The eleventh power character of 2

By *Philip A. Leonard* at Tempe, *Brian C. Mortimer* at Edmonton, and *Kenneth S. Williams* at Ottawa*

1. Introduction

Let e be an odd prime and let p be a prime $\equiv 1 \pmod e$. If $e=3$, an integer x_1 is uniquely determined by

$$(1.1) \qquad 4p = x_1^2 + 27x_2^2, \quad x_1 \equiv -1 \pmod 3,$$

and Jacobi [1] showed that 2 is a cube $(\bmod p)$ if and only if $x_1 \equiv 0 \pmod 2$. If $e=5$, an integer x_1 is uniquely determined by

$$(1.2) \qquad \begin{cases} 16p = x_1^2 + 50x_2^2 + 50x_3^2 + 125x_4^2, & x_1 \equiv -1 \pmod 5, \\ x_2^2 - x_3^2 + x_1x_4 + 4x_2x_3 = 0, \end{cases}$$

and Lehmer [2] showed that 2 is a fifth power $(\bmod p)$ if and only if $x_1 \equiv 0 \pmod 2$. If $e=7$, an integer x_1 is uniquely determined by (see [3])

$$(1.3) \qquad \begin{cases} 72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \quad x_1 \equiv -1 \pmod 7, \\ 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 \\ \qquad + 48x_3x_4 + 98x_5x_6 = 0, \\ 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 \\ \qquad + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0, \end{cases}$$

provided $(x_1, x_2, x_3, x_4, x_5, x_6) \neq (6t, \pm 2u, \mp 2u, \pm 2u, 0, 0)$, where $p = t^2 + 7u^2$, $t \equiv 1 \pmod 7$; and Leonard and Williams [4] showed that 2 is a seventh power $(\bmod p)$ if and only if $x_1 \equiv 0 \pmod 2$. It is the purpose of this paper to treat the next case, namely $e=11$. In this case the system corresponding to (1. 1), (1. 2), (1. 3), again excluding two trivial solutions as in the case $e=7$, determines not a unique integer but rather three integers x_{11}, x_{12}, x_{13}. The corresponding necessary and sufficient conditions for 2 to be an eleventh power are expressed in terms of certain parity conditions on x_{11}, x_{12}, x_{13}, independent of how the three integers are labeled (see Theorem 2). Before proving Theorem 2 in § 4 we state in § 2, without proof, the relevant facts regarding the appropriate diophantine system (see Theorem 1), and in § 3 we prove two preliminary lemmas, the first of which is essentially due to Pepin [6]. For the proof of Theorem 1 the reader is referred to [5].

*) The research of the third author was supported by a grant (no. A7233) from the National Research Council of Canada.

2. The diophantine system

The following theorem is contained in [5].

Theorem 1. *Let p be a prime* $\equiv 1 \pmod{11}$. *Then there are exactly* 32 *integral solutions* $(x_1, \ldots, x_{10})$ *satisfying* $x_1 \equiv -1 \pmod{11}$, *of the diophantine system*

