EXPOSITIONES MATHEMATICAE

Expo. Math. 2 (1984) 223–234

Tests de primalité

Jean Louis Nicolas

Abstract. In the first part of this paper, classical primality tests are listed, all based on Fermat's theorem. The cryptography code of Rivest, Shamir, Adleman, pseudo primes and strong pseudo primes are also remembered.

Then the new test of Adleman and Rumely is given with a short introduction to characters and Gaussian sums. The presentation is as elementary as possible.

1 Introduction

Soit n un nombre entier naturel impair assez grand (par exemple d'une centaine de chiffres décimaux). Est-il possible de vérifier que ce nombre n est premier ou composé? La méthode classique consistant à diviser n par les nombres premiers successifs jusqu'à $\sqrt{n}$ prendrait un temps astronomique même avec les meilleurs ordinateurs actuels qui font au mieux 10^8 opérations à la seconde. $\left(\text{On sait que le nombre des nombres premiers } \leq x \text{ est à peu près égal à } \frac{x}{\log x}\right)$. Cette méthode classique, lorsqu'elle fonctionne, fournit un diviseur premier de n, et, en la répétant, la décomposition en facteurs premiers de n. Nous distinguerons le test de primalité, algorithme qui à partir de n donne comme réponse «n est premier», ou «n est composé», d'une méthode de factorisation, qui, lorsque n est composé en fournit un diviseur explicite. D'autres méthodes de factorisation que celle décrite ci-dessus et plus rapides ont été développées récemment (voir par exemple [Guy], [Knu], [Nic]). Cependant, parmi les algorithmes actuellement connus, les tests de primalité sont beaucoup plus rapides que les méthodes de factorisation.

2 Cryptographie

L'une des raisons qui a conduit a intensifier les recherches dans ce domaine est la découverte par Rivest, Shamir et Adleman, (cf. [Riv] d'une méthode de cryptographie à clé publique. Pour construire un code secret, un chef de réseau choisit deux nombres premiers p et q d'une cinquantaine de chiffres, il calcule $n=pq$ et $\phi(n)=(p-1)(q-1)$. La fonction ϕ est la fonction d'Euler; $\phi(n)$ est le nombre d'en-

0723-0869/84/030223-12$3.90

tiers naturels m, vérifiant $1 \leq m \leq n$ et premiers avec n. Il choisit un nombre d entre 2 et $\phi(n)$ et premier avec $\phi(n)$. Il calcule e tel que $ed \equiv 1 \bmod \phi(n)$. Il publie dans un annuaire n et e et garde secret p, q, $\phi(n)$, d.

N'importe qui peut envoyer un message au chef de réseau. Ce message est d'abord mis sous forme d'un (ou plusieurs) nombre M compris entre 1 et n par une méthode qui n'a pas besoin d'être compliquée et qui figure dans l'annuaire public: par exemple on remplace A par 01, B par 02, ..., Z par 26. Ensuite on calcule $C \equiv M^e \bmod n$ et on envoie le message codé C. Le chef du réseau décode C en calculant $C^d \bmod n$ qui vaut M, puisque d'après le théorème de Fermat $M^{\phi(n)} \equiv 1 \bmod n$, ce qui entraîne $M^{ed} \equiv M \bmod n$.

Toutes ces opérations, notamment le calcul d'une puissance se font très vite en ordinateur. Pour percer le code, il faut connaître d, donc $\phi(n)$, et c'est aussi difficile que de calculer les diviseurs premiers de n. La méthode tient essentiellement sur les deux points suivants: il est facile de construire de grands nombres premiers, et quasiment impossible actuellement de trouver les facteurs premiers d'un nombre de 100 chiffres.

3 Théorème de Fermat

Les tests de primalité que nous présenterons sont basés sur le théorème de Fermat:

Théorème. *Soit p premier, et a non multiple de p, alors*

$$a^{p-1} \equiv 1 \bmod p.$$

Première démonstration. Soit $n \in \mathbb{N}$, $n \geq 2$. L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ forme un groupe que l'on désigne par $(\mathbb{Z}/n\mathbb{Z})^*$ et qui a $\phi(n)$ éléments. Si a est premier avec n, alors la classe de a modulo n, $\dot{a}$, appartient à $(\mathbb{Z}/n\mathbb{Z})^*$, et dans un groupe fini, un élément élevé à la puissance cardinal du groupe est égal à l'élément neutre. Cela nous donne ici

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Lorsque n est premier, $\phi(n) = p-1$ et cela démontre le théorème.

