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 $\pmod p$, so that if D is not an eth power residue $\pmod p$ 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 $p \equiv 1 (\mathrm{mod}\ 5)$, 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 $\pmod p$ 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

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

In this paper we treast the Case $p \equiv 1 \pmod 7$. For such primes Williams [4] has shown that the triple of diophantine equations

$$
(1.5)\quad \begin{cases} 72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2)\ , \\ 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 \\ \qquad + 48x_3x_4 + 98x_5x_6 = 0\ , \\ 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 \\ \qquad + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0,\ (x_1 \equiv 1 \pmod 7))\ , \end{cases}
$$

has exactly 6 nontrivial solutions, the two trivial ones being $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$. Out of the nontrivial solutions if one is

$$
(1.6)\quad \begin{cases} S_1 = (x_1, x_2, x_3, x_4, x_5, x_5) \text{ the other five are} \\ S_2 = (x_1, -x_2, -x_3, -x_4, x_5, x_6) \\ S_3 = \left(x_1, -x_4, x_2, -x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)\right) \\ S_4 = \left(x_1, x_2, -x_2, x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)\right) \\ S_5 = \left(x_1, x_3, -x_4, -x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)\right) \\ S_6 = \left(x_1, -x_3, x_4, x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)\right)\ . \end{cases}
$$

Here we obtain a congruence analogous to (1.4) together with a congruence condition fixing uniquely one out of these six solutions.

2. In the sequel p is a prime $\equiv 1 \pmod 7$. For any $D \not\equiv 0 \pmod p$ we define the Jacobsthal sum

$$
(2.1)\qquad \phi_7(D) = \sum_{x=1}^{p-1} \left(\frac{x(x^7 + D)}{p}\right)
$$

where $(\cdot/p)$ is the Legendre symbol. Using Euler's criterion we expand $(x^8 + xD)^{(p-1)/2}$ by the binomial theorem and interchange signs of summation, the result is

$$
\begin{aligned} \phi_7(D) &\equiv \sum_{j=0}^{(p-1)/2} D^j \binom{\frac{p-1}{2}}{j} \sum_{x=1}^{p-1} x^{4(p-1)-7j} \pmod p \\ &\equiv \sum_{j=0}^{(p-1)/2} D^j \binom{\frac{p-1}{2}}{j} \sum_{x=1}^{p-1} x^{-7j} \pmod p\ . \end{aligned}
$$

But

$$\sum_{x=1}^{p-1} x^{-7j} \equiv \begin{cases} -1 \pmod p; & \text{if } 7j \equiv 0 \pmod{p-1} \\ 0 \pmod p; & \text{otherwise} \end{cases}$$

and $7j \equiv 0 \pmod{p-1}$ if and only if $f \mid j$, i.e., if and only if $j = mf$, $m = 0, 1, 2, 3$.
Hence we obtain

$$\begin{aligned} \phi_7(D) &\equiv -\sum_{m=0}^{3} D^{mf}\binom{\frac{p-1}{2}}{mf} \pmod p \\ &\quad -[1 + (D)] \\ &\equiv D^f\binom{\frac{p-1}{2}}{f} + D^{2f}\binom{\frac{p-1}{2}}{2f} + D^{3f}\binom{\frac{p-1}{2}}{3f} \pmod p\,. \end{aligned} \tag{2.2}$$

We write (2.2) for $D = 4d^r$, $r = 0, 1, 2, 3, 4, 5, 6$ where d is any septic nonresidue $\pmod p$.

Let

$$\begin{cases} C_r = -[1 + \phi_7(4d^r)] \quad (r = 0, 1, 2, 3, 4, 5, 6) \\ \gamma_1 = 4^f\binom{\frac{p-1}{2}}{f}, \quad \gamma_2 = 4^{2f}\binom{\frac{p-1}{2}}{2f}, \quad \gamma_3 = 4^{3f}\binom{\frac{p-1}{2}}{3f}\,. \end{cases} \tag{2.3}$$

