

Quelques tests de primalité

emmanuel _____ hallouin@univ-tlse2.fr _____ http://www.math.univ-toulouse.fr/~hallouin/eh-agreg.html _____ hallouin

Voici un petit survol sur les **tests de primalité**, c'est-à-dire les algorithmes qui permettent de décider si un entier est premier ou non. Pour préparer ce document, je me suis principalement basé sur trois ouvrages : [Dem97, Sti03, CP05]. Je me suis aussi appuyé sur le bref «survey» de R.Schoof [Sch08] qui est un excellent article pour rentrer dans le domaine.

1 Philosophie des tests de primalité

Soit $n \in \mathbb{N}^*$ un entier. Un **test de primalité** est un algorithme permettant de répondre à la question suivante : «l'entier n est-il **premier**?». Evidemment, un soin particulier est accordé à l'efficacité : on veut que les algorithmes proposés soient de **complexité polynomiale**, c'est-à-dire exigeant un nombre d'opérations en $O(\log(n)^c)$ avec $c > 0$ aussi petit que possible.

L'idée est toujours de chercher des «témoins» de non-primalité. Soit n un entier dont on cherche à montrer la primalité ou la non-primalité. Les premiers témoins de non-primalité pour n auxquels on pense sont bien sûr les diviseurs non triviaux de n (ou plus généralement les entiers dont le pgcd avec n est non trivial). Cependant, il est exclu de baser un algorithme efficace sur ces derniers car en trouver ne serait-ce qu'un revient à factoriser n , ce que l'on ne sait pas faire efficacement.

La plupart des tests de primalité consistent donc à exhiber d'autres témoins de non primalité. Souvent on les déduira d'une propriété $\mathcal{P}(n, x)$ du type :

$$n \text{ premier} \implies \forall x \in \mathbb{Z}, \mathcal{P}(n, x) \text{ est vraie.}$$

Du coup tout entier x tel que la propriété $\mathcal{P}(n, x)$ soit fausse est un témoin de la non primalité de n .

On va présenter dans la suite plusieurs propriétés sur lesquelles on peut baser un test de primalité. Un tel test sera d'autant plus efficace que les témoins de non-primalité pour un entier n composé seront nombreux.

2 Témoins de Fermat

Le «petit théorème de Fermat» fournit des exemples de témoins de non primalité d'un entier n autres que les diviseurs de n ou que les entiers non premiers à n .

Théorème 2.1 (Petit théorème de Fermat) *Si p est premier alors pour tout $x \in \mathbb{Z}$ premier à p on a $x^{p-1} \equiv 1 \pmod{p}$.*

Définition 2.2 (Témoin de Fermat) *Soit $n \geq 2$ un entier. On dit que $x \in \mathbb{Z}$ est un **témoin de Fermat** pour n si $x^{n-1} \not\equiv 1 \pmod{n}$.*

Par exemple, si n n'est pas premier, les diviseurs stricts de n , ou plus généralement les entiers non premiers à n , sont des témoins de Fermat pour n .

Question 1. Le montrer.

On en déduit facilement la proposition :

Proposition 2.3 *Un entier n est composé si et seulement s'il existe $1 < x < n$ témoin de Fermat pour n .*

Question 2. Faire la preuve de cette proposition.

Question 3. En déduire un test de primalité basé sur la recherche de témoins de Fermat.

Question 4. a. Écrire en `maple` une fonction `FermatWitness` prenant en paramètre deux entiers n et x et qui réponde `true` si et seulement si x est un témoin de Fermat pour n . Quel est le coût de cette fonction ?

b. Implémenter le test de primalité de la question précédente.

Question 5. a. Ecrire une fonction en `maple` qui énumère tous les témoins de Fermat d'un entier donné.

b. La faire tourner avec de petits entiers puis avec l'entier 561. Que remarquez-vous ?

Bien sûr, les témoins de Fermat n'ont d'intérêt, pour les tests de primalité, que dans la mesure où ils apportent de nouveaux témoins. Malheureusement, ce n'est pas toujours le cas : il existe des entiers composés n'admettant pas de témoins de Fermat non triviaux, c'est-à-dire autres que les entiers non premiers à n .

