Université Bordeaux 1
Mathématiques

Préparation à l'agrégation
Année 2009–2010

Test de primalité de Lucas, nombres de Mersenne

Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury demande que la discussion soit accompagnée d'exemples traités sur ordinateur. Il est souhaitable que vous organisiez votre présentation comme si le jury n'avait pas connaissance du texte. Le jury aura néanmoins le texte sous les yeux pendant votre exposé.

1. Introduction

On peut se poser trois questions distinctes sur la nature arithmétique de $N \in \mathbb{N}$:

- N est-il composé ?
- N est-il premier ?
- Factoriser N.

Si les trois questions semblent équivalentes, elles sont en fait de difficulté largement différente. On s'intéresse ici aux deux premières. A savoir, comment montrer qu'un nombre est composé, puis, si la réponse est « apparemment pas », comment montrer qu'il est premier. Les tests proposés utilisent les notions nécessaires aux calculs et raisonnements dans $\mathbb{Z}/n\mathbb{Z}$, où n est un entier, parfois premier. On utilise également un calcul sur un corps fini quadratique sur $\mathbb{F}_p$ (p étant un nombre premier) pour le test de primalité de Lucas.

2. Tests de non primalité

Le petit théorème de Fermat fournit un test qui peut permettre de montrer qu'un nombre N n'est pas premier. Si en effet en calculant $2^{N-1} \bmod N$, on trouve un résultat distinct de 1, on est certain que N n'est pas premier. Par contre, si on trouve 1, cela ne veut pas dire que N est premier. On peut alors prendre d'autres valeurs a que 2, et calculer a^{N-1}. Si l'on trouve 1 à chaque fois, cela ne prouvera pas non plus que N n'est pas premier. Il existe des nombres composés pour lesquels on n'a que très peu de chances de conclure ainsi : les nombres de Carmichael, c'est-à-dire les nombres composés N tels que $a^{N-1} \equiv 1 \bmod N$ pour tout a premier avec N. Il a été démontré qu'il existe une infinité de tels nombres.

Un renforcement de ce test a été donné par Rabin et Miller en 1977. Il se base sur le théorème suivant.

Théorème 2.1. *Soit N un nombre premier impair, et a un entier premier à N. Si $N-1 = 2^e q$, où q est un entier impair, alors :*

(1) *Soit $a^q \equiv 1$ mod N.*
(2) *Soit il existe i tel que $0 \leqslant i \leqslant e-1$ tel que $a^{2^i q} \equiv -1$ mod N.*

Là encore, la réciproque est fausse, comme le montre l'exemple où $N = 3277$ et $a = 2$. Si un entier $a \in \{1, \dots N-1\}$ vérifie l'une des propriétés (1) ou (2) du théorème de Rabin-Miller, on dit que N est pseudo-premier (de Miller-Rabin) pour la base a.

Toutefois, la situation est meilleure que pour le test venant directement du petit théorème de Fermat. Le théorème suivant montre en effet que si un nombre N n'est pas premier, et si l'on essaie un nombre suffisant de valeurs de a, on a une très forte probabilité de trouver une base a pour laquelle N n'est pas pseudo-premier.

Théorème 2.2. *Si N est composé, alors il est pseudo-premier dans au plus $1/4$ des bases a.*

Pour démontrer ce théorème, on peut procéder de la manière suivante. On écrit la décomposition de N en produit de facteurs premiers $N = \prod_p p^{f_p}$. En utilisant le théorème chinois, on voit que le nombre A d'éléments a qui satisfont le test est égal à

$$\prod_p \#\{x \colon qx \equiv 0 \mod (p-1)p^{f_p-1}\}$$
$$+ \sum_{i=0}^{e-1} \prod_p \#\left\{x \colon q2^i x \equiv (p-1)p^{f_p-1}/2 \mod (p-1)p^{f_p-1}\right\}.$$

