Therefore, $k_m = k_n$, and we have the relation

$$p_m(z) = z^{m-n}p_n(z) = z^{m-n}(k_n z^n + l_n).$$

We have assumed, until now, that the sequence $p_2(0), p_3(0), \cdots$ contained a nonzero term. If this is not the case, the last result still holds with $n = 1$, as may be seen from (4) in the same way as before.

Now we have, if $m \geqq n$, $m' \geqq n$, $m \neq m'$,

$$\int_{-\pi}^{+\pi} f(\theta)e^{i(m-m')\theta} \left| k_n z^n + l_n \right|^2 d\theta = 0, \qquad z = e^{i\theta}.$$

Whence, except on a set of measure zero, we have

$$f(\theta) = \text{const.} \left| k_n z^n + l_n \right|^{-2}, \qquad z = e^{i\theta}. \tag{11}$$

We conclude the proof with the obvious remark that the polynomials $1, z, z^2, \cdots, z^{n-1}$ are orthogonal on the unit circle $|z| = 1$ with the weight function (11).

STANFORD UNIVERSITY

A FACTORIZATION THEOREM APPLIED TO A TEST FOR PRIMALITY*

D. H. LEHMER

Certain tests for primality based on the converse of Fermat's theorem and its generalizations have been devised and applied by the writer during the past ten years.† Perhaps the most useful test for the investigation of a large number N of no special form may be given as follows:‡

THEOREM 1. *If N divides $a^{N-1}-1$ but is relatively prime to $a^{(N-1)/p}-1$, where p is a prime, then all the possible factors of N are of the form $p^\alpha x+1$, if $N-1$ is divisible by p^α, $(\alpha \geqq 1)$.*

Strictly speaking this is not a test for primality since the theorem merely gives a restriction on the factors of N. If $p^\alpha > N^{1/2}$ then, obviously, N is a prime. If p^α is only fairly large, the theorem gives

* Presented to the Society, February 26, 1938.

† This Bulletin, vol. 33 (1927), pp. 327–340; vol. 34 (1928), pp. 54–56; vol. 35 (1929), pp. 349–350; vol. 38 (1932), pp. 383–384; vol. 39 (1933), pp. 105–108; Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448; Journal of the London Mathematical Society, vol. 10 (1935), pp. 162–165; American Mathematical Monthly, vol. 43 (1936), pp. 347–354.

‡ This Bulletin, vol. 33 (1927), p. 331.

a good restriction on the factors of N and a much better restriction on the values of u in the equation

$$N = u^2 - v^2 = (u + v)(u - v);$$

in fact $2u \equiv N+1 \pmod{p^{2\alpha}}$. If no large divisor p^α of $N-1$ is known, it may be necessary to apply Theorem 1 several times and to combine the several restrictions thus obtained. Finally if no divisor p^α (other than the trivial factor $p^\alpha = 2$) of $N-1$ is known, then Theorem 1 tells us nothing at all.

It thus appears that the problem of proving N a prime is closely allied to the factorization of $N-1$. In general it is impossible to say anything about the factors of $N-1$ beyond the obvious remark that $N-1$ is even. In the interesting case where N is a divisor of a number of the form y^n-1, it is possible to make the factorization of $N-1$ depend upon the factors* of y^k-1, where $k<n$. It is the purpose of this note to indicate how this may be done.

To be more specific, let n be a positive integer, and let $Q_n(x) = x^\phi + \cdots$ be the irreducible polynomial whose roots are the primitive nth roots of unity, so that we have the familiar factorization

$$y^n - 1 = \prod_{\delta \mid n} Q_\delta(y), \tag{1}$$

where δ, as indicated, ranges over all the divisors of n. Then the factorization of numbers of the form y^n-1 depends on the factorization of $N = Q_n(y)$. If we suspect that N is a prime, it may be tested for primality provided something is known of the factors of $N-1$. Before discussing this topic, we need two lemmas.

LEMMA 1.† *If $n = sd$, where s is the product of all distinct prime factors of n, and $d \geqq 1$, then*

$$Q_n(y) = Q_s(y^d). \tag{2}$$

LEMMA 2. *If n is not divisible by the prime q, then*

$$Q_{nq}(y) = Q_n(y^q)/Q_n(y). \tag{3}$$

Both lemmas can be made to follow easily from the familiar‡ Dedekind inversion of (1):

* See Cunningham and Woodall, *Factorization of $y^n \pm 1$*, London, 1925, for extensive tables for $y \leqq 12$. For $y > 12$, see Cunningham, Messenger of Mathematics, vol. 57 (1927), pp. 72–80; see also Kraitchik, *Recherches sur la Théorie des Nombres*, vol. 2, Paris, 1929, pp. 84–159.

† Trudi, Annali di Matematica, (2), vol. 2 (1868–1869), pp. 160–162.