Proposition 2.4 Soit $n \geq 1$ un entier. Alors sont équivalentes :

1. l'entier n est sans facteur carré et pour tout premier p divisant n , on a $p - 1$ qui divise $n - 1$;
2. pour tout x premier à n , on a $x^{n-1} \equiv 1 \pmod{n}$.

Question 6. Le montrer.

Les entiers composés qui satisfont cette proposition s'appellent les **nombre de Carmichael**. On sait depuis peu, qu'ils sont en nombre infini. Ils jouent incontestablement les trouble-fêtes dans les critères de primalité issus du petit théorème de Fermat.

Question 7. a. Montrer qu'un nombre de Carmichael est forcément impair et produit d'au moins trois premiers.

b. A l'aide de `maple`, essayer de trouver des nombres de Carmichael.

3 Témoins de Miller

Pour contrer l'obstacle des nombres de Carmichael, Miller propose d'autres témoins en s'appuyant sur le raffinement suivant du petit théorème de Fermat :

Proposition 3.1 Soit p un premier. Ecrivons $p - 1 = 2^\alpha q$ avec $q \in \mathbb{N}$ impair. Alors pour tout $x \in \mathbb{Z}$ premier à p on a :

$$x^q \equiv 1 \pmod{p} \quad \text{ou} \quad \exists 0 \leq i \leq \alpha - 1, x^{2^i q} \equiv -1 \pmod{p}.$$

Question 8. La montrer.

On en déduit la notion de témoin de Miller :

Définition 3.2 (Témoin de Miller) Soit $n \geq 2$ un entier. Ecrivons $n - 1 = 2^\alpha m$ avec $m \in \mathbb{N}$ impair. Un entier $x \in \mathbb{Z}$ tel que :

$$x^m \not\equiv 1 \pmod{n} \quad \text{et} \quad \forall i = 0, 1, \dots, \alpha - 1, x^{2^i m} \not\equiv -1 \pmod{n},$$

s'appelle un **témoin de Miller** pour n .

Question 9. a. Implémenter en `maple` une fonction qui décide si un entier x est un témoin de Miller pour un autre entier n .

b. Ecrire une fonction qui énumère la liste de tous les témoins de Miller d'un entier n . Expérimenter, par exemple en re-considérant l'exemple de $n = 561$.

Cette fois, on peut montrer que tout entier composé possède beaucoup de témoins de Miller. Plus précisément :

Proposition 3.3 *Si n est un entier composé alors au moins les trois quarts des entiers x tels que $1 < x < n$ sont des témoins de Miller pour n .*

C'est une conséquence du résultat suivant :

Théorème 3.4 (Rabin) *Soit n un entier impair composé et > 9 . Posons $n - 1 = 2^\alpha m$ avec m impair et introduisons l'ensemble \mathcal{M} défini par :*

$$\mathcal{M} = \left\{ x \in \mathbb{Z}/n\mathbb{Z} \mid x^m = 1 \text{ ou } x^{2^i m} = -1 \text{ pour un } i \in \{0, 1, \dots, \alpha - 1\} \right\}.$$

Alors $\#\mathcal{M} \leq \frac{\varphi(n)}{4}$, où φ désigne la fonction indicateur d'Euler.

Il est clair que cet énoncé est lié au nombre d'éléments de $\mathbb{Z}/n\mathbb{Z}^*$ d'ordre divisant $n - 1$. La recherche d'éléments d'ordre donné (ou divisant un entier donné) est facile dans les groupes cycliques. Nous allons nous appuyer sur ce fait et sur le fait que $\mathbb{Z}/n\mathbb{Z}^*$ est un produit de groupes cycliques.

Lemme 3.5 *Pour tout premier p impair et tout $\varepsilon > 0$, le groupe $\mathbb{Z}/p^\varepsilon\mathbb{Z}^*$ des inversibles de $\mathbb{Z}/p^\varepsilon\mathbb{Z}$ est cyclique de cardinal $p^{\varepsilon-1}(p-1)$.*

Question 10. En faire la preuve et donner un générateur.

