I.R.E.M. A.P.M.E.P

UNIVERSITE DE NANTES
Faculté des Sciences et des Techniques
Département de Mathématiques et d'Informatique

* * *

Séminaire de Mathématiques. Conférence du 4 Avril 1990

*

Philippe BARKAN

UNE EXCURSION DANS LA THEORIE DES NOMBRES

UNE EXCURSION DANS LA THEORIE DES NOMBRES

par Philippe BARKAN

Si A est un anneau intègre et K son corps des fractions , A est dit annaau des entiers de K . Parmi les problèmes réputés intéressants il y a le problème de la factorisation d'éléments de K par des éléments de A, qui est lié au problème de la détermination des éléments premiars de A .On s'intéresse ici au problème de la détermination des éléments premiers de $\mathbb{Z}$, qui se réduit en fait à leur étude dans $\mathbb{N}$.

On définit un nombre premier dans $\mathbb{N}$ comme un nombre qui n'a que deux diviseurs distincts , 1 et lui même . Par exemple 2 , 3 , 5,...,1789 ,... sont premiers . Un nombre différent de 1 qui n'est pas premier est dit composé .

Le théorème fondamental de l'arithmétique dit que tout entier naturel supérieur à 1 est produit de puissances de nombres premiers d'une manière unique à l'ordre près , ce qui explique l'importance des nombres premiers .

On sait depuit EUCLIDE (315? - 255? av. J.C.) que l'ensemble P des nombres premiers de N est infini . Pour le montrer on remarque d'abord que l'ensemble des diviseurs > 1 d'un nombre n est non vide (il contient n si $n > 1$) .Il a donc un plus petit élément (car N est "bien ordonné"). Ce plus petit diviseur > 1 est nécessairement premier . Supposons P fini, $P = \{ 2,3,5,\ldots, p_n \}$. On forme les nombres $P_n = 2.3.5\ldots p_n + 1$ (ou encore $Q_n = 2.3.5\ldots p_n - 1$). Ils ont chacun un plus petit diviseur premier p qui est différent des nombres de P .Sinon on aurait $p \mid P_n$ et $p \mid 2.3.5\ldots p_n$ d'où $p \mid (P_n - 2.3.5\ldots p_n)$, soit $p \mid 1$, ce qui est exclu par définition d'un nombre premier . Donc $p > p_n$, c'est à dire que pour tout nombre premier il en existe un plus grand . P est donc infini .

Le nombre P_n est parfois premier . Les seules valeurs de $p_n \leqslant 1031$ rendant P_n premier sont 2 , 3 , 5 , 7 , 11 , 31 , 379 , 1019 , 1021 . De même Q_n est premier pour 2 , 3 , 5 , 11 , 13 , 41, ... , 337 ,...

La preuve d'Euclide admet une infinité de variantes . Au lieu de P_n ou Q_n , on peut prendre $n! + 1$ ou $n! - 1$ ou ppcm (1, 2, 3, ... , n) ± 1 . Voir [A1].

Le crible d'ERATOSTHENE (284 - 192 av. J.C.)

La première méthode de détermination de la suite des nombres premiers est celle d'Eratosthène .

Par cette méthode , dite du crible d'Eratosthène , on trouve tous les nombres premiers impairs inférieurs à N donné, par les règles :

(1) Ecrire les entiers impairs de 3 à N .

(2) Barrer 3^2 et tous les multiples de 3 au delà , puis barrer 5^2 et tous les multiples de 5 au delà de 5^2 .

(3) Continuer jusqu'à ce que le premier nombre restant suivant celui dont les multiples ont été barrés a son carré supérieur à N .

Cette méthode permet de déterminer tous les nombres premiers inférieurs à N en $O(N \ln \ln(\sqrt{N}))$ opérations ,mais quand N est grand cette estimation ne tient pas compte de la très grande mémoire nécessaire qui croît sans limite supérieure . Quand N est grand (10^{11} p.ex.) il faut procéder par criblage de progressions arithmétiques de même raison , par exemple 30n + 1, + 7,+11,+13,+17,+19,+23 .

