MILLER's PRIMALITY TEST

H W LENSTRA, Jr
Mathematisch Instituut Roetersstraat 15 1018 WB Amsterdam The Netherlands

Received 11 June 1978 revised version received 14 October 1978

Primality test, prime

In this paper we prove the following simplification of Miller's primality criterion [2]

Theorem 1 *Assume that for every integer d that is* 1 mod 4 *and either prime or the product of two primes, the L function* $\Sigma_{k=1}^{\infty}(k/d)\ k^{-s}$ *satisfies the generalized Riemann hypothesis, where* (k/d) *denotes the Jacobi symbol, defined below Let n be an odd integer,* $n > 1$, *and write* $n - 1 = 2^t u$, *with t and u integers, and u odd Then n is a prime number if and only if for every prime number* $a < c\ (\log n)^2$, $a \not\equiv n$, *we have*

$$a^u \equiv 1 \bmod n \tag{1}$$

or

$$a^{2^j u} \equiv -1 \bmod n \quad \text{for some integer } j,\ 0 \leqslant j < t \tag{2}$$

Here c is some constant not depending on n, and log denotes the natural logarithm

This theorem differs in two respects from Miller's result In the first place, we require the generalized Riemann hypothesis for a smaller set of L functions than Miller does This results from a simplification of Miller's proof, which has been observed by several people and which consists in eliminating the modified Carmichael function from the argument In the second place, we have suppressed Miller's condition that n is no perfect power i e $n \neq m^s$ for all integers m, s with $s \geqslant 2$ This point could have been dealt with by applying Montgomery's version of Ankeny's theorem [3 Theorem 13 1] to a character of order p that is defined modulo p^2, for p prime but this would have required the generalized Riemann hypothesis for the L functions attached to such characters Instead we give a completely elementary argument, which requires no unproved hypotheses, and which leads to the following two results

Theorem 2 *Let n be a positive integer,* $n \neq 4$, *and assume that* $a^{n-1} \equiv 1 \bmod n$ *for every prime number* $a < (\log n)^2$ *Then n is the product of distinct prime numbers*

Theorem 3 *Let p be an odd prime number Then we have* $a^{p-1} \not\equiv 1 \bmod p^2$ *for some prime number* $a < 4\ (\log p)^2$

It will be clear from the proof of Theorem 3, that for every $\epsilon > 0$ we can take $a < (4e^{-2} + \epsilon)\ (\log p)^2$ for all p exceeding a bound depending on ϵ, here $4e^{-2} = 0\ 54134$

Theorem 3 is probably far from best possible, since it is likely that we can take $a = 2$ or $a = 3$ for every p The heuristic argument for this is as follows Fix an integer $a > 1$ Fermat's little theorem [5, Theorem 13] asserts that, for p a prime not dividing a, the 'Fermat quotient' $(a^{p-1} - 1)/p$ is an integer Let us regard it as an 'arbitrary' integer modulo p, and assume that it is divisible by p with 'probability' $1/p$ Then we are led to expect that the total number of primes $p \leqslant x$ for which $a^{p-1} \equiv 1 \bmod p^2$ is asymptotically equal to

$$\Sigma_{p \text{ prime},\, p \leqslant x}\ 1/p \sim \log \log x$$

for x tending to infinity, an expectation that is borne

out by the numerical material of Brillhart, Tonascia and Weinberger [1]. Let now p be a prime >3. Assuming that the 'events' $2^{p-1} \equiv 1 \bmod p^2$ and $3^{p-1} \equiv 1 \bmod p^2$ are independent, we find that they occur simultaneously with 'probability' $(1/p)^2$. But $\Sigma_{p \text{ prime}}(1/p)^2$ is convergent, so it is likely that the number $N(x)$ of primes $p \leqslant x$ for which we have both $2^{p-1} \equiv 1 \bmod p^2$ and $3^{p-1} \equiv 1 \bmod p^2$ tends to a finite limit as $x \to \infty$. Since $N(3 \cdot 10^9) = 0$, by [1], it is reasonable to conjecture that this limit is zero. In a similar way one is led to expect that, for any fixed integer $a > 1$, there exist only finitely many primes for which $a^{p-1} \equiv 1 \bmod p^3$.

