ELEMENTARY TREATMENT OF A QUADRATIC PARTITION OF PRIMES $p \equiv 1 \pmod 7$

BY

KENNETH S. WILLIAMS[1]

This paper is dedicated to the memory of the great American mathematician Leonard Eugene Dickson, who was born 100 years ago on January 22, 1874 in Independence, Iowa, U.S.A., and who served as a professor of mathematics at the University of Chicago for 41 years.

1. Introduction

Let e be an integer > 1, p a prime congruent to 1 (mod e), and g a primitive root (mod p). The cyclotomic number $(h, k)_e$ is the number of solutions s, t of the trinomial congruence $g^{es+h} + 1 \equiv g^{et+k} \pmod p$, where the values of s and t are each selected from $0, 1, \cdots, f-1$, where $f = (p-1)/e$. A central problem in the theory of cyclotomy is to obtain formulae for the numbers $(h, k)_e$ in terms of the solutions of certain diophantine systems. For example [1] when $e = 3$ the cyclotomic numbers of order 3 can be given in terms of the solutions a, b of the single diophantine equation $4p = a^2 + 27b^2$, with $a \equiv 1 \pmod 3$, and when $e = 5$ the cyclotomic numbers of order 5 can be given in terms of the solutions x, u, v and w of the pair of diophantine equations

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2,\ xw = v^2 - 4uv - u^2 \quad \text{with} \quad x \equiv 1 \pmod 5.$$

Recently P. A. Leonard and the author [3] evaluated the cyclotomic numbers of order 7 in terms of the solutions $(x_1, x_2, x_3, x_4, x_5, x_6)$ of the triple of diophantine equations

$$72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \tag{1.1}$$

$$12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0, \tag{1.2}$$

$$12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0. \tag{1.3}$$

(Another application of this system has been given in [4].) Clearly all solutions $(x_1, \cdots, x_6)$ of (1.1)–(1.3) satisfy $x_1 \equiv \pm 1 \pmod 7$. Moreover if $(x_1, \cdots, x_6)$ is a solution so is $(-x_1, \cdots, -x_6)$. Thus without any loss of

Received December 17, 1973.

[1] This research was supported by a grant from the National Research Council of Canada. The author's sabbatical leave at the University of British Columbia was also supported by National Research Council travel grant.

generality we restrict our attention to those solutions satisfying

$$x_1 \equiv +1 \pmod 7. \tag{1.4}$$

The nature of the solutions of the system (1.1)–(1.4) was obtained from the work of Dickson [1] by P. A. Leonard and the author [5], using a number of results from algebraic number theory, for example, that the ring $Z[\zeta]$, $\zeta = \exp(2\pi i/7)$, is a unique factorization domain, the form of the prime factorizations of p and certain Jacobi sums in $Z[\zeta]$, etc. It is the aim of this paper to give a completely elementary, self-contained treatment of the system (1.1)–(1.4) without reference to the theory of algebraic numbers.

As p is a prime $\equiv 1 \pmod 7$ there are integers t and u such that $p = t^2 + 7u^2$. t is uniquely determined if we require $t \equiv 1 \pmod 7$, in which case u is determined up to sign. Then $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$ give two solutions of (1.1)–(1.4). We call these the *trivial* solutions of (1.1)–(1.4), any solution of the system different from these two will be called a non-trivial solution. In order to give explicit expressions for the non-trivial solutions of (1.1)–(1.4) it is convenient to introduce the Jacobsthal sums $\phi_e(n)$ defined for any integer n by

$$\phi_e(n) = \sum_{h=1}^{p-1} \left(\frac{h}{p}\right)\left(\frac{h^e + n}{p}\right). \tag{1.5}$$

where the symbol (h/p) is the Legendre symbol giving the quadratic character of h with respect to p.