Une conséquence directe de cette méthode est donnée par le calcul direct du nombre de nombres premiers inférieurs à N , noté $\pi(N)$. Si (p_n) est la suite croissante des nombres premiers et si $p_k < \sqrt{N} < p_{k+1}$ on a

$$\pi(N) - \pi(\sqrt{N}) = N - 1 - \sum_{1 \leq i \leq k} \mathrm{Int}\left(\frac{n}{p_i}\right) + \cdots$$

$$+ \sum_{1 \leq i_1 < i_2 \leq k} \mathrm{Int}\left(\frac{n}{p_{i_1} p_{i_2}}\right) - \cdots + (-1)^k \mathrm{Int}\,\frac{n}{p_1 p_2 \cdots p_k}$$

Cette formule donne $\pi(N)$ connaissant les nombres premiers inférieurs à $\sqrt{N}$.

Par une variante de cette formule , on obtient le tableau suivant :

N	$\pi(N)$	N	$\pi(N)$
10^2	25	10^{10}	455 052 511
10^3	168	10^{11}	4 118 054 813
10^4	1 229	10^{12}	37 607 912 018
10^5	9 592	10^{13}	346 065 536 839
10^6	78 498	10^{14}	3 204 941 750 802
10^7	664 579	10^{15}	29 844 570 422 669
10^8	5 761 455	10^{16}	279 238 341 033 925
10^9	50 847 534	4.10^{16}	1 075 292 778 753 150

Détermination des nombres premiers par divisions .

L'idée est implicite dans le crible d'Eratosthène mais Léonard de Pise (1202) semble avoir été le premier à remarquer dans un écrit publié que pour déterminer la primalité de N , on n'a besoin que d'effectuer les essais de division par les nombres premiers $\leqslant \sqrt{N}$. Cette méthode ewt trop lente pour des nombres de 25 chiffres ou plus , mais peut servir en association avec d'autres tests .

Les nombres premiers jumeaux .

En examinant une table de nombres premiers on constate la présence de couples $(p , p + 2)$ avec p et $p + 2$ premiers . Par exemple (11 , 13) , (107 , 109). De tels nombres sont dits premiers jumeaux . Il existe de grands nombres premiers jumeaux . Par exemple les nombres de 1040 chiffres décimaux [A2], [A3] : $256200945.2^{3426} \pm 1$ sont de ce type . On ignore s'il en existe une infinité , mais la série $\sum_{\substack{p \in P \\ \text{et } p+2 \in P}} \left(\frac{1}{p} + \frac{1}{p+2} \right)$ est convergente [A4] alors que la série $\sum_{p \in P} \frac{1}{p}$ est divergente .

Les nombres parfaits et les nombres de Mersenne.

Les nombres parfaits , connus depuis Euclide , sont des entiers naturels égaux à la somme de leurs diviseurs propres . Par exemple : $6 = 1 + 2 + 3$ et aussi $28 = 1 + 2 + 4 + 7 + 14$. Euclide montra que si $N = 2^{n-1}(2^n - 1)$ et si $2^n - 1$ est premier , alors N est parfait . EULER (1707 - 1783) montra que les nombres parfaits pairs doivent être de cette forme . Un nombre parfait impair , s'il en existe, est $> 10^{50}$ et on conjecture qu'il n'y en a pas .

Si $M_n = 2^n - 1$ est premier , alors n doit être premier . La réciproque est fausse car $2^{11} - 1 = 23.89$.

Les nombres de la forme $2^p - 1$ avec p premier sont dits nombres de MERSENNE (1588 - 1648) parce que cet auteur a proposé sans preuve une liste d'entiers premiers de ce type (avec trois omissions et deux erreurs) . le problème de la détermination de ces nombres date d'au moins 1644 . Par division puis à l'aide de tests de primalité énoncés par Edouard LUCAS en 1876 , on a trouvé 31 nombres premiers de ce type .

M_p est premier pour $p = 2 , 3 , 5 , 7 , 13 , 17 , 19 , 31 , 61 , 89 , 107 , 127 , 521 , 607 , 1279 , 2203 , 2281 , 3217 , 4253 , 4423 , 9689 , 9941 , 11213 , 19937 , 21701 , 23209 , 44497 , 86243 , 110503 , 132049 , 216091$. La liste est complète pour $p \leqslant 132049$. Le dernier a 65050 chiffres décimaux et a été le plus grand nombre premier connu jusqu'au 6 août 1989, date de la découverte du nombre premier $391581 . 2^{216193} - 1$, qui a 65087 chiffres en base dix . [A6]
On verra plus loin un test qui permet son identification .

La conjecture de Mersenne modifiée a reparu récemment [A7] .

