Université Bordeaux 1
Mathématiques

Préparation à l'agrégation
Année 2009–2010

Tests de non primalité, tests de primalité

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. À 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. suivant.

Théorème 1.1. *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 1.2. *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

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

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.

2. 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, trouvé par Pocklington et amélioré par Lehmer, basé sur le théorème suivant.

Théorème 2.1. *Soit $N > 1$ un entier. Alors N est un nombre premier si et seulement si pour tout diviseur premier p de $N-1$ on peut trouver un entier a_p tel que*

$$a_p^{N-1} \equiv 1 \pmod N \quad \textit{et} \quad (a_p^{(N-1)/p} - 1, N) = 1.$$

En effet, si N est premier, et si g est une racine primitive modulo N, alors il suffit de poser $a_p = g$ pour tout p. Réciproquement, soit d un diviseur premier de N, on montre que pour tout p divisant $N-1$, $p^{v_p(N-1)}$ divise $d-1$, ce qui permet ensuite de conclure que $N = d$.

Ce théorème fournit un test de primalité rapide, dès que l'on connaît la factorisation de $N-1$. La factorisation d'un entier est un problème difficile et peut être un obstacle à l'utilisation de ce test. Il arrive toutefois qu'il ne soit pas trop difficile de factoriser $N-1$. De plus, on n'a pas vraiment besoin de la factorisation complète de $N-1$, comme le montrent les théorèmes 2.2 et 2.3 ci-dessous, auxquels la démonstration du théorème 2.1 s'applique, avec quelques modifications.

Théorème 2.2. *Soit $N > 1$ un entier. On suppose qu'on sait écrire $N - 1 = FU$, où $(F, U) = 1$, $F = \prod_{i=1}^{g} p_i^{f_i}$ est complètement factorisé, et où $U < F$. Alors N est premier si et seulement si pour tout élément $x = p_i$, $i \in \{1, \ldots, r\}$, on peut trouver un entier a_x tel que*

$$a_x^{N-1} \equiv 1 \pmod{N} \quad et (a_x^{(N-1)/x} - 1, N) = 1.$$

Théorème 2.3. *Soit $N > 1$ un entier. On suppose qu'on sait écrire $N - 1 = FU$, où $(F, U) = 1$, $F = \prod_{i=1}^{g} p_i^{f_i}$ est complètement factorisé, où tous les diviseurs premiers de U sont plus grand qu'un entier B, et où $BF \geqslant \sqrt{N}$. Alors N est premier si et seulement si pour tout élément $x = p_i$, $i \in \{1, \ldots, r\}$ et $x = U$, on peut trouver un entier a_x tel que*

$$a_x^{N-1} \equiv 1 \pmod{N} \quad et \quad (a_x^{(N-1)/x} - 1, N) = 1.$$

3. Suggestions

Plusieurs affirmations sont données sans preuve. Le candidat est invité à les démontrer. Il est 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 peut aussi chercher à illustrer expérimentalement la proportion des bases pour lesquelles un nombre composé est pseudo-premier.