‡ Journal für die reine und angewandte Mathematik, vol. 54 (1857), pp. 25–26.

$$Q_n(y) = \prod_{\delta \mid n} (y^{n/\delta} - 1)^{\mu(\delta)}, \tag{4}$$

where μ is the Möbius function defined by $\mu(1) = 1$, and for $k > 1$ by $\mu(k) = (-1)^h$ or zero according as k is a product of h distinct primes or not.

To prove Lemma 1, we note that $\mu(\delta) = 0$, except when δ is a divisor of s. Therefore (4) may be written

$$Q_n(y) = \prod_{\delta \mid s} \{(y^d)^{s/\delta} - 1\}^{\mu(\delta)} = Q_s(y^d).$$

Lemma 2 may be established by noting that the divisors of nq are of the forms δ and $q\delta$, where δ ranges over the divisors of n, so that (4) becomes in this case

$$Q_{nq}(y) = \prod_{\delta \mid n} (y^{nq/\delta} - 1)^{\mu(\delta)} \prod_{\delta \mid n} (y^{n/\delta} - 1)^{\mu(q\delta)}. \tag{5}$$

Since q does not divide δ, $\mu(q\delta) = -\mu(\delta)$, and we obtain Lemma 2 at once on comparing (5) with (4).

Returning to the problem of factoring $N-1 = Q_n(y) - 1$ we find that three cases present themselves according as n has 0, 1, or more than one odd prime factor.

Case 1. If $n = 2^\lambda$, we exclude as trivial the cases $n = 1$ and 2 in which $Q_1(y) = y - 1$, and $Q_2(y) = y + 1$. For $n = 2^\lambda$, $(\lambda > 0)$, (4) gives

$$N = Q_n(y) = (y^n - 1)/(y^{n/2} - 1) = y^{n/2} + 1;$$

so the factorization of $N-1$ is obvious. As a matter of fact, when y is odd N is oddly even, and we are really concerned with $N/2$ and hence with factoring

$$(N/2) - 1 = \tfrac{1}{2}(y^{n/2} - 1) = \tfrac{1}{2}(y - 1)(y + 1)(y^2 + 1) \cdots (y^{n/4} + 1).$$

The decomposition of these binomials into their prime factors may be thought of as known, since their exponents are all considerably less than $n/2$.

Case 2. Assume that $n = 2^\lambda q^\beta$, $\lambda \geqq 0$, q an odd prime, $\beta \geqq 1$. In case $\lambda = 0$, formula (4) gives

$$N = Q_n(y) = (y^n - 1)/(y^{n/q} - 1).$$

Hence

$$N - 1 = y^{n/q}(y^\phi - 1)/(y^{n/q} - 1),$$

where $\phi = \phi(n) = n - n/q = q^{\beta-1}(q-1)$. In case $\lambda > 0$, (4) gives

$$N = Q_n(y) = (y^{n/2} + 1)/(y^{n/2q} + 1).$$

Hence

$$N - 1 = y^{n/2q}(y^{\phi} - 1)/(y^{n/2q} + 1),$$

where, in this case,

$$\phi = \phi(n) = (n/2) - (n/2q) = 2^{\lambda-1}q^{\beta-1}(q - 1).$$

In either case, then, the factorization of $N-1$ can be made to depend on that of binomials of much lower degree. For example, if $n=200$,

$$N - 1 = Q_{200}(y) - 1 = y^{20}(y^{80} - 1)/(y^{20} + 1) = y^{20}(y^{40} + 1)(y^{20} - 1).$$

Case 3. Assume that n has more than one odd prime factor. The final case is much more complicated; it is no longer true that all the prime factors of $N-1$ divide either y or y^m-1 for $m<n$. However, it is possible to account in this way for some of the factors of $N-1$ by the following theorem:

THEOREM 2. *Let $N=Q_n(y)$, and write $n=ds=qtd$, where s is the product of the distinct prime factors of n and q is any prime factor of N; then $N-1$ is divisible by y^d and also by $y^{d(q-1)}-1$, unless t divides $q-1$ in which case $N-1$ is divisible by the integer $(y^{d(q-1)}-1)/Q_t(y^d)$.*

PROOF. It is well known that for every $s>1$, $Q_s(0)=1$. In other words $Q_s(x)-1$ is divisible by x. Hence by Lemma 1

$$N - 1 = Q_n(y) - 1 = Q_s(y^d) - 1 \tag{6}$$

is divisible* by y^d. By Lemma 2, replacing n and y by t and y^d, respectively, we may write, in view of (6),

$$N - 1 = Q_{tq}(y^d) - 1 = \frac{Q_t(y^{dq}) - Q_t(y^d)}{Q_t(y^d)}. \tag{7}$$

The polynomial $Q_t(y^{dq})-Q_t(y^d)$ is divisible by $y^{dq}-y^d$ and hence by $y^{d(q-1)}-1$. In fact, if $f(x)=a_0+a_1x+a_2x^2+\cdots$ is any polynomial, every term of the difference

$$f(u) - f(v) = a_1(u - v) + a_2(u^2 - v^2) + a_3(u^3 - v^3) + \cdots$$

is divisible by $u-v$. Now since (7) is an identity in y^d, we may replace y^d by z and write

$$Q_t(z^q) - Q_t(z) = z(z^{q-1} - 1)P(z), \tag{8}$$

* Incidentally, $N-1$ does not contain a higher power of y than y^d since the penultimate term of $Q_s(x)$ is $-\mu(s)x=\pm x$.

