

D'autre part, pour $k_1 = 1$ nous avons

$$\begin{aligned}n &\geq (2q_1-1)(2q_2-1)(2q_3-1)\\ &= 8q_1q_2q_3 - 4(q_1q_2 + q_1q_3 + q_2q_3) + 2(q_1+q_2+q_3) - 1.\end{aligned}$$

On en déduit facilement (si l'on a la chance d'avoir des bons moyens de calcul sous la main) que

$$\begin{aligned}4n - 15|C_D(n)| &\geq 2q_1q_2q_3 - (q_1q_2 + q_1q_3 + q_2q_3) - 7(q_1+q_2+q_3) + 11\\ &= 2(q_1-3)(q_2-5)(q_3-7)\\ &\quad + 13(q_1-3)(q_2-5) + 9(q_1-3)(q_3-7) + 5(q_2-5)(q_3-7)\\ &\quad + 51(q_1-3) + 25(q_2-5) + 15(q_3-7) + 45.\end{aligned}$$

Cela prouve que $4n - 15|C_D(n)| > 0$ dès que l'on a

$$q_1 \geq 3, \quad q_2 \geq 5, \quad q_3 \geq 7.$$

Cela règle tous les cas sauf, à permutation des indices près, celui où $p_1 = 3$ et celui où $p_1 = 5$ et $p_2 = 7$.

Si $p_1 = 3$ alors on vérifie que

$$\begin{aligned} 4n - 15|C_D(n)| &\geq 12(2q_2 - 1)(2q_3 - 1) - 15q_2q_3 \\ &= 33(q_2 - 3)(q_3 - 3) + 73(q_2 - 3) + 75(q_3 - 3) + 165 > 0. \end{aligned}$$

Si $p_1 = 5$ et $p_2 = 7$ alors

$$\begin{aligned} 4n - 15|C_D(n)| &\geq 4 \cdot 5 \cdot 7(2q_3 - 1) - 4(q_3 - 1) - 9q_3 \\ &= 85(q_3 - 5) + 345 > 0. \end{aligned}$$

• Enfin, le cas où $s \geq 4$. Le lemme 6.3 indique que

$$|C_D(n)| \leq \phi_D(n)/2^{s-1} = \frac{1}{2^{s-4}}\phi_D(n)/8.$$

Avec la majoration de 6.4, on obtient

$$\begin{aligned} |C_D(n)| &\leq \frac{96}{385}\left(\frac{6}{11}\right)^{s-4} n \\ &\leq \frac{96}{385}n \leq \frac{4}{15}n. \end{aligned}$$

Ceci termine enfin (!) la démonstration. □

Exceptions

Il est facile de trouver des exemples de la famille d'exceptions citées dans le théorème 6.2. En voici quelques uns :

$$\begin{aligned} n = 143 = 11 \cdot 13, &\qquad C_{17}(143) = 49, \\ n = 323 = 17 \cdot 19, &\qquad C_5(323) = 145, \\ n = 899 = 29 \cdot 31, &\qquad C_{19}(899) = 421. \end{aligned}$$

7. Analogues des nombres de Carmichael

A la lumière des sections précédentes, nous reprenons ici les résultats de [10]. Pour D entier, Williams considère les entiers vérifiant une propriété qui peut s'énoncer ainsi :

7.1. — Définition. Pour D entier fixé, nous appelons *nombre de Lucas-Carmichael* tout entier positif et composé tel que $\mathrm{pgcd}(n, 2D) = 1$ et qui soit pseudo-premier de Lucas pour tout couple d'entiers (P, Q) vérifiant

$$P^2 - 4Q = D, \qquad \mathrm{pgcd}(Q, n) = 1.$$

Par analogie avec la fonction de Carmichael (qui à n associe l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, voir 1.1.4), nous sommes tentés d'utiliser la notation que voici :

7.2. — Notation. Pour D entier non nul et pour n impair et premier avec D, nous notons $\lambda_D(n)$ le plus petit entier m tel que l'on ait

$$x^m = 1 \qquad \text{pour tout } x \text{ élément de } (\mathcal{O}/n)\hat{}\,.$$

où $\mathcal{O}$ désigne l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

On peut calculer la fonction λ_D en utilisant les formules suivantes :

$$\lambda_D(p^r) = p^{r-1}\left(p - \left(\frac{D}{p}\right)\right) \qquad \text{pour } r \geq 1 \text{ et } p \text{ premier ne divisant pas } 2D$$

$$\lambda_D(n_1 n_2) = \mathrm{ppcm}(\lambda_D(n_1), \lambda_D(n_2)) \qquad \text{pour } n_1 \text{ et } n_2 \text{ premiers entre eux et avec } D.$$

Grâce aux résultats de la section 4, il est clair qu'un entier composé n premier avec $2D$ est de Lucas-Carmichael si et seulement si $\lambda_D(n)$ divise $n - (D/n)$. On en déduit immédiatement le résultat principal de [10] :

7.3. — Théorème. *Pour D fixé, un entier composé n est un nombre de Lucas-Carmichael si et seulement s'il est le produit $p_1 \cdots p_s$ de nombres premiers distincts, impairs, ne divisant pas D et tels que*

$$p - \varepsilon(p) \mid n - \varepsilon(n).$$

avec, comme d'habitude, $\varepsilon(a) = (D/a)$. □

On rencontrera, dans le chapitre 6, des nombres de Lucas-Carmichael n avec $\varepsilon(n) = -1$. Une question importante pour les tests de primalité est cependant sans réponse actuellement : existe-t-il des nombres n qui soient à la fois des nombres de Carmichael classiques et des nombres de Lucas-Carmichael avec $\varepsilon(n) = -1$? Dans [10], on montre que de tels entiers, s'ils existent, sont le produit $p_1 \cdots p_s$ de nombres premiers p_i tels que $\varepsilon(p_i) = -1$ et avec $s \geq 5$ impair.

8. Bibliographie

[1] R. Baillie, S. Wagstaff Jr : *Lucas pseudoprimes.* Mathematics of Computation, vol. 35, n° 152, oct. 1980, pp. 1391–1417.

[2] C. Boyd : *Probabilistic prime tests.* Dans : Computers and Mathematical Research, N.M. Stephens et M.P. Thorne, Clarendon Press, 1988, pp. 57–68.

[3] J. Brillhart, D.H. Lehmer, J.L. Selfridge : *New primality criteria and factorizations of* $2^n \pm 1$. Mathematics of Computation, vol. 29, 1975, pp. 620–647.

[4] E. Lucas : *Théorie des fonctions numériques simplement périodiques.* American Journal of Mathematics, vol. 1, 1878, pp. 184–240, 289–321.

[5] C. Pomerance, J.L. Selfridge, S.S. Wagstaff : *The pseudoprimes to* $25 \cdot 10^9$. Mathematics of Computation, vol. 35, n° 151, 1980, pp. 1003–1026.

[6] P. Ribenboim : *The Book of Prime Number Records.* Springer-Verlag, 1988.

[7] A. Rotkiewicz : *On pseudoprimes with respect to the Lucas sequences.* Bulletin de l'Académie Polonaise des Sciences, vol. 21, 1973, pp. 793-797.

[8] M. Ward : *Tests for primality based on Sylvesters cyclotomic numbers.* Pacific Journal of Mathematics, vol. 9, 1959, pp. 1269–1272.

[9] M. Ward : *The prime divisors of Fibonacci numbers.* Pacific Journal of Mathematics, vol. 11, 1961, pp. 379–389.

[10] H.C. Williams : *On numbers analogous to the Carmichael numbers.* Bulletin Canadien de Mathématiques, vol. 20, 1977, pp. 133–143.

[11] H.C. Williams : *A* $p+1$ *method of factoring.* Mathematics of Computation, vol. 39, juillet 1982, pp. 225–234.

Chapitre 5

Estimations de la fonction ϕ_D

Par analogie avec la fonction ϕ d'Euler définie par :

$$\begin{cases} \phi(p^r) = p^{r-1}(p-1) & \text{pour } p \text{ premier, } r \in \mathbb{N}^* \\ \phi(n_1 n_2) = \phi(n_1)\phi(n_2) & \text{pour } n_1 \text{ et } n_2 \text{ premiers entre eux,} \end{cases}$$

on considère la fonction ψ :

$$\begin{cases} \psi(p^r) = p^{r-1}(p+1) & \text{pour } p \text{ premier, } r \in \mathbb{N}^* \\ \psi(n_1 n_2) = \psi(n_1)\phi(n_2) & \text{pour } n_1 \text{ et } n_2 \text{ premiers entre eux,} \end{cases}$$

et, pour $D \in \mathbb{N}$ non carré parfait, la fonction ϕ_D (définie seulement pour n premier avec $2D$) rencontrée dans le chapitre 4 :

$$\begin{cases} \phi_D(p^r) = p^{r-1}(p-\varepsilon(p)) & \text{pour } p \text{ premier, } p \nmid 2D,\ r \in \mathbb{N}^*, \\ \phi_D(n_1 n_2) = \phi_D(n_1)\phi_D(n_2) & \text{pour } n_1 \text{ et } n_2 \text{ premiers entre eux,} \end{cases}$$

où $\varepsilon(p)$ désigne le symbole de Legendre (D/p).

Les résultats suivants sur le comportement de ϕ sont bien connus (voir [1] et [2]) :

0.1. — Proposition. *On a la relation suivante :*

$$\limsup \frac{\phi(n)}{n} = 1.$$

0.2. — Théorème. *On a la relation suivante :*

$$\liminf \frac{\phi(n)}{n} e^{\gamma} \ln\ln n = 1.$$

où γ désigne la constante d'Euler.

Le but de ces pages est de montrer des résultats analogues pour les fonctions ψ et ϕ_D.

1. Rappels

Ordre de grandeur de fonctions usuelles

Désignons par $\pi(x)$ le nombre de nombres premiers inférieurs à x et par θ la fonction de Čhebyshev :

$$\pi(x) = \sum_{p \le x} 1, \qquad \theta(x) = \sum_{p \le x} \ln p.$$

Le *théorème des nombres premiers* s'exprime par l'une ou l'autre des relations

$$\pi(x) \sim \frac{x}{\ln x}, \qquad \theta(x) \sim x.$$

On a aussi le résultat suivant ([1, p 341]) :

1.1. — Théorème. *Pour $x \in \mathbb{N}^*$, on a*

$$\theta(n) < (2 \ln 2)n.$$

1.2. — Théorème (Mertens).

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln x}.$$

La fonction ζ

1.3. — Définition. *On appelle fonction ζ de Riemann la série suivante :*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Elle est convergente pour $s > 1$ réel.

1.4. — Lemme. *Au point $s = 2$ la fonction ζ de Riemann vaut*

$$\zeta(2) = \pi^2/6.$$

1.5. — Théorème (Identité d'Euler). *Pour $s > 1$, on a l'égalité*

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

où le produit est indexé sur l'ensemble de tous les nombres premiers.

Démonstration — Elle résulte essentiellement de l'égalité

$$\frac{1}{1 - p^{-s}} = \sum_{k=0}^{\infty} p^{-ks}.$$

2. Préliminaires

2.1. — Théorème. *On a la relation*

$$\prod_{p\leq x}\left(1+\frac{1}{p}\right)\sim\frac{6}{\pi^2}e^{\gamma}\ln x.$$

Démonstration — Remarquons que le lemme 1.4 peut aussi s'écrire, d'après 1.5,

$$\prod_{p}\left(1-\frac{1}{p^2}\right)=6/\pi^2. \tag{1}$$

Le résultat est alors une conséquence de la formule de Mertens 1.2 et de l'identité

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)\prod_{p\leq x}\left(1+\frac{1}{p}\right)=\prod_{p\leq x}\left(1-\frac{1}{p^2}\right).$$ □

2.2. — Lemme. *Les deux suites*

$$\left(1\pm\frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}$$

convergent vers 1.

Démonstration — Nous traitons le cas du signe plus. Posons $t=1/\ln n$, la limite cherchée est

$$\lim_{t\to 0^+}(1+t)^{-1/(t\ln t)}=\lim_{t\to 0^+}\exp\left(-\frac{\ln(1+t)}{t}\frac{1}{\ln t}\right)=1.$$

2.3. — Lemme. *Soit $n\in\mathbb{N}$ et soit ρ le nombre de facteurs premiers de n supérieurs à $\ln n$. On a la majoration*

$$\rho\leq\ln(n)/\ln\ln(n).$$

Démonstration — On a clairement

$$(\ln n)^{\rho}\leq\prod_{\substack{p\,|\,n\\ p\geq\ln n}}p\leq n.$$

En prenant les logarithmes des deux membres extrêmes, on obtient le résultat. □

3. La fonction ψ

Notons tout d'abord que la fonction $\psi(n)/n$ s'écrit sous la forme :

$$\frac{\psi(n)}{n} = \prod_{p|n}\left(1+\frac{1}{p}\right). \tag{2}$$

3.1. — Proposition. *On a la relation suivante :*

$$\liminf \frac{\psi(n)}{n} = 1.$$

Démonstration — On voit clairement que, pour tout $n \in \mathbb{N}^*$, on a $\psi(n)/n > 1$. Donc la limite inférieure considérée est supérieure ou égale à 1. Or la sous-suite

$$\frac{\psi(p)}{p} = \left(1+\frac{1}{p}\right) \qquad \text{pour } p \text{ premier}$$

converge vers 1. □

3.2. — Théorème. *On a la relation suivante :*

$$\limsup \frac{\psi(n)e^{-\gamma}}{n\ln\ln n} = 6/\pi^2.$$

Démonstration — On majorera d'abord $(\psi(n)e^{-\gamma})/(n\ln\ln n)$ par une suite convergeant vers $6/\pi^2$, puis on minorera une sous-suite par une autre suite convergeant vers $6/\pi^2$.