$$(2.1)\quad \begin{cases} 1200p = 12x_1^2 + 33x_2^2 + 55x_3^2 + 110x_4^2 + 330x_5^2 + 660 \cdot (x_6^2 + x_7^2 + x_8^2 + x_9^2 + x_{10}^2)\,, \\ 45x_2^2 + 5x_3^2 + 20x_4^2 - 540x_5^2 + 720x_6^2 - 720x_{10}^2 - 288x_1x_5 + 30x_2x_3 \\ \quad - 120x_2x_4 - 72x_2x_5 + 200x_3x_4 - 360x_3x_5 + 360x_4x_5 + 1440x_6x_7 \\ \quad - 1440x_6x_8 + 1440x_7x_8 - 1440x_7x_9 + 1440x_8x_9 - 1440x_8x_{10} \\ \quad + 2880x_9x_{10} = 0\,, \\ 45x_2^2 - 35x_3^2 - 80x_4^2 + 720x_9^2 - 720x_{10}^2 - 144x_1x_4 - 144x_1x_5 + 150\ x_2x_3 \\ \quad - 96x_2x_4 - 216x_2x_5 + 160x_3x_4 + 120x_3x_5 + 240x_4x_5 + 2880x_6x_7 \\ \quad - 1440x_6x_9 + 1440x_7x_8 - 1440x_7x_{10} + 1440x_8x_9 + 1440x_8x_{10} \\ \quad + 1440x_9x_{10} = 0\,, \\ 45x_2^2 + 5x_3^2 + 20x_4^2 - 540x_5^2 + 720x_7^2 - 720x_{10}^2 - 96x_1x_3 - 48x_1x_4 - 144x_1x_5 \\ \quad + 126x_2x_3 + 108x_2x_4 - 36x_2x_5 + 20x_3x_4 - 60x_3x_5 + 600x_4x_5 \\ \quad + 1440x_6x_7 + 1440x_6x_8 - 1440x_6x_{10} + 1440x_7x_8 + 1440x_7x_{10} \\ \quad + 2880x_8x_9 + 1440x_9x_{10} = 0\,, \\ 27x_2^2 + 35x_3^2 - 40x_4^2 - 360x_5^2 + 720x_8^2 - 720x_{10}^2 - 72x_1x_2 - 24x_1x_3 \\ \quad - 48x_1x_4 - 144x_1x_5 + 114x_2x_3 + 48x_2x_4 + 144x_2x_5 + 320x_3x_4 \\ \quad + 1440x_6x_7 + 1440x_6x_9 + 1440x_6x_{10} + 2880x_7x_8 + 1440x_7x_9 \\ \quad + 1440x_8x_9 + 1440x_9x_{10} = 0\,, \\ x_3 + 2x_4 + 2x_5 \equiv 0 \pmod{11}\,, \\ x_2 - x_4 + 3x_5 \equiv 0 \pmod{11}\,. \end{cases}$$

Of these 32 solutions, 2 trivial solutions are given by

$$(2.2)\qquad (5a, 0, 0, 0, 0, \pm b, \mp b, \pm b, \pm b, \pm b)\,,$$

where

$$(2.3)\qquad 4p = a^2 + 11b^2, \quad a \equiv 9 \pmod{11}\,.$$

Amongst the remaining 30 non-trivial solutions we can find 3 "generating" solutions

$$(2.4)\qquad (x_{1i}, \ldots, x_{10i}) \qquad (i = 1, 2, 3)$$

such that all 30 solutions are given by

$$(2.5)\qquad (x_{1i}, \ldots, x_{10i}) \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1/4 & -1/4 & -1/4 & -1/4 & 0 & 0 & 0 & 0 & 0 \\ 0 & -5/12 & -5/12 & 7/12 & -1/12 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5/3 & -1/3 & 1/6 & -1/6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1/2 & -1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{bmatrix}^k$$

for $i=1, 2, 3$ and $k=0, 1, 2, \ldots, 9$. Thus (2. 1) determines three integers x_{11}, x_{12}, x_{13} if the two trivial solutions (2. 2) are excluded.

We next indicate how the 32 solutions of (2. 1) arise. For full details the reader should consult [5]. Let $\zeta=\exp(2\pi i/11)$, and let $Q(\zeta)$ denote the cyclotomic field formed by adjoining ζ to the rational field Q. For $i=1, 2, \ldots, 10$ we let σ_i denote the automorphism of $Q(\zeta)$ defined by $\sigma_i(\zeta)=\zeta^i$. For any element $\lambda\in Q(\zeta)$ we set $\lambda_i=\sigma_i(\lambda)$ $(i=1, 2, \ldots, 10)$, so that in particular $\lambda_1=\lambda$. If π is any prime factor of p in $Z[\zeta]$—the ring of integers of $Q(\zeta)$—we define the eleventh power character $\left(\frac{\cdot}{\pi}\right)_{11}$ modulo π, for any $\lambda\in Z[\zeta]$, by

$$(2.\ 6)\qquad \left(\frac{\lambda}{\pi}\right)_{11}=\begin{cases}\zeta^r, & \text{if } \lambda\not\equiv 0 \pmod{\pi} \text{ and } \lambda^{\frac{p-1}{11}}\equiv\zeta^r \pmod{\pi}, \quad 1\leqq r\leqq 10\,,\\ 0, & \text{if } \lambda\equiv 0 \pmod{\pi}\,.\end{cases}$$

