J. Austral. Math. Soc. (*Series A*) **46** (1989), 469–472

AN INDETERMINATE IN NUMBER THEORY

EMMA LEHMER

(Received 30 September 1987)

Communicated by J. H. Loxton

Abstract

This paper studies quintic residuacity of primes p of the form

$$16p = v^4 + 250v^2 + 3125, \qquad p = 5f + 1,$$

for which the expression for 4^f modulo p given in the first volume of this journal becomes indeterminate, and replaces it by a much simpler expression.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 A 15.

Introduction

Although the criterion that $D^f \equiv 1 \pmod{p}$ for $p = kf + 1$ if and only if D is a kth power residue of the prime p goes back to Euler, expressions for D^f modulo p in case $D^f \not\equiv 1 \pmod{p}$ so that D is a kth root of unity were first given by the author in [2] for cubic, quartic and quintic residues.

In the quintic case D^f modulo $p = 5f + 1$ is given in terms of the variables (x, u, v, w) in the Dickson form

$$\begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw &= v^2 - u^2 - 4uv, \qquad x \equiv 1 \pmod{5}. \end{aligned} \tag{1}$$

The congruence given in [2], namely

$$4^f \equiv \frac{w(125w^2 - x^2) - 2(xw + 5uv)(25w + x + 10u + 20v)}{w(125w^2 - x^2) - 2(xw + 5uv)(25w + x - 10u - 20v)} \pmod{p} \tag{2}$$

was recently found by Katre and Rajwade [1] to become zero over zero in case $u = -2v$ with v odd. This is also the case for the expressions for 3^f and 5^f of K. S. Williams [6]. Katre and Rajwade [1] find alternative expressions for these quantities which do not become indeterminate. The purpose of this note is to study this special case in detail and to give a very simple expression for 2^f and 4^f in this case.

1. An expression for $2^f \pmod p$ in case $u = -2v$

The form (1) has four solutions, namely

$$(x, u, v, w), \quad (x, -u, -v, w), \quad (x, -v, u, -w), \quad (x, v, -u, -w).$$

We choose the unique solution in which $v \equiv -x \pmod 4$ is odd. This implies that 2 is a quintic non-residue, which together with $u = -2v$ implies that $xw = 5v^2$ by (1). Also since $x \equiv 1 \pmod 5$ and since x and w cannot have a common factor with v we have $w = \pm 5$ and $x = \pm v^2$. Hence either $v \equiv \pm 1 \pmod 5$ and $w = 5$, or $v = \pm 2 \pmod 5$ and $w = -5$. Therefore by (1) we have

$$16p = v^4 + 250v^2 + 3125 = (v^2 + 125)^2 - 5 \cdot 50^2. \tag{3}$$

The expression for 2^f in [2] is unambiguous and is

$$2^f \equiv \frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)} \pmod p.$$

This, is easily seen to simplify with $u = -2v$, $x = \pm v^2$ and $w = \pm 5$ to

$$2^f \equiv \begin{cases} (5 - v)/(5 + v) \pmod p & \text{if } v \equiv \pm 1 \pmod 5, \\ (5 + v)/(5 - v) \pmod p & \text{if } v \equiv \pm 2 \pmod 5. \end{cases} \tag{4}$$

We see at once that 4^f is simply the square of these expressions and that the two remaining primitive fifth roots of unity are their reciprocals. We note, by the way, that these can be obtained by changing the sign of v. We also note that 5 is always a quintic non-residue of the primes in (3), since the condition for the quintic residuacity of 5 is $u \equiv 2v \pmod 5$ [3].

We also note that the expression (4) can be used to obtain 5^f, provided that the solution of (1) is used for which $2u + v \equiv 4 \pmod 5$. (See [6].) Hence for our set of primes in (3) we have $2^f \equiv 5^f \pmod p$ if and only if

https://doi.org/10.1017/S1446788700030949 Published online by Cambridge University Press

$v \equiv 2 \pmod 5$. We have not discovered a relation between 2^f and 5^f in the remaining cases.

2. Absolute artiads

Our primes in (3) are a subset of primes for which $u \equiv -2v \pmod 5$ which were called "artiads" by Lloyd Tanner [5]. The author showed in [3] that these primes have the Fibonacci roots $\theta = (1 \pm \sqrt{5})/2$ as quintic residues. In our case, by (3) we have $\sqrt{5} \equiv (v^2 + 125)/50 \pmod p$, so that

$$\theta_1 = (v^2 + 175)/100 \quad \text{and} \quad \theta_2 = -(v^2 + 75)/100 \pmod p$$

are quintic residues of p.

The discriminant of the period equation [4] becomes in this case

$$D = p^4 v^4 [(v^2 - 125)/4]^2 [(9v^2 + 125)/2]^2 = p^4 v^4 d_1^2 d_2^2. \tag{5}$$

Hence all the prime factors of v, d_1 and d_2 are also quintic residues of the primes in (3).

We conclude with a short table of primes less than 10000 together with v, θ_1 and θ_2 and the prime factors of d_1 and d_2.

p	v	θ_1	θ_2	d_1	d_2
211	−1	179	33	−31	67
1871	−9	1200	672	−11	7.61
3001	−11	123	2879	−1	607
4621	13	1667	2955	13	11
9931	17	5566	4366	41	29.47

All the integers in the table are quintic residues of the corresponding prime.

References

[1] S. A. Katre and A. J. Rajwade, 'Euler criterion for quintic non-residues,' *Canad. J. Math.* **37** (1985), 1008–1024.

[2] Emma Lehmer, 'On Euler's criterion,' *J. Austral. Math. Soc.* **1** (1959), 64–70.

[3] Emma Lehmer, 'Artiads characterized,' *J. Math. Anal. Appl.* **15** (1966), 118–131.

[4] Emma Lehmer, 'On the divisors of the discriminant of the period equation,' *Amer. J. Math.* **90** (1968), 375–379.

[5] H. W. Tanner, 'On the binomial equation $x^p - 1$: Quintesection,' *Proc. London Math. Soc.* **18** (1866–7), 214–234.
[6] Kenneth S. Williams, 'On Euler's criterion for quintic nonresidues,' *Pacific J. Math.* **61** (1975), 543–550.

1180 Miller Avenue
Berkeley, California 94708
U.S.A.