En 1965 , J.M.GANDHI a trouvé une formule de récurrence donnant la suite des nombres premiers

$$p_{n+1} = \left[1 - \log_2 \left(\frac{1}{2} + \sum_{r=1}^{n} \sum_{1 \leq i_1 < i_2 \cdots < i_r} \frac{(-1)^r}{2^{p_{i_1} \cdots p_{i_r}} - 1} \right) \right]$$

dans laquelle $[x]$ désigne la partie entière de x. [A 8].

En 1837 , P.G.LEJEUNE-DIRICHLET a montré par une méthode analytique que toute suite arithmétique (an + b) où (a,b) = 1 , contient une infinité de nombres premiers .[A 9]

On ignore cependant s'il existe une infinité de nombres premiers de la forme $4n^2 + 1$, ou plus généralement dans la suite des valeurs prises par un polynôme à valeurs entières .

Les nombres de FERMAT

En 1640 , Pierre de FERMAT conjectura que $F_n = 2^{2^n} + 1$ est toujours premier , en remarquant que c'est vrai pour $0 \leq n \leq 4$.

L'intérêt des mathématiciens pour ces nombres est motivé par le remarquable résultat de C.F.GAUSS : Un polygône avec un nombre premier de côtés de la forme F_n peut se construire avec une règle et un compas . On peut ainsi construire les polygones réguliers dont le nombre de côtés est un diviseur de $2^k.3.5.17.257.65537$ multiplié par d'autres F_n premiers , s'il en existe .

Mais la conjecture de FERMAT s'est révélée fausse car,en 1732,L.EULER découvre que $F_5 = 641.6700417$. Depuis on a montré que F_n est composé pour $5 \leq n \leq 19$ et pour une cinquantaine de valeurs de n plus grandes. On est plutôt de l'avis que F_n est composé pour tout $n \geq 5$.[A 10].

En 1878, Edouard LUCAS a montré que les facteurs premiers possibles de F_n sont de la forme $k.2^{n+2} + 1$, ce qui , par essais successifs , permet de montrer que le plus petit facteur de F_{6537} est $17.2^{6539} + 1$.

On a montré que

F_6 = 274 177 . 67 280 421 310 721 (CLAUSEN 1844 , LANDRY 1880)

F_7 = 59 649 589 127 497 217 . 5 704 689 200 685 129 054 721 (BRILLHART 1970)

F_8 = 1 238 926 361 552 897 . (premier de 62 chiffres) [A12]

$F_{13} = 0 \pmod{2\,710\,954\,639\,361}$

$F_{17} = 0 \pmod{31\,065\,037\,602\,817}$

La factorisation de F_7 a été obtenue par une méthode utilisant les fractions continues . [A 13]

Pour d'autres facteurs voir [A 10] et [A 11]

Le théorème de FERMAT-EULER

Soit n un entier naturel , et soit φ la fonction indicateur d'EULER telle que $\varphi(n)$ est le nombre d'entiers naturels inférieurs à n et premiers avec n .

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ alors on montre que

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1)$$

ou

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

En particulier si p est premier $\varphi(p) = p - 1$.

Théorème 1 (Le "petit" théorème de Fermat)

Si p est un nombre premier et a est un entier premier à p, alors

$$a^{p-1} \equiv 1 \pmod{p}$$

Théorème 2 (Euler)

Soit m un entier naturel et a un entier premier à m , alors

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Pour une démonstration voir [14] p.54-55 ou [8]

Calcul de a^n modulo p pour (a , p) = 1

Pour calculer les restes modulo p d'une puissance a^n avec $n > 1000$ par exemple on a besoin d'un algorithme plus rapide que le calcul à l'aide de n - 1 multiplications par a et autant de réductions modulo p .

Il existe plusieurs méthodes pour lesquelles le nombres d'opérations est proportionnel au nombre de chiffres de n en base deux .

A) L'algorithme suivant est presque optimal . Soit par exemple à calculer a^{23}:

$23 = 2x11 + 1$, $11 = 2x5 + 1$, $5 = 2x2 + 1$, $2 = 2x1 + 0$, $1 = 2x0 + 1$

d'où $23_{dix} = 10111_{deux}$ et

$23 = ((((\,0x2 + 1)x2)x2 + 1)x2 + 1)x2 + 1$

En partant de $a^0 = 1$ on a donc

$$a^{23} = (((((a^0)^2 x\, a)^2)^2 x\, a)^2 x\, a)^2 x\, a$$

Notons Q l'élévation au carré et M la multiplication par a . En partant de $a^0 = 1$, on obtient a^{23} par la suite d'opérations

QMQQMQMQM

Cette suite d'opérations se déduit immédiatement de la représentation de 23 en base deux : on remplace 1 par QM et 0 par Q .

