Tests rapides de nombres premiers

Lenstra, H.W.

TESTS RAPIDES DE NOMBRES PREMIERS (*)

Hendrik W. Lenstra, Jr

Universite d'Amsterdam

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

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

Dans le contraire, n est appele **premier** Voici deux problemes fondamentaux de la theorie elementaire des nombres

A Comment peut-on voir, rapidement, si un nombre donne est premier ?

B Si n n'est pas premier, comment trouver des entiers $a > 1$, $b > 1$ tels que $a \quad b = n$?

Bien que ces problemes se ressemblent fort, les techniques mathematiques qu'on emploie pour les resoudre different du tout au tout

Dans cet expose, je m'occuperai presque exclusivement du probleme A Des progres recents, concernant ce probleme, ont ete realises par les mathematiciens americains L M AD' FMAN et R S RUMELY En collaboration avec H COHEN (Bordeaux), j'ai developpe une version simplifiee de leur methode, version qui a ete programmee pour le systeme d'ordinateur CDC Cyber 170-750 du centre de calcul SARA d'Amsterdam, avec la collaboration de D T WINTER et A K I ENSTRA

Avant d'aborder la theorie qui sert de base au programme, j'examine quelques exemples numeriques Ceux-ci ne sont, par eux-mêmes, guere plus que des curiosites, mais donnent tout de même une idee de ce qui actuellement, peut, ou ne peut pas, être fait

---

(*) Article paru dans WISKUNDE EN ONDERWIJS (Tijdschrift van de Vlaamse Vereniging Wiskundeleraars) n° 34 pp 171 a 178
Traduit du neerlandais par I Nachtergaele Une 2eme version de cet article a ete publiee en anglais dans NIEUW ARCHIEF VOOR WISKUNDE (4), Vol 1 1983 pp 133 a 144

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

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'etaient pas en mesure de decider si $10^{100} + 267$ est premier

Un nombre premier typique de 200 chiffres demanderа environ 6 minutes, quand notre programme sera adapte à cet objet

Le nombre $\frac{10^{1031} - 1}{9} = \underbrace{111 \ldots 111}_{1031 \times}$ 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 demontre, avec l'aide d'un ordinateur CRAY X MP, que le nombre

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

est premier Cela aura demande 65 minutes de temps de calcul Ce nombre est a l'heure actuelle le plus grand nombre premier connu

Tous ces exemples concernent le problème A Le probleme B est bien plus gênant. Actuellement, avec les meilleures methodes 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

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

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) :

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

A propos de ce théoreme, il faut remarquer qu'il est aise, même pour n tres grand, — du moins pour un ordinateur, — d'examiner si la congruence $a^n \equiv a \bmod n$ est verifiee On le fait non pas en calculant a^n (ceci, même pour un ordinateur

rapide, n'est pas réalisable si $n \simeq 10^{100}$ et $a = 2$) mais seulement le reste de la division de a^n par n, ce reste étant calculé par une série d'élévations au carré et de multiplications modulo n. Et si on trouve fût-ce un seul élément de $\mathbb{Z}$ pour lequel la congruence $a^n \equiv a \bmod n$ 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 $1729 = 7.13.19$ n'est pas premier et cependant

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

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 pourrons-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* $(a + b)^n \equiv a^n + b^n \bmod nA$

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

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 réciprique 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 polynomes $\mathbb{Z}[X]$ 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 $(\frac{a}{n})$; 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

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

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

$(\frac{a}{n}) = (\frac{a}{p_1})(\frac{a}{p_2}) \ldots (\frac{a}{p_t})$ si $n = p_1 p_2 \ldots p_t$, p_i premiers.

Pour la commodité, nous poserons $(\frac{a}{n}) = 0$ si 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 $(\frac{a}{n})$, même sans connaître la décomposition de n en facteurs premiers.

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

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

Ici encore, il est facile, même pour n très grand, d'examiner, en se servant de l'ordinateur, si pour a donné la congruence $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ 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, $a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n$ pour au moins la moitié de tous les $a \in \{1,2,\ldots,n-1\}$ avec 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(mod 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 $\{1,2,\ldots n-1\}$ et pour chaque valeur tirée, vérifions si $a^{(n-1)/2} \equiv (\frac{a}{n}) = \pm 1 \bmod n$.

S'il existe fût-ce un seul a pour lequel cette congruence n'est pas verifiee on sait avec certitude que n est compose Si la congruence se verifie pour les cent valeurs de a, n a une grande probabilite d'être premier

En effet, supposons que n ne soit pas premier dans ce cas, suivant le theoreme de LEHMER, chaque a a une probabilite inferieure a $\frac{1}{2}$ de satisfaire a la congruence ci dessus, donc la probabilite que les cent a y satisfassent est inferieure a $(\frac{1}{2})^{100}$ qui est strictement inferieur a 0,00000000000000000000000000001 Il devient difficile de douter que n soit premier

Cette methode, proposee par R SOLOVAY et V STRASSEN, n'est pas, en principe, en etat de fournir une demonstration strictement mathematique du fait qu'un nombre est premier En revanche, c'est une methode vraiment tres rapide, et on peut toujours l'appliquer avant de mettre en œuvre la methode, tres coûteuse en temps, que j'exposera tout a l'heure

