PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 54, January 1976

SOME SUFFICIENT CONDITIONS FOR QUINTIC RESIDUACITY

YUN-CHENG ZEE

ABSTRACT. It is shown that for a prime p of the form $5f + 1$, a prime $q > 5$ is a quintic residue $(\text{mod}\, p)$ if $u \equiv 0$, $v \equiv kw$ or $u \equiv kw$, $v \equiv 0$ $(\text{mod}\, q)$, where k satisfies $k^2 \equiv -3$, 5 or -15 $(\text{mod}\, q)$.

In his study of cyclotomy of order 5, L. E. Dickson [1, Theorem 8] showed that for each prime $\equiv 1 \pmod 5$, there are exactly four simultaneous solutions of the Diophantine equations

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \tag{1}$$

$$xw = v^2 - u^2 - 4uv, \tag{2}$$

with $x \equiv 1 \pmod 5$. If (x, u, v, w) is one solution, the other three are $(x, -u, -v, w)$, $(x, v, -u, w)$ and $(x, -v, u, -w)$. The values of x, u, v and w have been used in giving criteria for the quintic residuacity of the primes $q = 2, 3$ [2, pp. 13, 15], 5 [4, p. 122]. E. Lehmer [4, p. 124] showed that q is a quintic residue $(\text{mod}\, p)$ if $u \equiv v \equiv w \equiv 0 \pmod q$. A more general result giving a sufficient condition for the rth power residuacity of q is due to J. B. Muskat [6, Theorem 3]. When $r = 5$, Muskat's condition, restated in terms of x, u, v and w, becomes $u \equiv v \equiv 0 \pmod q$.

Let p be a prime of the form $ef + 1$, g a primitive root of p and ξ a pth root of unity. The periods η_k, where $k = 0, 1, \ldots, e - 1$, are defined by

$$\eta_k = \sum_{t=1}^{f-1} \xi^{g^{et+k}}.$$

The equation

$$\varphi(y) = \prod_{i=0}^{e-1} (y - \eta_i) = 0$$

is called the period equation of degree e. A theorem of Kummer [3, p. 436] states that if e is a prime, then each prime divisor of the numbers represented by $\varphi(y)$ is an eth power residue $(\text{mod}\, p)$. The reduced period equation

$$F(z) = \prod_{i=1}^{e-1} (z - \rho_i) = 0$$

with the roots $\rho_i = e\eta_i + 1$ is simpler than $\varphi(y) = 0$. $F(z)$ and $\varphi(y)$ are

Received by the editors December 11, 1974 and, in revised form, March 17, 1975.

AMS (MOS) subject classifications (1970). Primary 10A15; Secondary 10C05, 12C20.

Key words and phrases. Cyclotomy, cyclotomic numbers, quintic residuacity, period, period equation.

related by $e^e\varphi(y) = F(z)$, where $z = ey + 1$. The following lemma is then obvious:

LEMMA. *If e is a prime, then each prime divisor $\neq e$ of the numbers represented by $F(z)$ is an eth power residue* (mod p).

THEOREM. *Let p be a prime of the form $5f + 1$. A prime $q > 5$ is a quintic residue* (mod p) *if* $u \equiv 0$, $v \equiv kw$ *or* $u \equiv kw$, $v \equiv 0$ (mod q), *where k satisfies* $k^2 \equiv -3, 5$ *or* -15 (mod q).

PROOF. The reduced period equation of degree 5 is [2, (10)]

$$F(z) = z^5 - 10pz^3 - 5pxz^2 - 5p\left[(x^2 - 125w^2)/4 - p\right]z \\ + p^2x - p\left[x^3 + 625(u^2 - v^2)w\right]/8. \tag{3}$$