Lemme 3.6 *Dans un groupe (multiplicatif) cyclique G , le nombre de solutions de l'équation $g^\varepsilon = 1$ est égal à $\text{pgcd}(\#G, \varepsilon)$.*

Question 11. En faire la preuve.

Tout est prêt pour la preuve du théorème de Rabin.

Preuve du théorème 3.4 — Ecrivons $n = \prod_{p|n} p^{\varepsilon_p}$ et pour tout premier p divisant n , posons $p - 1 = 2^{\alpha_p} m_p$ avec m_p impair. Enfin notons $\beta = \min\{\alpha_p, p \mid n\}$; ainsi 2^β est la plus grande puissance de 2 divisant tous les entiers $(p - 1)$ pour p diviseur premier de n .

Soit $\mathcal{N}_+, \mathcal{N}_-$ et \mathcal{N} , les ensembles définis par :

$$\mathcal{N}_+ = \left\{ x \in \mathbb{Z}/n\mathbb{Z} \mid x^{2^{\beta-1}m} = 1 \right\}, \quad \mathcal{N}_- = \left\{ x \in \mathbb{Z}/n\mathbb{Z} \mid x^{2^{\beta-1}m} = -1 \right\}, \quad \text{et } \mathcal{N} = \mathcal{N}_+ \cup \mathcal{N}_-.$$

On va montrer successivement que $\mathcal{M} \subset \mathcal{N}$, puis que $\#\mathcal{N} \leq \frac{\varphi(n)}{4}$, ce qui permet directement de conclure.

• Commençons par vérifier que $\mathcal{M} \subset \mathcal{N}$. Cela repose sur le théorème chinois qui nous permet de décomposer $\mathbb{Z}/n\mathbb{Z}^*$ en produit :

$$\mathbb{Z}/n\mathbb{Z}^* \simeq \prod_{p|n} \mathbb{Z}/p^{\varepsilon_p}\mathbb{Z}^*. \tag{1}$$

Grâce au lemme 3.5, on sait que chaque composante du produit de droite est un groupe cyclique de cardinal $\varphi(p^{\varepsilon_p}) = p^{\varepsilon_p-1}(p-1)$. Cela étant, pour $x \in \mathbb{Z}/n\mathbb{Z}^*$, si $x^m = 1 \pmod n$, il est évident que $x \in \mathcal{N}$. Si maintenant $x^{2^i m} = -1$ pour un $i \in \{0, 1, \dots, \alpha - 1\}$, alors $(x^m)^{2^i} = -1 \pmod n$. A fortiori, $(x^m)^{2^i} = -1 \pmod{p^{\varepsilon_p}}$ pour tout premier p divisant n . En particulier, cela veut dire que x^m est d'ordre 2^{i+1} modulo p^{ε_p} pour tout premier p divisant n . Par conséquent $2^{i+1} \mid \varphi(p^{\varepsilon_p})$ pour tout p si bien que $i+1 \leq \beta$. Il en résulte bien que $x \in \mathcal{N}$.

• Dénombrer \mathcal{N}_+ revient à compter les solutions de l'équation $x^{2^{\beta-1}m} = 1$ modulo p^{ε_p} pour chaque premier p divisant n . En vertu du lemme 3.6, on a donc :

$$\#\mathcal{N}_+ = \prod_{p|n} \text{pgcd}\left(2^{\beta-1}m, p^{\varepsilon_p-1}(p-1)\right) = \prod_{p|n} 2^{\beta-1} \text{pgcd}(m, p-1).$$

De la même façon, dénombrer \mathcal{N}_- revient, pour chaque diviseur premier p de n , à compter le nombre de solutions de l'équation $x^{2^{\beta-1}m} = -1$ modulo p^{ε_p} . On remarque alors que :

$$\{x \in \mathbb{Z}/p^{\varepsilon_p}\mathbb{Z} \mid x^{2^{\beta-1}m} = -1\} = \{x \in \mathbb{Z}/p^{\varepsilon_p}\mathbb{Z} \mid x^{2^{\beta}m} = 1\} \setminus \{x \in \mathbb{Z}/p^{\varepsilon_p}\mathbb{Z} \mid x^{2^{\beta-1}m} = 1\}$$