• On a les relations

$$\begin{aligned}\frac{\psi(n)}{n} &= \prod_{\substack{p\,|\,n\\ p\le \ln n}}\left(1+\frac{1}{p}\right)\prod_{\substack{p\,|\,n\\ p>\ln n}}\left(1+\frac{1}{p}\right)\\ &\le \prod_{p\le \ln n}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{\ln n}\right)^{\rho}\end{aligned}$$

où ρ est le nombre de facteurs premiers de n supérieurs à $\ln n$. Ainsi, d'après 2.3,

$$\frac{\psi(n)e^{-\gamma}}{n\ln\ln n} \le \frac{e^{-\gamma}}{\ln\ln n}\prod_{p\le \ln n}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}.$$

D'après 2.2, le dernier facteur de cette majoration tend vers 1 et, d'après 2.1, le facteur restant est équivalent à $6/\pi^2$. Le tout tend donc vers $6/\pi^2$, ce qui termine la démonstration du premier point.

• Posons $n_k = \prod_{p\le k} p$. On a l'égalité $\ln n_k = \theta(k)$ donc, d'après le théorème 1.1,

$$\ln\ln n_k < \ln 2 + \ln\ln 2 + \ln k. \tag{3}$$

D'autre part,

$$\frac{\psi(n_k)}{n_k} = \prod_{p|n_k}\left(1+\frac{1}{p}\right) = \prod_{p\le k}\left(1+\frac{1}{p}\right).$$

Donc, en utilisant (3),

$$\frac{\psi(n_k)e^{-\gamma}}{n_k \ln\ln n_k} \ge \prod_{p\le k}\left(1+\frac{1}{p}\right)\frac{e^{-\gamma}}{\ln 2+\ln\ln 2+\ln k}.$$

Mais, d'après 2.1, le membre de droite est équivalent à $(6/\pi^2)\ln k/(\ln 2+\ln\ln 2+\ln k)$. Il a donc $6/\pi^2$ pour limite, ce qui termine la démonstration. □

4. Progressions arithmétiques

Pour k et l entiers premiers entre eux avec $k>0$, on pose

$$\pi_{k,l}(x) = \sum_{\substack{p\le x\\ p\equiv l\ (k)}} 1, \qquad \theta_{k,l}(x) = \sum_{\substack{p\le x\\ p\equiv l\ (k)}} \ln p.$$

Le *théorème des nombres premiers* se généralise ainsi (voir par exemple [5]) :

4.1. — Théorème. *On a les relations*

$$\pi_{k,l}(x) \sim \frac{1}{\phi(k)}\frac{x}{\ln x}, \qquad \theta_{k,l}(x) \sim \frac{x}{\phi(k)}.$$

Pour D non carré parfait et en notant $\varepsilon(p) = (D/p)$ (où p est un premier impair), nous poserons

$$\pi^+(x) = \sum_{\substack{p\le x\\ \varepsilon(p)=1}} 1, \qquad \theta^+(x) = \sum_{\substack{p\le x\\ \varepsilon(p)=1}} \ln p.$$

Nous utiliserons le théorème précédent sous la forme suivante :

4.2. — Théorème. *On a les relations*

$$\pi^+(x) \sim \frac{1}{2}\frac{x}{\ln x}, \qquad \theta^+(x) \sim x/2.$$

5. Produits partiels

Cette section est une généralisation évidente de [6]. Introduisons quelques notations : posons

$$A_+ = \prod_{\varepsilon(p)=1}\left(1-\frac{1}{p^2}\right), \qquad A_- = \prod_{\varepsilon(p)=-1}\left(1-\frac{1}{p^2}\right), \qquad A_0 = \prod_{p|2D}\left(1-\frac{1}{p^2}\right),$$

de telle sorte que $A_0A_+A_- = 6/\pi^2$ d'après (1). On pose aussi

$$l = L(1,\varepsilon) = \prod_p \left(1 - \frac{\varepsilon(p)}{p}\right)^{-1}$$

où $L(s,\varepsilon) = \sum_{n=1}^{\infty} \varepsilon(n)/n^s$ est la L-fonction de Dirichlet associée au caractère ε. Il est connu en particulier que si $D = -1$ alors $l = \pi/4$.

Nous allons exprimer les valeurs asymptotiques des fonctions

$$P_+(x) = \prod_{\substack{p\le x\\ \varepsilon(p)=1}} \left(1-\frac{1}{p}\right), \qquad P_-(x) = \prod_{\substack{p\le x\\ \varepsilon(p)=-1}} \left(1-\frac{1}{p}\right),$$
$$Q_+(x) = \prod_{\substack{p\le x\\ \varepsilon(p)=1}} \left(1+\frac{1}{p}\right), \qquad Q_-(x) = \prod_{\substack{p\le x\\ \varepsilon(p)=-1}} \left(1+\frac{1}{p}\right),$$

à l'aide des constantes introduites ci-dessus et de

$$P_0 = \prod_{p\mid 2D} \left(1-\frac{1}{p}\right).$$

5.1. — **Théorème.** *On a les valeurs asymptotiques suivantes :*

$$P_+(x) \sim \sqrt{\frac{e^{-\gamma}}{lA_-P_0\ln x}}, \qquad P_-(x) \sim \sqrt{\frac{e^{-\gamma}lA_-}{P_0\ln x}},$$
$$Q_+(x) \sim A_+\sqrt{e^{\gamma}lA_-P_0\ln x}, \qquad Q_-(x) \sim \sqrt{\frac{e^{\gamma}A_-P_0\ln x}{l}}.$$

Démonstration — Notons tout d'abord les relations

$$P_-(x)Q_-(x) = \prod_{\substack{p\le x\\ \varepsilon(p)=-1}} \left(1-\frac{1}{p}\right) \prod_{\substack{p\le x\\ \varepsilon(p)=-1}} \left(1+\frac{1}{p}\right) = \prod_{\substack{p\le x\\ \varepsilon(p)=-1}} \left(1-\frac{1}{p^2}\right) \sim A_-,$$

$$P_+(x)Q_-(x) = \prod_{\substack{p\le x\\ \varepsilon(p)=1}} \left(1-\frac{1}{p}\right) \prod_{\substack{p\le x\\ \varepsilon(p)=-1}} \left(1+\frac{1}{p}\right) = \prod_{p\le x} \left(1-\frac{\varepsilon(p)}{p}\right) \sim 1/l. \tag{4}$$

On en déduit

$$\frac{P_-(x)}{P_+(x)} = \frac{P_-(x)Q_-(x)}{P_+(x)Q_-(x)} \sim lA_-.$$

Les valeurs asymptotiques de $P_+(x)$ et $P_-(x)$ s'obtiennent alors facilement en remarquant que, par la formule de Mertens 1.2, on a

$$P_0P_+(x)P_-(x) \sim \frac{e^{-\gamma}}{\ln x}.$$

Ensuite, l'équation (4) permet de calculer la valeur asymptotique de $Q_-(x)$. Pour déterminer celle de $Q_+(x)$, remarquons que

$$P_+(x)P_-(x)Q_+(x)Q_-(x) \sim A_+A_-,$$

et donc, par (4),

$$P_-(x)Q_+(x) \sim lA_+A_-.$$

ce qui permet de conclure. □

6. La fonction ϕ_D

Nous allons montrer ici les résultats suivants :

6.1. — Théorème.

$$\liminf \frac{\phi_D(n)}{n} e^{\gamma/2}\sqrt{\ln\ln n} = \frac{1}{\sqrt{lA_-P_0}}.$$

6.2. — Théorème.

$$\limsup \frac{\phi_D(n)e^{-\gamma/2}}{n\sqrt{\ln\ln n}} = \sqrt{\frac{A_-P_0}{l}}.$$

Démonstration du théorème 6.1

Nous commençons par minorer $\phi_D(n)e^{\gamma/2}\sqrt{\ln\ln n}/n$ par une suite ayant $1/\sqrt{lA_-P_0}$ pour limite, puis nous extrairons une sous-suite convergeant vers $1/\sqrt{lA_-P_0}$.

• On a

$$\begin{aligned}\frac{\phi_D(n)}{n} &= \prod_{\substack{p\mid n\\ p>\ln n}}\left(1-\frac{\varepsilon(p)}{p}\right)\prod_{\substack{p\mid n\\ p\le\ln n}}\left(1-\frac{\varepsilon(p)}{p}\right)\\ &\ge \left(1-\frac{1}{\ln n}\right)^{\rho}\prod_{\substack{p\le\ln n\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)\end{aligned}$$

où ρ est le nombre de facteurs premiers de n supérieurs à $\ln n$. Mais puisque nous avons $\rho \le \ln(n)/\ln\ln(n)$ (cf. la démonstration de 3.2), nous obtenons :

$$\frac{\phi_D(n)}{n}e^{\gamma/2}\sqrt{\ln\ln n} \ge e^{\gamma/2}\sqrt{\ln\ln n}\prod_{\substack{p\le\ln n\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}.$$

D'après 2.2, le dernier facteur de cette majoration tend vers 1 et, d'après 5.1, le facteur restant tend vers $1/\sqrt{lA_-P_0}$. Le tout converge donc vers $1/\sqrt{lA_-P_0}$, ce qui termine la démonstration du premier point.

• Posons

$$n_k^+ = \prod_{\substack{p\le k\\ \varepsilon(p)=1}} p$$

de telle sorte que $\ln n_k^+ = \theta^+(k)$. On a

$$\frac{\phi_D(n_k^+)}{n_k^+} = \prod_{p|n_k^+}\left(1-\frac{1}{p}\right) = \prod_{\substack{p\le k\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right).$$

Donc, d'après 5.1,

$$\begin{aligned}\frac{\phi_D(n_k^+)}{n_k^+}e^{\gamma/2}\sqrt{\ln\ln n_k^+} &= \frac{\phi_D(n_k^+)}{n_k^+}e^{\gamma/2}\sqrt{\ln k}\sqrt{\frac{\ln\theta^+(k)}{\ln k}}\\ &= \prod_{\substack{p\le k\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)e^{\gamma/2}\sqrt{\ln k}\sqrt{\frac{\ln\theta^+(k)}{\ln k}}\\ &\sim \frac{1}{\sqrt{lA_-P_0}}\end{aligned}$$

puisque

$$\begin{cases}\theta^+(x)\sim x/2\\ \lim\limits_{+\infty} x = +\infty\end{cases} \Longrightarrow \ln\theta^+(x)\sim \ln\frac{x}{2}\sim \ln x.$$

Ainsi s'achève la démonstration du deuxième point. □

Démonstration du théorème 6.2

• Par les mêmes méthodes, nous obtenons

$$\frac{\phi_D(n)e^{-\gamma/2}}{n\sqrt{\ln\ln n}} \le \frac{e^{-\gamma/2}}{\sqrt{\ln\ln n}}\prod_{\substack{p\le \ln n\\ \varepsilon(p)=-1}}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}.$$

D'après 2.2 et 5.1, le membre de droite converge vers $\sqrt{\frac{A_-P_0}{l}}$.

• En posant

$$n_k^- = \prod_{\substack{p\le k\\ \varepsilon(p)=-1}} p,$$

le second point de la démonstration est semblable à celui du théorème précédent ; il suffit de considérer cette fois-ci la sous-suite

$$\frac{\phi_D(n_k^-)e^{-\gamma/2}}{n_k^-\sqrt{\ln\ln n_k^-}}$$

et de montrer qu'elle est équivalente à $Q_-(k)e^{-\gamma/2}/\sqrt{\ln k}$ et donc qu'elle converge vers $\sqrt{\frac{A_-P_0}{l}}$. □

7. Bibliographie

[1] G.H. Hardy, E.M. Wright : *An Introduction to the Theory of Numbers.* Clarendon Press, 1960–1979 (5th edition).

[2] P. Ribenboim : *The Book of Prime Number Records.* Springer-Verlag, 1988.

[3] G. Robin : *Grandes valeurs de la fonction somme des diviseurs et Hypothèse de Riemann.* Journal de Mathématiques Pures et Appliquées, vol. 63, 1984, pp. 187–213.

[4] G. Robin : *Grandes valeurs de la fonction somme des diviseurs dans les progressions arithmétiques.* Journal de Mathématiques Pures et Appliquées, vol. 66, 1987, pp. 337–349.

[5] A. Selberg : *An elementary proof of the prime-number theorem for arithmetical progressions.* Canadian Journal of Mathematics, vol. 2, 1950, pp. 66–78.

[6] S. Uchiyama : *On some products involving primes.* Proceedings of the American Mathematical Society, vol. 28, 1971, pp. 629–630.

Chapitre 6

Nombres de Carmichael fortement pseudo-premiers, pseudo-premiers forts de Lucas, dans plusieurs bases

Ce chapitre décrit une méthode pour construire des nombres de Carmichael, fortement pseudo-premiers dans plusieurs bases choisies à l'avance, ainsi que des pseudo-premiers forts de Lucas pour plusieurs couples de paramètres. Nous l'appliquons pour trouver des nombres composés, différents de ceux produits par la méthode décrite dans le chapitre 3, passant le test de Rabin, tel qu'il est implémenté dans les systèmes de calcul formel `Maple V.2` et `Axiom 1.1`.