L'inconvénient de cette méthode est qu'il faut avoir trouvé tous les chiffres en base deux pour calculer la puissance.

B) L'algorithme suivant , dû à E.W.DIJKSTRA en 1972 ,qui porte le nom d'exponentiation indienne , n'a pas cet inconvénient . Voir [6] p.70.

Soit par exemple à calculer a^{90}. On a successivement :

$90 = 2x45 + 0$, $45 = 2x22 + 1$, $22 = 2x11 + 0$, $11 + 2x5 + 1$

$5 = 2x2 + 1$, $2 = éx1 + 0$, $1 = 2x0 + 1$.

De là

$$a^{90} = a^{2x45 + 0}$$

$$= a^{2(x22 + 1)} = a^{2^2 x\ 22\ +\ 2^1}$$

$$= a^{2^2(2x11 + 0) + 2} = a^{2^3 x11 + 2^1}$$

$$= a^{2^3(2x5 + 1) + 2} = a^{2^4 x5\ +\ 2^3 + 2}$$

$$\equiv a^{2^4(2x2 + 1) + 2^3 + 2} = a^{2^5 x2 + 2^4 + 2^3 + 2}$$

$$= a^{2^6 + 2^4 + 2^3 + 2} = a^{64 + 16 + 8 + 2}$$

Chacune des puissances de 2 qui apparaissent provient d'un quotient impair donnant un reste 1 .

Le programme BASIC suivant donne A^N modulo P pour N , A , $P < 10^5$.

```
1Ø  INPUT  N , A , P
15  Y = 1 , Z = A
2Ø  R = N - 2 * INT(N/2)
3Ø  N = INT(N/2)
4Ø  IF R = Ø   THEN 7Ø
5Ø  Y = Y * Z 6 P * INT ((Y * Z)/P)
6Ø  IF N = Ø   THEN PRINT Y
7Ø  Z = Z * Z - P * INT ((Z * Z)/P)
8Ø  GOTO 2Ø
9Ø  END
```

Exemples :

N = 280 , A = 5 , P = 561 donne $5^{280} \equiv 67 \pmod{561}$

N = 9990 , A = 2 , P = 9991 donne $2^{9990} \equiv 3362 \pmod{9991}$

Pour ces deux algorithmes le nombre d'opérations est proportionnel au nombre de chiffres en base deux de N , c'est à dire à $\log_2(N)$, donc aussi à $\ln(N)$. Ces deux algorithmes ne sont pas optimaux .Par exemple le calcul de a^{31} nécessite 5 multiplications et 5 élévations au carré par ces deux algorithmes alors que a^{31} se calcule avec 8 multiplications par axaxa = a^3 = b, bxbxb = a^9 , $a^9 x a = a^{10}$, $a^{10} x\ a^{10} x\ a^{10} = a^{30}$, $a^{30} x\ a = a^{31}$.

Les nombres pseudo-premoers et les nombres de Carmichaël.

F. Sarrus fit en 1819 la remarque que la congruence $2^{n-1} \equiv 1 \pmod{n}$ peut être vérifiée pour certains nombres composés , par exemple pour $n = 341$. En effet $341 = 11.31$ et $2^{10} - 1 = 1023 = 3.11.31$ d'où $2^{10} \equiv 1 \pmod{341}$ donc $2^{340} \equiv 1 \pmod{341}$.

Cela montre que le théorème de FERMAT est une condition nécessaire mais pas suffisante pour que n soit premier .

On peut montrer qu'il y a une infinité de nombres composés m tels que la congruence $b^{m-1} \equiv 1 \pmod{m}$ est vérifiée pour certaines valeurs de b . Ces nombres m sont dits pseudo- premiers en base b .

Il existe aussi des nombres composés m tels que $b^{m-1} \equiv 1 \pmod{m}$ pour tout b premier avec m . De tels nombres sont appelés nombres de Carmichaël, du nom du mathématicien qui a mis cette propriété en évidence [A 14].

