

TESTS RAPIDES DE NOMBRES PREMIERS (*)

Hendrik W. Lenstra, Jr

Université d'Amsterdam

Tout au long de cet exposé, n désignera un nombre plus grand que 1. Nous appelons n **composé** s'il existe des entiers a et b tels que

$$n = a \cdot b, a > 1, b > 1$$

Dans le contraire, n est appelé **premier**. Voici deux problèmes fondamentaux de la théorie élémentaire des nombres :

- A. Comment peut-on voir, rapidement, si un nombre donné est premier ?
- B. Si n n'est pas premier, comment trouver des entiers $a > 1, b > 1$ tels que $a \cdot b = n$?

Bien que ces problèmes se ressemblent fort, les techniques mathématiques qu'on emploie pour les résoudre diffèrent du tout au tout.

Dans cet exposé, je m'occuperai presque exclusivement du problème A. Des progrès récents, concernant ce problème, ont été réalisés par les mathématiciens américains L.M. ADLEMAN et R.S. RUMELY. En collaboration avec H. COHEN (Bordeaux), j'ai développé une version simplifiée de leur méthode, version qui a été programmée pour le système d'ordinateur CDC Cyber 170-750 du centre de calcul SARA d'Amsterdam, avec la collaboration de D.T. WINTER et A.K. LENSTRA.

Avant d'aborder la théorie qui sert de base au programme, j'examine quelques exemples numériques. Ceux-ci ne sont, par eux-mêmes, guère plus que des curiosités, mais donnent tout de même une idée de ce qui actuellement, peut, ou ne peut pas, être fait.

(*) Article paru dans WISKUNDE EN ONDERWIJS (Tijdschrift van de Vlaamse Vereniging Wiskunde-
raars), n° 34, pp. 171 à 178.
Traduit du néerlandais par J. Nachtergaele. Une 2ème version de cet article a été publiée en anglais dans
NIEUW ARCHIEF VOOR WISKUNDE (4), Vol. 1, 1983, pp. 133 à 144.

$$\text{Le nombre } 10^{100} + 267 = \underbrace{100 \dots 00 267}_{97 \times}$$

est le plus petit nombre premier de 101 chiffres. Notre programme fut en mesure de prouver, en 42,8 secondes, qu'il est premier. Ceci est un temps de calcul "typique" pour des nombres de cet ordre de grandeur. Des programmes plus anciens n'étaient pas en mesure de décider si $10^{100} + 267$ est premier.

Un nombre premier typique de 200 chiffres demandera environ 6 minutes, quand notre programme sera adapté à cet objet.

$$\text{Le nombre } \frac{10^{1031} - 1}{9} = \underbrace{111 \dots 111}_{1031 \times} \text{ est très vraisemblablement premier.}$$

Ce que cela veut dire, exactement, nous l'examinerons tout à l'heure. Un calcul grossier apprend que notre méthode, sur la même machine, aurait besoin, pour ce nombre, d'environ une semaine.

Pour des nombres qui ont une forme particulière, on peut aller beaucoup plus loin. Ainsi le Dr Slowinski a démontré, avec l'aide d'un ordinateur CRAY X MP, que le nombre

$$2^{132049} - 1 = 512 \dots 311 \text{ (39751 chiffres)}$$

est premier. Cela aura demandé 65 minutes de temps de calcul. Ce nombre est à l'heure actuelle le plus grand nombre premier connu.

Tous ces exemples concernent le problème A. Le problème B est bien plus gênant. Actuellement, avec les meilleures méthodes connues, on peut décomposer en facteurs des nombres de 40 à 50 chiffres, pour la plupart, en deux heures environ, mais, pour un nombre comme

$$2^{293} - 1 = 159 \dots 791$$

qui a 89 chiffres, on ne connaît aucun diviseur premier; cependant on sait que ce nombre n'est pas premier.