si bien que :

$$\begin{aligned} \#\{x \in \mathbb{Z}/p^{\varepsilon_p}\mathbb{Z} \mid x^{2^{\beta-1}m} = -1\} &= \text{pgcd}\left(2^{\beta}m, p^{\varepsilon_p-1}(p-1)\right) - \text{pgcd}\left(2^{\beta-1}m, p^{\varepsilon_p-1}(p-1)\right) \\ &= 2^{\beta} \text{pgcd}(m, p-1) - 2^{\beta-1} \text{pgcd}(m, p-1) \\ &= 2^{\beta-1} \text{pgcd}(m, p-1). \end{aligned}$$

Ainsi $\#\mathcal{N}_+ = \#\mathcal{N}_-$ et :

$$\#\mathcal{N} = 2 \prod_{p|n} 2^{\beta-1} \text{pgcd}(m, p-1).$$

Il nous faut donc prouver que :

$$\frac{\#\mathcal{N}}{\varphi(n)} = 2 \prod_{p|n} \frac{2^{\beta-1} \text{pgcd}(p-1, m)}{(p-1)p^{\varepsilon_p-1}} \stackrel{?}{\leq} \frac{1}{4} \iff \prod_{p|n} \frac{(p-1)}{2^{\beta-1} \text{pgcd}(p-1, m)} \times p^{\varepsilon_p-1} \stackrel{?}{\geq} 8. \quad (2)$$

Comme $\frac{(p-1)}{2^{\beta-1} \text{pgcd}(p-1, m)}$ est un entier ≥ 2 , si n est divisible par au moins trois premiers distincts, l'inégalité (2) est satisfaite. Dans le cas où n ne possède que deux premiers p et q dans sa décomposition primaire, on distingue deux possibilités. Soit, par exemple $\varepsilon_p \geq 2$ auquel cas le membre de gauche de (2) est clairement $\geq 4p \geq 8$. Soit $n = pq$; le seul cas de figure où l'inégalité (2) pourrait ne pas être satisfaite, c'est quand :

$$\frac{(p-1)}{2^{\beta-1} \text{pgcd}(p-1, m)} \times p^{\varepsilon_p-1} = \frac{(q-1)}{2^{\beta-1} \text{pgcd}(q-1, m)} \times q^{\varepsilon_q-1} = 2,$$

ou encore $\varepsilon_p = \varepsilon_q = 1$ et :

$$\begin{cases} p-1 = 2^{\beta} \text{pgcd}(p-1, m) = 2^{\alpha_p} m_p \\ q-1 = 2^{\beta} \text{pgcd}(q-1, m) = 2^{\alpha_q} m_q \end{cases} \implies \begin{cases} \alpha_p = \alpha_q = \beta \\ \text{pgcd}(p-1, m) = m_p \\ \text{pgcd}(q-1, m) = m_q. \end{cases}$$

Ainsi m_p doit diviser m et $(p-1)$. Ceci est impossible car en raisonnant modulo m_p , on s'aperçoit que :

$$2^{\beta} m_q = q-1 \equiv pq-1 \equiv n-1 \equiv 2^{\alpha} m \equiv 0 \pmod{m_p} \implies m_p \mid m_q.$$

Par symétrie, on a aussi $m_q \mid m_p$ donc $m_p = m_q$ puis $p = q$, ce qui n'est pas vrai. Enfin, si n est la puissance d'un seul premier $n = p^{\varepsilon}$ alors, comme n est supposé composé, impair et > 9 , on a $p \geq 5$ et $\varepsilon_p \geq 2$ ou $p \geq 3$ et $\varepsilon_p \geq 3$; dans les deux cas l'inégalité (2) est encore trivialement satisfaite. \square

4 Le test de Miller-Rabin

Le test de primalité de Miller-Rabin qui découle de ce qui précède consiste à tirer au hasard un entier x dans l'intervalle $[2, n-2]$ puis de vérifier s'il est ou non un témoin de Miller pour n .

Question 12. Implémenter en `maple` le test de Miller-Rabin.