Thus for any rational integer x we have

$$(2.\ 7)\qquad \left(\frac{x}{\pi_k}\right)_{11}=\left(\frac{x}{\pi}\right)_{11}^k, \qquad k=1, 2, \ldots, 10\,.$$

In terms of this character we define the Jacobi sum of order 11, for any pair of integers m, n by

$$(2.\ 8)\qquad J_\pi(m, n)=\sum_{x=0}^{p-1}\left(\frac{x}{\pi}\right)_{11}^m\left(\frac{1-x}{\pi}\right)_{11}^n \quad (\in Z[\zeta])\,.$$

If none of m, n, $m+n$ is divisible by 11 it has the properties

$$(2.\ 9)\qquad J_\pi(m, n)\equiv -1 \pmod{(1-\zeta)^2}\,,$$

$$(2.\ 10)\qquad J_\pi(m, n)=J_\pi(n, m)=J_\pi(-m-n, n)=J_\pi(-m-n, m)\,,$$

$$(2.\ 11)\qquad J_\pi(m, n)\,\overline{J_\pi(m, n)}=p\,.$$

We next define integers a_i, b_i, c_i $(i=1, \ldots, 10)$, which we will need in the proof of Theorem 2, in terms of certain Jacobi sums. The integers a_i, b_i $(i=1, 2, \ldots, 10)$ are defined by

$$(2.\ 12)\qquad \alpha=J_\pi(1, 1)=\sum_{i=1}^{10} a_i\zeta^i\,,$$

$$(2.\ 13)\qquad \beta=J_\pi(1, 2)=\sum_{i=1}^{10} b_i\zeta^i\,.$$

Now it is known that

$$\alpha=\varepsilon\pi_1\pi_3\pi_4\pi_6\pi_9, \quad \beta=\eta\pi_1\pi_2\pi_4\pi_6\pi_8\,,$$

where ε, η are units in $Z[\zeta]$. Thus we have

$$\alpha_7=\varepsilon_7\pi_6\pi_7\pi_8\pi_9\pi_{10}\,,$$
$$\alpha_{10}=\varepsilon_{10}\pi_2\pi_5\pi_7\pi_8\pi_{10}\,,$$
$$\beta_7=\eta_7\pi_1\pi_3\pi_6\pi_7\pi_9\,,$$

and so

$$\gamma=\frac{\alpha_{10}\beta_7}{\alpha_7}=\varepsilon_7^{-1}\varepsilon_{10}\eta_7\pi_1\pi_2\pi_3\pi_5\pi_7\in Z[\zeta]\,,$$

as $\varepsilon_7^{-1}\varepsilon_{10}\eta_7$ is a unit of $Z[\zeta]$. Thus we can define the integers c_i $(i=1, 2, \ldots, 10)$ by

$$\gamma = \frac{\alpha_{10}\beta_7}{\alpha_7} = \sum_{i=1}^{10} c_i\zeta^i . \tag{2. 14}$$

The 30 non-trivial solutions of (2. 1) are obtained from $\alpha_1, \ldots, \alpha_{10}$, $\beta_1, \ldots, \beta_{10}$, $\gamma_1, \ldots, \gamma_{10}$, as follows: if $\sum_{i=1}^{10} k_i\zeta^i$ is one of these then $(x_1, \ldots, x_{10})$ given by

$$\left\{\begin{array}{l} x_1 = k_1+k_2+k_3+k_4+k_5+k_6+k_7+k_8+k_9+k_{10} , \\ x_2 = k_1+k_2+k_3+k_4-4k_5-4k_6+k_7+k_8+k_9+k_{10} , \\ x_3 = k_1+k_2+k_3-3k_4-3k_7+k_8+k_9+k_{10} , \\ x_4 = k_1+k_2-2k_3-2k_4+k_9+k_{10} , \\ x_5 = k_1-k_2-k_9+k_{10} , \\ x_6 = k_1-k_{10} , \\ x_7 = k_2-k_9 , \\ x_8 = k_3-k_8 , \\ x_9 = k_4-k_7 , \\ x_{10} = k_5-k_6 , \end{array}\right. \tag{2. 16}$$

is a non-trivial solution of (2. 1) with $x_1 \equiv -1 \pmod{11}$. The three integers x_{11}, x_{12}, x_{13} are given by

$$\left\{\begin{array}{l} x_{11} = a_1 + \cdots + a_{10} , \\ x_{12} = b_1 + \cdots + b_{10} , \\ x_{13} = c_1 + \cdots + c_{10} . \end{array}\right. \tag{2. 17}$$