Il peut paraître surprenant qu'on sache, d'un nombre, qu'il n'est pas premier, sans en connaître un diviseur. Ceci est généralement dû au théorème suivant ou à une de ses variantes :

Théorème de Fermat (Pierre de Fermat 1601-1665) :

$$n \text{ est premier} \Rightarrow \forall a \in \mathbb{Z}, a^n \equiv a \pmod{n}$$

A propos de ce théorème, il faut remarquer qu'il est aisé, même pour n très grand, — du moins pour un ordinateur, — d'examiner si la congruence $a^n \equiv a \pmod{n}$ est vérifiée. On le fait non pas en calculant a^n (ceci, même pour un ordinateur

rapide, n'est pas réalisable si $n \approx 10^{100}$ et $a = 2$) mais seulement le reste de la division de a^n par n , ce reste étant calculé par une série d'élevations au carré et de multiplications modulo n . Et si on trouve fût-ce un seul élément de \mathbb{Z} pour lequel la congruence $a^n \equiv a \pmod{n}$ n'est pas vérifiée, alors on sait avec certitude que n est pas premier, sans connaître pour autant un facteur de n .

Si on veut prouver qu'un nombre n est premier, on a besoin de la réciproque du théorème de Fermat. Ici, se présentent deux difficultés :

- I. En premier lieu, la réciproque directe où " \Rightarrow " est remplacé par " \Leftarrow " n'est pas vraie; le nombre de Ramanujan $1729 = 7 \cdot 13 \cdot 19$ n'est pas premier et cependant

$$a^{1729} \equiv a \pmod{1729} \text{ pour tout } a \in \mathbb{Z}$$

- II. En second lieu, même si la réciproque était vraie, cela ne nous aiderait guère, parce qu'il complètement irréalisable d'essayer tous les entiers a . Comment pourrions-nous surmonter ces difficultés ?

On surmonte la première en considérant une variante plus restrictive du théorème de Fermat, dont la réciproque, cette fois, est vraie.

Nous commençons par une généralisation algébrique.

Théorème : *Si n est premier, pour tout anneau commutatif A et tous éléments a et b de A , on a la congruence $(a + b)^n \equiv a^n + b^n \pmod{nA}$*

nA désigne ici l'idéal de A : $\{x + x + \dots + x \text{ (} n \text{ termes)} \mid x \in A\}$

La démonstration se fonde sur le binôme de Newton et sur la remarque que les coefficients binomiaux $\binom{n}{i}$, pour $0 < i < n$, sont divisibles par n si n est premier.

Prenons $A = \mathbb{Z}$ et $b = 1$, et nous retrouvons, par récurrence sur a , le théorème de Fermat.

On peut démontrer que la réciproque du théorème énoncé ci-dessus est vraie : "si la congruence énoncée dans le théorème est vérifiée pour tout A et pour tous a, b éléments de A , n est premier". En fait, il suffit de prendre pour A l'anneau des polynômes $\mathbb{Z}[X]$ et $a = X, b = 1$.

Avant d'aborder une généralisation, dans le domaine de la théorie des nombres, du théorème de Fermat, nous traitons quelques propriétés du symbole de Jacobi $\left(\frac{a}{n}\right)$; pour plus de détails, voir les traités, comme [2].

A partir de maintenant, nous supposons que n est impair. Si n est premier, il résulte du théorème de Fermat que

$a^{n-1} \equiv 1 \pmod{n}$ si a appartient à \mathbb{Z} et si le pgcd de a et n est 1;
donc $a^{(n-1)/2} \equiv 1$ ou $-1 \pmod{n}$.

Le symbole de Jacobi $\left(\frac{a}{n}\right) \in \{1, -1\}$ est, pour $a \in \mathbb{Z}$ et $\text{pgcd}(a, n) = 1$, défini par $\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod n$ si n est premier,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_t}\right) \text{ si } n = p_1 p_2 \dots p_t, p_i \text{ premiers.}$$

Pour la commodité, nous poserons $\left(\frac{a}{n}\right) = 0$ si $\text{pgcd}(a, n) > 1$.

Le symbole de Jacobi est l'objet d'une théorie mathématique développée par Gauss, dont le point central est la loi de réciprocité quadratique, (voir [2]). Si l'on se sert de cette loi, on peut — et il est intéressant de le savoir pour la suite, — calculer rapidement le symbole de Jacobi $\left(\frac{a}{n}\right)$, même sans connaître la décomposition de n en facteurs premiers.