Then (2.2) gives us the following 7 congruences

$$\begin{aligned} C_0 &\equiv \gamma_1 + \gamma_2 + \gamma_3 \\ C_1 &\equiv \gamma_1 d^f + \gamma_2 d^{2f} + \gamma_3 d^{3f} \\ C_2 &\equiv \gamma_1 d^{2f} + \gamma_2 d^{4f} + \gamma_3 d^{6f} \\ C_3 &\equiv \gamma_1 d^{3f} + \gamma_2 d^{6f} + \gamma_3 d^{2f} \\ C_4 &\equiv \gamma_1 d^{4f} + \gamma_2 d^{f} + \gamma_3 d^{5f} \\ C_5 &\equiv \gamma_1 d^{5}{}_{f} + \gamma_2 d^{3f} + \gamma_3 d^{f} \\ C_6 &\equiv \gamma_1 d^{6f} + \gamma_2 d^{5f} + \gamma_3 d^{4f}\,. \end{aligned} \tag{2.4}$$

We first get $\gamma_1, \gamma_2, \gamma_3 \pmod p$ in terms of $C_0, C_1, C_2, C_3, C_4, C_5, C_6$. Let

$\alpha = d^f + d^{2f} + d^{4f}$ [Note that 1, 2, 4 are quadratic residues and
$\beta = d^{3f} + d^{5f} + d^{6f}$ 3, 5, 6 are quadratic non residues (mod 7).]

Then $\alpha + \beta \equiv -1 \pmod p$ and $\alpha\beta \equiv 2 \pmod p$.

$$\alpha - \beta \equiv \sum_{x=0}^{6} (d^f)^{x^2} \pmod p \tag{2.5}$$

is a Gaussian sum and $(\alpha - \beta)^2 \equiv -7 \pmod p$, since $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta \equiv 1 - 8 \equiv -7 \pmod p$.

We take suitable combinations of the latter six congruences in (2.4). These combinations are motivated by noting that the quadratic residues (mod 7) are 1, 2, 4 and the nonresidues are 3, 5, 6; while since 3 is a primitive root (mod 7) the nonzero residues are $3, 3^2, 3^3, 3^4, 3^5, 3^6$. These form three classes

$$\begin{aligned} A_0 &= \{3^3, 3^6\} = \{6, 1\} \\ A_1 &= \{3, 3^4\} = \{3, 4\} \\ A_2 &= \{3^2, 3^5\} = \{2, 5\} \end{aligned}$$

where $3^j \in A_i$ if and only if $j \equiv i \pmod 3$.

All congruences below are taken $\pmod p$.

$$\begin{aligned} C_1C_2 + C_1C_4 + C_2C_4 + C_3C_5 + C_3C_6 + C_5C_6 \\ \equiv -(\gamma_1^2 + \gamma_2^2 + \gamma_3^2) - 2\gamma_1\gamma_2 + 5\gamma_2\gamma_3 + 5\gamma_3\gamma_1 \end{aligned} \tag{2.6}$$

$$C_1C_6 + C_2C_5 + C_3C_4 \equiv (\gamma_1^2 + \gamma_2^2 + \gamma_3^2) - (\gamma_1\gamma_2 + \gamma_2\gamma_3 + \gamma_3\gamma_1) \tag{2.7}$$

$$C_1 + C_2 + C_4 - C_3 - C_5 - C_6 \equiv (\gamma_1 + \gamma_2 - \gamma_3)(\alpha - \beta) \tag{2.8}$$

$$\begin{aligned} C_1C_2 + C_1C_4 + C_2C_4 - C_3C_5 - C_3C_6 - C_5C_6 \\ \equiv (\gamma_1^2 + \gamma_2^2 - \gamma_3^2 + \gamma_1\gamma_3 - \gamma_2\gamma_3)(\beta - \alpha) \end{aligned} \tag{2.9}$$

$$C_1C_2C_4 + C_3C_5C_6 \equiv 2(\gamma_1^3 + \gamma_2^3 + \gamma_3^3) + \gamma_1\gamma_2\gamma_3 + C_0(\gamma_1\gamma_2 + \gamma_2\gamma_3 + \gamma_3\gamma_1) . \tag{2.10}$$

Squaring the first congruence in (2.4) and using (2.7) we obtain

$$\gamma_1^2 + \gamma_2^2 + \gamma_3^2 \equiv \frac{1}{7}(C_0^2 + 2(C_1C_6 + C_2C_5 + C_3C_4)) \tag{2.11}$$

$$\gamma_1\gamma_2 + \gamma_2\gamma_3 + \gamma_3\gamma_1 \equiv \frac{1}{7}(3C_0^2 - (C_1C_6 + C_2C_5 + C_3C_4)) . \tag{2.12}$$