Deuxième démonstration. On peut considérer seulement le cas où $1 \leq a \leq p-1$. Tous les termes de la suite finie $a \bmod p$, $2a \bmod p, \ldots, (p-1)a \bmod p$ sont distincts: en effet si l'on avait $xa \bmod p = ya \bmod p$ avec $1 \leq x < y \leq p-1$ cela entraînerait p divise $ya - xa = (y-x)a$ et p ne divise ni a ni $y-x$. Donc cette suite finie est une permutation de $\{1, 2, \ldots, p-1\}$. Le produit des termes de ces deux suites sont égaux et cela donne:

$$\prod_{x=1}^{p-1} (xa) \equiv \prod_{x=1}^{p-1} x \bmod p$$

donc p divise $(a^{p-1}-1)\prod_{x=1}^{p-1} x$, et comme il ne divise pas le produit des x, cela donne le théorème.

4 Nombres pseudo premiers

Le théorème de Fermat entraîne le corollaire suivant:

Corollaire. *Si a et n sont premiers entre eux, et si n ne divise pas $a^{n-1}-1$, alors n est composé.*

Ce corollaire peut montrer très rapidement qu'un nombre est composé, puisqu'il existe un algorithme de calcul de $a^{n-1} \bmod n$ qui est polynomial en $\log n$. Malheureusement, il ne marche pas toujours, comme on le verra plus loin. Le théorème de Wilson:

$$(n-1)!+1 \equiv 0 \bmod n \Leftrightarrow n \text{ premier}$$

est une condition nécessaire et suffisante de primalité. Mais on ne peut l'utiliser faute d'un bon algorithme de calcul de la factorielle.

Definition. *On dit que n est pseudo premier (p.p.) en base a, s'il est premier avec a, non premier, et vérifie: $a^{n-1} \equiv 1 \bmod n$.*

Le plus petit nombre p.p. en base 2 est $341 = 11.31$. Il est facile de voir que

$$2^{10} \equiv 1 \bmod 11 \text{ et donc } 2^{340} \equiv 1 \bmod 11$$
$$2^{5} \equiv 1 \bmod 31 \text{ et donc } 2^{340} \equiv 1 \bmod 31$$

et comme 11 et 31 divisent $2^{340}-1$, leur produit aussi divise $2^{340}-1$. On sait démontrer que pour a fixé, il existe une infinité de nombres p.p. en base a (cf. [Sie] p. 214, [Pom]).

On remarque aussi que les nombres de Mersenne, c'est-à-dire de la forme 2^p-1, où p est premier et les nombres de Fermat, c'est-à-dire de la forme $2^{2^n}+1$ qui ne sont pas premiers sont p.p. en base 2.

Définition. *On dit que n est un nombre de Carmichaël, si n est non premier, et si pour tout a premier avec n, on a $a^{n-1} \equiv 1 \bmod n$.*

Le plus petit nombre de Carmichael est $561 = 3 \cdot 11 \cdot 17$. On conjecture qu'il y a une infinité de tels nombres, mais on ne sait pas le démontrer (cf. [Pom]).

5 Une réciproque du théorème de Fermat

Théorème. *Supposons que a et n soient premiers entre eux, que $a^{n-1} \equiv 1 \bmod n$ et que pour tout diviseur premier p de $n-1$ on ait $a^{(n-1)/p} \not\equiv 1 \bmod n$. Alors n est premier.*

Démonstration. L'ensemble des $x \in \mathbb{Z}$ tels que $a^x \equiv 1 \bmod n$ forme un sous-groupe de $\mathbb{Z}$, et est donc de la forme $r\mathbb{Z}$ avec $r>0$. Les hypothèses du théorème donnent: $n-1 \in r\mathbb{Z}$ et

$$\forall p | n-1, \quad (n-1)/p \notin r\mathbb{Z}.$$

Ceci entraîne que $r=n-1$ (La première assertion entraîne $n-1=rs$; si $s \neq 1$, soit p un diviseur de s, donc de $n-1$, $(n-1)/p$ serait un multiple de r).

Maintenant les nombres $a^x \bmod n$ pour $1 \leq x \leq n-1$ sont tous distincts: Si l'on avait $a^x \equiv a^y \bmod n$ avec $1 \leq x < y \leq n-1$ on aurait $a^{y-x} \equiv 1 \bmod n$ avec $1 \leq y-x < r$ et $y-x \in r\mathbb{Z}$. On a donc

$$\{a^x \bmod n; 1 \leq x \leq n-1\} = \{m; 1 \leq m \leq n-1\}.$$

Enfin, comme a est premier avec n, a^x est premier avec n et $a^x \bmod n$ est premier avec n. Le nombre n étant tel que tous les nombres m plus petits que lui sont premiers avec lui, est donc premier.

