Pacific Journal of Mathematics

TESTS FOR PRIMALITY BASED ON SYLVESTER'S CYCLOTOMIC NUMBERS

MORGAN WARD

Vol. 9, No. 4 August 1959

TESTS FOR PRIMALITY BASED ON SYLVESTERS CYCLOTOMIC NUMBERS

MORGAN WARD

Introduction. Lucas, Carmichael [1] and others have given tests for primality of the Fermat and Mersenne numbers which utilize divisibility properties of the Lucas sequences (U) and (V); in this paper we are concerned only with the first sequence;

$$(U):\ U_0,\ U_1,\ U_2,\ \cdots,\ U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ \cdots .$$

Here α and β are the roots of a suitably chosen quadratic polynomial $x^2 - Px + Q$, with P and Q coprime integers. (For an account of these tests, generalizations and references to the early literature, see Lehmer's Thesis [2]).

I develop here a test for primality of a less restrictive nature which utilizes a divisibility property of the Sylvester cyclotomic sequence [3]:

$$(Q) : Q_0 = 0,\ Q_1 = 1,\ Q_2,\ \cdots,\ Q_n = \prod_{\substack{1 \le r \le n \\ (r,n)=1}} (\alpha - e^{\frac{2\pi i r}{n}}\beta),\ \cdots$$

Here α and β have the same meaning as before. (U) and (Q) are closely connected [4]; in fact

$$U_n = \prod_{d \mid n} Q_d \,. \tag{1.1}$$

The divisibility property is expressed by the following theorem proved in § 3 of this paper.

THEOREM. *If m is an odd number dividing some cyclotomic number Q_n whose index n is prime to m, then every divisor of m greater than one has the same rank of apparition n in the Lucas sequence (U) connected with (Q).*

Here the rank of apparition or rank, of any number d in (U) means as usual the least positive index x such that $U_x \equiv 0 \pmod{d}$.

The following primality test is an immediate corollary.

Primality test. If m is odd, greater than two, and divides some cyclotomic number Q_n whose index n is both prime to m and greater than the square root of m, then m is a prime number except in two trivial cases: $m = (n-1)^2$, $n - 1$ a prime greater than 3, or $m = n^2 - 1$ with $n - 1$ and $n + 1$ both primes.

Received January 14, 1959.

The primality tests of Lucas and Carmichael are the special case when $n = m \pm 1$ is a power of two (which allows Q_n to be expressed in terms of V_n) with $X^2 - Px + Q$ suitably specialized.

2. Notations. We denote the rational field by R, and the ring of rational integers by I. The polynomial

(2.1) $$f(x) = x^2 - Px + Q\ , \qquad P,\ Q,\ \text{in } I \text{ and co-prime}$$

is assumed to have distinct roots α and β.

We denote the root field of $f(x)$ by $\mathscr{A}$ and the ring of its integers by $\mathscr{I}$. Thus $\mathscr{A}$ is either R itself, or a simple quadratic extension of R.

Let p be an odd prime of I, and $\mathfrak{p}$ a prime ideal factor of p in $\mathscr{I}$. Every element ρ of $\mathscr{A}$ may be put in the form $\rho = \alpha/a$ with α in $\mathscr{I}$ and a in I. The totality of such ρ with $(a, p) = 1$ forms a subring $\mathscr{I}_p$ of $\mathscr{A}$. Evidently $\mathscr{A} \supset \mathscr{I}_p \supset \mathscr{I} \supseteq I$. If we extend $\mathfrak{p}$ into $\mathscr{I}_p$ in the obvious way, we obtain a prime ideal $\mathfrak{P}$. The homomorphic image of $\mathscr{I}_p$ modulo $\mathfrak{P}$ is a field, $\mathscr{F}_p$. We denote the mapping of $\mathscr{I}_p$ onto $\mathscr{F}_p$ by $(\mathfrak{P})$.

Let $F_n(z)$ denote the cyclotomic polynomial of degree $\phi(n)$. $F_n(z)$ has coefficients in I, and if n is greater than one, then (Lehmer [2], Carmichael [1])

(2.2) $$Q_n = \beta^{\phi(n)} F_n\left(\frac{\alpha}{\beta}\right)\ ,$$

Furthermore

(2.3) $$z^n - 1 = \prod_{d|n} F_n(z)\ .$$

3. Proof of theorem. Let m be an odd number greater than one which divides some term of (Q) whose index n is prime to m, so that

(3.1) $$Q_n \equiv 0 \pmod{m}\ , \qquad (n,\ m) = 1.$$

Throughout the next three lemmas, p stands for a fixed prime factor of m.

LEMMA 1. *If $\mathfrak{p}$ is any ideal factor of p in $\mathscr{I}$, then*

(3.2) $$(Q,\ p) = (\alpha,\ \mathfrak{p}) = (\beta,\ \mathfrak{p}) = (1)\ .$$

Proof. It suffices to prove that $(Q, p) = (1)$. Assume the contrary. Then $(p, P) = 1$. Since $U_1 = 1$ and $U_{x+2} = PU_{x+1} - QU_x \equiv PU_{x+1} \pmod{p}$, it follows by induction that $U_n \not\equiv 0 \pmod{p}$. Then by (1.1), $Q_n \not\equiv 0$

(mod p). But p divides m so that by (3.1) $Q_n \equiv 0 \pmod{p}$ a contradiction.