Now (2.11), (2.12) and (2.6) give us

$$\begin{aligned} 7\gamma_1\gamma_2 \equiv 2C_0^2 \\ - (C_1C_6 + C_2C_5 + C_3C_4 + C_1C_2 + C_1C_4 + C_2C_4 + C_3C_5 + C_3C_6 + C_5C_6) \end{aligned}$$

and from (2.10) we get

$$7\gamma_1\gamma_2\gamma_3 \equiv C_1C_2C_4 + C_3C_5C_6 + C_0(C_0^2 - C_1C_6 - C_2C_5 - C_3C_4)$$

(using the identity $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$) so that

$$\left(\begin{aligned} \gamma_3 \equiv \frac{C_1C_2C_4 + C_3C_5C_6}{2C_0^2 - (C_1C_6 + C_2C_5 + C_3C_4 + C_1C_2} \\ \times \frac{+ C_0(C_0^2 - C_1C_6 - C_2C_5 - C_3C_4)}{+ C_1C_4 + C_2C_4 + C_3C_5 + C_3C_6 + C_5C_6)} \end{aligned} \right) . \tag{2.13}$$

Also (2.8) yields

$$(\alpha-\beta)(C_0-2\gamma_3) \equiv C_1+C_2+C_4-C_3-C_5-C_6$$

or

$$\alpha-\beta \equiv \frac{C_1+C_2+C_4-C_3-C_5-C_6}{C_0-2\gamma_3}\,. \tag{2.14}$$

(2.9) together with (2.11) leads to

$$\gamma_1-\gamma_2 \equiv \frac{(C_1C_2+C_1C_4+C_2C_4-C_3C_5-C_3C_6-C_5C_6)(\beta-\alpha)^{-1} \times \left(+\,2\gamma_3^2-\frac{1}{7}(C_0^2+2(C_1C_6+C_2C_5+C_3C_4))\right)}{\gamma_3}$$

whereas

$$\gamma_1+\gamma_2 \equiv C_0-\gamma_3\,.$$

Thus we obtain

$$\gamma_1 \equiv \frac{(C_1C_2+C_1C_4+C_2C_4-C_3C_5-C_3C_6-C_5C_6)(\beta-\alpha)^{-1} \times \left(+\,\gamma_3^2+C_0\gamma_3-\frac{1}{7}(C_0^2+2(C_1C_6+C_2C_5+C_3C_4))\right)}{2\gamma_3} \tag{2.15}$$

$$\gamma_2 \equiv \frac{-(C_1C_2+C_1C_4+C_2C_4-C_3C_5-C_3C_6-C_5C_6)(\beta-\alpha)^{-1} \times \left(-3\gamma_3^2+C_0\gamma_3+\frac{1}{7}(C_0^2+2(C_1C_6+C_2C_5+C_3C_4))\right)}{2\gamma_3}\,. \tag{2.16}$$

Since γ_3 is a function of the C's therefore so is $\alpha-\beta$ and hence γ_1, γ_2, γ_3 all are functions of the C's.

If $(x_1, x_2, \cdots, x_6)$ is a solutions of (1.5), then in [4] the C's have been evaluated interms of the x's viz.

$$\begin{cases} C_0 = -x_1 \\ 12C_1 = 2x_1 - 42x_2 - 49x_5 - 147x_6 \\ 12C_2 = 2x_1 - 42x_3 - 49x_5 + 147x_6 \\ 12C_3 = 2x_1 - 42x_4 + 98x_5 \\ 12C_4 = 2x_1 + 42x_4 + 98x_5 \\ 12C_5 = 2x_1 + 42x_3 - 49x_5 + 147x_6 \\ 12C_6 = 2x_1 + 42x_2 - 49x_5 - 147x_6\,. \end{cases} \tag{2.17}$$

Thus $\gamma_1, \gamma_2, \gamma_3$ are functions of the x's say:

$$(2.18) \qquad \gamma_i \equiv g_i(x_1, x_2, x_3, x_4, x_5, x_6) \quad i = 1, 2, 3 .$$

Also (2.14) gives the Gaussian sum $\alpha - \beta$ as a function of the x's say

$$(2.19) \qquad \alpha - \beta \equiv \psi(x_1, x_2, x_3, x_4, x_5, x_6) .$$

3. In this section we show that g_1, g_2, g_3 in (2.18) are independent of the choice of solutions of (1.5).

Let $S_1 = (x_1, x_2, \cdots, x_6)$ be a solution of (1.5) and the C's be given as in (2.17). For a change of solution $S_1 \rightarrow S_j$, $j = 2, 3, 4, 5, 6$ we want to see how the C's change.