THEOREM 1. *There are exactly six distinct non-trivial solutions* $(x_1, \cdots, x_6)$ *of* (1.1)–(1.4). *These are given by*

$$\begin{aligned}
x_1 &= 1 + \phi_7(4),\\
7x_2 &= \phi_7(4g^{i^*}) - \phi_7(4g^{6i^*}),\\
7x_3 &= \phi_7(4g^{2i^*}) - \phi_7(4g^{5i^*}),\\
7x_4 &= \phi_7(4g^{3i^*}) - \phi_7(4g^{4i^*}),\\
49x_5 &= \phi_7(4g^{i^*}) + \phi_7(4g^{2i^*}) - 2\phi_7(4g^{3i^*}) - 2\phi_7(4g^{4i^*}) + \phi_7(4g^{5i^*})\\
&\quad + \phi_7(4g^{6i^*}),\\
49x_6 &= \phi_7(4g^{i^*}) - \phi_7(4g^{2i^*}) - \phi_7(4g^{5i^*}) + \phi_7(4g^{6i^*}),
\end{aligned} \tag{1.6}$$

where $i = 1, 2, 3, 4, 5, 6$ and i^* denotes the unique integer satisfying $ii^* \equiv 1 \pmod 7$, $1 \le i^* \le 6$.

Theorem 1 will be proved by proving two theorems from which it follows immediately.

THEOREM 2. *If*

$$x_1 = 1 + \phi_7(4),$$

$$7x_2 = \phi_7(4g) - \phi_7(4g^6),$$
$$7x_3 = \phi_7(4g^2) - \phi_7(4g^5),$$
$$7x_4 = \phi_7(4g^3) - \phi_7(4g^4),$$
$$49x_5 = \phi_7(4g) + \phi_7(4g^2) - 2\phi_7(4g^3) - 2\phi_7(4g^4) + \phi_7(4g^5) + \phi_7(4g^6),$$
$$49x_6 = \phi_7(4g) - \phi_7(4g^2) - \phi_7(4g^5) + \phi_7(4g^6),$$

then $(x_1, x_2, x_3, x_4, x_5, x_6)$ *is a non-trivial solution of* (1.1)–(1.4).

THEOREM 3. *If* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *is a non-trivial solution of* (1.1)–(1.4) *then all non-trivial solutions are given by*

$$(x_1, x_2, x_3, x_4, x_5, x_6)\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & -\frac{3}{2} & -\frac{1}{2} \end{bmatrix}^k$$

where $k = 0, 1, 2, 3, 4, 5$.

Theorem 2 is proved by using results due to Whiteman [6] and Theorem 3 is proved following a method of Dickson [1].

2. Cyclotomy and Jacobsthal sums

We will make use of the following results concerning the cyclotomic numbers and Jacobsthal sums of order 7 which we state here for convenience. For proofs and references the reader is referred to Whiteman [6].

(2.1) $$(h, k)_7 = (h + 7l, k + 7m)_7, \qquad (h, k)_7 = (k, h)_7 = (7 - h, k - h)_7,$$

(2.2) $$\phi_7(4g^k) = 7\{\textstyle\sum_{l=0}^{6}(l, k - l)_7 - f\},$$

(2.3) $$\textstyle\sum_{h=0}^{6}(h, k)_7 = f - 1 \quad \text{if} \quad k = 0,$$
$$= f \qquad \text{if} \quad 1 \le k \le 6,$$

(2.4) $$\textstyle\sum_{k=0}^{6}\phi_7(4g^k) = -7,$$

(2.5) $$\textstyle\sum_{k=0}^{6}\{\phi_7(4g^k)\}^2 = 42p + 7,$$

(2.6) $$\textstyle\sum_{k=0}^{6}\phi_7(4g^k)\phi_7(4g^{k+s}) = -7p + 7 \quad (s = 1, 2, 3),$$

(2.7) $$\textstyle\sum_{k=0}^{6}\phi_7(4g^k)\zeta^k/7 = \sum_{x=2}^{p-2}\zeta^{\mathrm{ind}_g\,(x(1-x))},$$

where $\zeta = \exp(2\pi i/7)$ and $\mathrm{ind}_g(a)$ $(a \not\equiv 0 \pmod p)$ denotes the unique integer b such that $a \equiv g^b \pmod p$, $0 \le b \le p - 2$.

3. Existence of non-trivial solutions—proof of Theorem 2

By (2.1) the 49 cyclotomic numbers $(h, k)_7$ $(h, k = 0, 1, 2, 3, 4, 5, 6)$ reduce to the 12 cyclotomic numbers

$$A = (0,0)_7,\quad B = (0,1)_7,\quad C = (0,2)_7,\quad D = (0,3)_7,$$
$$E = (0,4)_7,\quad F = (0,5)_7,\quad G = (0,6)_7,\quad H = (1,2)_7, \tag{3.1}$$
$$I = (1,3)_7,\quad J = (1,4)_7,\quad K = (1,5)_7,\quad L = (2,4)_7.$$