Next we indicate where the two trivial solutions come from. We have

$$\alpha_2 = \varepsilon_2\pi_1\pi_2\pi_6\pi_7\pi_8, \quad \alpha_3 = \varepsilon_3\pi_1\pi_3\pi_5\pi_7\pi_9 ,$$

so that

$$\delta = \frac{\alpha_3\beta_1}{\alpha_2} = \varepsilon_2^{-1}\varepsilon_3\eta_1\pi_1\pi_3\pi_4\pi_5\pi_9 \in Z[\zeta] , \tag{2. 18}$$

as $\varepsilon_2^{-1}\varepsilon_3\eta_1$ is a unit of $Z[\zeta]$. Moreover as ζ is invariant under the mapping σ_3 it must be an integer of $Q(\sqrt{-11})$ $(\subset Q(\zeta))$. From (2. 9), (2. 11) and (2. 18) we have $\delta\bar{\delta}=p$, $\delta \equiv -1 \pmod{(1-\zeta)^2}$, so that

$$\left\{\begin{array}{l} \delta_1 = \delta_3 = \delta_4 = \delta_5 = \delta_9 = \frac{1}{2}(a+b\sqrt{-11}) , \\ \delta_2 = \delta_6 = \delta_7 = \delta_8 = \delta_{10} = \frac{1}{2}(a-b\sqrt{-11}) , \end{array}\right. \tag{2. 19}$$

where $4p = a^2 + 11b^2$, $a \equiv 9 \pmod{11}$. Using δ_1 and δ_2 in (2. 16) gives the two trivial solutions of (2. 1) noting that

$$\delta = \frac{1}{2}(b-a)(\zeta+\zeta^3+\zeta^4+\zeta^5+\zeta^9) - \frac{1}{2}(b+a)(\zeta^2+\zeta^6+\zeta^7+\zeta^8+\zeta^{10}) . \tag{2. 20}$$

Finally we note one further relationship we will need. If g is a primitive root $(\bmod\, p)$ such that $\left(\frac{g}{\pi}\right)_{11} = \zeta$ then

$$11a_i = \Phi_{11}(4g^i) - \Phi_{11}(4), \qquad i=1, 2, \ldots, 10 , \tag{2. 21}$$

where $\Phi_{11}(m)$ is the Jacobsthal sum of order 11 defined by

(2. 22) $$\Phi_{11}(m)=\sum_{x=0}^{p-1}\left(\frac{x(x^{11}+m)}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ denotes Legendre's symbol.

3. Two preliminary lemmas

We prove

Lemma 1. *Let p be a prime* $\equiv 1 \pmod{11}$.

(a) 2 *is an eleventh power* $(\bmod p)$ *if and only if*

$$a_1 \equiv a_2 \equiv \cdots \equiv a_{10} \equiv 1 \pmod 2.$$

(b) 2 *is not an eleventh power* $(\bmod p)$ *if and only if*

$$a_1 \equiv \cdots \equiv a_{k-1} \equiv a_{k+1} \equiv \cdots \equiv a_{10} \equiv 0 \pmod 2,$$
$$a_k \equiv 1 \pmod 2,$$

for some k with $1 \leqq k \leqq 10$.