Chaque vérification du fait que x est un témoin ou non pour n requiert $\log(n)$ produits dans $\mathbb{Z}/n\mathbb{Z}$, d'où une complexité en $O(\log(n)^3)$ pour chaque vérification. On peut répéter à l'envie les tirages pour augmenter les chances de tomber sur un témoin. Si on effectue moins de $\log(n)$, le test de primalité ainsi obtenu est bien polynomial puisque de complexité en $O(\log(n)^4)$.

Ce test rentre dans la classe des algorithmes dits **probabilistes** dans la mesure où une des ses étapes fait appel à un tirage au hasard. Plus précisément, c'est un algorithme de type **Monte-Carlo** car il est

possible qu'il retourne une réponse erronée. Cela vient du fait qu'il peut décréter un entier n premier sans qu'il le soit. Cependant, si l'entier n est composé, compte tenu de ce qui précède, la probabilité qu'après $\log(n)$ tirages au hasard indépendants, l'entier n soit décrété premier est $\leq \frac{1}{4^{\log(n)}} \leq \frac{1}{n}$. Si on effectue $\log(n)^2$ tirages, cette probabilité devient ridiculement petite.

Pour espérer rendre l'algorithme de Miller-Rabin déterministe, il suffirait de prouver que tout entier composé possède un petit — c'est-à-dire de l'ordre $O(\log(n)^c)$ — témoin de Miller. À l'heure actuelle, on ne sait pas montrer un tel résultat... sauf en admettant l'**hypothèse de Riemann généralisée**. Dans ce cas une version déterministe et polynomiale du test de Miller-Rabin résulte du résultat suivant.

Théorème 4.1 *Sous l'hypothèse de Riemann généralisée, pour $n \in \mathbb{Z}$ est composé, il existe un témoin de Miller $\leq 2 \log(n)^2$.*

Question 13. Donner, en `maple`, la version déterministe (non prouvée) du test de Miller-Rabin.

Le théorème 4.1 se déduit d'un autre résultat dont la seule preuve connue à ce jour utilise l'hypothèse de Riemann généralisée :

Théorème 4.2 (Bach) *Sous l'hypothèse de Riemann généralisée, on a :*

- pour tout premier p , il existe $x \in \mathbb{N}$ **non-résidu quadratique modulo p** tel que $x \leq 2 \log(p)^2$;
- pour tous premiers p, p' , $p \neq p'$, il existe $x \in \mathbb{N}$ qui est **non-résidu quadratique modulo p** , **résidu quadratique modulo p'** , et qui satisfait $x \leq 2 \log(pp')^2$.

Question 14. Soit p un premier impair et $x \in \mathbb{Z}/p\mathbb{Z}^*$. Montrer les équivalences :

$$x \text{ est un carré} \iff x^{\frac{p-1}{2}} = 1, \quad x \text{ n'est pas un carré} \iff x^{\frac{p-1}{2}} = -1.$$

Cela s'énonce aussi en termes de **résidus quadratiques** : pour p premier et $x \in \mathbb{Z}$, on définit la symbole de Legendre $\left(\frac{x}{p}\right)$ comme suit :

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } x, \\ 1 & \text{si } x \text{ est premier à } p \text{ et s'il est un carré modulo } p, \\ -1 & \text{si } x \text{ est premier à } p \text{ et s'il n'est pas un carré modulo } p. \end{cases}$$

Il s'agit donc d'établir que $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p}$.

Preuve du théorème 4.1 — On raisonne par l'absurde en supposant que tous les entiers $1 \leq x \leq 2 \log(n)^2$ ne sont pas des témoins de Miller, c'est-à-dire que :

$$x^m \equiv 1 \pmod{n} \quad \text{ou} \quad \exists 0 \leq i \leq \alpha - 1, x^{2^i m} \equiv -1 \pmod{n} \quad (3)$$

où $n - 1 = 2^\alpha m$ avec m impair. Notons dès à présent que cela implique que tous les entiers $\leq 2 \log(n)^2$ sont premiers à n .

On commence par montrer que n est forcément sans facteur carré.