Hence by (2.2) we have

$$\phi_7(4) = 7\{A + 2H + 2J + 2L - f\}, \tag{3.2}$$
$$\phi_7(4g) = 7\{2B + D + 2I + 2L - f\}, \tag{3.3}$$
$$\phi_7(4g^2) = 7\{2C + G + 2I + 2J - f\}, \tag{3.4}$$
$$\phi_7(4g^3) = 7\{C + 2D + 2H + 2K - f\}, \tag{3.5}$$
$$\phi_7(4g^4) = 7\{2E + F + 2H + 2I - f\}, \tag{3.6}$$
$$\phi_7(4g^5) = 7\{B + 2F + 2J + 2K - f\}, \tag{3.7}$$
$$\phi_7(4g^6) = 7\{E + 2G + 2K + 2L - f\}. \tag{3.8}$$

Using (3.3)–(3.8) we obtain

$$\phi_7(4g) - \phi_7(4g^2) - \phi_7(4g^5) + \phi_7(4g^6) = 7\{B - 2C + D + E - 2F + G - 4J + 4L\} \tag{3.9}$$

and

$$\phi_7(4g) + \phi_7(4g^2) - 2\phi_7(4g^3) - 2\phi_7(4g^4) + \phi_7(4g^5) + \phi_7(4g^6) = 7\{3B - 3D - 3E + 3G - 8H + 4J + 4L\}. \tag{3.10}$$

Now from (2.3) we have (taking $k = 1, 2, 3$):

$$B + G + 2H + I + J + K = f, \tag{3.11}$$
$$C + F + H + I + K + 2L = f, \tag{3.12}$$
$$D + E + I + 2J + K + L = f, \tag{3.13}$$

so that forming (3.11) − 2(3.12) + (3.13) and 3(3.11) − 3(3.13) we obtain

$$B - 2C + D + E - 2F + G + 3J - 3L = 0 \tag{3.14}$$

and

$$3B - 3D - 3E + 3G + 6H - 3J - 3L = 0. \tag{3.15}$$

Using (3.14) and (3.15) in (3.9) and (3.10) we deduce

$$\phi_7(4g) - \phi_7(4g^2) - \phi_7(4g^5) + \phi_7(4g^6) = 49(L - J) \tag{3.16}$$

and

$$\phi_7(4g) + \phi_7(4g^2) - 2\phi_7(4g^3) - 2\phi_7(4g^4) + \phi_7(4g^5) + \phi_7(4g^6) = 49(-2H + J + L). \tag{3.17}$$

Equations (3.2)–(3.8), (3.16) and (3.17) show that we can define integers $x_1, \cdots, x_6$ by

$$
\begin{aligned}
x_1 &= 1 + \phi_7(4), \\
7x_2 &= \phi_7(4g) - \phi_7(4g^6), \\
7x_3 &= \phi_7(4g^2) - \phi_7(4g^5), \\
7x_4 &= \phi_7(4g^3) - \phi_7(4g^4), \\
49x_5 &= \phi_7(4g) + \phi_7(4g^2) - 2\phi_7(4g^3) - 2\phi_7(4g^4) + \phi_7(4g^5) + \phi_7(4g^6), \\
49x_6 &= \phi_7(4g) - \phi_7(4g^2) - \phi_7(4g^5) + \phi_7(4g^6),
\end{aligned} \tag{3.18}
$$

with $x_1 \equiv 1 \pmod 7$. Now from (2.4) and (3.18) we obtain

$$
\begin{aligned}
\phi_7(4) &= -1 + x_1, \\
12\phi_7(4g) &= -12 - 2x_1 + 42x_2 + 49x_5 + 147x_6, \\
12\phi_7(4g^2) &= -12 - 2x_1 + 42x_3 + 49x_5 - 147x_6, \\
12\phi_7(4g^3) &= -12 - 2x_1 + 42x_4 - 98x_5, \\
12\phi_7(4g^4) &= -12 - 2x_1 - 42x_4 - 98x_5, \\
12\phi_7(4g^5) &= -12 - 2x_1 - 42x_3 + 49x_5 - 147x_6, \\
12\phi_7(4g^6) &= -12 - 2x_1 - 42x_2 + 49x_5 + 147x_6,
\end{aligned} \tag{3.19}
$$