We see that:

$$(3.1) \quad \begin{cases} \text{If } \ S_1 \longrightarrow S_2 \ \text{ then} \\ C_1 \longrightarrow C_6, C_2 \longrightarrow C_5, C_3 \longrightarrow C_4, C_4 \longrightarrow C_3, C_5 \longrightarrow C_2, C_6 \longrightarrow C_1; \\ \quad : S_1 \longrightarrow S_3 \ \text{ then} \\ C_1 \longrightarrow C_4, C_2 \longrightarrow C_1, C_3 \longrightarrow C_5, C_4 \longrightarrow C_2, C_5 \longrightarrow C_6, C_6 \longrightarrow C_3; \\ \quad : S_1 \longrightarrow S_4 \ \text{ then} \\ C_1 \longrightarrow C_3, C_2 \longrightarrow C_6, C_3 \longrightarrow C_2, C_4 \longrightarrow C_5, C_5 \longrightarrow C_1, C_6 \longrightarrow C_4; \\ \quad : S_1 \longrightarrow S_5 \ \text{ then} \\ C_1 \longrightarrow C_2, C_2 \longrightarrow C_4, C_3 \longrightarrow C_6, C_4 \longrightarrow C_1, C_5 \longrightarrow C_3, C_6 \longrightarrow C_5; \\ \quad : S_1 \longrightarrow S_6 \ \text{ then} \\ C_1 \longrightarrow C_5, C_2 \longrightarrow C_3, C_3 \longrightarrow C_1, C_4 \longrightarrow C_6, C_5 \longrightarrow C_4, C_6 \longrightarrow C_2 . \end{cases}$$

We observe that C's get permuted in such a way that the set $\{C_1, C_2, C_4\}$ with suffixes quadratic residues (mod 7) either remains unaltered or interchanges with the set $\{C_3, C_5, C_6\}$ with sufixes quadratic non-residues (mod 7).

This implies that the combinations of the C's taken in (2.6), (2.7) and (2.10) do not change with the change of solutions while (2.8) and (2.9) either both remain the same or change signs simultaneously. Thus $(C_1C_2 + C_1C_4 + C_2C_4 - C_3C_5 - C_3C_6 - C_5C_6)(\beta - \alpha)$ is also unchanged under the change of solutions.

This shows in view of (2.13), (2.15), (2.16) that g_i's are independent of choice of solutions of (1.5).

4. In the last section we fix a solution of (1.5) uniquely. For any $\lambda \not\equiv 0 \pmod 7$ $\lambda, 2\lambda, 3\lambda, 4\lambda, 5\lambda, 6\lambda$ is a reduced residue system (mod 7) therefore we write λr for r in the latter six congruences in (2.4) to get

$$(4.1)\qquad \begin{cases} C_\lambda \equiv \gamma_1 d + \gamma_2 d^{2\lambda f} + \gamma_3 d^{3\lambda f} \\ C_{2\lambda} \equiv \gamma_1 d^{2\lambda f} + \gamma_2 d^{4\lambda f} + \gamma_3 d^{6\lambda f} \\ C_{3\lambda} \equiv \gamma_1 d^{3\lambda f} + \gamma_2 d^{6\lambda f} + \gamma_3 d^{2\lambda f} \\ C_{4\lambda} \equiv \gamma_1 d^{4\lambda f} + \gamma_2 d^{\lambda f} + \gamma_3 d^{5\lambda f} \\ C_{5\lambda} \equiv \gamma_1 d^{5\lambda f} + \gamma_2 d^{3\lambda f} + \gamma_3 d^{\lambda f} \\ C_{6\lambda} \equiv \gamma_1 d^{6\lambda f} + \gamma_2 d^{5\lambda f} + \gamma_3 d^{4\lambda f} . \end{cases}$$