De la définition de $\left(\frac{a}{n}\right)$ résulte directement le théorème suivant, plus puissant que le théorème de Fermat.

Théorème : n est premier \Rightarrow
 $(\forall a \in \mathbb{Z}, \text{pgcd}(a, n) = 1 \Rightarrow a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n)$

Ici encore, il est facile, même pour n très grand, d'examiner, en se servant de l'ordinateur, si pour a donné la congruence $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n$ est effectivement vérifiée.

D.H. LEHMER a démontré en 1976 que la réciproque du théorème ci-dessus est vraie. Plus précisément :

Théorème : *Si n est un nombre impair composé, $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod n$ pour au moins la moitié de tous les $a \in \{1, 2, \dots, n-1\}$ avec $\text{pgcd}(a, n) = 1$.*

Grâce à ces résultats, la difficulté I est résolue de manière satisfaisante.

Dans le test de nombres premiers tel qu'il est vraiment réalisé, nous travaillons en fait avec une combinaison des deux approches : nous nous servons de congruences dans les anneaux d'extension de \mathbb{Z} et ces congruences comprennent un symbole qui est une généralisation du symbole de Jacobi.

Nous restons aux prises avec la difficulté II : il reste irréalisable de tester tous les $a \pmod n$ et absolument irréalisable d'examiner tous les anneaux A .

La première méthode que nous considérons pour surmonter la difficulté II est de nature probabiliste. Elle travaille comme suit : tirons, de manière aléatoire, cent nombres a de l'ensemble $\{1, 2, \dots, n-1\}$ et pour chaque valeur tirée, vérifions si $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) = \pm 1 \pmod n$.

S'il existe fût-ce un seul a pour lequel cette congruence n'est pas vérifiée on sait avec certitude que n est composé. Si la congruence se vérifie pour les cent valeurs de a , n a une grande probabilité d'être premier.

En effet, supposons que n ne soit pas premier : dans ce cas, suivant le théorème de LEHMER, chaque a a une probabilité inférieure à $\frac{1}{2}$ de satisfaire à la congruence ci-dessus, donc la probabilité que les cent a y satisfassent est inférieure à $(\frac{1}{2})^{100}$ qui est strictement inférieur à 0,000000000000000000000000000001. Il devient difficile de douter que n soit premier.

Cette méthode, proposée par R. SOLOVAY et V. STRASSEN, n'est pas, en principe, en état de fournir une démonstration strictement mathématique du fait qu'un nombre est premier. En revanche, c'est une méthode vraiment très rapide, et on peut toujours l'appliquer avant de mettre en œuvre la méthode, très coûteuse en temps, que j'exposera tout à l'heure.

G.L. MILLER et M.O. RABIN ont proposé une amélioration du test présenté, qui atteint la même probabilité d'erreur moyennant moins de la moitié du temps de calcul.

La deuxième méthode pour surmonter la difficulté II est de nature futuriste, étant donné qu'elle s'appuie sur une présomption qui n'a pas encore été prouvée, l'hypothèse de Riemann généralisée. Celle-ci est une assertion concernant la position des zéros de certaines fonctions complexes qui interviennent dans la théorie analytique des nombres, assertion dont l'exactitude est très généralement admise, mais qui, jusqu'à présent, n'a pas encore été démontrée.

Supposant cette hypothèse vraie, G. MILLER a démontré en 1976 qu'il suffit, dans le test décrit ci-dessus, de tester uniquement les nombres a tels que $a < 70(\log n)^2$, a étant premier. Si toutes ces valeurs de a satisfont à la congruence $a^{(n-1)/2} \equiv (\frac{a}{n}) \pmod{n}$, on peut montrer, grâce à l'hypothèse de Riemann généralisée, que de fait n est premier.

