PACIFIC JOURNAL OF MATHEMATICS
Vol. 72, No. 2, 1977

DETERMINATION OF A UNIQUE SOLUTION OF THE QUADRATIC PARTITION FOR PRIMES $p \equiv 1 \pmod 7$

BUDH SINGH NASHIER AND A. R. RAJWADE

Let p be a rational prime $\equiv 1 \pmod 7$. Williams shows that a certain triple of a Diophantine system of quadratic equations has exactly six nontrivial solutions. We obtain here a congruence condition which uniquely fixes one of these six solutions. Further if 2 is not a seventh power residue $\pmod p$ then we obtain a congruence $\pmod p$ for $2^{(p-1)/7}$ in terms of the above uniquely fixed solution.

1. Introduction. Let e be an integer $\geqq 2$ and p a prime $\equiv 1 \pmod e$. Eulers criterion states that

$$D^f \equiv 1 \pmod p\,, \quad p = ef + 1 \tag{1.1}$$

if and only if D is an eth power residue $(\bmod\, p)$, so that if D is not an eth power residue $(\bmod\, p)$ then

$$D^f \equiv \alpha_e \pmod p \tag{1.2}$$

for some eth root $\alpha_e \not\equiv 1 \pmod p$ of unity.

Obviously $\alpha_2 = -1$. For $D = 2$ and $e = 3, 4, 5, 8$ Lehmer [2] gave an expression for α_e in terms of certain quadratic partition of p. For arbitrary eth power nonresidue D, Williams [6], [7] treated the cases $e = 3, 5$.

When $e = 5$ Dickson [1] (Theorem 8, page 402) proved that for a prime $p \equiv 1 (\bmod\, 5)$, the pair of Diophantine equations

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2 \\ xw = v^2 - 4uv - u^2 \ (x \equiv 1 \pmod 5)\,. \end{cases} \tag{1.3}$$

has exactly four solutions. If one of these is (x, u, v, w) the other three are given by $(x, -u, -v, w)$, $(x, v, -u, -w)$, $(x, -v, u, -w)$. Lehmer [2] (case $k = 5$) gave a method of fixing a solution uniquely. She proves that if 2 is a quintic nonresidue $(\bmod\, p)$ then

$$2^{(p-1)/5} \equiv \frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)} \pmod p \tag{1.4}$$

for a unique solution (x, u, v, w) fixed by the condition

$$2 \mid u,\ v \equiv (-1)^{u/2} x \pmod 4\,. \tag{1.4$'$}$$