and substituting these values into (2.5) and (2.6), the latter in the form

$$
\begin{aligned}
\textstyle\sum_{k=0}^{6} \phi_7(4g^k)\{\phi_7(4g^{k+1}) - \phi_7(4g^{k+2})\} &= 0, \\
\textstyle\sum_{k=0}^{6} \phi_7(4g^k)\{\phi_7(4g^{k+1}) - \phi_7(4g^{k+3})\} &= 0,
\end{aligned}
$$

we obtain (1.1), (1.2), (1.3), showing that (3.18) gives a solution of the diophantine system. All that remains to be done, is to show that the solution given by (3.18) is a non-trivial solution. Suppose not; then

$$x_1 = -6t, \quad x_2 = \pm 2u, \quad x_3 = \pm 2u, \quad x_4 = \mp 2u, \quad x_5 = 0, \quad x_6 = 0,$$

and (3.19) gives

$$
\begin{aligned}
\phi_7(4) &= -1 - 6t, \\
\phi_7(4g) &= \phi_7(4g^2) = \phi_7(4g^4) = -1 + t \pm 7u, \\
\phi_7(4g^3) &= \phi_7(4g^5) = \phi_7(4g^6) = -1 + t \mp 7u.
\end{aligned} \tag{3.20}
$$

We define a seventh power character χ by

$$
\begin{aligned}
\chi(x) &= \zeta^{\mathrm{ind}_g(x)} \quad \text{if} \quad x \not\equiv 0 \pmod p, \\
&= 0 \qquad\quad \text{if} \quad x \equiv 0 \pmod p.
\end{aligned} \tag{3.21}
$$

For any integers m, n we define the Jacobi and Gauss sums by

$$(3.22)\quad J(m,n)=\sum_{x=0}^{p-1}\chi^m(x)\chi^n(1-x),\qquad G(m)=\sum_{x=0}^{p-1}\chi^m(x)\zeta^x.$$

These sums have the following simple properties (see for example [2]):

$$(3.23)\quad \begin{aligned} J(m,n)&=G(m)G(n)/G(m+n)\quad \text{if}\quad m+n\not\equiv 0 \pmod 7,\\ G(m)G(7-m)&=p\quad \text{if}\quad m\not\equiv 0 \pmod 7.\end{aligned}$$

Hence from (3.23) we have

$$\begin{aligned} pJ(1,2)&=G(3)G(4)\cdot\frac{G(1)G(2)}{G(3)}=G(1)G(2)G(4)\\ &=\frac{G(1)^2}{G(2)}\cdot\frac{G(2)^2}{G(4)}\cdot\frac{G(4)^2}{G(1)},\end{aligned}$$

that is

$$(3.24)\qquad pJ(1,2)=J(1,1)J(2,2)J(4,4).$$

From (2.7), (3.20), (3.21), (3.22) we have

$$\begin{aligned} J(1,1)&=\sum_{x=0}^{p-1}\chi(x)\chi(1-x)=\sum_{x=2}^{p-1}\zeta^{\mathrm{ind}_g(x(1-x))}\\ &=\sum_{i=0}^{6}\phi_7(4g^i)\zeta^i/7=t\pm u\sqrt{-7},\end{aligned}$$

and similarly $J(2,2)=J(4,4)=t\pm u\sqrt{-7}$. Thus from (3.24) and $p=t^2+7u^2$ we obtain

$$J(1,2)=(t\pm u\sqrt{-7})^3/p=(-3t\mp u\sqrt{-7})+(4t^3/p\pm(4t^2u\sqrt{-7})/p).$$

Clearly $4t^3/p$, $4t^2u/p$ are not rational integers so that $J(1,2)$ is not an integer of $Q(\sqrt{-7})$. This is a contradiction as $J(1,2)$, being an element of $Q(\sqrt{-7})$ and an integer of $Q(\zeta)\supset Q(\sqrt{-7})$, must be an integer of $Q(\sqrt{-7})$.

4. Necessary and sufficient conditions for trivial solutions

In this section we derive convenient conditions for identifying trivial solutions of (1.1)–(1.4). Condition (E) of Lemma 2 will be used in the proof of Theorem 2.

LEMMA 1. *The only integral solution (x, y) of the diophantine equation*

$$(4.1)\qquad x^3+9x^2y-xy^2-y^3=0$$

is $(x, y)=(0, 0)$.