Proof. Let m be an integer $\not\equiv 0 \pmod p$ and set

$$P=\text{Number of } x\,(1 \leqq x \leqq p-1) \text{ such that } \left(\frac{x(x^{11}+m)}{p}\right)=+1,$$
$$N=\text{Number of } x\,(1 \leqq x \leqq p-1) \text{ such that } \left(\frac{x(x^{11}+m)}{p}\right)=-1,$$
$$Z=\text{Number of } x\,(1 \leqq x \leqq p-1) \text{ such that } \left(\frac{x(x^{11}+m)}{p}\right)=\ \ 0,$$

so that

$$P+N+Z=p-1.$$

Now $\Phi_{11}(m)=\sum_{x=1}^{p-1}\left(\frac{x(x^{11}+m)}{p}\right)=P-N$, so that eleminating p we obtain

$$\Phi_{11}(m)=p-1-2N-Z \equiv Z \pmod 2.$$

But

$$Z=\begin{cases} 11, & \text{if } m \text{ is an eleventh power} \pmod p, \\ 0, & \text{otherwise}, \end{cases}$$

so modulo 2

(3. 1) $$\Phi_{11}(m) \equiv \begin{cases} 1, & \text{if } m \text{ is an eleventh power} \pmod p, \\ 0, & \text{otherwise}. \end{cases}$$

(a) If g is a primitive root $(\bmod p)$ such that $\left(\frac{g}{\pi}\right)_{11}=\zeta$ then

2 is an eleventh power (mod p)

$$\text{iff} \begin{cases} 4 \text{ is an eleventh power } (\text{mod } p) \text{ and} \\ 4g^k \text{ is not an eleventh power } (\text{mod } p), & k=1,2,\ldots,10, \end{cases}$$

$$\text{iff } \Phi_{11}(4) \equiv 1 \ (\text{mod } 2), \ \Phi_{11}(4g^k) \equiv 0 \ (\text{mod } 2), \qquad k=1,2,\ldots,10 \ (\text{by } (3.\ 1)),$$

$$\text{iff } a_k \equiv 1 \ (\text{mod } 2), \qquad k=1,2,\ldots,10 \ (\text{by } (2.\ 21)).$$

(b) Again for g a primitive root (mod p) such that $\left(\dfrac{g}{\pi}\right)_{11} = \zeta$ we have

2 is not an eleventh power (mod p)

$$\text{iff} \begin{cases} 4g^k \text{ is an eleventh power } (\text{mod } p) \text{ for some } k,\ 1 \leqq k \leqq 10, \\ 4g^i \text{ is not an eleventh power } (\text{mod } p) \text{ for } i=0,\ldots,10,\ i \neq k, \end{cases}$$

$$\text{iff} \begin{cases} \Phi_{11}(4g^k) \equiv 1 \ (\text{mod } 2) \\ \Phi_{11}(4g^i) \equiv 0 \ (\text{mod } 2),\ i \neq k, \end{cases}$$

$$\text{iff } a_i \equiv \begin{cases} 0 \ (\text{mod } 2),\ i \neq k \\ 1 \ (\text{mod } 2),\ i = k \end{cases},\quad i=1,2,\ldots,10.$$

Lemma 2. *Let p be a prime* $\equiv 1$ (mod 11). *Then* 2 *is an eleventh power* (mod p) *if and only if* $x_{11} \equiv 0$ (mod 2).

Proof. From (2. 17) and (2. 21) we have, as

$$\sum_{i=0}^{10} \Phi_{11}(4g^i) = -11, \quad x_{11} = -\left(1 + \Phi_{11}(4)\right)$$

so that from (3. 1) we have

2 is an eleventh power (mod p)
iff 4 is an eleventh power (mod p)
iff $\Phi_{11}(4) \equiv 1$ (mod 2)
iff $x_{11} \equiv 0$ (mod 2).

4. Proof of Theorem 2

We suppose that 3 solutions of (2. 1) are known, which generate the 30 non-trivial solutions by means of (2. 5). Thus we know x_{11}, x_{12}, x_{13} in some *unknown* order. We write u, v, w for x_{11}, x_{12}, x_{13} in some order, and prove, with a, b, given by (2. 3),

Theorem 2. *Let p be a prime* $\equiv 1$ (mod 11).

(a) *If* $a \equiv b \equiv 0$ (mod 2) *then* 2 *is an eleventh power* (mod p) *if and only if* $u \equiv v \equiv w \equiv 0$ (mod 2).