We solve the above system for $d^{\lambda f}$ as follows. Take suitable combinations of four of the above congruences and get

$$\begin{aligned} &C_{4\lambda} - d^{\lambda f}C_{3\lambda} \equiv \gamma_2(d^{\lambda f} - 1) + \gamma_3(d^{5\lambda f} - d^{3\lambda f}) \\ &C_{5\lambda} - d^{\lambda f}C_{2\lambda} \equiv \gamma_1(d^{5\lambda f} - d^{3\lambda f}) + \gamma_2(d^{3\lambda f} - d^{5\lambda f}) + \gamma_3(d^{\lambda f} - 1) \\ &d^{3\lambda f}C_{4\lambda} - d^{5\lambda f}C_{3\lambda} \equiv \gamma_1(1 - d^{\lambda f}) + \gamma_3(d^{\lambda f} - 1) \end{aligned}$$

or

$$\begin{aligned} &d^{\lambda f}(\gamma_2 + C_{3\lambda}) + d^{3\lambda f}(-\gamma_3) + d^{5\lambda f}(\gamma_3) \equiv \gamma_2 + C_{4\lambda} \\ &d^{\lambda f}(\gamma_3 + C_{2\lambda}) + d^{3\lambda f}(\gamma_2 - \gamma_1) + d^{5\lambda f}(\gamma_1 - \gamma_2) \equiv \gamma_3 + C_{5\lambda} \\ &d^{\lambda f}(\gamma_3 - \gamma_1) + d^{3\lambda f}(-C_{4\lambda}) + d^{5\lambda f}(C_{3\lambda}) \equiv \gamma_3 - \gamma_1 . \end{aligned}$$

Solving this system by Cramer's rule we obtain

$$(4.2)\qquad d^{\lambda f} \equiv \frac{C_{4\lambda}(\gamma_2 - \gamma_1) + C_{5\lambda}(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2}{C_{3\lambda}(\gamma_2 - \gamma_1) + C_{2\lambda}(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2} \pmod p$$

so that by putting $\lambda = 1$ we find

$$(4.2')\qquad d^{f} \equiv \frac{C_4(\gamma_2 - \gamma_1) + C_5(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2}{C_3(\gamma_2 - \gamma_1) + C_2(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2} \pmod p .$$

This last expression depends on the choice of the solution S_i since the C's depend on the choice of the solution of (1.5). Indeed the R.H.S. of (4.2′) takes different values (mod p) for different solutions. This is seen as follows:

It is easy to see that $\phi_7(n) = \phi_7(n')$ if $\operatorname{ind}_p(n) \equiv \operatorname{ind}_p(n') \pmod 7$ (see [3]) hence $C_l = C_m$ if $l \equiv m \pmod 7$.

In view of (3.1) and (4.2) we see that if $S_1 \rightarrow S_j$, $j = 2, 3, 4, 5, 6$; the R.H.S. of (4.2′) takes value

$$\equiv d^{6f}, d^{4f}, d^{3f}, d^{2f}, d^{5f}$$

respectively which are distinct (mod p).

Thus precisely one (out of the 6) solution satisfies (4.2′). When 2 is not a seventh power residue, (mod p) then for $d = 2$ we can identify which solution shall satisfy (4.2′). This is done as follows: We have

$$(4.3)\qquad \begin{cases} C_1 = -[1 + \phi_7(2^3)],\ C_2 = -[1 + \phi_7(2^4)],\ C_3 = -[1 + \phi_7(2^5)] \\ C_4 = -[1 + \phi_7(2^6)],\ C_5 = -[1 + \phi_7(1)],\ C_6 = -[1 + \phi_7(2)] \,. \end{cases}$$

Since $X^7 + 1 \equiv 0 \pmod p$ has exactly 7 solutions, $\phi_7(1)$ is composed exclusively of $p - 8$ plus and minus ones and hence must be odd.

Moreover $(2^j)^f = (2^f)^j \not\equiv 1 \pmod p$, $j = 1, 2, 3, 4, 5, 6$ so that by Euler's criterion $X^7 + 2^j \equiv 0 \pmod p$ is not solvable. Therefore $\phi_7(2^j)$ ($j = 1, 2, 3, 4, 5, 6$) is even. Thus we conclude that C_5 is even and the other C's are odd.