Proof. Let (x, y) be an integral solution of (4.1). If $y=0$ then clearly (4.1) implies $x=0$. If $y\neq 0$ we can define a rational number z by

$$z=(x-3y)/2y.$$

From (4.1) we deduce that z satisfies $z^3-7z+7=0$. This is a contradiction as, by Eisentein's criteria, z^3-7z+7 is irreducible over the rationals.

LEMMA 2. *The solution* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *of* (1.1)–(1.4) *is one of the two trivial solutions* $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$, *where* $p = t^2 + 7u^2$ *and* $t \equiv 1 \pmod 7$, *if and only if any one of the following is satisfied:*

(A) $x_5 = x_6 = 0$,

(B) $x_2 = x_3 = -x_4$,

(C) $x_1 = -6t$, $x_2 + x_3 - x_4 = \pm 6u$,

(D) $x_1^2 + 7(x_2 + x_3 - x_4)^2 \equiv 0 \pmod p$,

(E) $42x_2 \equiv \varepsilon w\{-2x_1 + 7x_5 - 63x_6\} \pmod p$,
$42x_3 \equiv \varepsilon w\{-2x_1 - 35x_5 + 21x_6\} \pmod p$,
$43x_4 \equiv \varepsilon w\{2x_1 - 28x_5 - 42x_6\} \pmod p$,

where $\varepsilon = \pm 1$ *and* w *is a fixed solution of* $w^2 \equiv -7 \pmod p$.

Proof. Clearly if $(x_1, x_2, x_3, x_4, x_5, x_6)$ is trivial then (A), (B), (C), (D), (E) are satisfied.

(A) If $x_5 = x_6 = 0$ then (1.2) and (1.3) give

$$x_2^2 - x_4^2 + 2x_2x_3 - 2x_2x_4 + 4x_3x_4 = 0, \tag{4.2}$$

$$x_3^2 - x_4^2 + 4x_2x_3 + 2x_2x_4 + 2x_3x_4 = 0. \tag{4.3}$$

Subtracting (4.3) from (4.2) we obtain

$$(4x_2 - 2x_3)x_4 = x_2^2 - 2x_2x_3 - x_3^2.$$

Using this in (4.2) we obtain after some simplification

$$(x_2 - x_3)(x_2^3 + 9x_2^2x_3 - x_2x_3^2 - x_3^3) = 0.$$

If $x_2^3 + 9x_2^2x_3 - x_2x_3^2 - x_3^3 = 0$, by Lemma 1, we must have $x_2 = x_3 = 0$, and hence

$$x_2 = x_3 = x_4 = x_5 = x_6 = 0,$$

so that (1.1) gives $72p = 2x_1^2$, which is impossible.
Hence we must have $x_2 = x_3$ and so from (4.3) we obtain $x_2 = x_3 = -x_4$. Then (1.1) gives $36p = x_1^2 + 63x_2^2$ implying that $x_1 = -6t$, $x_2 = \pm 2u$. This proves that $(x_1, x_2, x_3, x_4, x_5, x_6)$ is the trivial solution $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$.

(B) Next, if $x_2 = x_3 = -x_4$ then (1.3) − (1.2) and (1.2) give

$$8x_1x_5 = 7(+x_5^2 - 18x_5x_6 - 3x_6^2), \qquad 8x_1x_6 = 7(-3x_5^2 - 2x_5x_6 + 9x_6^2),$$

so that

$$x_5(-3x_5^2 - 2x_5x_6 + 9x_6^2) = x_6(x_5^2 - 18x_5x_6 - 3x_6^2),$$

which reduces to $x_6^3 + 9x_6^2x_5 - x_6x_5^2 - x_5^2 = 0$. Hence by Lemma 1 we have $x_5 = x_6 = 0$ and (A) shows that $(x_1, \cdots, x_6)$ is the trivial solution.

(C) Now if $x_1 = -6t$, $x_2 + x_3 - x_4 = \pm 6u$,
then (1.1) gives

$$0 = 12(x_2^2 + x_3^2 + x_2x_3 \mp 6ux_2 \mp 6ux_3 + 12u^2) + 49(x_5^2 + 3x_6^2),$$

that is

$$0 = 6(x_2 \mp 2u)^2 + 6(x_3 \mp 2u)^2 + 6(x_2 + x_3 \mp 2u)^2 + 49(x_5^2 + 3x_6^2),$$

so that

$$x_2 = x_3 = \pm 2u, \qquad x_4 = \pm 2u, \qquad x_5 = x_6 = 0,$$

and the solution is trivial by (A) or (B).