(b) *If* $a \equiv b \equiv 1$ (mod 2) *then* 2 *is an eleventh power* (mod p) *if and only if exactly one of* u, v, w *is even, say*, $u \equiv 0$ (mod 2), $v \equiv w \equiv 1$ (mod 2), $u_2 \equiv \cdots \equiv u_{10} \equiv 0$ (mod 2), *where* $(u_1, \ldots, u_{10})$ *is any solution of* (2. 1) *with* $u_1 = u$.

Proof. (a) If 2 is an eleventh power (mod p) then by Lemma 1 we have

(4. 1) $$a_1 \equiv a_2 \equiv \cdots \equiv a_{10} \equiv 1 \pmod 2$$

so that

(4. 2) $$x_{11} = a_1 + \cdots + a_{10} \equiv 0 \pmod 2 .$$

Also from (4. 1) and (2. 12) we have

$$\alpha_k \equiv 1 \pmod 2 \qquad (k = 1, 2, \ldots, 10)$$

and so by (2. 18)

$$\delta \equiv \beta_1 \pmod 2 ,$$

giving modulo 2

$$b_1 \equiv b_3 \equiv b_4 \equiv b_5 \equiv b_9 \equiv \frac{1}{2}(b-a), \quad b_2 \equiv b_6 \equiv b_7 \equiv b_8 \equiv b_{10} \equiv \frac{1}{2}(b+a) .$$

Hence we obtain

(4. 3) $$x_{12} = b_1 + \cdots + b_{10} \equiv 5b \equiv 0 \pmod 2 .$$

Also from (4. 1) and (2. 14) we have

$$\gamma \equiv \beta_7 \pmod 2$$

giving modulo 2

$$c_1 \equiv b_8,\ c_2 \equiv b_5,\ c_3 \equiv b_2,\ c_4 \equiv b_{10},\ c_5 \equiv b_7,\ c_6 \equiv b_4,\ c_7 \equiv b_1,\ c_8 \equiv b_9,\ c_9 \equiv b_6,\ c_{10} \equiv b_3 .$$

Hence we have

(4. 4) $$x_{13} = c_1 + \cdots + c_{10} \equiv b_1 + \cdots + b_{10} \equiv 0 \pmod 2 .$$

Thus from (4. 2), (4. 3), (4. 4) we have

$$u \equiv v \equiv w \equiv 0 \pmod 2 .$$

Conversely if $u \equiv v \equiv w \equiv 0 \pmod 2$ then $x_{11} \equiv 0 \pmod 2$ and Lemma 2 shows that 2 is an eleventh power (mod p).

(b) If 2 is an eleventh power (mod p) then by Lemma 1 we have

(4. 5) $$a_1 \equiv a_2 \equiv \cdots \equiv a_{10} \equiv 1 \pmod 2 .$$

and so

(4. 6) $$x_{11} \equiv x_{21} \equiv \cdots \equiv x_{10\,1} \equiv 0 \pmod 2$$

for any solution $(x_{11}, \ldots, x_{10\,1})$ arising from one of $\alpha_1, \ldots, \alpha_{10}$. Also from (4. 5) and (2. 12) we have

$$\alpha_k \equiv 1 \pmod 2 \qquad (k = 1, 2, \ldots, 10)$$

and so from (2. 18) we obtain

(4. 7) $$\delta \equiv \beta_1 \pmod 2 ,$$

giving modulo 2

$$b_1 \equiv b_3 \equiv b_4 \equiv b_5 \equiv b_9 \equiv \frac{1}{2}(b-a), \quad b_2 \equiv b_6 \equiv b_7 \equiv b_8 \equiv b_{10} \equiv \frac{1}{2}(b+a).$$