Remarques. Si n est premier, n'importe quel a premier avec n ne convient pas toujours. En fait a doit être un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$, et il y a $\phi(n-1)$ générateurs. Après quelques essais, on arrive à trouver une valeur de a qui marche. Le plus difficile est de connaître la factorisation de $n-1$. On recherche d'abord les petits facteurs de $n-1$; soit n_1 leur produit. Alors n s'écrit $n_1 n_2$. Si $a^{n_2-1} \bmod n_2 = 1$ pour quelques valeurs de a, on peut penser que n_2 est premier et on essaie de le démontrer par le théorème ci-dessus (cf. [Knu]).

D'autres théorèmes similaires se basant sur la factorisation de $n+1$ ou de n^2+n+1 ont été donnés. (cf. [Wil]).

Le théorème ci-dessus permet de construire des nombres premiers très grands: on calcule un produit de nombres premiers connus: $P=\prod_i p_i$. On applique le théorème précédent à $n=mP+1$ pour différentes valeurs de m, et on trouve vite un nombre premier. Cette méthode ne peut être appliquée en cryptographie car il existe des méthodes de calcul des diviseurs premiers p d'un nombre lorsque les diviseurs premiers de $(p-1)$ sont petits (cf. [Guy], p. 73).

6 Tests plus récents

Lorsque n est premier, le théorème de Fermat dit que

$$a^{n-1} \equiv 1 \bmod n.$$

Que vaut $a^{\frac{n-1}{2}} = x$? On a $x^2 \equiv 1 \bmod n$, et dans le corps $\mathbb{Z}/n\mathbb{Z}$, cette équation a exactement deux racines $x = \pm 1$. On en déduit un nouveau test: Si $a^{(n-1)/2} \not\equiv \pm 1 \bmod n$, alors certainement n n'est pas premier. Ainsi 561 n'est pas premier car

$$5^{280} \equiv 67 \bmod 561.$$

Cependant il existe des nombres qui vérifient ce test pour tout a premier avec n, et qui ne sont pas premiers, par exemple 1729.

Définition. *Soit n un nombre impair. On écrit:*

$$n-1=m2^s \quad \textit{avec } m \textit{ impair.}$$

On dit que n est pseudo premier fort (p.p.f.) en base a, si

ou bien $a^m \equiv 1 \bmod n$

ou bien $\exists r,\ 0 \leq r \leq s-1$ *avec* $a^{m2^r} \equiv -1 \bmod n$.

Un nombre premier n, qui ne divise pas a, est p.p.f. en base a. En effet, considérons la suite finie: a^m, a^{2m}, ..., $a^{2^s m}$, mod n; elle se termine par 1. Ou bien tous les éléments sont égaux à 1. Ou bien soit r le plus grand entier tel que $a^{2^r m} = x$ soit différent de 1. On a $0 \leq r \leq s-1$ et $x^2 \equiv 1 \bmod n$ donc x vaut ± 1, et comme il a été choisi différent de 1, il faut -1.

Selfridge et Wagstaff ont calculé que le plus petit nombre non premier, et p.p.f. pour les bases $a \in A$ sont:

$$N_1 = 2047 = 23 \cdot 89 \qquad A = \{2\}$$

$$N_2 = 1373653 = 829 \cdot 1657 \qquad A = \{2, 3\}$$

$$N_3 = 25326001 = 2251 \cdot 11251 \qquad A = \{2, 3, 5\}$$

$$N_4 = 3215031751 = 151 \cdot 751 \cdot 28351 \qquad A = \{2, 3, 5, 7\}$$

et N_4 est le seul nombre non premier $\leq 2{,}5\ 10^{10}$ qui soit p.p.f. en base 2, 3, 5, 7. Il en résulte un test de primalité pour tous les nombres jusqu'à 10 chiffres decimaux, adaptables sur les calculettes programmables. Ce test est plus long en temps que la simple vérification que le nombre n figure dans une table de nombres premiers, mais une telle table serait très encombrante.

Enfin, il n'existe pas de nombres de Carmichaël fort: M.O. Rabin a démontré le résultat suivant (cf. [Rab]):

Théorème. *Si n n'est pas premier, le nombre de bases a, vérifiant $1 \leq a \leq n-1$ pour lesquelles n est p.p.f. est inférieur à $(n-1)/4$.*

Il déduit de son théorème le test «probabiliste» suivant: Par un générateur de nombres au hasard, on construit k nombres $a_1, \ldots, a_k$ compris entre 2 et $n-1$. Si n est p.p.f. en les bases $a_1, \ldots, a_k$, alors n est premier avec une probabilité d'erreur $\leq 4^{-k}$. Bien sûr, cette dernière phrase n'a pas de sens pour un arithméticien: Un nombre est premier, ou ne l'est pas. Les défenseurs de ce type de test disent que dans un but commercial (par exemple la cryptographie) la garantie de primalité est suffisante lorsque $k \geq 50$, et en particulier supérieure à la fiabilité des ordinateurs.