(D) If $x_1^2 + 7(x_2 + x_3 - x_4)^2 \equiv 0 \pmod{p}$
we define an integer h by $x_1^2 + 7(x_2 + x_3 - x_4)^2 = hp$. Now in view of the trivial inequality $a^2 + b^2 \geq \pm 2ab$, for any real numbers a and b, we have

$$\begin{aligned} 0 \leq hp &= x_1^2 + 7x_2^2 + 7x_3^2 + 7x_4^2 + 14x_2x_3 - 14x_2x_4 - 14x_3x_4, \\ &\leq x_1^2 + 21(x_2^2 + x_3^2 + x_4^2), \\ &\leq \tfrac{1}{2}(2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \\ &= 36p, \end{aligned}$$

so that $0 \leq h \leq 36$. Now from (1.1) we have that $x_5^2 + 3x_6^2$ is even so that $x_5^2 + 3x_6^2 \equiv 0 \pmod 4$, giving

$$0 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod 2,$$

so that $x_1^2 + 7(x_2 + x_3 - x_4)^2$ is even and hence

$$x_1^2 + 7(x_2 + x_3 - x_4)^2 \equiv 0 \pmod 4.$$

Thus we may set $h = 4g$, with $0 \leq g \leq 9$, and we have, with $y = x_2 + x_3 - x_4$,

$$x_1^2 + 7y^2 = 4gp. \tag{4.4}$$

We now show that none of the possibilities $g = 0, 1, \cdots, 8$ can occur. If $g = 0$ then $x_1 = 0$ and (1.1) implies that $72p \equiv 0 \pmod 7$ which is impossible. If $g = 1, 4, 7, 8$ then (4.4) gives $x_1^2 \equiv 0, 2$, or $4 \pmod 7$, which is impossible as $x_1 \equiv 1 \pmod 7$. If $g = 2$ then (4.4) gives $x_1 = \pm(t \pm 7u)$. Substituting this value into (1.1) we obtain $t \equiv 0 \pmod 7$ which is clearly impossible. $g = 3, 5$ and 6 are impossible for otherwise $x_1^2 + 7y^2$ would have a prime q, such that $(-7/q) = -1$, dividing it to the first power. Hence we must have $g = 9$ and so $x_1^2 + 7(x_2 + x_3 - x_4)^2 = 36p$, giving

$$x_1 \equiv x_2 + x_3 - x_4 \equiv 0 \pmod 6,$$

say $x_1 = -6t$, $x_2 + x_3 - x_4 = 6u$, with $p = t^2 + 7u^2$.

(C) then proves that the solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ is trivial.

(E) Finally, if we have

$$\begin{aligned} 42x_2 &\equiv \varepsilon w\{-2x_1 + 7x_5 - 63x_6\} \pmod p, \\ 42x_3 &\equiv \varepsilon w\{-2x_1 - 35x_5 + 21x_6\} \pmod p, \\ 42x_4 &\equiv \varepsilon w\{2x_1 - 28x_5 - 42x_6\} \pmod p, \end{aligned}$$

then $42(x_2 + x_3 - x_4) \equiv -6\varepsilon w x_1 \pmod{p}$, that is

$$x_1 \equiv \varepsilon w(x_2 + x_3 - x_4) \pmod{p},$$

or

$$x_1^2 + 7(x_2 + x_3 - x_4)^2 \equiv 0 \pmod{p},$$

and the triviality of the solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ follows from (D).

5. Congruence conditions for non-trivial solutions

Let r be an integer of exponent 7 (mod p), that is, $r^7 \equiv 1 \pmod{p}$, $r \not\equiv 1 \pmod{p}$, so that

$$1 + r + r^2 + r^3 + r^4 + r^5 + r^6 \equiv 0 \pmod{p}. \tag{5.1}$$

We set

$$R = r + r^6, \quad S = r^2 + r^5, \quad T = r^3 + r^4. \tag{5.2}$$

Appealing to (5.1) we see that R, S, T satisfy

$$R + S + T = -1, \quad RS + ST + TR \equiv -2, \quad RST \equiv 1, \tag{5.3}$$

$$RS \equiv T + R, \quad ST \equiv R + S, \quad TR \equiv S + T, \tag{5.4}$$

$$R^2 \equiv -2R - S - 2T, \; S^2 \equiv -2R - 2S - T, \; T^2 \equiv -R - 2S - 2T, \tag{5.5}$$

where all congruences (here and, unless stated otherwise, thereafter) are taken modulo p. We prove