1. Motivations

Il y a principalement deux raisons qui ont motivé la recherche de cette méthode. La première est due à une remarque de François Morain : amusé par les nombres qui déjouaient le test de `ScratchPad`, il se rendit compte que ces nombres ne passaient pas le test de `Maple`. En effet, celui-ci contient une ligne de code supplémentaire (voir section 5) qui interceptait les nombres construits par la méthode du chapitre 3. Il me demanda alors si je pouvais relever ce nouveau défi. La deuxième raison est que le système `ScratchPad` a évolué : soucieux de contrer les attaques portées à l'intégrité de son test de primalité, les concepteurs de la nouvelle version `Axiom` ont cherché à le rendre invulnérable. Pour cela, J. Davenport [5] a ajouté des contrôles spécifiques qui interceptaient les nombres embarrassants en concluant ensuite : *we do not believe we can break [the Axiom test] by the technology we know*. Ce fût pour moi l'occasion de me piquer de nouveau au jeu...

Les améliorations de Davenport

Expliquons les différentes raisons qui font que les nombres produits par la méthode du chapitre 3 ne passent pas le test d'`Axiom`.

• Premièrement, le jeu de bases de pseudo-primalité utilisé a changé. Il est maintenant l'ensemble des dix premiers nombres premiers impairs 3, 5, 7, 11, 13, 17, 19, 23, 29 et 31. Cette modification est mineure et ne contre pas la méthode du chapitre 3. (L'exemple qui y est donné n'est-il pas fortement pseudo-premier de base 31 ?)

• Deuxièmement, le test de pseudo-primalité forte en base b d'un entier $n = 2^k q + 1$ s'effectue par le calcul de b^q modulo n suivi d'un certain nombre (parfois nul) d'élévation au carré modulo n qui, si le test se termine avec succès, conduit à la valeur -1. Donc, et

sauf si $b^q \equiv \pm 1$ modulo n, il apparaît une racine carrée de -1 modulo n au cours du calcul. L'idée de Davenport est alors la suivante : mémoriser et compter les différentes racines carrées de -1 obtenues au cours des tests de pseudo-primalité forte dans les différentes bases. Si plus de deux telles racines sont obtenues, alors le nombre testé est composé. Cette modification est une réelle amélioration et le fait que l'on obtienne les trois racines carrées de -1 suivantes

$$\left[\begin{array}{l} 46756643159547032300809487344996896 0154154806 \\ 92625030448501505070536859539001071 1599278545 \\ 26881846431025074181299272033510564 0298967036, \end{array}\right.$$

lors du test de l'exemple (4) du chapitre 3 en est une illustration.

• Troisièmement, les nombres produits par la méthode du chapitre 3 sont tous de la forme $n = (u+1)(2u+1)$ avec $u \in \mathbb{N}$. Il en résulte que

$$8n + 1 = 8(u+1)(2u+1) + 1 = (4u+3)^2.$$

c'est pourquoi, pour chaque entier n qui a passé les tests de pseudo-primalité forte, `Axiom` vérifie que $8n+1$ n'est pas un carré parfait avant de le déclarer premier.

Une quatrième modification a été apportée. Elle n'est d'aucune utilité pour intercepter les nombres du chapitre 3 mais est efficace (ainsi que la deuxième et une variante de la troisième) pour contrer celui exhibé par Jaeschke [6] :

$$J = 5689719352694202437032697 2321 = 137716125329053 \cdot 413148375987157.$$

Elle consiste à repérer les candidats n vérifiant

$$b^{(n-1)/2} \equiv 1 \text{ modulo } n$$

pour chacune des dix bases b utilisées. Ces nombres sont considérés comme suspects par `Axiom` et sont testés avec des bases supplémentaires jusqu'à ce que l'on ait trouvé un b tel que $b^{(n-1)/2} \equiv -1$ modulo n ou bien qu'ils se révèlent composés. De plus, des bases supplémentaires sont aussi utilisées pour les entiers dépassant une certaine limite (10^{20}). Le nombre de bases utilisées est alors proportionnel à la taille (le nombre de chiffres) de l'entier testé. Notons que, puisque le nombre de bases utilisées n'est plus fixe, la complexité du test n'est plus en $\log^3 n$ mais en $\log^4 n$. Notons aussi que les nombres qui vérifient, comme ceux décrits par 3.1.3,

$$b^{(n-1)/2} \equiv -1 \text{ modulo } n$$

pour chacune des dix bases, ne sont pas considérés comme suspects...

2. Préliminaires

Dans tout ce chapitre, le nombre n désigne un produit de facteurs premiers impairs $p_1 p_2 \cdots p_h$ avec h **impair** supérieur ou égal à 3 et $p_1 < p_2 < \cdots < p_h$. De plus, on pose $\varepsilon = \pm 1$ et

$$k_i = \frac{p_i - \varepsilon}{p_1 - \varepsilon} \quad \text{et} \quad m_i = \frac{\prod_{j \neq i} p_j - 1}{p_i - \varepsilon}, \qquad \text{pour } 1 \leq i \leq h. \tag{1}$$

Commençons par rappeler deux lemmes simples. Pour $s \in \mathbb{N}^*$, on note $v_2(s)$ le plus grand entier t tel que $2^t \mid s$:

2.1. — **Lemme.** *Si les coefficients k_i sont des entiers, ils sont tous impairs si et seulement si on a*

$$v_2(p_1-\varepsilon)=v_2(p_2-\varepsilon)=\cdots=v_2(p_h-\varepsilon)=v_2(n-\varepsilon).$$

DÉMONSTRATION — Posons $v=v_2(p_1-\varepsilon)$. Il est clair que $v_2(p_i-\varepsilon)=v$ si et seulement si k_i est impair. Si c'est le cas pour tout i, on a $p_i\equiv 2^v+\varepsilon$ modulo 2^{v+1}. D'où, puisque h est impair,

$$n\equiv(2^v+\varepsilon)^h\equiv 2^v+\varepsilon \text{ modulo } 2^{v+1}$$

c'est-à-dire $v_2(n-\varepsilon)=v$. □

2.2. — **Lemme.** *On a les implications suivantes :*

$$p_i-\varepsilon \text{ divise } n-\varepsilon \iff m_i \text{ est entier,}$$
$$k_i \text{ est entier pour tout } i \implies m_1 \text{ est entier.}$$

DÉMONSTRATION — Les deux membres de la première affirmation s'écrivent respectivement

$$n\equiv\varepsilon \text{ modulo } (p_i-\varepsilon) \quad\text{et}\quad \prod_{j\neq i}p_j\equiv 1 \text{ modulo } (p_i-\varepsilon)$$

leur équivalence résulte de la congruence triviale $p_i\equiv\varepsilon$ modulo $(p_i-\varepsilon)$. De même, la deuxième affirmation est claire si l'on écrit le membre de gauche sous la forme $p_i\equiv\varepsilon$ modulo $(p_1-\varepsilon)$. □

2.3. — **Remarque.** Les formules $p_j=k_j(p_1-\varepsilon)+\varepsilon$ montrent que les coefficients k_i et m_i vérifient une relation du type $k_im_i=f_i(p_1)$ où $f_i(X)$ est le polynôme

$$f_i(X)=\frac{\prod_{j\neq i}\big(k_i(X-\varepsilon)+\varepsilon\big)-1}{X-\varepsilon}.$$

Par exemple, pour $h=3$, les égalités $p_1p_j-1=p_1(p_j-\varepsilon)+\varepsilon(p_1-\varepsilon)$ permettent d'écrire les relations

$$f_2(X)=k_3X+\varepsilon \qquad\text{et}\qquad f_3(X)=k_2X+\varepsilon.$$

La condition "m_i est entier" s'écrit alors sous la forme "p_1 est une racine de f_i modulo k_i".

3. Nombres de Carmichael fortement pseudo-premiers

Nombres de Carmichael

Dans cette section et les deux suivantes, on impose $\varepsilon=1$. Rappelons qu'un entier composé positif n est un nombre de Carmichael (définition 1.1.3) s'il vérifie

$$b^{n-1}\equiv 1 \text{ modulo } n \qquad \text{pour tout entier } b \text{ premier avec } n.$$

Il est bien connu (voir [8] ou [9]) qu'un entier n est de Carmichael si et seulement s'il est sans facteurs carrés et si l'on a $p-1\mid n-1$ pour tout facteur premier p de n. Avec les notations de la section 2, cela signifie que n est un nombre de Carmichael si et seulement si p_i-1 divise $n-1$ pour tout i tel que $1\leq i\leq h$ c'est-à-dire, d'après le lemme 2.2, si et seulement si les m_i sont entiers. Nous utiliserons plus précisément le lemme 2.2 sous la forme :

3.1. — **Lemme.** *Si les nombres k_i et m_i sont des entiers pour tout i tel que $2 \leq i \leq h$ alors n est de Carmichael.* □

Remarque. Dans le lemme précédent, le fait que les coefficients m_i soient entiers est nécessaire pour que n soit de Carmichael. Par contre, il n'est pas nécessaire que les coefficients k_i le soient. Par exemple, $6601 = 7 \cdot 23 \cdot 41$ est de Carmichael.

Pseudo-primalité forte

Supposons que $n = p_1 p_2 \cdots p_h$ soit un nombre de Carmichael et soit b un entier premier avec n. Ce dernier est pseudo-premier de base b. Nous allons déterminer des conditions suffisantes pour que n soit fortement pseudo-premier de base b.

3.2. — **Lemme.** *Supposons que les coefficients k_i et m_i définis dans la section 2 soient des entiers (donc que $n = p_1 p_2 \cdots p_h$ soit un entier de Carmichael) et que les k_i soient impairs. Soit b un entier premier avec n. Pour que n soit fortement pseudo-premier de base b (définition 1.1.5), il suffit que les relations suivantes soient vérifiées :*

$$\left(\frac{b}{p_i}\right) = -1 \qquad \text{pour tout } i \text{ tel que } 1 \leq i \leq h. \tag{2}$$

Démonstration — D'après le lemme 2.1, le quotient $(n-1)/(p_i - 1)$ est impair pour tout i. Donc, puisque $b^{(p_i-1)/2} \equiv \pm 1$ modulo p_i, on a

$$b^{\frac{n-1}{2}} \equiv b^{\frac{p_i-1}{2}} \equiv \left(\frac{b}{p_i}\right) \qquad \text{modulo } p_i \qquad \text{pour } 1 \leq i \leq h.$$

Ainsi, les conditions du lemme impliquent $b^{(n-1)/2} \equiv -1$ modulo n, ce qui est suffisant pour que n soit fortement pseudo-premier de base b. □

Si b est premier, la loi de réciprocité quadratique permet alors de déterminer une partie NS_b de $\mathbb{Z}/4b\mathbb{Z}$ telle que, pour p premier, on ait l'équivalence

$$\left(\frac{b}{p}\right) = -1 \iff [p]_{4b} \in NS_b.$$

ainsi, en utilisant les égalités (1), les conditions (2) s'écrivent

$$[k_i(p_1 - 1) + 1]_{4b} \in NS_b \qquad \text{pour tout } i \text{ tel que } 1 \leq i \leq h$$

ou bien, si les coefficients k_i sont inversibles modulo b,

$$[p_1]_{4b} \in \bigcap_{i=1}^{h} k_i^{-1}(NS_b + k_i - 1). \tag{3}$$

4. Théorèmes d'extension

Nombres de Carmichael

Le "Théorème d'extension" de Chernick [4] peut s'énoncer ainsi :

4.1. — Théorème (Chernick). *Soit $c = p_1 p_2 \cdots p_s$ un nombre de Carmichael et posons*

$$\Lambda = \lambda(c) = \operatorname*{ppcm}_{1 \le i \le s}(p_i - 1).$$

Si p_{s+1} est un nombre premier ne divisant pas c et tel que

$$\Lambda \mid p_{s+1} - 1 \mid c - 1, \tag{4}$$

alors le nombre $c' = cp_{s+1}$ est aussi un nombre de Carmichael.

Démonstration — Il s'agit de montrer que $c' \equiv 1$ modulo $p_i - 1$ pour $1 \le i \le s+1$. Pour $i \le s$, on a les relations $c \equiv 1$ modulo $p_i - 1$ puisque c est de Carmichael. D'après (4), on a aussi $p_{s+1} \equiv 1$ modulo $p_i - 1$ d'où la relation cherchée. Pour $i = s+1$, cela résulte de la deuxième partie de (4) et de la relation triviale $p_{s+1} \equiv 1$ modulo $p_{s+1} - 1$. □

Extension de nombres fortement pseudo-premiers

La méthode décrite dans ce chapitre permet de produire des leurres au test de Rabin, composés d'un nombre impair de facteurs premiers. Le théorème suivant permet d'en déduire des nombres analogues mais ayant un nombre pair de facteurs premiers.

4.2. — Théorème. *Avec les notations de la section 2 (pour $\varepsilon = 1$), supposons que les hypothèses et conditions du lemme 3.2 soient vérifiées. Posons*

$$\Lambda = \lambda(n) = \operatorname*{ppcm}_{1 \le i \le h}(p_i - 1).$$

Si p_{h+1} est un nombre premier ne divisant pas n vérifiant

$$\Lambda \mid p_{h+1} - 1 \mid n - 1, \tag{5}$$

et tel que $(b/p_{h+1}) = -1$, alors le nombre $n' = np_{h+1}$ est aussi un nombre de Carmichael fortement pseudo-premier de base b.