Posons $n = pp'r$ avec p, p' premiers distincts et $r \in \mathbb{N}$ et écrivons $p - 1 = 2^\beta q$, $q - 1 = 2^{\beta'} q'$ avec q, q' impairs. Remarquons le fait suivant : modulo p , toutes les puissances impaires d'un élément x qui sont d'ordre une puissance de 2 ont en fait le même ordre (à savoir la plus grande puissance de 2 divisant l'ordre de x) et engendrent donc le même sous-groupe de $\mathbb{Z}/p\mathbb{Z}^*$.

Montrons que $\beta = \beta'$. D'après le théorème de Bach, il existe $x \leq 2 \log(p)^2 \leq 2 \log(n)^2$, non résidu quadratique modulo p . Il vérifie donc $x^{2^{\beta-1}q} \equiv -1 \pmod{p}$. Autrement dit x^q est d'ordre 2^β . D'autre part, comme $x \leq 2 \log(n)^2$, il satisfait par hypothèse les conditions (3). Cela veut dire que x^m est d'ordre une puissance de 2 modulo n . A fortiori, x^m est d'ordre une puissance de 2 modulo p . Compte tenu de la remarque précédente, on en déduit que x^m est aussi d'ordre 2^β modulo p . Dès lors $x^{2^{\beta-1}m} \equiv -1 \pmod{p}$ d'où il résulte que $x^{2^{\beta-1}m} \equiv -1 \pmod{n}$. En particulier, cela entraîne que x^m est d'ordre 2^β modulo p' donc $\beta \leq \beta'$. Par symétrie, on en déduit bien que $\beta = \beta'$.

On utilise à nouveau le théorème de Bach pour montrer l'existence de $y \leq 2 \log(n)^2$ qui est non-résidu modulo p mais résidu modulo p' . Ainsi $x^{2^{\beta-1}q} \equiv -1 \pmod{p}$. On en déduit comme précédemment que $x^{2^{\beta-1}m} \equiv -1 \pmod{n}$ puis $x^{2^{\beta-1}m} \equiv -1 \pmod{p'}$, ce qui contredit le fait que y soit résidu quadratique modulo p' . \square

5 Un certificat de primalité

Dans les applications, la quasi-certitude de la primalité d'un entier n'est pas toujours suffisante. On dispose alors d'algorithmes «ad hoc» adaptés à certains cas particulier. L'un des plus simples repose sur le résultat suivant :

Théorème 5.1 (Lucas) *Soit n un entier impair. S'il existe $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \pmod{n}$ mais que $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ pour tout premier q divisant $n-1$, alors n est premier.*

Preuve — La condition nous informe que a est d'ordre $n-1$ dans $\mathbb{Z}/n\mathbb{Z}^*$ qui du coup est lui même d'ordre $n-1$. Autrement dit, tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles. Cela implique que n est premier. \square

Evidemment, pour mettre en pratique ce critère, encore faut-il connaître la factorisation de l'entier $n-1$. C'est possible si ce dernier est «friable», c'est-à-dire produit de petits premiers. Le cas le plus frappant est celui des entiers de Fermat $F_k = 2^{2^k} + 1$ pour lesquels $F_k - 1$ est on ne peut plus friable. On peut même montrer que l'on peut toujours choisir $a = 3$:

Théorème 5.2 (Critère de Pepin) *Pour $k \geq 1$, l'entier de Fermat $F_k = 2^{2^k} + 1$ est premier si et seulement si $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$.*

Preuve — Si la condition $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$ est satisfaite, d'après le théorème de Lucas, l'entier F_k est premier.

Réciproquement si l'entier F_k est premier, on utilise la loi de réciprocité quadratique :

$$\left(\frac{3}{F_k}\right) = (-1)^{\frac{(3-1)(F_k-1)}{4}} \left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

car $4 \mid F_k - 1$ et car $F_k \equiv 2 \pmod{3}$. On conclut en se souvenant que $\left(\frac{3}{F_k}\right) \equiv 3^{\frac{F_k-1}{2}} \pmod{F_k}$. \square

Question 15. a. Montrer que si $2^\alpha + 1$ est premier alors α est une puissance de 2

b. Grâce à `maple`, étudier la primalité ou non des premiers entiers de Fermat.