Proof of Theorem 3. By [1], we may assume that $p > 3 \cdot 10^9$. Put $A = 4 \cdot (\log p)^2$, $K = 2 \cdot \log p / \log A$, and let k be the greatest integer $\leqslant K$. We denote the number of primes $<A$ by M; by [4], we have $M > A/\log A$.

Suppose that every prime $a < A$ satisfies $a^{p-1} \equiv 1 \bmod p^2$. If b is an integer which can be written as the product of at most k primes $<A$, then we have

$$0 < b \leqslant A^K = p^2, \qquad b^{p-1} \equiv 1 \bmod p^2.$$

The number of such b is

$$\frac{(M+1) \cdot (M+2) \cdots (M+k)}{k!} \geqslant \frac{M^k}{k!},$$

and all these b are mutually incongruent modulo p^2. But it is well known that the congruence $x^{p-1} \equiv 1 \bmod p^2$ has only $p - 1$ solutions modulo p^2. We conclude that

$$\frac{M^k}{k!} \leqslant p - 1 < p.$$

On the other hand, using Stirling's inequality

$$k! \leqslant \left(\frac{k}{\mathrm{e}}\right)^k \cdot \mathrm{e}^{1/(12k)} \cdot \sqrt{2\pi k},$$

where $\mathrm{e}^{1/(12x)} \cdot \sqrt{2\pi x}$ is a monotonically increasing function of x, for $x \geqslant 1/6$, we find that

$$\frac{M^k}{k!} \geqslant \left(\frac{\mathrm{e} \cdot A}{k \cdot \log A}\right)^k \cdot (\mathrm{e}^{1/(12k)} \cdot \sqrt{2\pi k})^{-1}$$

$$\geqslant \left(\frac{\mathrm{e} \cdot A}{2 \cdot \log p}\right)^k \cdot (\mathrm{e}^{1/(12K)} \cdot \sqrt{2\pi K})^{-1}$$

$$\geqslant (2\mathrm{e} \cdot \log p)^{K-1} \cdot (\mathrm{e}^{1/(12K)} \cdot \sqrt{2\pi K})^{-1}.$$

For $p > 2 \cdot 10^{12}$ we have

$$\mathrm{e}^K \geqslant 2\mathrm{e} \cdot \log p \cdot (\mathrm{e}^{1/(12K)} \cdot \sqrt{2\pi K})$$

and therefore

$$\frac{M^k}{k!} \geqslant (2 \cdot \log p)^K = A^{K/2} = p,$$

contradicting what we found before. To deal with the remaining cases, we observe that

$M^k/k! > 8 \cdot 10^9$ if $p > 3 \cdot 10^9$,

$M^k/k! > 10^{10}$ if $p > 8 \cdot 10^9$,

$M^k/k! > 6 \cdot 10^{11}$ if $p > 10^{10}$,

$M^k/k! > 3 \cdot 10^{12}$ if $p > 6 \cdot 10^{11}$,

so $M^k/k! > p$ for all p with $3 \cdot 10^9 < p < 2 \cdot 10^{12}$. This proves Theorem 3.

Proof of Theorem 2. Suppose that n is not the product of distinct prime numbers. Then p^2 divides n for some prime number p. We have $2 < (\log n)^2$ since $n \neq 4$, so $2^{n-1} \equiv 1 \bmod n$ by the hypothesis of the theorem. It follows that n, and hence p, is odd.

Let $a < 4 \cdot (\log p)^2$ be a prime number. Then $a < (\log n)^2$, so $a^{n-1} \equiv 1 \bmod n$, and a fortiori $a^{n-1} \equiv 1 \bmod p^2$. Therefore the multiplicative order of a modulo p^2 is a divisor of $n - 1$; in particular, it is relatively prime to p. Since by Euler's theorem [5, Theorem 14] this multiplicative order is also a divisor of the Euler function $\varphi(p^2) = p(p - 1)$ we conclude that it is a divisor of $p - 1$. Hence $a^{p-1} \equiv 1 \bmod p^2$ for every prime $a < 4 \cdot (\log p)^2$, contradicting Theorem 3. This proves Theorem 2.