Démonstration — La première affirmation résulte de 4.1. Démontrons la deuxième. Toujours d'après 4.1, le nombre $n' - 1$ est divisible par $p_1 - 1$. Il existe donc un entier $t > 0$ tel que

$$\frac{(n'-1)/2^t}{(p_1-1)/2}$$

soit un entier impair. Nous allons montrer que $b^{(n'-1)/2^t} \equiv -1$ modulo n' ce qui montrera que n' est fortement pseudo-premier de base b. Puisque l'on a $b^{(p_i-1)/2} \equiv -1$ modulo p_i pour $1 \le i \le h+1$, il suffit de montrer que

$$\frac{(n'-1)/2^t}{(p_i-1)/2}$$

est un entier impair, pour tout i. C'est bien un entier d'après 4.1. Pour montrer qu'il est impair, il suffit de prouver que $v_2(p_i - 1) = v_2(p_1 - 1)$. Pour $i \le h$ cela résulte du fait que les coefficients k_i soient impairs. Pour $i = h+1$, notons que 2.1 montre que $v_2(\Lambda) = v_2(n-1)$. Donc, d'après (5), on a bien $v_2(p_{h+1} - 1) = v_2(p_1 - 1)$ ce qui termine la démonstration. □

5. Application aux tests de primalité de Maple et d'Axiom

Le test de Maple

Le test de primalité de `Maple V.2` fonctionne en trois étapes. Dans la première, il vérifie que l'entier n passé en paramètre n'admet pas de diviseur propre inférieur à 1000. La seconde est un test de Rabin proprement dit : il vérifie si le paramètre est fortement pseudo-premier dans les bases 2, 3, 5, 7, 11 (si on le demande explicitement, il fait cette vérification pour plus de bases). Enfin, dans la troisième, il vérifie que n n'est pas de la forme

$$(u+1)(k\frac{u}{2}+1) \quad \text{avec } 3 \leq k \leq 9$$

ou

$$(u+1)(ku+1) \quad \text{avec } 5 \leq k \leq 20.$$

Cette troisième étape est probablement motivée par [9], qui fournit trois exemples de nombres de cette forme fortement pseudo-premiers dans quatre de ces cinq bases. Dans le code de `Maple`, on trouve aussi le commentaire suivant : *Presently there are no composite numbers known to us that will make* `isprime()` *return true.*

Et pourtant, il est facile de vérifier que, pour $h = 3$, $k_2 = 13$ et $k_3 = 41$, le membre de droite de (3) est non vide pour chacune des cinq bases qu'utilise `Maple` : par exemple, la condition (3) est vérifiée dès que p_1 vérifie les congruences de la table 1.

pour $b = 2$:	$p_1 \equiv 3$	(mod 8)
pour $b = 3$:	$p_1 \equiv 7$	(mod 12)
pour $b = 5$:	$p_1 \equiv 3$	(mod 20)
pour $b = 7$:	$p_1 \equiv 15$	(mod 28)
pour $b = 11$:	$p_1 \equiv 23$	(mod 44)

Table 1

De plus, les égalités $p_1 p_i - 1 = p_1(p_i - 1) + (p_1 - 1)$ (pour $i = 2, 3$) permettent d'exprimer les coefficients m_i sous la forme (voir la remarque 2.3) :

$$m_2 = \frac{k_3 p_1 + 1}{k_2} \qquad \text{et} \qquad m_3 = \frac{k_2 p_1 + 1}{k_3}.$$

Ce sont des entiers dès que

$$p_1 \equiv \begin{cases} -k_3^{-1} = 6 & \text{modulo } 13 \\ -k_2^{-1} = 22 & \text{modulo } 41. \end{cases}$$

Par l'algorithme d'Euclide étendu, on calcule que ces deux congruences et celles de la table 1 sont ensemble équivalentes à l'unique congruence suivante :

$$p_1 \equiv 827443 \text{ modulo } 4924920. \tag{6}$$

d'où le lemme :

5.1. — Lemme. *Soit p_1 un nombre premier vérifiant la congruence (6) et tel que $p_2 = 13(p_1-1)+1$ et $p_3 = 41(p_1-1)+1$ soient premiers. Alors, le nombre $p_1p_2p_3$ est un Carmichael fortement pseudo-premier dans les bases 2, 3, 5, 7 et 11.* □

Il ne reste alors plus qu'à trouver un entier p_1 vérifiant les conditions de ce lemme. Le nombre 286472803 convient et fournit l'entier 3-composé suivant :

$$125307596077844960105845739 23 = 286472803 \cdot 3724146427 \cdot 11745384883$$

qui passe le test de `Maple`.

Extensions

Continuons avec le même exemple. Il existe deux nombres premiers vérifiant les conditions du théorème 4.2, à savoir

$$152690003467 \qquad \text{et} \qquad 5576391616581787.$$

Voici donc deux nombres 4-composés qui passent le test de `Maple` :

$$\begin{aligned} &19133217279567582560450062609995877910 41 \\ &\qquad = 286472803 \cdot 3724146427 \cdot 11745384883 \cdot 152690003467, \\ &69876422826251144928143383863659397076940401 \\ &\qquad = 286472803 \cdot 3724146427 \cdot 11745384883 \cdot 5576391616581787. \end{aligned}$$

Le test de Maple (bis)

Donnons un autre exemple avec, cette fois-ci, $h = 5$. Choisissons les coefficients k_i tels que les deux conditions suivantes soient vérifiées :

• Le membre de droite de (3) est non vide pour chacune des 5 bases qu'utilise `Maple`. Les valeurs 13, 41, 53 et 101 feront l'affaire pour les coefficients respectifs k_2, k_3, k_4 et k_5 et les conditions de la table 1 seront à nouveau suffisantes pour que (3) soit vérifiée.

• Les polynômes $f_i(X) \in \mathbb{Z}[X]$ définis par

$$f_i(X) = \frac{\prod_{j\neq i}\big(k_i(X-1)+1\big)-1}{X-1}$$

ont une racine modulo k_i. Pour les valeurs des k_i annoncées ci-dessus, les polynômes f_i admettront p_1 pour racine modulo k_i dès que les conditions suivantes seront vérifiées :

$$p_1 \equiv \begin{cases} 4 \text{ modulo } 13 \\ 21 \text{ modulo } 41 \\ 41 \text{ modulo } 53 \\ 54 \text{ modulo } 101. \end{cases}$$

A nouveau, l'algorithme d'Euclide étendu permet de rassembler les conditions de la table 1 et les quatre ci-dessus sous la forme

$$p_1 \equiv 14354973403 \text{ modulo } 26363096760 \tag{7}$$

ce qui permet d'énoncer le lemme suivant :

5.2. — **Lemme.** *Soit p_1 un nombre premier vérifiant la congruence (7) et tel que $p_2 = 13(p_1-1)+1$, $p_3 = 41(p_1-1)+1$, $p_4 = 53(p_1-1)+1$ et $p_5 = 101(p_1-1)+1$ soient premiers. Alors, le nombre $p_1p_2p_3p_4p_5$ est un Carmichael fortement pseudo-premier dans les bases 2, 3, 5, 7 et 11.* □

Un court programme informatique permet alors de trouver un entier p_1 vérifiant les conditions de ce lemme. Par exemple, le nombre

$$p_1 = 343367327175643$$

fournit l'entier 5-composé suivant :

$$n = 136181869469132489020293365852256182377286394691192846117390651100308384927201 63$$

qui passe le test de `Maple`.

Contributions extérieures

Cette méthode a déjà été exposée dans [1] et plusieurs personnes l'ont appliquée. En particulier, je dois à Daniel Bleichenbacher* le bel exemple suivant :

$$A = 52082187873997051$$
$$B = 68961718847249643841965 1$$
$$C = 879099819460496703982467331516772068063782239 1001$$
$$D = 116401090397683563810044154832907018469916261377041583601.$$

Les quatre nombres ci-dessus sont tous déclarés premiers par `Maple`, et pourtant, il est facile de vérifier que $AD = BC$, contredisant le théorème 0.0.1 !

Le test d'Axiom

Malgré les améliorations du test d'`Axiom` décrites dans la section 1, nous avons appliqué la méthode décrite ci-dessus. Nous avons remarqué qu'avec les valeurs $h = 3$, $k_2 = 37$ et $k_3 = 41$, le membre de droite de (3) est non vide pour chacune des dix bases qu'utilise `Axiom`. La condition (3) est en particulier vérifiée dès que p_1 vérifie les congruences de la table 2.

De plus, d'après la remarque 2.3, les coefficients m_2 et m_3 sont entiers dès que l'on a

$$p_1 \equiv \begin{cases} 9 \text{ modulo } 37 \\ 31 \text{ modulo } 41. \end{cases}$$

Les douze congruences ainsi obtenues sont équivalentes à

$$p_1 \equiv 356794315112467 \quad \text{modulo } 608500527054420.$$

* Departement Informatik, Swiss Federal Institute of Technology (ETH), Zurich.

pour $b = 3$:	$p_1 \equiv 7$	(mod 12)
pour $b = 5$:	$p_1 \equiv 7$	(mod 20)
pour $b = 7$:	$p_1 \equiv 15$	(mod 28)
pour $b = 11$:	$p_1 \equiv 23$	(mod 44)
pour $b = 13$:	$p_1 \equiv 11$	(mod 52)
pour $b = 17$:	$p_1 \equiv 11$	(mod 68)
pour $b = 19$:	$p_1 \equiv 39$	(mod 76)
pour $b = 23$:	$p_1 \equiv 39$	(mod 92)
pour $b = 29$:	$p_1 \equiv 43$	(mod 116)
pour $b = 31$:	$p_1 \equiv 63$	(mod 124)

Table 2

Le nombre $p_1 = 220633985108812507$ vérifie cette relation et, puisque p_1, $p_2 = 37(p_1-1)+1$ et $p_3 = 41(p_1 - 1) + 1$ sont premiers, le produit des trois

$$n = 162930656995886348108319337637811414987504506600788230 67$$

est fortement pseudo-premier dans les dix bases testées par `Axiom`.

De plus, cette méthode déjoue aussi les raffinements apportés au test par J. Davenport et ce nombre passe le test d'`Axiom` (ainsi que le test de `Maple` puisque l'ensemble des bases utilisées par `Maple` est contenu dans celui des bases utilisées par `Axiom`).

6. Construire des pseudo-premiers de Lucas

On se propose de construire de **vrais** (je veux dire tels que $\varepsilon(n) = -1$) nombres fortement pseudo-premiers de Lucas pour des paramètres P et Q fixés. Nous utiliserons les notations du chapitre 4 sur les suites de Lucas (section 4.1), ainsi que les notations et lemmes de la section 2 en imposant l'égalité $\varepsilon = -1$. En particulier, le lemme 2.2 s'interprète de la manière suivante :

Pseudo-primalité

6.1. — Lemme. *Soit $D = P^2 - 4Q$ et $h \geq 3$ un entier impair. Avec les notations de la section 2, supposons que $\varepsilon = -1$, que les coefficients k_i et m_i soient entiers et que l'on ait les relations*

$$\left(\frac{D}{p_i}\right) = -1 \qquad \textit{pour tout } i \textit{ vérifiant } 1 \leq i \leq h,$$

alors n est pseudo-premier de Lucas de paramètres P et Q.

Démonstration — D'après le lemme 2.2, les quotients $(n+1)/(p_i+1)$ sont des entiers pour tout i. Désignons, comme dans le chapitre 4, par τ le quotient modulo n des deux racines du polynôme $X^2 - PX + Q$. Le théorème 4.1.1 indique que $\tau^{p_i+1} \equiv 1$ modulo p_i

et donc que $\tau^{n+1} \equiv 1$ modulo p_i. Ainsi, pour tout i, l'entier p_i divise U_{n+1} ; il en est donc de même de n. De plus, puisque h est impair, on a

$$\left(\frac{D}{n}\right) = \prod_{i=1}^{h} \left(\frac{D}{p_i}\right) = -1$$

ce qui termine la démonstration. □

Pseudo-primalité forte

6.2. — **Lemme.** *Si, en plus des hypothèses du lemme précédent, on suppose que les k_i sont impairs et que*

$$\left(\frac{Q}{p_i}\right) = -1 \qquad \textit{pour tout } i \textit{ vérifiant } 1 \leq i \leq h,$$

alors n est fortement pseudo-premier de Lucas de paramètres P et Q.