Remarquons ici que la méthode de cryptographie décrite au §2 marche si l'on choisit pour p ou q un nombre de Carmichaël au lieu d'un nombre premier. Le seul inconvénient est qu'elle risque alors d'être décodée plus facilement.

Le calcul de la probabilité se fait par analogie avec la situation suivante; on associe à un nombre premier une urne ne contenant que des boules rouges (tous les a, $1 \leq a \leq n$, sont des bases fortes) et à un nombre composé une urne contenant au plus $\frac{1}{4}$ de boules rouges et des boules noires. Le résultat suivant de probabilités est indiscutable. Si l'on pioche k fois dans l'un de ces deux types d'urnes, et si l'on ramène une boule rouge à chaque fois, la probabilité que l'urne ne contienne que des boules rouges est $\geq 1-4^{-k}$.

Théorème. *Si n n'est pas premier, et si l'hypothèse généralisée de Riemann est vraie, alors il existe a, $2 \leq a \leq 4\log^2 n$ pour lequel n est p.p.f. en base a.*

On peut déduire de ce théorème un test de primalité (cf. [Knu] ou [Coh]). Malheureusement l'hypothèse de Riemann généralisée est une des conjectures les plus célèbres et les plus difficiles des mathématiques.

7 Le test de Adleman, Rumely, Pomerance, Lenstra, Cohen

On a vu dans les tests récents que la considération de $a^{(n-1)/2}$ au lieu de a^{n-1} a amélioré grandement la situation. L'idée nouvelle ici va être de faire jouer aux petits nombres premiers p impairs, le rôle du 2 dans $(n-1)/2$.

a) Nombres premiers initiaux et Euclidiens. On choisit une famille de petits nombres p appelés initiaux. Par exemple la famille {2, 3, 5, 7, 11, 13, 17, 19} convient pour tester tous les nombres $n \leq 7 \cdot 10^{349}$. Asymptotiquement, pour tester n, il faut choisir au moins $c \log\log n$ nombres initiaux. On verra que le nombre de pas de l'algorithme est de l'ordre du produit P des nombres premiers initiaux.

Pour toute sous famille $p_{i_1}=2, p_{i_2}, \ldots, p_{i_j}$ de nombres premiers initiaux, si le nombre

$$p_{i_1} p_{i_2} \cdots p_{i_j} + 1$$

est premier, on l'appelle nombre premier Euclidien q. Pour la famille des $p \leq 19$, il y a 53 nombres q Euclidiens.

Les nombres initiaux et Euclidiens doivent être choisis de façon que Q, le produit des nombres Euclidiens soit $> \sqrt{n}$. Appelons $d(P)$ le nombre de diviseurs de P et $\omega(P)$ le nombre de diviseurs premiers de P. On a $d(P)=2^{\omega(P)}$ et d'après un résultat de G. Robin, (cf. [Rob]) a $\omega(P) \leq 1{,}38401 \dfrac{\log P}{\log\log P}$. On a ensuite

$$Q \leq \prod_{k|P}(k+1) \leq \prod_{k|P}(2k) = 2^{d(P)} P^{d(P)/2} \leq (2\sqrt{P})^{2^{1{,}4 \log P/\log\log P}}.$$

Pour avoir $Q > \sqrt{n}$, il faut choisir $P > (\log n)^{c \log\log\log n}$.

Inversement on peut montrer qu'il y a suffisamment de nombres Euclidiens associés à des nombres premiers initiaux et qu'en choisissant $P \leq (\log n)^{c' \log\log\log n}$ on aura $Q > \sqrt{n}$. Mais c'est un résultat assez difficile de théorie analytique des nombres (cf. [Adl]).

La première partie du test consiste à vérifier que les nombres premiers initiaux et euclidiens ne sont pas des diviseurs de n.

b) Caractère. Soit q un nombre premier. Le groupe multiplicatif $\mathbb{F}_q^* = \{1, \ldots, q-1\}$ est un groupe cyclique; c'est-à-dire, il existe un générateur (et en fait $\phi(q-1)$ générateurs) g tels que

$$\{g^x \bmod q;\ 1 \leq x \leq q-1\} = \{1, 2, \ldots, q-1\}.$$

On ne connaît guère de résultats sur le plus petit générateur g de $\mathbb{F}_q^*$. Il en existe des tables, et l'expérience montre qu'on le détermine assez facilement. Par exemple pour $q=7$, $g=3$ convient.

x	1	2	3	4	5	6
$3^x \bmod 7$	3	2	6	4	5	1

Tout nombre m, $1 \leq m \leq q-1$ peut donc se mettre sous la forme $g^x \bmod q$ avec $1 \leq x \leq q-1$ et ceci de façon unique. Si $m = g^x \bmod q$, x s'appelle l'indice de m en base g et vérifie la propriété du logarithme: l'indice d'un produit est égal à la somme des indices.