The Jacobi symbol (k/d), which occurs in Theorem 1, is defined for integers k and positive, odd integers d, in the following way. If p is an odd prime number, then Fermat's little theorem easily implies that $k^{(p-1)/2} \equiv -1, 0$ or $1 \bmod p$, for every integer k; and (k/p) is defined to be the unique element from the set $\{-1, 0, 1\}$ for which $k^{(p-1)/2} \equiv (k/p) \bmod p$. For non-prime values of d, the symbol (k/d) is defined by repeated applications of the rule $(k/d_1 d_2) = (k/d_1)(k/d_2)$. Notice that we have

$$(k_1 k_2/d) = (k_1/d)(k_2/d) \tag{3}$$

for all integers k_1, k_2 and positive, odd integers d.

Proof of Theorem 1. If n is prime, then for every integer a not divisible by n we have $a^{2^t u} = a^{n-1} \equiv 1 \bmod n$, so if $a^u \not\equiv 1 \bmod n$ then the last element in the sequence $a^u, a^{2u}, \ldots, a^{2^{t-1}u}$ which is not 1 mod n is -1 mod n. Hence (1) or (2) holds. Next suppose that n is not a prime number. We have to prove that there exists a prime $a < c(\log n)^2$ for which (1) and (2) both fail.

Let p, q be primes such that pq divides n. If $p = q$ then by Theorem 2 there exists a prime $a < (\log n)^2$ with $a^{n-1} \not\equiv 1 \bmod n$, and clearly this a does not satisfy (1) or (2). Hence suppose that $p \neq q$. Interchanging p and q, if necessary, we can achieve that $p - 1$ is divisible by at least the same power of 2 as $q - 1$ is. Put $d = pq$ if $p - 1$ and $q - 1$ are in fact divisible by the same power of 2, and $d = p$ otherwise. Notice that $d \equiv 1 \bmod 4$.

Denote by a the smallest positive integer for which the Jacobi symbol (a/d) equals -1. From (3) it is obvious that a is a prime number, and Montgomery's version of Ankeny's theorem [3, Theorem 13.1] implies that $a < c(\log d)^2 \leqslant c(\log n)^2$ if the L-function $\Sigma_{k=1}^{\infty} (k/d)\, k^{-s}$ satisfies the generalized Riemann hypothesis. Here c is some constant not depending on d. We show that a does not satisfy (1) or (2).

Put $b = a^u$. Since u is odd, we have $(b/d) = (a/d) = -1$. In particular, $b \not\equiv 1 \bmod d$, so (1) does not hold. If (2) holds, then

$$b^{2^j} \equiv -1 \bmod p, \qquad b^{2^j} \equiv -1 \bmod q$$

for some j, $0 \leqslant j < t$, so the multiplicative order of b modulo p and the multiplicative order of b modulo q are both equal to 2^{j+1}.

Let now first $d = p$. Then $p - 1$ is divisible by a higher power of 2 than $q - 1$. But by Fermat's little theorem, $q - 1$ is divisible by the order of b mod q, which equals 2^{j+1}. Consequently, $(p - 1)/2$ is divisible by 2^{j+1}. It follows that $b^{(p-1)/2} \equiv 1 \bmod p$, so $(b/p) = 1$, contradicting that $(b/p) = (b/d) = -1$.

Next suppose that $d = pq$. Then $(b/p) \cdot (b/q) = -1$, so interchanging p and q, if necessary, we can achieve that $(b/p) = -1$ and $(b/q) = 1$. Then $b^{(q-1)/2} \equiv 1 \bmod q$, so the order of b mod q, which equals 2^{j+1}, divides $(q - 1)/2$. But $(q - 1)/2$ is divisible by the same power of 2 as $(p - 1)/2$, so 2^{j+1} also divides $(p - 1)/2$. As in the first case, this implies that $(b/p) = 1$, which is again a contradiction.

This proves Theorem 1.

Acknowledgement

Research for this paper was supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

References

[1] J. Brillhart, J. Tonascia and P. Weinberger, On the Fermat quotient, in: A.O.L. Atkin and B.J. Birch (eds), Computers in Number Theory, Proc. Atlas Symp. 2, Oxford 1969 (Academic Press, London, New York, 1971) 213–222.

[2] G.L. Miller, Riemann's hypothesis and tests for primality, J. Comput. System Sci. 13 (1976) 300–317.

[3] H.L. Montgomery, Topics in Multiplicative Number Theory, Lecture Notes in Mathematics 227 (Springer Verlag, Berlin 1971).

[4] J. Barkley Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64–94.

[5] D. Shanks, Solved and Unsolved Problems in Number Theory (Spartan Books, New York, 1962).