Les sept nombres de Carmichaël inférieurs à 10000 sont : $561 = 3.11.17$, $1105 = 5.13.17$, $1729 = 7.13.19$, $2465 = 5.17.29$, $2821 = 7.13.31$, $6601 = 7.23.41$ et $8911 = 7.19.67$

Le théorème suivant permet de construire des nombres de Carmichaël :

THEOREME . - Une condition nécessaire et suffisante pour que m soit un nombre de Carmichaël est que

$$m - 1 \equiv 0 \pmod{(p_i - 1)}$$

pour tout nombre premier p_i divisant m .

On ignore s'il existe une infinité de tels nombres . Le tableau ci-dessous compare la croissance du nombre $C_2(N)$ du nombre de pseudo-premiers en base 2 inférieurs à N , du nombre $C(N)$ de nombres de Carmichaël inférieurs à N et de $\pi(N)$, nombre des nombres premiers $< N$.

N	$C_2(N)$	$C(N)$	$\pi(N)$
10^3		1	168
10^4	22	7	1229
10^5	78	16	9592
10^6	245	43	78498
10^7	750	105	664579
10^8	2057	255	5761455
10^9	5597	646	50847534
10^{10}	14884	1547	455052511
$2,5 \times 10^{10}$	21853	2163	

On conjecture que $C(N) \geq C_0 \dfrac{\sqrt[3]{N}}{(\ln N)^3}$

On sait qu'un nombre de Carmichaël a au moins trois facteurs premiers distincts , qu'il est impair et sans facteur premier carré .

D.SHANKS remarque([22] p.229) que les nombres $n(m) = (6m+1)(12m+1)(18m+1)$ sont tous des nombres de Carmichaël si les trois facteurs sont premiers , ce qui a lieu pour $m = 1 , 6 , 35 , 45 , 51 , 55 , 100 , 121 , 206 , \ldots$

De même si

$$n_k(m) = (6m+1)(12m+1) \prod_{i=1}^{k-2} (9.2^i m + 1)$$

si tous les facteurs sont premiers et si $2^{k-4} \mid m$ ($k \geqslant 4$) , alors $n_k(m)$ est un nombre de Carmichaël .

La congruence $b^{m-1} \equiv 1 \pmod m$ ne permettant pas de caractériser les nombres premiers on a cherché d'autres critères donnant une condition suffisante de primalité .

Tests de primalité,

On sait par le théorème de WILSON (1741-1793) qu'une condition nécessaire et suffisante pour qu'un nombre p soit premier est que

$$(p-1)! \equiv -1 \pmod p$$

soit aussi $(p-2)! \equiv 1 \pmod p$

Pour une preuve voir [8]p. 87, ou [14] p. 65.

Si p est impair , la première congruence peut aussi s'écrire

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

De même si a et b sont tels que $a + b = p - 1$, p impair , on a

$$a!b! \equiv (-1)^{a+1} \pmod p$$

Ces critères , intéressants du point de vue théorique ,sont impraticables dès que $p > 100$ car on ne connait pas de formule de duplication pour la fonction factorielle (pour un argument entier), ou pour les coefficients du binôme, qui réduirait par dichotomie le nombre de multiplications et de réductions modulo p à un multiple du nombre de chiffres en base deux de p , c'est à dire en $O(\ln p)$ opérations.

On connait aussi des critères du même type pour les nombres premiers jumeaux les triplets , les quadruplets , avec le même inconvénient. Par exemple :

p et p + 2 sont premiers jumeaux si et seulement si

$$4((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}$$

Il existe des réciproques partielles du théorème de Fermat , c'est à dire des conditions suffisantes pour qu'un entier soit premier .

Définition . - Soient a et m deux entiers naturels premiers entre eux. Si $a^d \equiv 1 \pmod m$ pouruun entier $d > 1$ et si $a^x \equiv 1 \pmod m$ pour $1 < x < d$ on dit que d est l'ordre de a modulo m , et on note $d = \mathrm{ord}_m(a)$.

THEOREME [8] p.71 :

(1) Si $d = \mathrm{ord}_m(a)$, alors $d \mid \varphi(m)$.

(2) La congruence $a^x \equiv 1 \pmod m$ est vraie ou fausse suivant que x est ou n'est pas multiple de d .