Sans rentrer dans une théorie générale des caractères modulaires, (cf. pour cela [Ell], ch. 7), si p divise $q-1$, on pose $\zeta_p = e^{2i\pi/p}$. La fonction χ définie sur $\mathbb{F}_q^*$ et à valeur dans $\langle \zeta_p \rangle$ = ensemble des racines $p^{\text{ièmes}}$ de $1 = \{\zeta_p^k;\ 0 \leq k \leq p-1\}$, par $\chi(g^x) = \zeta_p^x$ pour $x = 1, 2, \ldots, q-1$ est un caractère de conducteur q et d'ordre p. Les autres caractères de conducteur q et d'ordre p sont $\chi^2, \chi^3, \ldots, \chi^{p-1}$. On remarque que χ^p vaut 1. Un caractère est multiplicatif, c'est-à-dire $\chi(mm') = \chi(m)\chi(m')$.

Lorsque $p=2$, $\zeta_p = -1$, il n'y a qu'un seul caractère de conducteur q et d'ordre 2 que l'on appelle le symbole de Legendre. Si $m = g^x \bmod q$, on le note:

$$\chi(m) = \left(\frac{m}{q}\right) = (-1)^x.$$

Les éléments m de $\mathbb{F}_q^*$ pour lesquels $\left(\frac{m}{q}\right) = +1$ sont des carrés dans $\mathbb{F}_q^*$, ils correspondent aux valeurs paires de x.

c) Somme de Gauss. Soit $\zeta_q = e^{2i\pi/q}$. On définit la somme de Gauss $\tau(x)$ associée au caractère χ par:

$$\tau(\chi) = \sum_{m=1}^{q-1} \chi(m)\, \zeta_q^m.$$

La détermination des sommes de Gauss est loin d'être achevée, comme le montre l'article de synthèse [Ber]. Cependant lorsque $p=2$ on sait que

$$\tau(\chi)=\sqrt{q} \quad \text{si } q\equiv 1 \bmod 4$$

$$\tau(\chi)=i\sqrt{q} \quad \text{si } q\equiv 3 \bmod 4.$$

On a le théorème suivant:

Théorème. *Si n est premier,*

$$(\tau(\chi))^n-\chi(n)^{-n}\tau(\chi^n)\equiv 0 \bmod n\mathbb{Z}[\zeta_p,\zeta_q].$$

Remarque. Le membre de gauche s'exprime comme un polynôme de la forme $\sum_{\substack{1\le u\le p-1\\ 1\le v\le q-1}} a_{u,v}X^uY^v$ avec $X=\zeta_p$, $Y=\zeta_q$ ce qui entraîne que $X^p=1$ et $Y^q=1$. Le théorème exprime que tous les coefficients $a_{u,v}$ sont multiples de n.

Démonstration. Si n est premier, les coefficients multinomiaux sont divisibles par n, ce qui entraîne:

$$(\tau(\chi))^n\equiv\sum_{m=1}^{q-1}\chi(m)^n\zeta_q^{mn} \bmod n\mathbb{Z}[\zeta_p,\zeta_q].$$

On fait le changement de variable $t=mn$, on obtient

$$(\tau(\chi))^n\equiv\sum_{1\le t\le q-1}\chi(n^{-1}t)^n\zeta_q^t=\chi(n^{-1})^n\sum_{1\le t\le q-1}\chi(t)^n\zeta_q^t$$

où n^{-1} désigne l'inverse de n dans $\mathbb{F}_q^*$. Comme χ est multiplicatif $\chi(n^{-1})=(\chi(n))^{-1}$ et cela achève la démonstration.