Mais cette méthode prête le flanc à deux objections. En premier lieu, une évaluation grossière montre que, pour des nombres de l'ordre de 100 chiffres, elle demande environ 500 fois plus de temps que la méthode qu'on va décrire ci-après, bien que pour n beaucoup plus grand, elle soit plus rapide. En second lieu, l'hypothèse de Riemann généralisée n'est toujours pas démontrée.

Nous nous tournons maintenant vers les méthodes qui sont en mesure de prouver avec une certitude mathématique qu'un nombre est premier. Il en existe plus que je n'ai le temps d'en énumérer dans cet exposé, mais elles reposent toutes d'une manière ou d'une autre sur le théorème que voici, qui est tellement trivial que je l'ai baptisé de mon nom.

Théorème de Lenstra

n est premier \Leftrightarrow tout diviseur r de n est une puissance de n .

Pour démontrer l'implication \Rightarrow il suffit de remarquer que $1 = n^0$ et $n = n^1$; je laisse au lecteur le soin de prouver l'implication \Leftarrow .

Quel rôle ce théorème joue-t-il dans des tests de nombres premiers ? Formulé de façon imprécise, il revient à ceci :

Supposons que n satisfasse à beaucoup de conditions du type

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n};$$

Dans ce cas, on peut montrer que tout diviseur r de n se comporte, à un certain point de vue, comme une puissance de n . Dans certaines circonstances, on peut en déduire que 1 et n sont les seuls diviseurs de n , de sorte que, de fait, n est premier.

Le théorème suivant peut servir d'illustration à ce processus. Nous supposons à partir de maintenant, que n n'est pas divisible par 3 .

Théorème :

Si $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ pour $a = -1, 2$ et 3 ,

et si de plus il existe un a élément de \mathbb{Z} pour lequel $a^{(n-1)/2} \equiv -1 \pmod{n}$, alors il existe, pour tout diviseur r de n , un entier $i \geq 0$ tel que $r \equiv n^i \pmod{24}$.

La condition "il existe a élément de \mathbb{Z} tel que $a^{(n-1)/2} \equiv -1 \pmod{n}$ " ne peut être négligée, comme il ressort de l'exemple donné plus haut de 1729 . Si n est effectivement premier, il est la plupart du temps facile de trouver un entier a qui satisfasse à cette condition.

Le théorème dit que tout diviseur r de n se comporte "à un certain point de vue" (c'est-à-dire modulo 24) comme une puissance n^i de n . En fait, nous pouvons prendre $i = 0$ ou $i = 1$, car $n^2 \equiv 1 \pmod{24}$.

Je ne donne pas ici la démonstration du théorème. Il s'appuie sur l'assertion suivante, valable pour tous les entiers n_1, n_2 qui ne sont divisible ni par 2 ni par 3 :

$$n_1 \equiv n_2 \pmod{24} \Leftrightarrow \left(\frac{a}{n_1}\right) = \left(\frac{a}{n_2}\right) \text{ pour } a = -1, 2 \text{ et } 3$$

Cette assertion est une conséquence de la loi, citée plus haut, de réciprocité quadratique.

Le théorème formulé ci-dessus n'est pas très utile pour les tests de nombres premiers, parce que nous ne pouvons pas exploiter davantage la conclusion. Il serait beaucoup plus utile d'avoir un théorème analogue où le nombre 24 soit remplacé par un nombre sensiblement plus grand.

Si on analyse la démonstration du théorème — qui n'est pas donnée ici — on découvre que la propriété cruciale du nombre 24 dont dépend le théorème, est la suivante :

$$m^2 \equiv 1 \pmod{24} \text{ pour tout } m \in \mathbb{Z} \text{ et tel que } \text{pgcd}(m,24) = 1.$$

On peut montrer que 24 est le plus grand nombre qui ait cette propriété. Si l'on veut remplacer 24 par un nombre plus grand, on devra, au lieu de carrés, envisager de plus hautes puissances, et ceci conduit à considérer des symboles qui généralisent le symbole de Jacobi.

Si nous remplaçons les carrés par des puissances 12èmes, nous trouvons que 24 peut être sensiblement augmenté :

$$m^{12} \equiv 1 \pmod{65520} \text{ pour tout } m \in \mathbb{Z} \text{ et tel que } \text{pgcd}(m,65520) = 1.$$

Ici, on a $65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.