LEMMA 2. *The rank of apparition of p in (U) is n.*

Proof. Since $U_n \equiv 0 \pmod{p}$, p has a positive rank of apparition in (U), r say. Then r divides n. But by (1.1), $U_r = \prod_{d|n} Q_d$. Hence $Q_d \equiv 0 \pmod{p}$ for some d dividing both r and n. Clearly, if $d = n$, then $r = n$ and we are finished. Assume that d is less than n.

The number $\alpha/\beta = \alpha^2/Q$ is in $\mathscr{I}_p$ by Lemma 1. Let τ be its image in $\mathscr{F}_p$ under the mapping $(\mathfrak{P})$. Then by (2.2) and Lemma 1 $F_n(\tau) = F_d(\tau) = 0$ in $\mathscr{F}_p$. Consequently the resultant of the polynomials $F_n(z)$ and $F_d(z)$ is zero in $\mathscr{F}_p$. Therefore its inverse image under the mapping is in $\mathfrak{P}$. But this resultant is evidently in I. Therefore it must be divisible by p. But by formula (2.3), since $d < n$ the resultant of $F_n(z)$ and $F_d(z)$ must divide the discriminant $\pm n^{n-1}$ of $z^n - 1$. Thus $n \equiv 0 \pmod{p}$ so that $(n, m) \equiv 0 \bmod p$ which contradicts (3.1) and completes the proof.

LEMMA 3. *The rank of apparition in (U) of any positive power of p which divides m is n.*

Proof. Let p^k divide m, $k \geq 1$ and let the rank of p^k in (U) be r. Now $U_n = \prod_{d|n} Q_d \equiv 0 \pmod{p^k}$. But by Lemma 2, each Q_d with $d < n$ is prime to p. Hence r must equal n.

The theorem proper now follows easily. For let m' be any divisor of m other than one. By Lemma 3, every prime power dividng m' has rank of apparition n in (U). But the rank of apparition of m' in (U) is the least common multiple of the ranks of the prime powers of maximal order diving m'. (Carmichael [1]). Hence m' also has rank of apparition n in (U).

4. Proof of primality test. Assume that (3.1) holds for some n greater than $\sqrt{m}$. If m is not a prime, it has a prime factor $\leq \sqrt{m}$. Let p be the smallest such factor, and let

$$m = pq\,, \qquad q \geq 3\,. \tag{4.1}$$

Then p has rank n in (U) by Lemma 3. But by a classical result of Lucas, $U_{p\pm 1} \equiv 0 \pmod{p}$. Hence n divides $p \pm 1$. If n is less than $p + 1$, $\sqrt{m} < p \leq \sqrt{m}$, a contradiction. Hence $n = p + 1$. If $p = \sqrt{m}$, then $m = (n-1)^2$ and $n - 1$ is a prime. Since m is odd, $n \geq 4$. This is the first trivial case.

If $p < \sqrt{m}$, then $q \geq p + 2$ and $m \geq p(p + 2)$. But if $m > p(p + 2)$, then $n^2 > m \geq (p+1)^2 = n^2$, a contradiction. Hence $m = p(p+2)$ where $p+2$ has no prime factor smaller than p. Hence $p+2$ is a prime and $m = n^2 - 1$ with both $n-1$ and $n+1$ primes. This is the second trivial case. In every other case then, m must be a prime.

5. Conclusion. The two trivial cases can actually occur. For if $P = 22$ and $Q = 3$, then $Q_6 = \alpha^2 - \alpha\beta + \beta^2 = P^2 - 3Q = 475$. Hence $Q_6 \equiv 0 \pmod{25}$ and $25 = (6-1)^2$. Again, if $P = 17$ and $Q = 3$, then $Q_6 = 280$. Hence $Q_6 \equiv 0 \pmod{35}$ and $35 = 6^2 - 1 = 5 \times 7$. It is worth noting that these trivial cases cannot occur if α and β are rational integers. (See [1], Theorem XII and remark.)

To illustrate the theorem, note that if $P = 2$ and $Q = 1$, $Q_9 = 73$. Since $\sqrt{73} < 9$ and $(9, 73) = 1$, 73 is a prime. But for $P = 3$ and $Q = 1$, $Q_9 = 91$. But $9 < \sqrt{91}$ so the test is inapplicable. As a matter of fact, 91 is the product of two primes. Evidently the test may be extended to cover such a case. That is, if $Q_n \equiv 0 \pmod{m}$, $(n, m) = 1$ and $n > \sqrt[3]{m}$, m will usually be either a prime, or the product of two primes.

References

1. R. D. Carmichael, *On the numerical factors of arithmetic forms*, Ann. of Math., **15** (1913-14), 30-70.

2. D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. **31** (1930), 419-448.

3. J. J. Sylvester, *On certain ternary cubic form equations*, Amer. J. Math. **2** (1879), 357-83.

4. Morgan Ward, *The mappings of the positive integers into themselves which preserve division*, Pacific J. Math. **5** (1955), 1013-1023.

CALIFORNIA INSTITUTE OF TECHNOLOGY

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics

Vol. 9, No. 4 August, 1959