Le théorème précédent joue le rôle du théorème de Fermat: Si la congruence n'est pas vérifiée, c'est que n est composé. On l'appliquera de la façon suivante:

Test. *Existe-t-il $\eta(\chi)\in\langle\zeta_p\rangle$ tel que*

$$\tau(\chi)^n-\eta(\chi)^{-n}\tau(\chi^n)\equiv 0 \bmod n\mathbb{Z}[\zeta_p,\zeta_q]?$$

Lorsque $p=2$, $\chi(m)=\pm 1$, et pour n impair $\chi^n=\chi$. Le test devient donc

$$\tau(\chi)^{n-1}\equiv\pm 1 \bmod n$$

et compte tenu de la valeur de $\tau(\chi)$,

$$q^{\frac{n-1}{2}}\equiv\pm 1 \bmod n.$$

d) Condition $\mathscr{L}_p$. Soit p un nombre premier ne divisant pas n. La condition $\mathscr{L}_p$ est vraie si pour tout r premier divisant n,

$$v_p(r^{p-1}-1)\ge v_p(n^{p-1}-1).$$

On désigne par $v_p(N)$ le plus grand exposant α tel que p^α divise N. Soit $k = v_p(n^{p-1}-1)$. Cette condition peut encore s'écrire:

$\mathscr{L}_p$: $\forall r$ premier divisant n, $r^{p-1} \equiv 1 \bmod p^k$.

Sous cette forme, on voit immédiatement qu'elle se généralise à tous les diviseurs R de n. On définit ensuite $l_p(R) \in \mathbb{Z}/p\mathbb{Z}$ par

$$l_p(R) = \frac{R^{p-1}-1}{n^{p-1}-1} \bmod p$$

c'est-à-dire, si $R^{p-1} = 1 + \lambda p^k$, $l_p(R) = \lambda \bmod p$. On a

$$l_p(RR') = l_p(R) + l_p(R')$$

et $l_p(n) = 1$.

Proposition 1. *Si le test marche (c'est-à-dire $\eta(\chi) \in \langle \zeta_p \rangle$) et si $\mathscr{L}_p$ est vraie, alors $\eta(\chi) = \chi(n)$ et pour tout diviseur R de n, $\chi(R) = \chi(n)^{l_p(R)}$.*

Proposition 2. *Si $n^{p-1} \not\equiv 1 \bmod p^2$ alors $\mathscr{L}_p$ est vraie. Si pour un certain q, tel que p divise $q-1$, on a $\eta(\chi) \neq 1$, alors $\mathscr{L}_p$ est vraie.*

La première moitié de la proposition 2 découle immédiatement du théorème de Fermat. On trouvera la démonstration de ces deux propositions dans [Len]. On voit d'après la proposition 1, que ce n'est pas la peine dans le test de vérifier que $\eta(\chi) = \chi(n)$, puisque ceci est assuré sous la condition $\mathscr{L}_p$. Enfin cette proposition 1 donne un renseignement sur un diviseur éventuel R de n.

e) Description de l'algorithme. Pour chaque p initial poser $\lambda_p = 0$

si $n^{p-1} \not\equiv 1 \bmod p^2$, poser $\lambda_p = 1$.

Pour chaque q euclidien tel que p divise $q-1$. Calculer $\eta(\chi)$

si $\eta(\chi) \notin \langle \zeta_p \rangle$ écrire «n est composé» et aller à fin
si $\eta(\chi) \neq 1$, poser $\lambda_p = 1$
q suivant.

Si $\lambda_p = 0$, essayer d'autres q premiers tels que p divise $q-1$, pour trouver un $\eta(\chi) \neq 1$. Si on n'en trouve pas, écrire «le test a échoué» et aller à fin.

p suivant.

Pour $0 \leq i \leq P-1$, s'assurer que $n^i \bmod Q$ n'est pas un diviseur non trivial de n.

Ecrire «n est premier»

f) Justification de l'algorithme. Supposons que n ait passé le test et ne soit pas premier. Il a alors un diviseur premier $r \leq \sqrt{n}$. Les nombres $l_p(r)$ existent pour tous les p initiaux, et par le théorème chinois, on peut assurer l'existence de l, $0 \leq l \leq P-1$, tel que

$l \equiv l_p(r) \bmod p$ pour chaque p initial.

On a alors,

$$\chi(r)=\chi(n)^{l_p(r)}=\chi(n)^l=\chi(n^l)$$

pour tous les caractères χ envisagés. Posons $n^l \bmod Q=r_l$ avec $0\le r_l<Q$. On a $\chi(r)=\chi(r_l)$ avec $0\le r\le\sqrt{n}<Q$.

Pour p et q fixés, que veut dire $\chi(a)=\chi(b)$? Si $a=g^x$ et $b=g^y$, cela veut dire p divise $(x-y)$. Si l'on a $\chi(a)=\chi(b)$ pour tous les caractères $\chi=\chi_{p,q}$ tels que p divise $q-1$, on aura donc, pour q fixé, $q-1$ divise $(x-y)$, c'est-à-dire $x=y$ et donc $a\equiv b \bmod q$. Si ceci est vrai pour tous les q, on aura $a\equiv b \bmod Q$.