Dans le programme d'ordinateur cité au début de cet exposé, on emploie des nombres encore beaucoup plus grands

$$m^{5040} \equiv 1 \pmod{s} \text{ pour tout } m \in \mathbb{Z} \text{ et tel que } \text{pgcd}(m,s) = 1.$$

Ici, $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ et s est un nombre de 53 chiffres

$$\begin{aligned} s &= 15321986788854443284662612735663611380010431225771200 \\ &= 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 113 \cdot 127 \\ &\quad 181 \cdot 211 \cdot 241 \cdot 281 \cdot 337 \cdot 421 \cdot 631 \cdot 1009 \cdot 2521 \end{aligned}$$

Il est intéressant pour nous que $s > \sqrt{n}$ si n n'a pas plus de 100 chiffres.

Je donne maintenant une description schématique et pas trop précise du test de nombres premiers que nous avons employé. Pour les détails et les références à la littérature, qu'on veuille bien consulter [1].

Test de nombres premiers pour $n < 10^{100}$

1er pas : Tester si le plus grand commun diviseur de n et s est égal à 1, avec s choisi comme ci-dessus (on peut déterminer ce pgcd par l'algorithme d'Euclide). Si ce n'est pas le cas, n est divisible par un des facteurs premiers de s , et nous ne calculons pas davantage.

2e pas : Tester 67 congruences dont chacune est analogue à

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

en remplaçant a par des éléments bien choisis des anneaux $\mathbb{Z} [e^{2\pi i/pk}]$

avec p premier, $k \geq 1$ et p^k diviseur de $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$.

et en remplaçant $(\frac{a}{n})$ par un symbole généralisé dont les valeurs sont des puissances de $e^{2\pi i/p^k}$ (pour $p^k = 2, e^{2\pi i/p^k} = -1$ et nous retrouvons le symbole de Jacobi).

Si au moins une de ces 67 congruences n'est pas vérifiée, n est composé, et on arrête.

Supposons maintenant que les 67 congruences soient vérifiées. Elles ont été choisies de telle manière qu'on peut prouver que, pour chaque diviseur r de n , il existe $i \in \mathbb{Z}$ tel que $r = n^i \pmod{s}$, $0 \leq i < 5040$.

3e pas : Partant de cette information, nous déterminons tous les diviseurs r de n tels que $r \leq \sqrt{n}$. Il est clair que cela suffit pour décomposer n en facteurs et donc pour savoir si n est premier.

De $r \leq \sqrt{n}$ résulte que $r < s$, donc r est entièrement déterminé si nous connaissons $r \pmod{s}$. En vertu de l'information fournie par le 2e pas, nous pouvons donc procéder ainsi : déterminer, pour chaque $i = 0, 1, \dots, 5039$, le nombre r_i satisfaisant à $r_i \equiv n^i \pmod{s}$, $0 \leq r_i < s$.

Tous les diviseurs $\leq \sqrt{n}$ de n apparaissent parmi les r_i , donc nous pouvons achever l'algorithme moyennant 5040 divisions-tests.

De la description du 3e pas faite ci-dessus, on ne doit cependant pas inférer que l'algorithme peut aussi aider à décomposer des nombres en facteurs. En pratique, en effet, tous les nombres composés n seront déjà découverts au 2e (ou même au 1er) pas.

Je termine par un nombre préparé spécialement pour la journée d'études de la VVWL, un nombre de cent chiffres dont notre programme a démontré en 33,573 secondes qu'il est premier.

22120101131905002205180514090709140700230919112114
04051205180101181900110004050305130205180019820029.

BIBLIOGRAPHIE

1. H. COHEN et H.W. LENSTRA, Jr, Primality testing and Jacobi sums, *Mathematics of Computation* **42** (1984), 297-330.
2. A. SCHOLZ et B. SCHOENEBERG, Einführung in die Zahlentheorie, Sammlung Göschen Bd. 1131, Walter de Gruyter & Co, Berlin, 1955.