THE QUINTIC CHARACTER OF 2 AND 3

By Emma Lehmer

1. Introduction. The cubic case. The problem of giving a criterion for the cubic character of 2 was essentially solved by Gauss when he enumerated the number $(0, 0)_3$ of consecutive cubic residues of the prime $p = 6n + 1$ in terms of L appearing in the quadratic partition

$$(1) \qquad 4p = L^2 + 27M^2, \qquad L \equiv 1 \pmod 3.$$

He found that

$$(2) \qquad 9(0, 0)_3 = L + p - 8.$$

A criterion for the cubic character of 2 in terms of the parity of L can be made to follow from the consideration of the parity of $(0, 0)_3$. To this effect we introduce a lemma which will be of use later.

Lemma 1. *If $(0, 0)_k$ denotes the number of consecutive k-th power residues, then if k is odd, $(0, 0)_k$ is odd or even according as 2 is a k-th power residue or not.*

Proof. For every pair $(r, r + 1)$ of residues there exists a complementary pair $(p - r - 1, p - r)$ which are also residues, since k is odd, and hence -1 is a residue of p. These two pairs will be distinct provided $r \neq (p - 1)/2$, so that $(0, 0)_k$ will be even if and only if $(p - 1)/2$ is not a residue of p, which will be the case if and only if 2 is not a residue of p.

It follows from (2) and Lemma 1 that *L is even if and only if 2 is a cubic residue of p.* From (1), M will also be even, and we can state: *The equation $p = l^2 + 27m^2$ has a pair of solutions for $p = 6n + 1$ if and only if 2 is a cubic residue of p.*

This criterion as well as further criteria for the cubic and higher power residuacity of small primes can be made to depend on a theorem of Libri [8; 121–122] in a form given by Lebesgue [7].

If k is any divisor of $p - 1$ and q any number (p, a prime), then the number $\gamma_q(k)$ of solutions $(x_1, x_2, \cdots, x_q)$ of the congruence

$$(3) \qquad 1 + x_1^k + x_2^k + \cdots + x_q^k \equiv 0 \pmod p$$

(where the $x_i = 1, 2, \cdots, p - 1$ are not necessarily distinct and two solutions are counted as distinct unless the same places are occupied by the same letter) is given by $p\gamma_q(k) = [(p - 1)/k]^q + S_{q+1}^{(k)}$, where $S_{q+1}^{(k)} = \sum_{i=0}^{k-1} \eta_i^{q+1}$ and the periods η_i are defined as usual by

$$\eta_i = \sum_{\nu=1}^{(p-1)/k} r^{g^{k\nu+i}} \qquad (i = 0, 1, \cdots, k - 1)$$

(r is a primitive p-th root of unity and g is a primitive root of p).

Received March 7, 1949.