Démonstration — Notons tout d'abord qu'il suffit de montrer que l'on a la relation

$$n \mid V_{(n-1)/2}.$$

Or, par hypothèse, on a $Q^{(p_i-1)/2} \equiv -1$ modulo n et donc

$$Q^{(p_i+1)/2} \equiv -Q \text{ modulo } p_i \qquad \text{pour } 1 \leq i \leq h.$$

Compte-tenu des relations $\alpha\beta = Q$ et $\beta^{p_i+1} \equiv Q$ modulo p_i, on obtient $(\alpha\beta)^{(p_i+1)/2} \equiv -Q$ modulo p_i d'où

$$(\alpha\beta^{-1})^{(p_i+1)/2} \equiv -Q \text{ modulo } p_i \qquad \text{pour } 1 \leq i \leq h.$$

car p_i ne divise pas $Q = N(\beta)$. Il en résulte que

$$\tau^{(p_i+1)/2} \equiv -1 \text{ modulo } p_i \qquad \text{pour } 1 \leq i \leq h.$$

Comme k_i est impair, le lemme 2.1 montre que le quotient $(\frac{n+1}{2})/(\frac{p_i+1}{2})$ est impair et donc

$$\tau^{(n+1)/2} \equiv -1 \text{ modulo } p_i.$$

on a ainsi $\tau^{(n+1)/2} \equiv -1$ modulo n, ce qui veut bien dire que n divise $V_{(n+1)/2}$. □

$p_1 \equiv 3$	$(\mathrm{mod}\ 8)$
$p_1 \equiv 11$	$(\mathrm{mod}\ 12)$
$p_1 \equiv 7$	$(\mathrm{mod}\ 20)$
$p_1 \equiv 27$	$(\mathrm{mod}\ 28)$
$p_1 \equiv 43$	$(\mathrm{mod}\ 44)$
$p_1 \equiv 11$	$(\mathrm{mod}\ 52)$
$p_1 \equiv 23$	$(\mathrm{mod}\ 68)$

Table 3

7. Exemple

Nous sommes en mesure de construire facilement des pseudo-premiers forts de Lucas simultanément pour plusieurs jeux des paramètres (P, Q, D) comme, par exemple, les suivants :

$$(1,-1,5),\quad (1,2,-7),\quad (1,-3,13),\quad (1,-4,17),$$
$$(3,-1,13),\quad (3,5,-11),\quad (5,2,17),\quad (5,8,-7).$$

En effet, les conditions sur les symboles de Legendre des lemmes 6.1 et 6.2 sont vérifiées pour tous ces paramètres dès que l'on a

$$\left(\frac{-1}{p_i}\right) = \left(\frac{2}{p_i}\right) = \left(\frac{-3}{p_i}\right) = \left(\frac{5}{p_i}\right) = \left(\frac{-7}{p_i}\right) = \left(\frac{-11}{p_i}\right) = \left(\frac{13}{p_i}\right) = \left(\frac{17}{p_i}\right) = -1$$

pour tout $i = 1, 2, 3$. En choisissant les valeurs $k_2 = 23$ et $k_3 = 31$, les relations ci-dessus sont compatibles et elles sont vérifiées dès que p_1 satisfait les congruences de la table 3.

Afin que les coefficients m_2 et m_3 soient entiers il suffit, d'après la remarque 2.3, que p_1 vérifie

$$p_1 \equiv \begin{cases} 3 \text{ modulo } 23 \\ 27 \text{ modulo } 31. \end{cases}$$

Les sept congruences de la table 3 et les deux ci-dessus sont ensemble équivalentes à

$$p_1 \equiv 375566267 \quad \text{modulo } 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31.$$

Il suffit alors, pour construire un nombre composé fortement pseudo-premier de Lucas pour les huit jeux de paramètres annoncés, de trouver un premier p_1 vérifiant la congruence ci-dessus et tel que $p_2 = 23(p_1 + 1) - 1$ et $p_3 = 31(p_1 + 1) - 1$ soient aussi premiers. Le nombre $p_1 = 7655438867$ convient et fournit l'entier

$$n = 319889369713946602502766595032347$$

qui, en plus d'être pseudo-premier fort de Lucas pour les paramètres annoncés, l'est aussi pour d'autres valeurs (P, Q, D) comme :

$$(1,1,-3),\quad (1,-11,45),\quad (3,1,5),\quad (3,4,-7),\quad (5,9,11),\quad (5,13,-27).$$

8. Problème ouvert

Le nombre 377 est pseudo-premier de Lucas pour les paramètres 1 et -1. Les théorèmes 1.1.2 et 1.3.2 indiquent qu'il existe 16 bases dans lesquelles 377 est pseudo-premier, dont six d'entre elles pour lesquelles ils est fortement pseudo-premier. Il est facile de vérifier que ces six bases sont ± 1, ± 70 et ± 99. De manière symétrique, on découvre que 2047, le plus petit entier fortement pseudo-premier de base 2 est pseudo-premier de Lucas pour de nombreux couples de paramètres comme

$$(25, 155), \quad (71, 1259), \quad (285, 1882), \quad (331, 778), \quad (422, 1021), \quad \ldots$$

(d'après 4.5.2, l'entier 2047 est fortement pseudo-premier de Lucas pour 21 tels couples de discriminant 5). Cela illustre le fait qu'il soit facile de trouver des entiers (fortement) pseudo-premiers simultanément au sens classique et au sens de Lucas si l'on n'exige pas à l'avance la base b ou bien les paramètres P et Q. Par contre, il est en général très difficile de trouver des nombres simultanément pseudo-premiers au sens classique et au sens de Lucas pour des bases et paramètres **choisis à l'avance**. Par exemple, et même si cette difficulté a été signalée dans [9] depuis fort longtemps, nous ne connaissons aucun entier n qui soit fortement pseudo-premier de base 2 et qui soit pseudo-premier de Lucas pour les paramètres $(1, -1, 5)$ avec $(5/n) = -1$. Plus généralement, voici un test probabiliste de complexité $O(\log^3 n)$ décrit dans [2] et que personne n'a su tromper à l'heure actuelle :

Un test probabiliste difficile à tromper

8.1. — **Test de Baillie, Selfridge, Wagstaff.** Soit n un entier à tester, le déclarer premier si et seulement si il passe chacun des points suivants :

• Vérifier que n n'admet pas de facteur propre inférieur à un certaine limite fixe, par exemple 1000.

• Vérifier que n est fortement pseudo-premier de base 2.

• Vérifier que n n'est pas un carré parfait et déterminer un couple d'entiers (P, Q) en suivant l'une ou l'autre des procédures suivantes : prendre pour D le premier entier de la suite 5, -7, 9, -11, 13, ... tel que le symbole de Jacobi (D/n) soit égal à -1, puis poser $P = 1$ et $Q = (1 - D)/4$ (méthode A) ou prendre pour D le premier entier de la suite 5, 9, 13, 17, 21, ... tel que (D/n) soit égal à -1, prendre pour P le plus petit entier impair supérieur à $\sqrt{D}$ et poser $Q = (P^2 - D)/4$ (méthode B).

• Vérifier que n est (fortement) pseudo-premier de Lucas pour les paramètres P et Q.

Argument heuristique

Des raisons qui font que des nombres composés passant ce test soient rares sont esquissées dans [2]. Elles peuvent s'exprimer ainsi : soit $n = p_1 \cdots p_s$ un nombre pseudo-premier de base b et pseudo-premier de Lucas pour les paramètres (P, Q) avec $P^2 - 4Q = D$ et $(D/n) = -1$. Les hypothèses et le petit théorème de Fermat impliquent

$$\begin{cases} b^{\operatorname{pgcd}(n-1, p_i - 1)} = 1 & \text{dans } \mathbb{Z}/n\mathbb{Z} \\ \tau^{\operatorname{pgcd}(n+1, p_i - \varepsilon(p_i))} = 1 & \text{dans } \mathcal{O}/n\mathcal{O} \end{cases} \qquad \text{pour chaque } i$$

où l'on désigne par $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ et par τ l'élément associé au couple (P,Q) par la proposition 4.4.2.

En posant

$$\begin{cases} d_i = \text{pgcd}(n-1, p_i - 1) \\ d'_i = \text{pgcd}(n+1, p_i - \varepsilon(p_i)) \end{cases}$$

on a les équivalences

$$b^{n-1} \equiv 1 \text{ modulo } p_i \iff b \text{ est une puissance } (\tfrac{p_i-1}{d_i})^{\text{ième}} \text{ modulo } p,$$

$$\tau^{n+1} = 1 \quad \text{dans } \mathcal{O}/p_i\mathcal{O} \iff \tau \text{ est une puissance } (\tfrac{p_i-\varepsilon(p_i)}{d'_i})^{\text{ième}} \text{ dans } (\mathcal{O}/p_i\mathcal{O})^\wedge.$$

Heuristiquement, ces relations ont très peu de chances d'êtres vérifiées si les entiers d_i et d'_i sont petits par rapport aux ordres des groupes $(\mathbb{Z}/p_i\mathbb{Z})^*$ et $(\mathcal{O}/p_i\mathcal{O})^\wedge$. Cela est confirmé par l'expérience puisque, pour tous les pseudo-premiers connus, les rapports $(p_i-1)/d_i$ sont toujours très petits et même souvent égaux à 1.

Or il est clair, pour $\varepsilon(p_i) = 1$, que l'on a la majoration

$$d_i d'_i = \text{pgcd}(n-1, p_i - 1)\,\text{pgcd}(n+1, p_i - 1) \leq 2(p_i - 1)$$

et donc que les deux pgcds ne peuvent tous deux être grands. (Rectifions une erreur rencontrée dans [2] : on y affirme que l'un au moins de ces pgcds est nécessairement inférieur à 2. Mais cela est contredit par l'exemple $n = 589$, $p = 31$ où ces deux pgcds valent respectivement 6 et 10).

Dans le cas $\varepsilon(p_i) = -1$, on a

$$\begin{cases} \text{pgcd}(n-1, p_i - 1) = \text{pgcd}(n-1, m_i - 1) \\ \text{pgcd}(n+1, p_i + 1) = \text{pgcd}(n+1, m_i - 1) \end{cases}$$

en posant $n = p_i m_i$. On en déduit comme précédemment que

$$d_i d'_i = \text{pgcd}(n-1, p_i - 1)\,\text{pgcd}(n+1, p_i + 1) \leq 2(m_i - 1)$$

ce qui laisse peu d'espoirs d'avoir de grands pgcds, en tout cas pour tous les facteurs premiers p_i de n.

9. Bibliographie

[1] F. Arnault : *Carmichaels fortement pseudo-premiers, pseudo-premiers de Lucas.* Département de mathématiques de l'Université de Poitiers, prépublication n° 73, janvier 1993.

[2] R. Baillie, S. Wagstaff Jr : *Lucas pseudoprimes.* Mathematics of Computation, vol. 35, n° 152, oct. 1980, pp. 1391–1417.

[3] B. Char, K. Geddes, G. Gonnet, B. Leong, M. Monagan, S. Watt : *Maple V Library Reference Manual.* Springer-Verlag and Waterloo Maple Publishing, 1991.

[4] J. Chernick : *On Fermat's simple theorem.* Bulletin of the Americal Mathematical Society, vol. 45, Avril 1939, pp. 269–274.

[5] J.H. Davenport : *Primality Testing Revisited.* Proceedings of ISSAC'92, publié par P.S. Wang, ACM, New-York 1992. Version révisée : Axiom Technical Report n° 6, NAG 1993.

[6] G. Jaeschke : *On strong pseudoprimes to several bases.* Mathematics of Computation, à paraître, octobre 1993.

[7] R. Jenks, R. Sutor : *Axiom, The Scientific Computation System.* Springer-Verlag 1992.

[8] A. Korselt : *Problème chinois.* l'Intermédiaire des Mathématiciens 6, 1899, pp. 142–143.

[9] C. Pomerance, J.L. Selfridge, S.S. Wagstaff : *The pseudoprimes to* $25 \cdot 10^9$. Mathematics of Computation, vol. 35, n° 151, 1980, pp. 1003–1026.

Chapitre 7

D'autres tests probabilistes de primalité

Dans ce chapitre, nous donnons un aperçu sur d'autres tests probabilistes de primalité, qui sont diverses généralisations des tests liés aux suites de Lucas. L'intérêt pratique de certains d'entre eux n'est pas toujours évident, mais ils font appel à des concepts variés et posent de nombreuses questions non résolues.

1. Généralisations des suites de Lucas

De nombreux auteurs ont décrit diverses généralisations des suites de Lucas, pouvant mener à de nouveaux tests de primalité et algorithmes de factorisation. Ce fut d'abord le cas de D.H Lehmer [8] (voir aussi [12]) qui eut l'idée de remplacer le paramètre entier P des suites de Lucas, par la racine carrée $\sqrt{R}$ d'un entier, afin que le nouveau discriminant $D = R - 4Q$ puisse prendre des valeurs congrues à 3 modulo 4.

Puis ce fut essentiellement le cas de Williams qui, développant les idées de Lehmer [14], proposa des critères de primalité ne faisant plus intervenir la factorisation de $n-1$ (comme le test de Pépin) ni celle de $n+1$ comme le test de Lucas-Lehmer, mais celle de n^2+1 [16] ou celle de $n^2 \pm n + 1$ [17]. Un excellent exposé de toutes ces méthodes se trouve dans [15].

2. La suite de Perrin

Nous avons vu que le test de primalité de Lucas s'exprime en termes de corps quadratiques. Le test dont il est question ici fait intervenir des suites à récurrence linéaire cubique et, bien sûr, des corps cubiques.

La suite récurrente d'entiers suivante :

$$A_0 = 3, \quad A_1 = 0, \quad A_2 = 2, \qquad A_{n+3} = A_{n+1} + A_n \quad \text{pour tout } n \in \mathbb{N}$$

a été étudiée depuis fort longtemps. Déjà dans [10], Lucas a prouvé que

$$p \mid A_p \qquad \text{pour tout nombre premier } p. \tag{1}$$

L'étude de cette suite est reprise dans [1], [2] et [7] qui en font une analyse particulièrement minutieuse.