where $P(z)$ is a polynomial with integral coefficients. But the right member of (8) is algebraically divisible by $Q_t(z)$; and since $Q_t(z)$ is irreducible it must divide either $z^{q-1}-1$ or else $P(z)$. By (1) it follows that $z^{q-1}-1$ is divisible by $Q_t(z)$ if and only if t divides $q-1$. Hence the theorem follows at once.

The algebraic factorization of $Q_n(y)-1$ under Case 3 may be given for a few values of n. By Lemma 1, we may confine ourselves to those values of n which are products of distinct primes and since, if k is odd,

$$Q_{2k}(x) = Q_k(-x), \tag{9}$$

we take only odd values of n which have no square factors. For the first five such values we have

$$\begin{aligned}
Q_{15}(y) - 1 &= y(y^4 - 1)(y^3 - y^2 + 1),\\
Q_{21}(y) - 1 &= y(y - 1)(y^3 + 1)(y^7 + y + 1),\\
Q_{33}(y) - 1 &= y(y^{10} - 1)(y^9 - y^8 + y^6 - y^5 + y^3 - y^2 + 1),\\
Q_{35}(y) - 1 &= y(y^2 + 1)(y^6 - 1)(y^{15} - y^{14} - y^{13} + y^{12} + y^{11}\\
&\qquad - y^9 + y^5 - y^2 + 1),\\
Q_{55}(y) - 1 &= y(y - 1)(y^2 + 1)(y^5 + 1)(y^{31} - y^{29} + y^{27} - y^{25}\\
&\qquad + y^{23} + y^{20} - y^{18} + y^{16} - y^{14} + y^{12} + y^{11}\\
&\qquad + y + 1).
\end{aligned} \tag{10}$$

The use of this table is illustrated by the following examples.

Let $N = Q_{60}(11) = 46\ 32945\ 35436\ 00481$. In view of Lemma 1 and (9), we have

$$Q_{60}(11) = Q_{30}(11^2) = Q_{15}(-11^2).$$

Substituting $y = -11^2$ in (10) we find

$$N - 1 = 11^2(11^8 - 1)(11^6 + 11^4 - 1),$$

from which we easily obtain the decomposition into primes

$$N - 1 = 2^5 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61 \cdot 7321 \cdot 1786201.$$

Choosing $p = 1786201$ for the application of Theorem 1 we find that

$$2^{(N-1)/p} - 1 \equiv 25\ 37813\ 44415\ 94865 = A - 1 \pmod{N}$$

and that $A-1$ is prime to N. Furthermore we find that

$$A^p = 2^{N-1} \equiv 1 \pmod{N}.$$

Hence by Theorem 1 the factors of N are of the form $1786201x+1$. Combining* this with $60x+1$ we get a restriction on the factors of N of the form $107172060x+1$. Only two numbers of this form exist below $N^{1/2}$, namely 107172061 and 214344121. Since neither of these is a factor of N, it follows that N is a prime.

As a second example consider

$$N = Q_{240}(2) = 18518\ 80056\ 39241\ 07521.$$

By Lemma 1 and (9) we have

$$N = Q_{240}(2) = Q_{30}(2^8) = Q_{15}(-2^8).$$

Hence by (10)

$$N-1 = 2^8(2^{32}-1)(2^{24}+2^{16}-1) = 2^8\cdot 3\cdot 5\cdot 17\cdot 257\cdot 65537\cdot 16842751,$$

the last factor being easily identified as a prime.† Armed with this complete factorization of $N-1$ we are now in a position to apply Theorem 1 to the number N, which has been investigated and declared prime by M. Kraitchik‡ in 1929 by a plausible though non-rigorous method.§ It turns out however that the first part of the hypothesis of Theorem 1 is not satisfied, that is, N does not divide $11^{N-1}-1$. Hence, by Fermat's theorem, N is composite. To settle this question we applied a new type of machine for combining linear congruences to the problem of factoring N with the result that

$$N = 394783681\cdot 46908728641.$$

LEHIGH UNIVERSITY

---

* Every factor of $Q_n(y)$ not dividing n is of the form $nx+1$.

† By the method given in the American Mathematical Monthly, vol. 43 (1936), pp. 347–354.

‡ *Recherches sur la Theorie des Nombres*, vol. 2, Paris, 1929, pp. 12–17.

§ This Bulletin, vol. 36 (1930), pp. 847–850.