For simplicity, congruences will be modulo q throughout. Assume $u \equiv 0$, $v \equiv kw \not\equiv 0$. Let j satisfy $jk \equiv 1$. By (2), $xw \equiv k^2w^2$, so that $w \equiv j^2x$ and $v \equiv jx$. Substituting u, v and w into (1) and (3) yields

$$16p \equiv (125j^4 + 50j^2 + 1)x^2, \tag{4}$$

$$8F(z) \equiv 8z^5 - 80pz^3 - 40pxz^2 - 5p\left[2x^2(1 - 125j^4) - 8p\right]z \\ + 8p^2x - px^3(1 - 625j^4), \tag{5}$$

respectively. In (5), let $z = x$ and simplify:

$$8F(x) \equiv x\left[8x^4 + (1875j^4 - 131)px^2 + 48p^2\right].$$

Multiplying by 16 and applying (4) give

$$\begin{aligned} 128F(x) &\equiv x^5\Big[128 + (1875j^4 - 131)(125j + 50j^2 + 1) \\ &\qquad\qquad + 3(125j^4 + 50j^2 + 1)^2\Big] \\ &\equiv x^5\left[128 + (125j^4 + 50j^2 + 1)(2250j^4 + 150j^2 - 128)\right] \\ &\equiv 6250x^5j^2(45j^6 + 21j^4 - j^2 - 1) \\ &\equiv 6250x^5j^2(3j^2 + 1)^2(5j^2 - 1). \end{aligned}$$

Hence

$$2^6k^8F(x) \equiv (5x)^5(3 + k^2)^2(5 - k^2).$$

Since $q \neq 2$, the last congruence implies that if $k^2 \equiv -3$ or 5, then $F(x) \equiv 0$ or $q|F(x)$. By the Lemma, q is a quintic residue, (mod p). Now, let $z = 0$ in (5) and simplify:

$$8F(0) \equiv px\left[8p - x^2(1 - 625j^4)\right].$$

Multiply by 2 and apply (4):

$$\begin{aligned} 16F(0) &\equiv px^3\left[(125j^4 + 50j^2 + 1) - (1 - 625j^4)\right] \\ &\equiv 50px^3j^2(15j^2 + 1). \end{aligned}$$

Hence

$$2^3k^4F(0) \equiv 5^2px^3(15 + k^2).$$

By the Lemma if $k^2 \equiv -15$, q is a quintic residue $(\bmod\, p)$. If we assume $u \equiv kw \not\equiv 0$, $v \equiv 0$ and let $jk \equiv 1$, we get $w \equiv -j^2x$, $u \equiv -jx$. Substitutions of u, v and w into (1) and (3) yield again (4) and (5) respectively, thus leading to the same condition on k. This completes the proof.

It is noted that for $q = 7$, the sufficient condition in the last theorem becomes $u \equiv 0$, $v \equiv \pm 2w$ or $u \equiv \pm 2w$, $v \equiv 0$, which is a partial restatement of Muskat's condition (see [5, Theorem 2]).

We give an illustration for $q = 11$. Since -3 and -15 are quadratic nonresidues (mod 11), the condition on k is reduced to $k^2 \equiv 5$ (mod 11). For primes of the form $5f + 1$ less than 2,000 this condition yields five primes, of which 11 is a quintic residue, as given by the following table:

p	x	u	v	w	k	ind 11(mod p)
311	-49	7	0	1	7	135
661	1	0	-3	9	-4	380
691	41	-2	11	5	4	335
751	71	4	11	-1	-4	715
1181	-64	0	16	-4	-4	160

The author wishes to thank Professor Muskat for the use of his collection of data on the cyclotomic numbers [1] of order 5 from which the values of x, u, v and w were computed at the Computer Center of the California State University, Fullerton. The author is grateful to the referee for his valuable suggestions.

REFERENCES

1. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.

2. E. Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. **18** (1951), 11–18. 7 **12**, 6779

3. ———, *Period equations applied to difference sets*, Proc. Amer. Math. Soc. **6** (1955), 433–442. MR **16**, 904.

4. ———, *Artiads characterized*, J. Math. Anal. Appl. **15** (1966), 118–131. MR **34** #1261.

5. ———, *On the divisors of the discriminant of the period equation*, Amer. J. Math. **90** (1968), 375–379. MR **37** #2718.

6. J. B. Muskat, *Reciprocity and Jacobi sums*, Pacific J. Math. **20** (1967), 275–280. MR **35** #1543.

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, FULLERTON, CALIFORNIA 92634