Le théorème suivant , dû à Edouard LUCAS en 1878 [A16] p.302 , donne une condition suffisante de primalité :

THEOREME . - Si pour un choix de a

(1) $$a^{m-1} \equiv 1 \pmod m$$

et si $a^{(m-1)/d} \not\equiv 1 \pmod m$ pour tout diviseur $d > 1$ de $m - 1$, alors m est premier .

Si (1) est faux pour une valeur de a , alors m est composé .

Preuve : Soient a et m premiers entre eux . Si $h = \mathrm{ord}_m(a)$ alors $h \mid (m-1)$ et $h \mid \varphi(m)$ d'après le théorème précédent . Puisque $a^h \equiv 1 \pmod m$, on doit avoir $h = m - 1$. Par suite $(m-1) \mid \varphi(m)$. Mais $\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$ est inférieur à $m - 1$ strictement si m est composé . Par suite m doit être premier . □

Remarques :

1) si m a été prouvé premier de cette façon , a est une racine primitive modulo m , c'est à dire un générateur du groupe cyclique $((\mathbb{Z}/m\mathbb{Z})^*, x)$.
2) Ce critère nécessite $0 (\ln m)$ multiplications et réductions modulo m , mais il faut connaître tous les facteurs premiers de $m - 1$.
3) La condition $a^{(m-1)/d} \not\equiv 1 \pmod m$ n'est pas nécessaire pour que m soit premier . Si par exemple $m = 127$, on a $2^{(m-1)/18} = 2^7 \equiv 1 \pmod{127}$ mais 127 est premier .

Le théorème suivant est pratique si $m - 1$ a un grand facteur premier .

THEOREME (PROTH , 1878 , [A 17]) . - Soient a et m premiers entre eux . Si $a^{(m-1)} \equiv 1 \pmod m$, si $m - 1 = kp$ où p est premier $> \sqrt{m}$ et si $a^k \not\equiv 1 \pmod m$, alors m est premier .

Si l'on est moins chanceux , on ne connaît que certains facteurs de $m - 1$. Dans ce cas une ou plusieurs applications du théorème précédent peuvent suffire à restreindre les facteurs premiers possibles de m à un point où leur inexistence complète peut être établie .

Si m appartient à certaines classes de nombres , on peut obtenir certaines conditions nécessaires et suffisantes pour que m soit premier :

THEOREME ([8] p.79)

Soit $n \geq 2$, k impair $< 2^n$ et $m = k.2^n + 1$ un non reste quadratique modulo p , pour un p premier impair . Alors une condition nécessaire et suffisante pour que m soit premier est que

$$p^{\frac{m-1}{2}} \equiv -1 \pmod{m}$$

Pour $k = 1$, $n = 2^r$ on a $m = F_r$ nombre de Fermat . On peut prendre $p = 3$ ou $p = 5$ dans le théorème précédent d'où le

COROLLAIRE . - Pour que le nombre $F_n = 2^{2^n} + 1$ soit premier , il faut et il suffit que

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$$

Pour les nombres de la forme $m = k.2^n - 1$, il faut utiliser les diviseurs de $m + 1$. Il existe un algorithme légèrement plus compliqué , basé sur la théorie des suites récurrentes linéaires du second ordre à coefficients constants . Cela donne un calcul seulement trois fois plus long que le précédent donc également en $0 (\ln m)$ opérations .

THEOREME . - Soit m un entier impair et soit b choisi de telle sorte que

$$\left(\frac{b}{m} \right) = \left(\frac{1 - 4b}{m} \right) = -1 \quad \text{(Symboles de Jacobi)}$$

Soient α et β les racines de $X^2 - X + b = 0$ et soit $v_n = \alpha^n + \beta^n$.

Supposons ensuite

(1) $$v_{\frac{m+1}{2}} \equiv 0 \pmod{m}$$

et

(2) $$v_{2\frac{m+1}{q}} \not\equiv 2\, b^{\frac{m+1}{q}} \pmod{m}$$

pour tous les diviseurs premiers impairs q de $m + 1$.

Alors m est premier.

Si par contre (1) est faux , alors m est composé.

Ce test permet , en prenant $b = 7$, de montrer que le nombre avec $k = 391581$ et $n = 216193$ est premier .

La combinaison des deux théorèmes précédents permet d'obtenir des couples de nombres premiers jumeaux .