On trouve alors que

$$A = \left(1 + \frac{2^{\omega E}-1}{2^\omega - 1}\right) \prod_p (q, p-1),$$

où ω est le nombre de facteurs premiers de N, et où $E = \min_p e_p$, l'entier e_p étant défini pour tout p par : $e_p = v_2(p-1)$. La probabilité P cherchée est égale à $A/(N-1)$. Si $\omega = 1$, on trouve $P = 1$ si $f_p = 1$, et $P \leqslant (p-1)/(p^{f_p}-1) \leqslant 1/(p+1) \leqslant 1/4$ si $f_p > 1$. Si $\omega > 1$, les inégalités $(q, p-1) \leqslant (p-1)/2^{e_p}$ et $\prod_p (p-1) \leqslant N-1$ montrent que

$$P \leqslant \left(1 + \frac{2^{\omega E}-1}{2^\omega - 1}\right) / 2^{\omega E}.$$

On obtient alors la majoration voulue, sauf dans le cas où $\omega = 2$, où on obtient seulement $P \leqslant 1/2$. Dans ce cas, on peut affiner les inégalités précédentes pour obtenir le bon résultat, sauf si $p-1$ divise $N-1$ pour tout p et si N est sans facteurs carrés. On montre alors que ce cas est impossible.

3. Tests de primalité

Supposons que N ait passé le test de Rabin-Miller. Nous sommes alors à peu près certains que N est premier. Le démontrer rigoureusement est un problème plus difficile. Nous donnons ici un exemple de test, dû à Lucas. Ce test suppose connue la factorisation de $N+1$. Il utilise les suites (U_n), appelées suites de Lucas, définies par récurrence :

$$U_0 = 0, \quad U_1 = 1, \quad U_{n+1} = SU_n - PU_{n-1},$$

pour $n \geqslant 2$, où S et P sont des nombres entiers. Soit D le discriminant du polynôme $Q(x) = x^2 - Sx + P$, et soit p un nombre premier impair ne divisant pas DP. On

considère la suite (U_n) modulo p. On note r et r' les racines de Q dans une clôture algébrique de $\mathbb{F}_p$. Alors $[U_n]_p = (r^n - r'^n)(r - r')^{-1}$. Si $\left(\frac{D}{p}\right) = 1$, alors $r^{p-1} = r'^{p-1} = 1$, donc $U_{p-1} \equiv 0 \bmod p$. Si $\left(\frac{D}{p}\right) = -1$, alors $r^p = r'$, donc $U_{p+1} \equiv 0 \bmod p$. De plus, si e est le plus petit entier tel que $U_e \equiv 0 \bmod p$, alors $U_n \equiv 0 \bmod p$ si et seulement si e divise n. On peut alors montrer le théorème suivant, qui donne un autre test de primalité.

Théorème 3.1. *Supposons que l'on puisse trouver une suite de Lucas (U_n) telle que $(N, DP) = 1$, et telle que*

$$(U_{(N+1)/p}, N) = 1, \quad \textit{pour tout premier } p \mid N+1$$

et

$$U_{N+1} \equiv 0 \pmod{N}.$$

Alors N est un nombre premier.

En effet, on peut démontrer que dans les conditions de ce théorème, si d est un diviseur premier de N et e le plus petit entier strictement positif tel que $U_e = 0$, alors $N + 1 \mid e \mid d + 1$. On en déduit alors que $N = d$.

4. Nombres de Mersenne

Si N est de la forme $2^n - 1$, la factorisation de $N + 1$ est simple et il est plus facile d'étudier la primalité de N. L'entier N ne peut être un nombre premier que si n est premier. Un nombre de cette forme $M_n = 2^n - 1$, où n est un nombre premier, est appelé nombre de Mersenne.

Pour donner un exemple déjà ancien, Euler a démontré que M_{31} est premier en utilisant le théorème suivant.

Théorème 4.1. *Soient p et q deux nombres premiers impairs. Si p divise M_q, alors $p \equiv 1 \pmod{q}$ et $p \equiv \pm 1 \pmod{8}$.*