La démonstration de la propriété (1) fait intervenir le corps de décomposition du polynôme

$$f(X) = X^3 - X - 1,$$

c'est-à-dire le corps $L = \mathbb{Q}(\alpha, \beta, \gamma)$ engendré par les trois racines α, β et γ de f. Il est facile de montrer par récurrence que les termes de la suite de Perrin s'expriment sous la forme

$$A_n = \alpha^n + \beta^n + \gamma^n. \tag{2}$$

La relation (1) est donc un cas particulier du résultat général suivant :

2.1. — Proposition. *Soit*

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$$

un polynôme unitaire irréductible sur $\mathbb{Q}$ et à coefficients entiers, soient α_i $(1 \leq i \leq d)$ ses racines et soit $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ son corps de décomposition. Considérons la suite ***d'entiers rationnels*** *suivante :*

$$V_n = \alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n \qquad \textit{pour } n \in \mathbb{N}.$$

Alors, on a la relation

$$V_p \equiv V_1 \text{ modulo } p. \tag{3}$$

Démonstration — On a les congruences suivantes dans l'anneau $\mathcal{O}_L$ des entiers de L :

$$\begin{aligned} V_p &= \alpha_1^p + \alpha_2^p + \cdots + \alpha_d^p \\ &\equiv (\alpha_1 + \alpha_2 + \cdots + \alpha_d)^p \text{ modulo } p\mathcal{O}_L \\ &= V_1^p. \end{aligned}$$

On en déduit la congruence $V_p \equiv V_1^p$ modulo p dans $\mathbb{Z}$ puisque $p\mathcal{O}_L \cap \mathbb{Z} = p\mathbb{Z}$. On a donc le résultat, par le petit théorème de Fermat. □

Signatures

La relation (1) peut être utilisée comme test probabiliste de primalité. (Il y a "peu" de nombres composés vérifiant cette relation. Le plus petit d'entre eux est $521^2 = 271441$.) Adams et Shanks ont cherché à renforcer ce test en décrivant des conditions nécessaires, pour que p soit premier, plus restrictives que (1) mais dont la vérification soit d'un coût comparable.

Adams et Shanks se placent dans un cadre un peu plus général que la suite de Perrin, puisqu'ils considèrent le polynôme

$$f(X) = X^3 - sX^2 + rX - 1 \tag{4}$$

ainsi que la suite V, que nous noterons parfois $V(r, s)$ pour éviter toute confusion, définie dans la proposition 2.1. Ils remarquent que la relation de récurrence que vérifie cette suite permet de la prolonger en l'indexant sur les entiers relatifs et non plus seulement sur les entiers naturels (elle est ainsi uniquement déterminée par la relation de récurrence et par les "conditions initiales" $V_{-1} = r$, $V_0 = 3$ et $V_1 = s$). Puis, ils définissent la *signature* d'un entier naturel n comme étant le sextuplet

$$(V_{-n-1}, V_{-n}, V_{-n+1}, V_{n-1}, V_n, V_{n+1}) \qquad \text{modulo } n,$$

et décrivent un algorithme qui permet de calculer cette signature en un temps $O(\log n)$ (il est implémenté en `Maple` dans l'appendice). Le calcul du terme V_n seul serait en fait sensiblement du même coût. Ils utilisent aussi la terminologie suivante : un nombre premier p est dit de type I, Q ou S (pour la suite V) suivant que le nombre de facteurs irréductibles de f modulo p est respectivement 1, 2 ou 3. Ils montrent alors le résultat suivant :

2.2. — Théorème [2, Théorème 6]. *Si p est un nombre premier alors sa signature est de l'un des trois types S, Q ou I suivants, selon le type de p,*

- *Type S :*

$$(s^2 - 2r, s, 3, 3, r, r^2 - 2s).$$

- *Type Q :*

$$(C_1, s, C_2, C_2, r, C_3)$$

où l'on a les relations

$$\begin{gathered}(s^3 - r^3)C_1 \equiv (s^2 - 3r)C_2^2 + s(4r^2 - s^2r - 3s)C_2 + (s^5 - 3s^3r + 6sr^2 - 2r^4) \text{ modulo } p \\ C_2^3 - rsC_2^2 + (r^3 + s^3 - 3rs)C_2 + (r^3 + s^3 - r^2s^2) \equiv 0 \text{ modulo } p \\ (r^3 - s^3)C_3 \equiv (r^2 - 3s)C_2^2 + r(4s^2 - r^2s - 3r)C_2 + (r^5 - 3r^3s + 6rs^2 - 2s^4) \text{ modulo } p.\end{gathered}$$

- *Type I :*

$$(r, s, C_4, C_5, r, s)$$

où C_4 et C_5 sont des racines modulo p distinctes du polynôme

$$X^2 - (rs - 3)X + r^3 + s^3 - 6rs + 9.$$

Déterminer si un premier est de type Q

De plus, il existe un algorithme qui permet de déterminer à l'avance (c'est-à-dire avant de calculer sa signature) le type d'un nombre p, sous réserve qu'il soit premier. En examinant ensuite la signature de p, c'est-à-dire en vérifiant qu'elle est bien de l'un des trois types S, Q ou I et qu'en plus elle est exactement du type indiqué par l'algorithme, on obtient un test probabiliste de primalité puissant. Cet algorithme repose en partie sur le théorème suivant, dû à Stickelberger :

2.3. — Théorème. *Soient K un corps fini de caractéristique $\neq 2$ et f un polynôme de degré n à coefficients dans K et sans facteurs carrés. La parité du nombre ω de facteurs irréductibles de f est donnée par la formule suivante :*

$$\left(\frac{D}{K}\right) = (-1)^{n-\omega}$$

où D désigne le discriminant de f.

Pour prouver ce théorème, démontrons d'abord le lemme suivant :

2.4. — Lemme. *Soient K un corps de caractéristique $\neq 2$ et f un polynôme irréductible de degré n à coefficients dans K et sans facteurs carrés. Soient D le discriminant de f et G son groupe de Galois. Alors D est un carré dans K si et seulement si G est pair (i.e. ne contient que des permutations paires).*

Démonstration — Désignons par $\alpha_1, \alpha_2, \cdots, \alpha_n$ les racines de f dans une extension. Par définition, le discriminant D et égal à δ^2 avec

$$\delta = \prod_{i<j}(\alpha_i - \alpha_j).$$

On voit alors que, si σ est un élément de G, alors $\sigma(\delta) = \varepsilon_\sigma \delta$ où ε_σ désigne la signature de σ. Or, D est un carré de K si et seulement si $\delta \in K$, c'est-à-dire si et seulement si δ est fixé par tout élément de G. □

Revenons à la démonstration de 2.3. Le lemme ci-dessus règle le cas où $\omega = 1$ puisque, le corps K étant fini, le groupe G est engendré par un cycle de longueur n. Pour le cas général, faisons une récurrence sur n. Pour $n = 1$ le théorème est trivial. Pour $n > 1$, on peut supposer $\omega > 1$ et donc écrire $f = f_1 f_2$ avec f_1 et f_2 non constants. Quitte à renuméroter les α_i, on peut supposer que α_i est racine de f_1 pour $i \leq m$ et de f_2 pour $i > m$. Le théorème résulte alors de la formule (où chaque produit est un élément de K)

$$\operatorname{disc} f_1 f_2 = \prod_{i<j\leq m} (\alpha_i - \alpha_j)^2 \prod_{m<i<j} (\alpha_i - \alpha_j)^2 \left(\prod_{i\leq m<j} (\alpha_i - \alpha_j) \right)^2$$

qui montre que le discriminant de f est le produit de celui de f_1 par celui de f_2 à un facteur carré près (le carré du résultant de f_1 et f_2). □

Dans le cas de la suite V associée au polynôme (4), le théorème 2.3 indique qu'un nombre premier est de type Q si et seulement si le symbole de Legendre (D/p) est égal à -1, où $D = r^2 s^2 - 4(r^3 + s^3) + 18rs - 27$ est le discriminant de f. Cela s'exprime bien sûr sous la forme d'une congruence modulo D. Par exemple, dans le cas de la suite de Perrin, le nombre premier p est de type Q si et seulement s'il vérifie la congruence :

$$p \equiv 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 \text{ ou } 22 \text{ modulo } 23. \tag{5}$$

Discerner les premiers de type S de ceux de type I

Le résultat suivant est beaucoup plus difficile à montrer. Il se déduit de la théorie des Corps de Classes. Pour en apprendre plus, une bonne référence est [4].

2.5. — Théorème. *Un nombre premier p est de type S pour la suite de Perrin, si et seulement s'il est représenté par la forme quadratique principale de discriminant -23, c'est-à-dire si et seulement si p est de la forme*

$$p = x^2 + xy + 6y^2, \qquad x, y \in \mathbb{Z}.$$

7.2. La suite de Perrin

Un nombre premier p est de type I pour la suite de Perrin si et seulement s'il est de la forme

$$p = 2x^2 \pm xy + 3y^2, \qquad x, y \in \mathbb{Z}.$$

Mais, déterminer qu'un nombre p est de type S ou I, sous réserve qu'il soit premier, en s'aidant du théorème ci-dessus nécessiterait de trouver des entiers b et c tels que $b^2 - 4pc = -23$ et de réduire la forme quadratique $px^2 + bxy + cy^2$. Même si ces opérations peuvent être effectuées de manière efficace, elles sont bien sûr plus coûteuses que la vérification de (5). C'est pourquoi Adams, Shanks, Kurtz et Williams choisissent d'étudier les nombres suivants, qu'ils appellent "admissibles" :

2.6. — Définition. *Un entier n est dit admissible (pour la suite $V(r, s)$) si et seulement s'il a une signature de type Q et vérifie la condition $(D/n) = -1$ (symbole de Jacobi), ou bien s'il a une signature de type S ou I et vérifie la condition $(D/n) = 1$ ou 0.*

Les nombres premiers sont bien sûr admissibles et les auteurs de [1], [2] et [7] ont recherché des nombres composés pour certaines suites $V(r, s)$, en particulier $V(0, -1)$ (suite de Perrin), $V(1, 0)$ et $V(1, -1)$. Ainsi, on note dans [7] qu'il existe seulement 55 composés admissibles pour la suite de Perrin inférieurs à $50 \cdot 10^9$. De plus ceux-ci ont tous une signature de type S.

Composés admissibles connus

En fait, pour chacune des suites $V(0, -1)$, $V(1, 0)$ et $V(1, -1)$, on connaît seulement deux catégories de composés admissibles. La première est celle des *nombres d'Owings généralisés*, qui sont des produits $n = p_1 p_2$ de deux facteurs premiers distincts de type S et tels que $p_1 - 1$ et $p_2 - 1$ soient tous les deux multiples de la période de la suite ($V(r, s)$ modulo n). La seconde est celle des nombres de Carmichael dont les facteurs premiers sont de type S. La table 1 (extraite de [7]) liste quelques composés admissibles pour la suite de Perrin : les plus petits nombres d'Owings généralisés ainsi que les quatre nombres de Carmichael inférieurs à $50 \cdot 10^9$ dont les facteurs premiers sont de type S.

$27\,664\,033 = 3037 \cdot 9109$
$46\,672\,291 = 4831 \cdot 9661$
$102\,690\,901 = 5851 \cdot 17551$
$130\,944\,133 = 6607 \cdot 19819$
$517\,697\,641 = 6311 \cdot 82031$
$7\,045\,248\,121 = 821 \cdot 1231 \cdot 6971$
$7\,279\,379\,941 = 211 \cdot 3571 \cdot 9661$
$24\,306\,384\,961 = 19 \cdot 53 \cdot 79 \cdot 89 \cdot 3433$
$43\,234\,580\,143 = 223 \cdot 5107 \cdot 37963$

Table 1

Construire des composés admissibles

Notons ici que la méthode du chapitre 6 peut être à nouveau utilisée pour construire des composés admissibles pour la suite de Perrin. En suivant les notations de la section 6.2, choisissons comme coefficients k_i des carrés parfaits λ_i^2 et recherchons p_1 sous la forme

$$p_1 = 1 + 23s^2, \qquad (\text{donc } p_i = 1 + 23(\lambda_i s)^2).$$

En vertu de l'égalité

$$(r-s)^2 + (r-s)(2s) + (2s)^2 = r^2 + 23s^2,$$

les p_i ainsi construits seront tous de type S pour la suite de Perrin. De plus, la condition $m_i \in \mathbb{Z}$ (voir lemme 6.2.2 et remarque 6.2.3) se traduit ici, pour $h = 3$,

$$\lambda_2^2 \mid \lambda_3^2 p_1 + 1, \quad \text{et} \quad \lambda_3^2 \mid \lambda_2^2 p_1 + 1.$$

Cela s'écrit aussi

$$\lambda_3^2(1 + 23s^2) \equiv -1 \text{ modulo } \lambda_2^2 \quad \text{et} \quad \lambda_2^2(1 + 23s^2) \equiv -1 \text{ modulo } \lambda_3^2,$$

ou encore, si 23, λ_2 et λ_3 sont premiers entre eux deux à deux,

$$s^2 \equiv -23^{-1}(\lambda_3^{-2} + 1) \text{ modulo } \lambda_2^2 \quad \text{et} \quad s^2 \equiv -23^{-1}(\lambda_2^{-2} + 1) \text{ modulo } \lambda_3^2 \qquad (6)$$

où les inverses s'entendent respectivement modulo λ_2^2 et λ_3^2.