Nous aurons donc ici $r=r_l$, puisque ces deux nombres sont dans l'intervalle $[0, Q-1]$. Or la dernière étape du test montre qu'aucun nombre r_l ne divise n.

Remarques. L'algorithme ci-dessus est probabiliste. S'il écrit «n est premier» alors cela garantit que n est premier. Mais il se peut que le test échoue. Cependant si le nombre n est premier, les valeurs de $\eta(\chi)$ se répartissent également dans $\langle\zeta_p\rangle$ pour les diverses valeurs de q, et il existe une très forte probabilité pour que le test marche. Le test probabiliste de Rabin garantissait qu'un nombre était composé, mais échouait pour certains nombres composés. Le test d'Adelman garantit qu'un nombre est premier mais échoue pour certains nombres premiers. Cependant il existe une version deterministe du test d'Adleman (cf. [Len]) plus compliquée, qui décide complètement si n est premier ou composé.

g) Calcul de $\eta(\chi)$. Lorsque $p=2$, on peut remplacer le calcul de $\eta(\chi)$ par celui de $\xi=q^{n-1/2} \bmod n$, avec les mêmes propriétés, c'est-à-dire: si $\xi\neq\pm 1$, écrire n est composé, et si $\xi=-1$, poser $\lambda_p=1$. En fait on a $\eta=\xi$ sauf si $n\equiv q\equiv 3 \bmod 4$, mais dans ce cas la condition $\mathscr{L}_2$ est automatiquement réalisée.

Lorsque $p\neq 2$, on peut grandement simplifier le calcul de $\eta(\chi)$ en utilisant le symbole de Jacobi, qui permet de travailler dans $\mathbb{Z}[\zeta_p]$ et comme p est petit, cela est relativement facile. Si χ et χ' sont deux caractères de conducteur q, on définit la somme de Jacobi:

$$j(\chi,\chi')=\sum_{2\le x\le q-1}\chi(x)\chi'(1-x).$$

La somme de Jacobi est reliée aux sommes de Gauss par la formule: Si $a, b\in\mathbb{Z}$ et p ne divise pas $ab(a+b)$,

$$j(\chi^a,\chi^b)=\frac{\tau(\chi^a)\tau(\chi^b)}{\tau(\chi^{a+b})}.$$

Soit G le groupe de Galois de l'extension $Q(\zeta_p)$ sur $\mathbb{Q}$. G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$, et l'élement $\sigma_x\in G$ agit sur ζ_p par

$$\zeta_p^{\sigma_x}=\zeta_p^x.$$

Un élément de $\mathbb{Z}[\zeta_p,\zeta_q]$, comme par exemple $\tau(\chi)$, s'écrit

$$\varrho = \sum_{m=0}^{p-1} A(m)\,\zeta_p^m \quad \text{avec } A(m) \in \mathbb{Z}[\zeta_q]$$

et σ_x agit sur ϱ par:

$$\varrho^{\sigma_x} = \sum_{m=0}^{p-1} A(m)\,\zeta_p^{mx}.$$

On voit que cette action revient à permuter les valeurs de $A(m)$.

On définit ensuite l'anneau $\mathbb{Z}[G]$ qui est l'ensemble des éléments de la forme $\mu = k_1\sigma_{x_1} + k_2\sigma_{x_2} + \ldots + k_j\sigma_{x_j}$. Un tel élément agit sur ϱ par:

$$\varrho^{\mu} = (\varrho^{\sigma_{x_1}})^{k_1}(\varrho^{\sigma_{x_2}})^{k_2}\ldots(\varrho^{\sigma_{x_j}})^{k_j}.$$

On a ainsi:

$$j(\chi^a, \chi^b) = \tau(\chi)^{\sigma_a + \sigma_b - \sigma_{a+b}}$$

et le test du c) s'écrit:

$$(\tau(\chi))^{n-\sigma_n} \equiv \eta(\chi)^{-n} \bmod \mathbb{Z}[\zeta_p, \zeta_q]$$

en remarquant que $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)q$ et donc que $\tau(\chi)$ est inversible modulo n. On est donc amené à chercher deux éléments α et β de $\mathbb{Z}[G]$ tels que

$$j(\chi^a, \chi^b)^{\alpha} = \tau(\chi)^{\beta(n-\sigma_n)} \quad \text{et} \quad \zeta_p^{\beta} \neq 1.$$

Par un calcul dans $\mathbb{Z}[G]$, (voir [Coh], p. 19), on peut prendre $a = b = 1$,

$$\alpha = \sum_{1 \le x \le p-1} \left[\frac{nx}{p}\right] \sigma_x^{-1}$$

$$\beta = \sum_{p/2 < x \le p-1} \sigma_x^{-1}$$

où $[w]$ est la partie entière de w et σ_x^{-1} est l'inverse dans G de σ_x. On a alors

$$j(\chi, \chi)^{\alpha} \equiv \eta(\chi)^{-\beta_1 n} \bmod n$$

avec $\beta_1 = 2\dfrac{2^{p-1}-1}{p}$. La condition $\zeta_p^{\beta} \neq 1$ est assurée si p ne divise pas β_1, ce qui est réalisé pour tous les $p \le 10^9$ excepté 1093 et 3511.