G L MILLER et M O RABIN ont propose une amelioration du test presente, qui atteint la même probabilite d'erreur moyennant moins de la moitie du temps de calcul

La deuxieme methode pour surmonter la difficulte II est de nature futuriste, etant donne qu'elle s'appuie sur une presomption qui n'a pas encore ete prouvee, l'hypothese de Riemann generalisee Celle-ci est une assertion concernant la position des zeros de certaines fonctions complexes qui interviennent dans la theorie analytique des nombres, assertion dont l'exactitude est tres generalement admise, mais qui, jusqu'a present, n'a pas encore ete demontree

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

Mais cette methode prête le flanc a deux objections. En premier lieu, une evaluation grossiere montre que, pour des nombres de l'ordre de 100 chiffres, elle demande environ 500 fois plus de temps que la methode qu'on va decrire ci-apres, bien que pour n beaucoup plus grand, elle soit plus rapide En second lieu, l'hypothese de Riemann generalisee n'est toujours pas demontree

Nous nous tournons maintenant vers les methodes qui sont en mesure de prouver avec une certitude mathematique qu'un nombre est premier Il en existe plus que je n'ai le temps d'en enumerer dans cet expose, mais elles reposent toutes d'une maniere ou d'une autre sur le theorème que voici, qui est tellement trivial que je l'ai baptise de mon nom

Theoreme de Lenstra

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

Pour demontrer 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 theoreme joue-t-il dans des tests de nombres premiers ? Formule de façon imprecise, il revient a ceci

Supposons que n satisfasse a beaucoup de conditions du type

$$a^{(n-1)/2} \equiv (\frac{a}{n}) \text{ mos } n,$$

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

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

Theoreme :

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

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

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

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

Je ne donne pas ici la demonstration du theoreme 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

$$n_1 \equiv n_2 \text{ mod } 24 <=> (\frac{a}{n_1}) = (\frac{a}{n_2}) \text{ pour } a = -1,2 \text{ et } 3$$

Cette assertion est une consequence de la loi, citee plus haut, de reciprocite quadratique

Le theoreme formule ci-dessus n'est pas tres 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 theoreme analogue ou le nombre 24 soit remplace par un nombre sensiblement plus grand

Si on analyse la demonstration du theoreme — qui n'est pas donnee ici — on decouvre que la propriete cruciale du nombre 24 dont depend le theoreme, est la suivante

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

On peut montrer que 24 est le plus grand nombre qui ait cette propriete Si l'on veut remplacer 24 par un nombre plus grand, on devra, au lieu de carres, envisager de plus hautes puissances, et ceci conduit a considerer des symboles qui generalisent le symbole de Jacobi

Si nous remplaçons les carres par des puissances 12emes, nous trouvons que 24 peut être sensiblement augmente

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

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

Dans le programme d'ordinateur cite au debut de cet expose, on emploie des nombres encore beaucoup plus grands

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

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

$$s = 153219867886544432846626127356636113800104312257712 00$$
$$= 2^6\, 3^3\, 5^2\, 7\, 11\, 13\, 17\, 19\, 29\, 31\, 37\, 41\, 43\, 61\, 71\, 73\, 113\, 127$$
$$181\, 211\, 241\, 281\, 337\, 421\, 631\, 1009\, 2521$$

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

Je donne maintenant une description schematique et pas trop precise du test de nombres premiers que nous avons employe Pour les details et les references a la litterature, 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 egal a 1, avec s choisi comme ci dessus (on peut determiner 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 a

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

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

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

et en remplaçant $(\frac{a}{n})$ par un symbole generalise 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 verifiee, n est compose, et on arrête

Supposons maintenant que les 67 congruences soient verifiees Elles ont ete choisies de telle maniere qu'on peut prouver que, pour chaque diviseur r de n, il existe $i \in \mathbb{Z}$ tel que $r = n^i \bmod s$, $0 \leqslant i < 5040$

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

De $r \leqslant \sqrt{n}$ resulte que $r < s$, donc r est entierement determine si nous connaissons r mod s En vertu de l'information fournie par le 2e pas, nous pouvons donc proceder ainsi determiner, pour chaque $i = 0,1, \ldots 5039$, le nombre r_i satisfaisant a $r_i \equiv n^i \bmod s$, $0 \leqslant r_i < s$

Tous les diviseurs $\leqslant \sqrt{n}$ 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 inferer que l'algorithme peut aussi aider a decomposer des nombres en facteurs En pratique, en effet, tous les nombres composes n seront deja decouverts au 2e (ou même au 1er) pas

Je termine par un nombre prepare specialement pour la journee d'etudes de la VVWL, un nombre de cent chiffres dont notre programme a demontre en 33,573 secondes qu'il est premier

$$2212010113190500220518051409070914070023091911211 4$$
$$0405120518010118190011000405030513020518001982002 9.$$

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, Einfuhrung in die Zahlentheorie, Samm lung Goschen Bd 1131, Walter de Gruyter & Co, Berlin, 1955.