Des méthodes plus élaborées utilisant des sommes de Gauss ou des sommes de Jacobi permettent à présent de savoir si un nombre de 100 chiffres sans particularité est premier en 30 secondes environ avec un ordinateur CDC Cyber.170-750. [A 21], [A 23]

Pour en savoir plus

[1] BACHMANN (Paul) . - Niedere Zahlentheorie , Chelsea reprint , 1968 .

[2] BELL (Eric Temple) . - Les grands mathématiciens , Payot , 1961 .

[3] BOREL (Emile) . - Les nombres premiers , 1ère éd. Que Sais-je ? n°571 P.U.F. , 1958 .

[4] DICKSON (L.E.) . - History of the theory of numbers , 3 vol. , Chelsea reprint , 1971 .

[5] DIEUDONNE (J.) .- Pour l'honneur de l'esprit humain , Hachette , 1987.

[6] ENGEL (Arthur) . - Mathématique et informatique , CEDIC/NATHAN , 1987 . Réédition de " Mathématiques élémentaires d'un point de vue algorithmique"

[7] GUY (R.K) . - Unsolved problems in number theory , Problem book in Mathematics , Unsolved problems in intuitive Mathematics , vol 1 ,Springer 1981 .

[8] HARDY (G.H.) and WRIGHT (E.M.) . - An introduction to number theory, 5e éd. 1975 , Oxford , Clarendon Press .

[9] HUA (Loo Keng) . - An introduction to number theory , Springer , 1981.

[10] ITARD (Jean) . - Les nombres premiers , 2e éd.(entièrement distincte de la première), Que Sais-je? , n°571 , P.U.F. , 1969.

[11] ITARD (Jean) . - Arithmétique et théorie des nombres , Que Sais-je? n°1093 , P.U.F. , 1963 .

[12] KRAITCHIK (Maurice) . - Introduction à la théorie des nombres , Gauthier-Villars , 1952 .

[13] LEHNING (H.) , JAKUBOWICZ (D.) ; - Mathématiques par l'informatique individuelle , t.1 , Le Basic , Arithmétique, cryptographie , équations , Masson , 1982 .

[14] LeVEQUE (William J.) . - Fundamentals of number theory , Addison Wesley , Reading , Massachusetts , 1977 .

[15] LUCAS (Edouard) . - Théorie des nombres , 1891 , Réimp. A.Blanchard, 1961.

[16] NARKIEWICZ (W;) . - Elementary and analytic theory of algebraic numbers , 2e éd. , Springer , 1990 .

[17] RADEMACHER (Hans) . - Lectures on elementary number theory , R.E.Krieger, Huntington , New-York , 1977 .

[18] RIBENBOIM (Paulo) . - The book of prime number records , Springer , 1988 (476p. dont 100p. de références) 2e éd. 1989 .

[19] Compte rendu de [18] par Carl Pomerance in American Mathematical monthly 96 (1989) p. 663-665 .

[20] RIESEL (Hans) . - Prime numbers and computers methods for factorization Birkhäuser Verlag , 1985 .

[21] ROSEN (Kenneth H.) . - Elementary number theory and its applications , 2e éd. , Addiwon Wesley , 1988 .

[22] SHANKS (Daniel) . - Solved and unsolved problems in number theory , 3e éd. , Chelsea , 1985 .

[23] SIERPINSKI (W.). - 250 problèmes de théorie élémentaire des nombres , Hachette-Université , Hachette , 1973 .

[24] STARK (H.M.) . - An introduction to number theory , Markham ,Chicago, 2e tirage , 1971 .

[25] VENKOV (B.A.) . - Elementary number theory , Wolters Noordhoff series of monographs ... , Wolters Noordhoff , Groningen , 1970 .

[26] VELU (Jacques) . _ Méthodes mathématiques pour l'informatique , Dunod-Informatique , Dunod , 1987 .

[27] Les progrès des mathématiques . Bibliothèque Pour la Science , Diffusion Belin , 1980 .

[28] Computational methods in number theory . Ed. by H.W.LENSTRA Jr et R.TIJDEMAN , Mathematical Centre Tracts , 154 et 155 (2 vol.), Amsterdam 2e éd. complétée , 1984 .

[29] Reviews in number theory , 1940-1972 , 6vol. , Ed. by Williams Judson LeVEQUE , American Math. Soc. , Providence , Rhode Island , 1974 .