Le calcul de $j(\chi, \chi)$ est fait une fois pour toutes, et le calcul de $\eta(\chi)$ se fait en un nombre de pas polynomial en $\log n$.

h) Remarques finales. Le même algorithme a été étudié par H. Cohen et H.W. Lenstra en y ajoutant des exposants aux nombres premiers initiaux et Euclidiens. Ils remplacent P par un nombre t pair et Q par

$$e(t) = 2 \prod_{\substack{q \text{ premier} \\ q-1 \mid t}} q^{v_q(t)+1}.$$

Cela permet d'accélérer l'algorithme en pratique, mais la théorie se complique et notamment le cas $p=2$ très simple ici, devient le plus difficile à traiter. On trouvera dans [Coh] un algorithme détaillé de cette méthode. En théorie, le nombre d'opérations de ce test est encore de l'ordre de $(\log n)^{c \log\log\log n}$, et l'existence d'un test de primalité polynomial en le nombre de chiffres de n n'est pas encore prouvée.

On peut voir, en conclusion, que l'utilisation des ordinateurs, et surtout les méthodes de cryptographie ont conduit les mathématiciens à intensifier leurs recherches dans un domaine de l'arithmétique – la recherche des facteurs premiers – qui n'intéressait, il y a 15 ans que les amateurs de curiosités scientifiques.

References

[Adl] L.M. Adleman, C. Pomerance, R.S. Rumely. – On distinguishing prime numbers from composite numbers. – Annals of Mathematics, vol. 117, 1983, p. 173–206.

[Ber] B.C. Berndt, R.J. Evans. – The determination of Gauss sums. – Bull. Amer. Math. Soc. new series, vol. 5, n° 2, 1981, p. 107–129.

[Coh] H. Cohen. – Test de primalité d'après Adleman, Rumely, Pomerance et Lenstra. – Publication du Laboratoire de Math. pures de l'Université Scientifique et Médicale de Grenoble. – Juin 1981.

[Ell] W.J. Ellison, M. Mendes-France. – Les nombres premiers. – Hermann, Paris, 1975. – Publications de l'Institut de Mathématiques de Nancago, IX.

[Guy] R.K. Guy. – How to factor a number. – Congressus Numerantium XVI, Proc. Fifth Manitoba Conf. on Numerical Math. Winnipeg, 1976, p. 49–89.

[Knu] D.E. Knuth. – The art of computer programming. – Vol. 2, seminumerical Algorithms, 2nd edition, Addison Wesley, 1981.

[Len] H.W. Lenstra, Jr. – Primality testing Algorithms (after Adleman, Rumely and Williams). – Séminaire Bourbaki, 33ème année, Juin 1981, n° 576.

[Nic] J.L. Nicolas. – Une méthode de factorisation utilisant les formes quadratiques à discriminant positif. – l'Iremois n° 6, p. 3–12. Publication de l'I.R.E.M. de Limoges.

[Pom] C. Pomerance, J.L. Selfridge, S.S. Wagstaff, Jr. – The Pseudoprimes to 25.10^9. – Math of Comp. Vol 35, n° 151, 1980, p. 1003–1026.

[Rab] M.O. Rabin – Probabilistic Algorithm for Testing Primality. – Journal of Number Theory 12, 1980, p. 128–138.

[Riv] R.L. Rivest, A. Shamir, L. Adleman. – A method for obtaining digital signatures and Public-Key cryptosystems. – Com. A.C.M. Fév. 1978, v. 21, n° 2, p. 120–126.

[Rob] G. Robin. – Estimation de la fonction de Tchebychef θ sur le k^{ieme} nombre premier, et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de n. À paraître. – Acta Arithmetica, Vol. 42, n° 4, 1983.

[Sie] W. Sierpinski. – Elementary number theory. – Warszawa 1964.

[Wil] H.C. Williams. – Primality testing on a computer. – Ars Combinatoria, Vol. 5, 1978, p. 127–185.

Received 16.5.83

Département de Mathématiques
Université de Limoges
123, Avenue A. Thomas
F-87060 Limoges Cedex