Hence we obtain

(4. 8) $$x_{12}=b_1+\cdots+b_{10}\equiv 5b\equiv 1 \pmod 2 .$$

Also from (4. 7) and (2. 14) we have

$$\gamma\equiv\beta_7 \pmod 2 ,$$

and so modulo 2 we have

$$c_1\equiv b_8,\ c_2\equiv b_5,\ c_3\equiv b_2,\ c_4\equiv b_{10},\ c_5\equiv b_7,\ c_6\equiv b_4,\ c_7\equiv b_1,\ c_8\equiv b_9,\ c_9\equiv b_6,\ c_{10}\equiv b_3 ,$$

giving

(4. 9) $$x_{13}=c_1+\cdots+c_{10}\equiv b_1+\cdots+b_{10}\equiv 1 \pmod 2 .$$

Thus from (4. 6), (4. 8), (4. 9) we see that exactly one of u, v, w is even, say $u\equiv 0 \pmod 2$, $v\equiv w\equiv 1 \pmod 2$, and that $u_2\equiv\cdots\equiv u_{10}\equiv 0 \pmod 2$ for any solution $(u_1,\ldots,u_{10})$ of (2. 1) with $u_1=u$.

We will prove the converse by showing that if 2 is not an eleventh power $(\operatorname{mod} p)$ then exactly one of u, v, w is even, say $u\equiv 0 \pmod 2$, $v\equiv w\equiv 1 \pmod 2$, but for any solution $(u_1,\ldots,u_{10})$ of (2. 1) with $u_1=u$ there is some $i(2\leqq i\leqq 10)$ with $u_i\equiv 1 \pmod 2$.

As 2 is not an eleventh power $(\operatorname{mod} p)$ by Lemma 1 we have for some $k(1\leqq k\leqq 10)$

(4. 10) $$a_1\equiv\cdots\equiv a_{k-1}\equiv a_{k+1}\equiv\cdots\equiv a_{10}\equiv 0 \pmod 2,\quad a_k\equiv 1 \pmod 2 ,$$

and so

(4. 11) $$x_{11}=a_1+\cdots+a_{10}\equiv 1 \pmod 2 .$$

We will just treat the case $k=1$; the other possibilities can be treated in the same way with only minor differences. Thus from (4. 10) (with $k=1$) and (2. 12) we have

(4. 12) $$\alpha_l\equiv\zeta^l \pmod 2 \qquad (l=1,2,\ldots,10)$$

and so from (2. 18) we obtain

$$\delta\equiv\zeta\beta \pmod 2$$

giving modulo 2

(4. 13) $$\begin{cases} b_1\equiv b_5\equiv b_6\equiv b_7\equiv b_9\equiv 1 , \\ b_2\equiv b_3\equiv b_4\equiv b_8\equiv 0 , \\ \quad b_{10}\equiv \frac{1}{2}(b-a) . \end{cases}$$

Hence we have

(4. 14) $$x_{12}=b_1+\cdots+b_{10}\equiv\frac{1}{2}(b+a) \pmod 2 .$$

Also from (4. 12) and (2. 14) we have

$$\gamma\equiv\zeta^3\beta_7 \pmod 2 ,$$

and so modulo 2

$$(4.15)\qquad \begin{cases} c_1 \equiv b_6 - b_9 \equiv 0\,, \\ c_2 \equiv b_3 - b_9 \equiv 1\,, \\ c_3 \equiv \quad - b_9 \equiv 1\,, \\ c_4 \equiv b_8 - b_9 \equiv 1\,, \\ c_5 \equiv b_5 - b_9 \equiv 0\,, \\ c_6 \equiv b_2 - b_9 \equiv 1\,, \\ c_7 \equiv b_{10} - b_9 \equiv \frac{1}{2}(b-a) + 1\,, \\ c_8 \equiv b_7 - b_9 \equiv 0\,, \\ c_9 \equiv b_4 - b_9 \equiv 1\,, \\ c_{10} \equiv b_1 - b_9 \equiv 0\,, \end{cases}$$

giving

$$(4.16)\qquad x_{13} \equiv c_1 + \cdots + c_{10} \equiv \frac{1}{2}(b-a)\,,$$

and so from (4. 14) and (4. 16) we obtain

$$(4.17)\qquad x_{12} + x_{13} \equiv b \equiv 1 \pmod 2\,.$$

Thus from (4. 11), (4. 17) x_{11} is odd and exactly one of x_{12}, x_{13} is even. If $x_{12} \equiv 0 \pmod 2$, the solution corresponding to β, say $(x_{12}, x_{22}, \ldots, x_{10\,12})$, has from (4. 13) and (2. 16)

$$x_{92} = b_4 - b_7 \equiv 1 \pmod 2\,,$$

and so by (2. 5) any solution arising from some β_i will have at least one odd coordinate. On the other hand if $x_{13} \equiv 0 \pmod 2$, the solution corresponding to γ, say $(x_{13}, x_{23}, \ldots, x_{10\,3})$ has from (4. 15) and (2. 16)

$$x_{83} = c_3 - c_8 \equiv 1 \pmod 2\,,$$

and so by (2. 5) any solution arising from some γ_i will have at least one odd coordinate.