Par exemple, pour $\lambda_2 = 5$ et $\lambda_3 = 7$, la condition (6) s'écrit

$$s \equiv 0 \text{ modulo } 5 \qquad \text{et} \qquad s \equiv 10 \text{ ou } 39 \text{ modulo } 47,$$

soit $s \equiv 10$ ou 235 modulo 245. En quelques secondes de recherche on peut alors trouver les composés admissibles suivants pour la suite de Perrin $V(0,-1)$:

$$\begin{aligned}
&611210799494827143622157668962845250001 && (s = 185700),\\
&373141743260616065311346611881376608825 01 && (s = 368490),\\
&37084507053136415595969665487016930994565 0001 && (s = 1708620),\\
&40460199284950982190920677248460022723048 2501 && (s = 1733610),\\
&48782924589820859949521786537024833396538 2501 && (s = 1788510),\\
&11902251473509289133215577003822909089557 20001 && (s = 2075160),\\
&14787297501525923430380537423090071505160 00001 && (s = 2151600),\\
&29188811386100275433766299794471540665411 82501 && (s = 2409810),\\
&43542546387833952899543971137335961925512 00001 && (s = 2575920),\\
&\vdots
\end{aligned}$$

Si en plus on impose les congruences

$$s \equiv 17 \text{ modulo } 31 \qquad \text{et} \qquad s \equiv 0 \text{ modulo } 44,$$

alors on aura en plus les relations

$$\left(\frac{-31}{p_i}\right) = \left(\frac{-44}{p_i}\right) = 1 \qquad \text{pour } i = 1, 2, 3.$$

Puisque le discriminant du polynôme (4) vaut respectivement -31 et -44 pour les valeurs $(1, 0)$ et $(1, -1)$ du couple (r, s), les p_i ainsi construits seront de type I ou S (mais pas de type Q) pour les suites $V(1, 0)$ et $V(1, -1)$. Puisque, d'après le théorème de densité de Čebotarev, il y a moitié moins de premiers de type S que de type I pour chacune de ces deux suites, on peut s'attendre à ce que la probabilité que p_1, p_2 et p_3 soient tous les trois de type S pour une suite donnée soit de $1/27$. De même la probabilité qu'ils soient tous trois de type S pour les deux suites $V(1, 0)$ et $V(1, -1)$ simultanément doit être de l'ordre de $1/27^2 = 1/729$ ce qui autorise une recherche par cette méthode de nombres composés admissibles simultanément pour les trois suites $V(0, -1)$, $V(1, 0)$ et $V(1, -1)$. C'est ainsi que nous avons pu découvrir pour la première fois un tel nombre :

$$75202994940709997915558585268844281289983659977659967780862576366300872272000 1$$
$$= 838737362199911808348000 1 \cdot 209684340549977952087000001 \cdot 410981307477956786090520001$$

3. Corps de degré quelconque

On note dans [2] que, pour la suite de Perrin V et pour p premier, on a :

$$\begin{cases} V_{p-1} \equiv 3 \\ V_p \equiv 0 \\ V_{p+1} \equiv 2 \end{cases} \quad \text{ou} \quad \begin{cases} V_{p-1} \equiv C_1 \\ V_p \equiv 0 \\ V_{p+1} \equiv -1 \end{cases} \quad \text{ou} \quad \begin{cases} V_{p-1} \equiv C_2 \\ V_p \equiv 0 \\ V_{p+1} \equiv 3C_2^2 - 2 \end{cases} \quad \text{modulo } p$$

où C_2 désigne une racine de f modulo p et C_1 désigne une racine de X^2+3X+8 modulo p. C'est en fait un cas particulier du théorème suivant :

L'approche de Gurak [6]

3.1. — **Théorème.** *Soit f un polynôme unitaire à coefficients entiers, de degré d et irréductible sur $\mathbb{Q}$. Soient α_i $(1 \le i \le d)$ ses racines et soit $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ son corps de décomposition. Soit p un premier et soit $\mathcal{P}$ un premier de L au-dessus de p. Notons σ le symbole d'Artin $(L/\mathbb{Q}/\mathcal{P})$. On a*

$$V_{p+r} \equiv \sum_{i=1}^{d} \sigma(\alpha_i)\alpha_i^r \quad \text{modulo } \mathcal{P} \qquad \textit{pour } r \in \mathbb{Z}. \tag{7}$$

Démonstration — Elle résulte de la définition du symbole d'Artin. □

Dans [6], on appelle pseudo-premier de type σ, où σ est un $\mathbb{Q}$-automorphisme de L, tout entier vérifiant les équations (7) pour $0 \le r < d$. On y définit aussi la généralisation suivante des nombres de Carmichael :

3.2. — Définition. *Avec les définitions du théorème précédent, soit σ un $\mathbb{Q}$-automorphisme de L et soit n un nombre composé, premier avec le discriminant de L. On dit que n est un nombre de L-Carmichael de type σ si et seulement si, pour tout entier β de L premier avec n, on a la relation :*

$$\beta^n \equiv \sigma(\beta) \text{ modulo } \mathcal{N}$$

où $\mathcal{N}$ est un idéal de L tel que $\mathcal{N} \cap \mathbb{Z} = n\mathbb{Z}$.

Bien peu de choses sont connues sur ces notions. Par exemple, on ne sait même pas s'il existe des nombres de L-Carmichael de type σ pour un σ distinct de l'identité.

4. Pseudo-premiers elliptiques

Pour que l'exposé soit plus complet, nous signalons ici l'existence d'un autre type de tests probabilistes : ceux basés sur les courbes elliptiques. Notons toutefois que l'intérêt pratique de ces tests est faible par rapport aux tests de Rabin ou Lucas et que les courbes elliptiques sont d'une bien plus grande utilité quand il s'agit de construire des tests déterministes de primalité (voir [11]) ou des algorithmes de factorisation (voir [9]).

Nous rappelons tout d'abord des définitions et résultats de base sur les courbes elliptiques. Une référence majeure dans ce domaine est [13].

Courbes elliptiques sur un corps

Soit K un corps parfait. Une courbe elliptique sur K est une courbe E du plan projectif $\mathbb{P}_2(K)$ définie par une équation (dite de Weierstrass) de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

et sans points singuliers. Elle admet un unique point "à l'infini", c'est-à-dire sur la droite d'équation $Z = 0$: le point de coordonnées homogènes $(0 : 1 : 0)$. On préfère souvent travailler avec la courbe affine associée qui est l'ensemble des points (x, y) de K^2 vérifiant

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

à laquelle on adjoint le point à l'infini.

Si K est de caractéristique distincte de 2 et 3, ce que nous supposerons désormais, alors un changement de variables permet de mettre l'équation affine sous la forme

$$Y^2 = X^3 + aX + b. \tag{W}$$

On appelle discriminant de E le nombre $\Delta = -16(4a^3 + 27b^2)$ et on vérifie aisément que l'absence de points singuliers est équivalente à la condition $\Delta \neq 0$.

Structure de groupe

L'une des remarquables propriétés des courbes elliptiques est qu'il y existe une structure naturelle de groupe. En effet, si P_1 et P_2 sont deux points d'un courbe elliptique E, alors la droite passant par P_1 et P_2 (la tangente si $P_1 = P_2$) coupe E en un unique autre point P_3 (en comptant chaque point avec sa multiplicité). Fixons un point P_0 de E, on montre qu'il existe une loi de groupe abélien vérifiant

$$P_1 + P_2 + P_3 = P_0$$

pour tout triplet de points P_1, P_2, P_3 comme ci-dessus et que cette loi admet P_0 pour élément neutre. On choisit en général le point à l'infini comme élément neutre et on le note 0. Avec ce choix, l'opposé d'un point (x, y) se calcule facilement, c'est $(x, -y)$. Calculons explicitement la somme $P_3 = (x_3, y_3)$ de deux points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$. Si P_1 ou P_2 est l'élément neutre, cela ne pose pas de problème, ainsi que s'ils sont opposés. Sinon, désignons par m le coefficient directeur de la droite passant par P_1 et P_2 (ou la tangente si $P_1 = P_2$), on a

$$m = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{si } P_1 \neq P_2, \qquad m = \frac{3x_1^2 + a}{2y_1} \quad \text{si } P_1 = P_2.$$

De plus, le changement de variables $x' = x$, $y' = y - mx$ transforme (W) en

$$y'^2 + 2mx'y' = x'^3 - m^2x'^2 + ax' + b.$$

Puisque P_1, P_2 et $-P_3$ sont sur la droite d'équation $y' = 0$, leurs abscisses sont les trois racines du polynôme $x'^3 - m^2x'^2 + ax' + b$. La somme de ces dernières est donc égale à $-m^2$ d'où

$$x_3 = m^2 - x_2 - x_1$$

et finalement,

$$-y_3 = y_1 + m(x_3 - x_1).$$

Endomorphismes et multiplication complexe

Soient K un corps et $\overline{K}$ sa clôture algébrique. Une courbe elliptique sur $\overline{K}$ est dite définie sur K si les coefficients de son équation de Weierstrass appartiennent à K.

Un morphisme (souvent appelé isogénie) d'une courbe elliptique E_1 dans une autre E_2 définies sur K est une application rationnelle :

$$\phi : E_1 \longmapsto E_2$$

telle que $\phi(0) = 0$. C'est un morphisme de groupes. Un endomorphisme d'une courbe elliptique E est un morphisme de E dans E. L'ensemble des endomorphismes de E, noté $\mathrm{End}(E)$ est un anneau pour l'addition et la composition.

Si m est un entier, la multiplication par m est un endomorphisme de E. Ainsi, l'anneau $\mathrm{End}(E)$ est une extension de $\mathbb{Z}$. Supposons que le corps $\overline{K}$ soit celui des nombres complexes $\mathbb{C}$. Si $\mathrm{End}(E)$ contient strictement $\mathbb{Z}$, alors on dit que E est à multiplication complexe. Dans ce cas, on montre que $\mathrm{End}(E)$ est un ordre dans un corps quadratique imaginaire.

Réduction modulo un entier

Soit E une courbe elliptique définie sur $\mathbb{Q}$ et telle que son équation de Weierstrass soit à coefficients entiers. Si p est un nombre premier, cette équation définit une courbe algébrique sur $\mathbb{F}_p$. Elle est appelée la réduction de E modulo p et est parfois notée E_p. C'est aussi une courbe elliptique (i.e. non singulière) si et seulement si le discriminant de E n'est pas divisible par p. Il est connu que le groupe E_p est, soit cyclique, soit le produit de $\mathbb{Z}/2\mathbb{Z}$ par un groupe cyclique.

Si la courbe E est à multiplication complexe par un ordre de $\mathbb{Q}(\sqrt{D})$ et si p est un nombre premier inerte dans $\mathbb{Q}(\sqrt{D})$ alors l'ordre du groupe E_p est $p+1$.

Soit n un entier supérieur ou égal à 2. L'espace projectif $\mathbb{P}_2(\mathbb{Z}/n\mathbb{Z})$ est défini comme étant l'ensemble des triplets $(x,y,z) \in (\mathbb{Z}/n\mathbb{Z})^3$ vérifiant $\mathrm{pgcd}(x,y,z,n) = 1$, quotienté par la relation d'équivalence qui identifie (x,y,z) avec (ux,uy,uz) pour u élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Dans le cas où n est premier, cette définition coïncide avec la définition habituelle. Si l'équation de E est à coefficients entiers et si ces coefficients ainsi que le discriminant de E sont premiers avec n, elle définit une courbe algébrique sur $\mathbb{P}_2(\mathbb{Z}/n\mathbb{Z})$ appelée la réduction de E modulo n.

La structure de groupe est en général perturbée par la réduction modulo un entier composé n. On esquive cette difficulté dans la pratique, en utilisant les formules d'addition usuelles comme si $\mathbb{Z}/n\mathbb{Z}$ était un corps, tant qu'elles gardent un sens. En effet, dans le cas contraire, ces formules échouent à cause de l'apparition d'un dénominateur non inversible, ce qui se traduit par la découverte d'un facteur propre de n. Or, pour qui veut tester la primalité de n, cet échec se transforme en aubaine. Toutefois, ce processus "d'addition" sur E_n n'est pas une véritable loi de groupe.

Soit k un entier. Etant donnée une *chaîne d'additions pour* k, c'est-à-dire une suite finie $1 = k_0, k_1, k_2, \ldots, k_r = k$ d'entiers tels que, pour tout i il existe j et j' inférieurs à i tels que $k_i = k_j + k_{j'}$, on peut calculer de proche en proche, en utilisant le processus d'addition ci-dessus, le "produit" d'un point P de E par l'entier k. Si n est premier, ce produit coïncide avec le produit de la structure de groupe, mais dans le cas contraire, il peut dépendre de la chaîne d'additions choisie.

Pseudo-premiers elliptiques

Dans [5], on trouve les définitions que voici :

4.1. — Définitions. *Soit E une courbe elliptique définie sur $\mathbb{Q}$, définie par une équation de la forme (W), à multiplication complexe par un ordre dans un corps quadratique $\mathbb{Q}(\sqrt{D})$ et soit P_0 un point d'ordre infini sur E. Soit n un entier composé et supposons qu'une chaîne d'additions a été choisie pour $n+1$. On dit que n est un pseudo-premier elliptique si l'on a*

$$\left(\frac{D}{n}\right) = -1 \qquad et \qquad (n+1)P_0 = 0 \quad sur\ E_n.$$

Pour n impair, posons $n+1 = 2^k q$ avec q impair et choisissons une chaîne d'additions pour q. On dit que n est un pseudo-premier elliptique fort si l'on a $(D/n) = -1$ ainsi que

l'une ou l'autre des situations suivantes sur E_n *:*

$qP_0 = 0$

ou

il existe un entier i *tel que* $0 \leq i < k$ *et* $2^i qP$ *soit de la forme* $(x, 0)$, $x \in \mathbb{Z}/n\mathbb{Z}$.