In (3.1) we notice that the corresponding C_5 of a solution is replaced by some other C_i under a change of solution, therefore for one and only one solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ we have

$$C_5 \equiv 0 \pmod 2$$

or what is the same thing

$$(4.4)\qquad \begin{aligned} &2x_1 + 42x_3 - 49x_5 + 147x_6 = 12C_5 \equiv 0 \pmod 8, \text{ i.e.,} \\ &2x_1 + 2x_3 - x_5 + 3x_6 \equiv 0 \pmod 8 \,. \end{aligned}$$

This determines a unique solution of (1.5). Our results can be stated as the following:

THEOREM. *Let $p \equiv 1 \pmod 7$ be a prime. If 2 is a septic non-residue* $(\bmod p)$, *then of the six nontrivial solutions of the quadratic partition* (1.5) *one and only one satisfies the two congruences*

$$(\text{i})\qquad 2^{(p-1)/7} \equiv \frac{C_4(\gamma_2 - \gamma_1) + C_5(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2}{C_3(\gamma_2 - \gamma_1) + C_2(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2} \pmod p$$

$$(\text{ii})\qquad 2x_1 + 2x_3 - x_5 + 3x_6 \equiv 0 \pmod 8$$

with $C_2, C_3, C_4, C_5, \gamma_1, \gamma_2, \gamma_3$ given as functions of the x_i's by (2.17) *and* (2.18).

This fixes a unique solution for us.

EXAMPLE. $p = 29 = 7.4 + 1$.
Here the six nontrivial solutions of (1.5) are

$$\begin{aligned} &S_1 = (1, -2, -3, -2, -1, 1)\,; && S_2 = (1, 2, 3, 2, -1, 1)\,, \\ &S_3 = (1, 2, -2, 3, 2, 0); && S_4 = (1, -2, 2, -3, 2, 0)\,. \\ &S_5 = (1, -3, 2, 2, -1, -1); && S_6 = (1, 3, -2, -2, -1, -1). \end{aligned}$$

Precisely one satisfies the two congruences of the theorem viz. S_1: $\gamma_1 \equiv 12$, $\gamma_2 \equiv -6$, $\gamma_3 \equiv -7 \pmod{29}$ and we have

$$2^{p-1/7} = 2^4 \equiv \frac{(-15)(-18) + 6(-7) + 36 + 49 + 72}{(-1)(-18) + 27(-7) + 36 + 49 + 72} \equiv \frac{9 + 16 + 12}{18 + 14 + 12}$$
$$\equiv \frac{8}{15} \equiv 16 \pmod{29} .$$

For the remaining five solutions the R.H.S. of (i) of the theorem takes value: 9, 25, 7, 24, 23 respectively (mod 29). We see that none satisfies (i) and of course none satisfies (ii).

By taking $\lambda = 3$ in (4.2) we have a similar expression

$$(4.5) \qquad 8^{(p-1)/7} \equiv \frac{C_5(\gamma_2 - \gamma_1) + C_1(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2}{C_2(\gamma_2 - \gamma_1) + C_6(\gamma_3) + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2} \pmod{p}$$

with the condition

$$2x_1 + 2x_3 - x_5 + 3x_6 \equiv 0 \pmod{8} .$$

By taking reciprocal of (i) of the theorem and (4.5) we can get expressions for $(2^6)^f$ and $(16)^f$ too.

We should like to thank Dr. Kenneth S. Williams for suggesting this problem.

References

1. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., **57** (1935), 391-424.
2. Emma Lehmer, *On Euler's Criterion*, J. Austral. Math. Soc., **1** (1959), 64-70.
3. A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math., **74** (1952), 89-99.
4. K. S. Williams, *Elementary treatment of quadraticp artition of primes* $= 1 \pmod 7$, Illinois J. Math., **18**, (1974), 608-621.
5. ———, *A quadratic partition of primes* $= 1 \pmod 7$, Math. Comp., **28**, (1974), 1133-1136.
6. ———, *On Euler's criterion for Cubic nonresidues*, Proc. Amer. Math. Soc., **49** (1975), 277-283.
7. ———, *On Euler's criterion of quintic nonresidues*, Pacific J. Math.. **51**, (1975), 543-550.

Recevied April 4, 1977.

PANJAB UNIVERSITY
CHANDIGARH-160014
INDIA