[30] Reviews in number theory , 1973-1983 , vol. 1a-6a , Ed. by Richard K. GUY , American Math. Soc. , Providence , Rhode Island , 1984 .

[A 1] BUHLER (J.P.), CRANDALL (R.E.), PENK (M.A.) . - Primes of the forms n! ± 1 and 2.3.5....p ± 1 , Math. Comp. 38 (1982),n°158 , p.639-643 .

[A 2] ATKIN (A.O.L.) , RICKERT (N.W.) . - On a larger pair of twin primes . Notices Amer. Math. Soc. , 26 (1979), A.373 .

[A 3] GARDNER (Martin) . - Mathematical games , Scientific American , 244, Février 1981 , p.20 .

[A 4] BRUN (Viggo). - La série 1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + 1/41 +1/43 + 1/59 + 1/61 + ... où les dénominateurs sont les nombres premiers jumeaux est convergente ou finie , Bull. Sci. MAth. 43 (1919) p. 101-104 , 124-128 .

[A 5] SHANKS (Daniel) et WRENCH (John W.) Jr . - Brun's constant , Math. Comp. 28 (1974) p. 293-299 .

[A 6] Science et Avenir , Novembre 1989, p.9 .

[A 7] BATEMAN (P.T.) , SELFRIDGE (J.L.) , WAGSTAFF Jr . - The Editor's corner: The new Mersenne conjecture . Amer. Math. Monthly, 96(1989) p.125-128 .

[A 8] GANDHI (J.M.) . - Formulae for the n-th prime . Proc. Washington State University . Conf. on Number Theory , Wash. State Univ. , Pullman , Washington , 1971 , p. 96-106 .

[A 9] LEJEUNE-DIRICHLET (G.) . - Beweis des Satzes dass jede unbegrenzte arithmetische Progression , ... ,unendlich viele Primzahlen enthält . G.LEJEUNE-DIRICHLET Werke , Chelsea reprint, 1969 , p.312-342 .

[A 10] WILLIAMS (Hugh Cowie). - Primality testing on a computer , Ars Combinatoria , 5 (1978) , p.127-185 .

[A 11] KELLER(W.) . - Factors of Fermat's numbers and large primes of the form $k.2^n + 1$, Math. Comp. 41 (1983) p.661-673 .

[A 12] BRENT (R.P.) et POLLARD (J.M.) . - Factorization of the eighth Fermat number , Math. Comp. 36 (1981) p. 627-630 .

[A 13] BRILLHART (J.), MORRISON (M.A.). - A method of factoring and the factorization of F_7 , Math. Comp. 29 (1975) , p. 183-205 .

[A 14] CARMICHAEL (R.D.) . - On composite numbers p which satisfy the Fermat's congruence $a^{p-1} \equiv 1 \pmod{p}$, Amer. Math. Monthly , 19(1912), p.22-27.

[A 15] WAGSTAFF (Samuel S.) . - Large Carmichaël numbers , Math. Journal of the Okayama University , 22 (1980) n°1 , p.33-41 .

[A 16] LUCAS (Edouard) . - Théorie des fonctions numériques simplement périodiques , Amer. Journal of Math. 1 (1878) p. 184-239 et 289-321 .

[A 17] PROTH (E.) . - Théorèmes sur les nombres premiers , C.R.Acad.Sc.Paris , 87 (1878) , p. 926.

[A 18] LEHMER (D.H.) . - Tests for primality by the converse of Fermat's theorem , Bull. Amer. Math. Soc. 33(1927) p.327-340 .

[A 19] ROBINSON (R.M.) . - The converse of Fermat's theorem , Amer. Math. Monthly , 64 (1957) p. 703-710 .

[A 20] BRILLHART (J.) , LEHMER (D.H.) , SELFRIDGE (J.L.) . - New primality criteria and factorization of $2^m + 1$, Math. Comp. , 29 (1975) p.620-647

[A 21] COHEN (H.), LENSTRA ,Jr,(H.W.) . - Primality testing and Jacobi sums , Math. Comp. 42 (1984) , p. 297-330 .

[A 22] DIXON (John D.) . - Factorization and primality tests , Amer. Math. Monthly , 91 (1984) p. 333-352 , Errata 92 (1985) p. 444.

[A 23] LENSTRA (H.W.,Jr) . - Primality testing in [28] p. 55-77 .

Philippe BARKAN
178 , Boulevard Aristide Briand
85000 LA ROCHE SUR YON