Un lemme classique

4.2. — **Lemme.** *Soit* E *une courbe elliptique définie sur un corps* K *par l'équation* $Y^2 = f(X)$ *avec* $f(X) = aX + b$. *Un point* (x, y) *de* E *distinct de l'élément neutre est un double si et seulement si le polynôme* $x - X$ *est un carré dans l'algèbre* $K[X]/f$.

Démonstration — Si $(x, y) = 2(x', y')$ alors il existe une droite d'équation $Y = uX + v$ passant par $(x, -y)$ et tangente à E en (x', y'). Le trinôme $(uX + v)^2 - f(X)$ admet x comme racine simple et x' comme racine double. On a donc l'égalité

$$(uX + v)^2 - f(X) = (x - X)(x' - X)^2.$$

Puisque $f(x')$ est différent de 0 (car $2(x', y') \neq 0$), l'élément $x' - X$ est inversible modulo f et la relation ci-dessus montre que $x - X$ est un carré modulo f.

Inversement, supposons que $x - X$ soit un carré $(\alpha X^2 + \beta X + \gamma)^2$ modulo f. Il est facile de voir que $\alpha \neq 0$. Posons $x' = \beta/\alpha$. On a alors

$$\begin{aligned}(x' - X)(\alpha X^2 + \beta X + \gamma) + \alpha f(X) &= (\alpha x' - \beta)X^2 + (\beta x' - \gamma + \alpha a)X + (\gamma x' + \alpha b) \\ &= uX + v \qquad \text{avec } u, v \in \mathbb{Z}.\end{aligned}$$

En élevant au carré, on obtient

$$(x' - X)^2(x - X) \equiv (uX + v)^2 \text{ modulo } f,$$

que l'on peut préciser en examinant le terme de degré 3 :

$$(x' - X)^2(x - X) = (uX + v)^2 - f(X). \tag{8}$$

Posons $y' = ux' + v$, $P' = (x', y')$ et $Q = (x, ux + v) = \pm P$. En substituant x à X dans l'équation (8), on voit que Q appartient à la droite Δ d'équation $Y = uX + v$. De même, en substituant x' à X, on voit que P' est sur Δ. De plus, le fait que $(uX + v)^2 - f(X)$ admette un zero double en x' exprime que la droite Δ est tangente à E en P'. On a donc $2P' = Q = \pm P$, donc $2(\pm P') = P$. □

Construire des pseudo-premiers elliptiques

Déterminons des conditions suffisantes pour qu'un entier n soit pseudo-premier elliptique. Pour cela, nous adaptons la méthode du chapitre 6. Soit donc E la courbe d'équation (W) à coefficients entiers et soit P_0 un point de E. Supposons de plus que E est à multiplication complexe par un ordre de $\mathbb{Q}(\sqrt{D})$ et choisissons une chaîne d'additions pour chaque entier. Nous reprenons les notations de la section 6.2 avec $\varepsilon = -1$. Nous pouvons alors énoncer l'analogue elliptique du lemme 6.6.1 :

4.3. — Lemme. *Supposons que les coefficients k_i et m_i soient entiers et que l'on ait la relation*

$$\left(\frac{D}{p_i}\right) = -1 \qquad \text{pour tout } i \text{ vérifiant } 1 \leq i \leq h,$$

alors n est pseudo-premier elliptique pour la courbe E et le point P_0, sous réserve que la chaîne d'additions utilisée pour $n+1$ ne fasse pas apparaître un facteur propre de n.

DÉMONSTRATION — La condition sur les symboles de Legendre exprime que les p_i sont inertes dans l'ordre $\mathrm{End}(E)$ et donc que le groupe E_{p_i} est d'ordre p_i+1. On a donc $(p_i+1)P_0 = 0$ sur E_{p_i} pour chaque i. D'après le lemme 6.2.2, les quotients $(n+1)/(p_i+1)$ sont des entiers. Ainsi, on a $(n+1)P_0 = 0$ sur chacune des courbes E_{p_i} donc sur E_n. □

Construire des pseudo-premiers elliptiques forts

Nous allons montrer que, pour une certaine classe de courbes elliptiques, nous pouvons appliquer la méthode du chapitre 6 pour construire des pseudo-premiers elliptiques forts, plus précisément des entiers n tels que $((n+1)/2)P_0$ soit un point de la forme $(x,0)$ sur E_n.

4.4. — Lemme. *Supposons, en plus des hypothèses du lemme 4.3, que l'équation de E soit de la forme $Y^2 = f(X)$, et que la factorisation du membre de droite en irréductibles sur Q soit du type $f(X) = (X-w)g(X)$ avec $w \in \mathbb{Z}$. Supposons aussi que les coefficients k_i soient impairs et que l'on ait les relations*

$$\left(\frac{d'}{p_i}\right) = \left(\frac{x_0 - w}{p_i}\right) = -1 \qquad \text{pour tout } i \text{ vérifiant } 1 \leq i \leq h$$

où d' est le discriminant du polynôme $g(X)$. Alors, l'entier n est pseudo-premier elliptique fort sous réserve que la chaîne d'additions utilisée ne fasse pas apparaître un facteur propre de n.

DÉMONSTRATION — Les hypothèses impliquent que le polynôme f n'admet que la seule racine w dans $\mathbb{F}_{p_i}$. Le groupe E_{p_i} n'admet donc qu'un seul point d'ordre 2 et sa 2-composante est cyclique (en fait le groupe E_{p_i} tout entier est cyclique). D'autre part, les hypothèses impliquent que le point P_0 n'est pas un double sur E_{p_i}.

En effet, si c'était un double alors, en posant $P_0 = (x_0, y_0)$, le polynôme $x_0 - X$ serait un carré modulo f, donc modulo $X-w$. Or, cela contredirait l'hypothèse $(x_0 - w/p_i) = -1$.

La projection de P_0 sur la 2-composante de E_{p_i} y est donc d'ordre 2^k et $((p_i+1)/2)P_0$ ne peut être l'élément neutre de E_{p_i}. Puisque $\frac{n+1}{2}/\frac{p_i+1}{2}$ est impair d'après 6.2.1, le point $((n+1)/2)P_0$ ne peut non plus être cet élément neutre. Il est donc d'ordre 2 et de la forme $(x_i, 0)$. Le point $((n+1)/2)P_0$ est donc de la forme $(x,0)$ sur E_n. □

Exemples

Voici quelques exemples basés sur des courbes rencontrées dans [5].

• Soit E la courbe définie par l'équation

$$Y^2 = X^3 - 5X$$

et P_0 le point $(5, 10)$. L'application de E dans E

$$[i] : (x, y) \longmapsto (-x, iy)$$

définit un endomorphisme de E dont le carré est la multiplication par -1. Cela montre que E est une courbe à multiplication complexe par $\mathbb{Z}[\sqrt{-1}]$. Les conditions du lemme 4.4 sont alors

$$\left(\frac{-1}{p_i}\right) = \left(\frac{5}{p_i}\right) = \left(\frac{5-0}{p_i}\right) = -1. \qquad \text{pour } 1 \leq i \leq h.$$

Elles s'expriment sous forme de congruences :

$$p_i \equiv 3 \text{ ou } 7 \quad \text{modulo } 20. \qquad \text{pour } 1 \leq i \leq h.$$

Choisissons par exemple $h = 3$, $k_2 = 11$ et $k_3 = 31$, on en déduit la condition suffisante suivante :

4.5. — **Lemme.** *Soit p_1 un nombre premier congru à 203 modulo $20 \cdot 11 \cdot 31$ (i.e. 5 mod 11, 17 mod 31, 3 mod 20) et tel que $p_2 = 11(p_1 + 1) - 1$ et $p_3 = 31(p_1 + 1) - 1$ soient premiers. Alors, sous réserve que la chaîne d'additions utilisée ne fasse pas apparaître un facteur propre de n, le produit $p_1p_2p_3$ est un pseudo-premier fort pour E et P_0. On obtient ainsi les pseudo-premiers elliptiques forts suivants :*

$$\begin{aligned}
3008665821141287 \qquad & (p_1 = 20663),\\
35581022678705104127 \qquad & (p_1 = 470783),\\
95791362631028178707 \qquad & (p_1 = 654923),\\
387646637607153762287 \qquad & (p_1 = 1043663),\\
4328122656227862312347 \qquad & (p_1 = 2332643),\\
3694831865328400848327 \qquad & (p_1 = 4767383),\\
4563973974557087950267 \qquad & (p_1 = 5115203),\\
6277307181855209054100047 \qquad & (p_1 = 12255743),\\
7478471845208837618539 67 \qquad & (p_1 = 12992303),\\
1343816484899234022041507 \qquad & (p_1 = 15795323),\\
\vdots &
\end{aligned}$$

• Soit E la courbe définie par l'équation

$$Y^2 = X^3 - 120X - 448$$

et P_0 le point $(64, 504)$. On peut montrer que cette courbe est à multiplication complexe par $\mathbb{Z}(\sqrt{-2})$. On a la factorisation

$$X^3 - 120X - 448 = (X + 8)(X^2 - 8X - 56)$$

et le discriminant réduit du deuxième facteur est 253. Les conditions du lemme 4.4 sont alors

$$\left(\frac{-2}{p_i}\right) = \left(\frac{253}{p_i}\right) = \left(\frac{64+8}{p_i}\right) = -1. \qquad \text{pour } 1 \leq i \leq h.$$

En prenant par exemple $h = 3$, $k_2 = 5$ et $k_3 = 13$, elles sont vérifiées entre autres pour

$$p_1 \equiv \begin{cases} 5 & \text{modulo } 8 \\ 2 & \text{modulo } 253 \\ 8 & \text{modulo } 13 \\ 2 & \text{modulo } 5 \end{cases}$$

c'est-à-dire

$$p_1 \equiv 125237 \quad \text{modulo } 131560.$$

On obtient de cette manière les pseudo-premiers elliptiques forts suivants :

$$\begin{aligned}
134882155524507600904109 \quad & (p_1 = 12754997), \\
17763066824160648027324 29 \quad & (p_1 = 30120917), \\
55123511267896155840042 29 \quad & (p_1 = 43934717), \\
11826640809898736801899 6469 \quad & (p_1 = 122081357), \\
20958898932812805355702 4669 \quad & (p_1 = 147735557), \\
23039934199396866246891 1229 \quad & (p_1 = 152471717), \\
52178040918324091802586 7109 \quad & (p_1 = 200227997), \\
10491424296600590613394 03949 \quad & (p_1 = 252720437), \\
11349426885576988157153 29109 \quad & (p_1 = 259429997), \\
12582973651135907767766 79149 \quad & (p_1 = 268507637), \\
\vdots \quad &
\end{aligned}$$

5. Bibliographie

[1] W.W. Adams : *Characterizing pseudoprimes for third-order linear recurrences.* Mathematics of Computation, vol. 48, n° 177, janv. 1987, pp. 1–15.

[2] W.W. Adams, D. Shanks : *Strong primality tests that are not sufficient.* Mathematics of Computation, vol. 39, n° 159, juil. 1982, pp. 225–300.

[3] S. Arno : *A note on Perrin pseudoprimes.* Mathematics of Computation, vol. 56, n° 193, janvier 1991, pp. 371–376.

[4] H. Cohn : *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer-Verlag, Coll. Universitext, 1978, 1988.

[5] D.M. Gordon : *On the number of elliptic pseudoprimes.* Mathematics of Computation. vol. 52, n° 185, janvier 1989, pp. 231–245.

[6] S. Gurak : *Pseudoprimes for higher-order linear recurrence sequences.* Mathematics of Computation, vol. 55, n° 192, oct. 1990, pp. 783–813.

[7] G.C. Kurtz, D. Shanks, H.C. Williams : *Fast primality tests for numbers less than* $50 \cdot 10^9$. Mathematics of Computation, vol. 46, n° 174, avril 1986, pp. 691–701.

[8] D.H. Lehmer : *An extended theory of Lucas' functions.* Annals of Mathematics, vol. 31, 1930, pp. 419–448.

[9] H.W. Lenstra, Jr. : *Factoring integers with elliptic curves.* Annals of Mathematics 126, 1987, pp. 649–673.

[10] E. Lucas : *Sur la recherche de grands nombres premiers.* A.F. Congrès de Clermont-Ferrand, 1876, pp. 61–68.

[11] F. Morain : *Courbes elliptiques et tests de primalité.* Thèse, Université Lyon I, septembre 1990.

[12] A. Rotkiewicz : *On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters* L, Q *in arithmetic progressions.* Mathematics of Computation, vol. 39, n° 159, juillet 1982, pp. 239–247.

[13] J.H. Silverman : *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[14] H.C. Williams : *A generalization of Lehmer's functions.* Acta Arithmetica, vol. 29, 1976.

[15] H.C. Williams : *Primality testing on a computer.* Ars Combinatoria, vol. 5, 1978, pp. 127–185.

[16] H.C. Williams, J.S. Judd : *Determination of the primality of* N *by using factors of* $N^2 \pm 1$. Mathematics of Computation, vol. 30, n° 133, janvier 1976, pp. 157–172.

[17] H.C. Williams, J.S. Judd : *Some algorithms for prime testing using generalized Lehmer functions.* Mathematics of Computation, vol. 30, n° 136, octobre 1976, pp. 867–886.