This completes the proof of Theorem 2.

5. Examples

(i) $p = 23$. As $4 \cdot 23 = 9^2 + 11 \cdot 1^2$ we have $a \equiv b \equiv 1 \pmod 2$. Three generating solutions of (2. 1) are

$$(21, 1, -3, 0, -4, 2, 2, 0, -1, 4)\,,$$
$$(-12, 3, -1, 8, -2, 2, -2, 1, 4, 1)\,,$$
$$(-1, 24, -4, 2, 0, -1, -1, 2, -2, 1)\,,$$

so that we can take

$$u = -12, \quad v = 21, \quad w = -1\,.$$

Thus by Theorem 2 as not all the coordinates in the second solution are even 2 is *not* an eleventh power (mod 23).

(ii) $p = 331$. As $4 \cdot 331 = 35^2 + 11 \cdot 3^2$ we have $a \equiv b \equiv 1 \pmod 2$. Three generating solutions of (2. 1) are

$$(32, -48, 0, -12, 12, 6, 2, 14, -6, -10),$$
$$(-67, 18, -14, 40, 0, 11, -3, -9, 1, -3),$$
$$(109, -6, 2, -16, 4, 5, 3, 11, -3, -13),$$

so that we can take

$$u = 32, \quad v = -67, \quad w = 109.$$

Thus by Theorem 2 as all the coordinates in the first solution are even, 2 is an eleventh power (mod 331). Indeed it is easy to check that

$$2 \equiv 62^{11} \pmod{331}.$$

(iii) $p = 397$. As $4 \cdot 397 = 2^2 + 11 \cdot 12^2$ we have $a \equiv b \equiv 0 \pmod 2$. Three generating solutions of (2. 1) are

$$(-45, 15, -9, 3, 29, -2, -13, -2, 2, -8),$$
$$(43, 43, -5, 25, -17, -2, -1, 18, 4, 0),$$
$$(-67, 13, 37, 10, -12, -6, -10, 17, 2, 0),$$

so that we can take $u = -45$, $v = 43$, $w = -67$. Thus, by Theorem 2, as $u \equiv v \equiv w \equiv 1 \pmod 2$, 2 is *not* an eleventh power (mod 397).

Unfortunately no example of the situation $a \equiv b \equiv 0 \pmod 2$, 2 an eleventh power $(\bmod p)$, occurs for $p < 1000$, the primes for which the authors know the solutions of (2. 1). These solutions were computed by the second author using the University of Alberta's computer.

References

[1] *C. G. J. Jacobi*, De residuis cubicis commentatio numerosa, J. reine angew. Math. **2** (1827), 66—69.

[2] *Emma Lehmer*, The quintic character of 2 and 3, Duke Math. J. **18** (1951), 11—18.

[3] *P. A. Leonard* and *K. S. Williams*, A diophantine system of Dickson, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **56** (1974), 145—150.

[4] *P. A. Leonard* and *K. S. Williams*, The septic character of 2, 3, 5 and 7, Pacific J. Math. **52** (1974), 143—147.

[5] *P. A. Leonard* and *K. S. Williams*, The cyclotomic numbers of order eleven, Acta Arith. **26** (1975), 367—383.

[6] *T. Pepin*, Mémoire sur les lois de reciprocité relatives aux résidues de puissances, Pontif Accad. Sci. **31** (1877), 40—148.

Arizona State University, Tempe, Arizona 85281, USA,

University of Alberta, Edmonton, Alberta, Canada,

Carleton University, Ottawa, Ontario, Canada

Eingegangen 29. April 1974