CYCLOTOMY AND THE CONVERSE OF FERMAT'S THEOREM

MORGAN WARD, California Institute of Technology

The following theorem of A. Hurwitz [1] was stated without proof in answer to a question raised by E. B. Escott [2] regarding a test for the primality of the Fermat numbers 2^k+1 (k a power of two) stated without proof by E. Lucas in his *Theorie des Nombres* [3].

HURWITZ'S THEOREM: *Let $Q_n(x)$ denote the cyclotomic polynomial of order n and degree $\phi(n)$. Then n is a prime number if there exists an integer a such that*

$$Q_{n-1}(a) \equiv 0 \pmod{n}. \tag{1}$$

This theorem is a simple consequence of the converse of Fermat's theorem. For let n be greater than one. Then the factorization of $x^{n-1}-1$ into its irreducible factors over the rational field is

$$x^{n-1} - 1 = \prod_{d \mid n-1} Q_d(x). \tag{2}$$

Here the product extends over all distinct divisors d of $n-1$.

The discriminant $\pm(n-1)^{n-1}$ of $x^{n-1}-1$ is prime to n. Consequently if d and d' are distinct divisors of $n-1$, the resultant of $Q_d(x)$ and $Q_{d'}(x)$ is always prime to n. Hence for any integer a and any proper divisor d of $n-1$, the three numbers $Q_{n-1}(a)$, $Q_d(a)$ and n are co-prime.

Now assume that the congruence (1) is satisfied. By what precedes, $Q_d(a)$ is prime to n for every proper divisor d of $n-1$. But by (2)

$$a^{n-1} - 1 \equiv \prod_{k \mid n-1} Q_k(a) \equiv 0 \pmod{n},$$

$$a^d - 1 \equiv \prod_{k \mid d} Q_k(a) \not\equiv 0 \pmod{n}, \qquad d \mid n-1;\ d < n-1.$$

Therefore n is a prime by the converse of Fermat's theorem. (For this converse see for example, O. Ore, *Number Theory*, Chapter XIV.)

For example, $Q_2(a) = a+1 \equiv 0 \pmod 3$ for $a=2$; $Q_6(a) = a^2-a+1 \equiv 0 \pmod 7$ for $a=3$. Hence 3 and 7 are primes. But the most interesting application of the theorem is that made by Hurwitz himself to the case when $n=2^k+1$ so that $Q_{n-1}(x) = x^{(n-1)/2}+1$; namely $n=2^k+1$ is a prime number if and only if there exists an integer a such that $a^{(n-1)/2} \equiv -1 \pmod n$. For $a=3$, this result is the test quoted by Lucas and used extensively by him and by other arithmeticians for investigating particular Fermat numbers.

References

1. A. Hurwitz, Mathematische Werke, vol. 2, page 747.

2. Intermédiare des Math., vol. II, 1896, pp. 80 and 214.

3. Lucas published proofs elsewhere, but the test is due to T. Pepin. For a history and references to other proofs see Dickson, *History of the Theory of Numbers*, vol. 1, Chap. XV.