Mais revenons aux suites de Lucas. Soit (V_n) définie par récurrence : $V_{n+1} = SV_n - PV_{n-1}$ pour $n \geqslant 1$, $V_0 = 2$ et $V_1 = S$. Alors $U_{2n} = U_n V_n$. Si N est un nombre de Mersenne, on a donc $U_{N+1} = U_{(N+1)/2} V_{(N+1)/2}$. On peut alors remplacer les deux conditions du théorème 3.1 par la seule condition : $V_{(N+1)/2} \equiv 0 \pmod{N}$. Pour calculer $V_{(N+1)/2}$, on peut remarquer que $V_{2n} = V_n^2 - 2P^n$. On pose alors $v_n = V_{2^n}$ et on obtient la récurrence $v_n = v_{n-1}^2 - 2P^{2^{n-1}}$. Il est donc intéressant de s'arranger pour que $P = 1$ ou -1, c'est-à-dire, si a et a' sont les racines de Q dans $\mathbb{C}$, pour que $aa' = 1$ ou -1. De plus, il est implicite dans le théorème 3.1 que si le test réussit, $\left(\frac{D}{N}\right) = -1$. On peut prendre pour D un carré multiplié par 3, et donc par exemple $a = 2 + \sqrt{3}$, ce qui donne pour Q : $Q(x) = x^2 - 4x + 1$.

Malheureusement, le fait que $P = 1$, avec $\left(\frac{D}{N}\right) = -1$, implique que $U_{\frac{N+1}{2}} \equiv 0 \bmod N$, ce qui empêche d'appliquer le théorème 3.1 directement.

On peut alors faire un autre choix pour a et a'. Par exemple :

$$a = \sqrt{2+\sqrt{3}} = \frac{\sqrt{3}+1}{\sqrt{2}}, \quad \text{et} \quad a' = \frac{\sqrt{3}-1}{\sqrt{2}},$$

ce qui donne le polynôme $x^2 - x\sqrt{6} + 1$. Le raisonnement précédent ne s'applique pas directement, puisque les coefficients ne sont plus dans $\mathbb{Z}$, mais on peut l'adapter pour obtenir un résultat similaire.

Pour cela, on peut remarquer qu'il existe un nombre premier q divisant N tel que $(\frac{3}{q}) = -1$. De plus, le théorème 4.1 permet d'affirmer que 2 est un carré modulo q. Soit α une racine carrée de 6 dans $\mathcal{F}_{q^2}$, et soient r et r' les racines dans une clôture algébrique de $\mathcal{F}_q$ de $X^2 - \alpha X + 1$. On peut démontrer que $r^q = -r'$, $r'^q = -r$ et $U_{q+1} \equiv 0 \pmod{q}$.

Soit (V) la suite correspondante, c'est-à-dire : $V_0 = 2$, $V_1 = \sqrt{6}$, $V_2 = 4$, etc. En posant $v_k = V_{2^{k+1}}$, pour $k \geqslant 0$, on peut démontrer le résultat suivant.

Théorème 4.2. *Soit n un entier impair. Alors M_n est premier si et seulement si $v_{n-2} \equiv 0 \pmod{M_n}$, où $v_{k+1} = v_k^2 - 2$ pour $k \geqslant 0$ et $v_0 = 4$.*

5. Problèmes ouverts

Signalons au passage une propriété intéressante des nombres de Mersenne : tout nombre parfait pair est de la forme $2^{n-1}M_n$, où M_n est premier. On rappelle qu'un nombre parfait est un nombre entier positif égal à la somme de ses diviseurs propres. Par exemple, 6 est un nombre parfait. Il n'est pas connu à ce jour de nombres parfaits impairs, et on ne sait pas s'il en existe.

Quant aux nombres de Mersenne, on ne sait pas s'il en existe une infinité qui soient premiers. On ne sait pas non plus s'il en existe une infinité qui soient composés. Il existe cependant un résultat (théorème 5.1 ci-dessous), dû à Euler, qui semble indiquer que la réponse à cette dernière question devrait être affirmative. On pense en effet qu'il existe une infinité de couples de nombres premiers $(p, 2p+1)$, où $p \equiv 3 \bmod 4$.

Théorème 5.1. *Si $k > 1$ et $p = 4k+3$ est un nombre premier, alors $2p+1$ est premier si et seulement si $2^p \equiv 1 \pmod{2p+1}$.*

6. Suggestions

- Plusieurs affirmations sont données sans preuve. Le candidat est invité à les démontrer. Il est cependant déconseillé d'essayer de démontrer qu'il existe une infinité de nombres de Carmichael.
- Par ailleurs, la preuve de certains théorèmes n'est qu'ébauchée. On pourra en fournir plus de détails.
- Plusieurs tests sont proposés. On pourra en implémenter certains et les commenter.
- On pourra aussi faire une liste de nombres premiers de Mersenne, de nombres parfaits, de nombres composés de Mersenne.