De façon générale, il n'y a aucune raison pour laquelle on puisse toujours choisir $a = 3$. On fait donc encore appel au hasard. Du coup, il convient de vérifier que si n est premier, les entiers a qui satisfont le théorème de Lucas ne se font pas trop rares. Un tel a est en fait une racine primitive du corps fini $\mathbb{Z}/n\mathbb{Z}$. On peut montrer que pour n grand, leur nombre dépasse $\frac{n}{2 \log(\log n)}$, ce qui est énorme !

Question 16. Implémenter un certificat de primalité basé sur le théorème de Lucas.

6 Pour la culture

Il existe d'autres tests de primalité.

- Très proche du test de Miller-Rabin, Sollovey et Strassen ont proposé un test qui porte maintenant leurs noms. Il s'appuie sur les résidus quadratiques et les symboles de Legendre et Jacobi. Comme le test de Miller-Rabin, ce test peut déclarer qu'un entier est premier sans qu'il le soit. Il est plutôt moins efficace que Miller-Rabin car on montre que les témoins de non-primalité ont une proportion d'au moins $\frac{\varphi(n)}{2}$ (à comparer aux $\frac{3\varphi(n)}{4}$ pour Miller-Rabin). En revanche, la preuve de cette proportion est beaucoup plus aisée que celle de Miller-Rabin.

- Un autre test primalité est basé sur les courbes elliptiques, le *ECPP* pour «Elliptic Curve Primality Proving». Il est encore probabiliste et sa complexité est en $O(\log(n)^6)$. Son gros avantage est que ses réponses sont toujours sûres ; en particulier, si l'algorithme décrète un entier premier, c'est qu'il l'est. En revanche, la complexité annoncée est heuristique. On ne sait pas la prouver complètement si bien qu'il se peut que l'algorithme ne donne aucune réponse «au bout de $O(\log(n)^6)$ calculs».

• Enfin, les trois indiens Agrawal, Kayal et Saxena, ont récemment fourni un algorithme déterministe et polynomial permettant de montrer ou non la primalité d'un entier ([AKS04]). Ce très beau résultat, assez inattendu, a surpris plus d'un spécialiste. Certes sa complexité en $O(\log(n)^{18})$ ou $O(\log(n)^{12+\epsilon})$ (selon que l'on utilise des versions optimisées de l'exponentiation modulaire ou non) ne rivalise pas avec le test de Miller-Rabin par exemple, mais le déjà célèbre algorithme AKS présente l'énorme avantage d'être déterministe ! Des chercheurs essaient maintenant d'optimiser l'algorithme AKS dans l'espoir de se rapprocher de la complexité des algorithmes probabilistes. A l'heure actuelle, c'est un domaine actif de recherche.

Voici le résultat sur lequel est basé l'algorithme AKS.

Théorème 6.1 *Soit n un entier impair et r un nombre premier. On suppose que :*

1. *l'entier n n'est pas divisible par aucun premier $\leq r$;*
2. *l'ordre de n modulo r est au moins $(\log n / \log 2)^2$;*
3. *pour tout $0 \leq j < r$, on a $(\zeta_r + j)^n \equiv \zeta_r^n + j \pmod{n\mathbb{Z}[\zeta_r]}$.*

Alors n est la puissance d'un premier.

Question 17. Implémenter le test AKS en maple.

Références

- [AKS04] M. Agrawal, N. Kayal, and N. Saxena. Primes is in p. *Annals of Mathematics*, 160, 2004.
- [CP05] Richard Crandall and Carl Pomerance. *Prime numbers : a computational perspective*. Springer, 2005.
- [Dem97] Michel Demazure. *Cours d'Algèbre — Primalité, Divisibilité, Codes*, volume 1 of *Nouvelle Bibliothèque mathématique*. Cassini, 1997.
- [Sch08] René Schoof. Four primality testing algorithms. In *Algorithmic Number Theory Lattices, Number Fields, Curves and Cryptography*, volume 44 of *MSRI Publications*. Cambridge University Press, 2008.
- [Sti03] Douglas Stinson. *Cryptographie — Théorie et pratique*. Vuibert, 2003.