LEMMA 3. *If $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a non-trivial solution of* (1.1)–(1.4) *then it satisfies one of the six triples of congruences:*

$$\begin{aligned}
294x_2 &\equiv \varepsilon w\{(10R - 2S + 6T)x_1 + (49R + 49S - 147T)x_5 \\
&\qquad + (147R + 147S + 147T)x_6\}, \\
294x_3 &\equiv \varepsilon w\{6R + 10S - 2T)x_1 + (147R + 49S + 49T)x_5 \\
&\qquad + (147R - 147S - 147T)x_6\}, \\
294x_4 &\equiv \varepsilon w\{(2R - 6S - 10T)x_1 + (98R + 98T)x_5 + (294S)x_6\},
\end{aligned} \tag{5.6}$$

$$\begin{aligned}
294x_2 &\equiv \varepsilon w\{(-2R + 6S + 10T)x_1 + (49R - 147S + 49T)x_5 \\
&\qquad + (147R + 147S + 147T)x_6\}, \\
294x_3 &\equiv \varepsilon w\{(10R - 2S + 6T)x_1 + (49R + 49S + 147T)x_5 \\
&\qquad + (-147R - 147S + 147T)x_6\}, \\
294x_4 &\equiv \varepsilon w\{(-6R - 10S + 2T)x_1 + (98S + 98T)x_5 + (294R)x_6\},
\end{aligned} \tag{5.7}$$

$$\begin{aligned}
294x_2 &\equiv \varepsilon w\{(6R + 10S - 2T)x_1 + (-147R + 49S + 49T)x_5 \\
&\qquad + (147T + 147S + 147T)x_6\},
\end{aligned} \tag{5.8}$$

$$294x_3 \equiv \varepsilon w\{(-2R + 6S + 10T)x_1 + (49R + 147S + 49T)x_5 + (-147R + 147S - 147T)x_6\},$$

$$294x_4 \equiv \varepsilon w\{(-10R + 2S - 6T)x_1 + (98R + 98S)x_5 + 294Tx_6\},$$

where $\varepsilon = \pm 1$ *and* w *is a fixed solution of* $w^2 \equiv -7 \pmod p$.

Proof. Let $(x_1, x_2, x_3, x_4, x_5, x_6)$ be a non-trivial solution of (1.1)–(1.4). Now it is easy to verify using (5.4) and (5.5) that

$$\begin{aligned}(-6R - 10S - 12T)(2x_1^2 + 343x_5^2 + 1029x_6^2) &+ (-7S - 21T)(147x_5^2 - 441x_6^2 + 56x_1x_6 + 98x_5x_6) \\ &+ (14S + 21T)(49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 490x_5x_6) \\ &\equiv \{(2R - 2T)x_1 + (35R + 42S + 70T)x_5 + (-21R - 84S - 42T)x_6\}^2\end{aligned}$$

and

$$\begin{aligned}-7\{(-6R - 10S - 12T)(-42x_2^2 - 42x_3^2 - 42x_4^2) &+ (-7S - 21T)(-12x_2^2 + 12x_4^2 - 24x_2x_3 + 24x_2x_4 - 48x_3x_4) \\ &+ (14S + 21T)(-12x_3^2 + 12x_4^2 - 48x_2x_3 - 24x_2x_4 - 24x_3x_4)\} \\ &\equiv \{(42S + 42T)x_2 + (-42R - 42S - 42T)x_3 + (-42T)x_4\}^2,\end{aligned}$$

so that as $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a solution of (1.1)–(1.3) it must satisfy

$$\begin{aligned}\pm w\{(2R - 2T)x_1 + (35R + 42S + 70T)x_5 &+ (-21R - 84S - 42T)x_6\} \\ &\equiv (42S + 42T)x_2 + (-42R - 42S - 42T)x_3 + (-42T)x_4,\end{aligned} \tag{5.9}$$

where w is a fixed solution of $w^2 \equiv -7 \pmod p$. Replacing r by r^2 (or r^5) (resp., r by r^3 (or r^4)), which has the effect of sending $R \to S$, $S \to T$, $T \to R$ (resp., $R \to T$, $S \to R$, $T \to S$), in (5.9), we obtain the system

$$\begin{aligned}42\{(S + T)x_2 - (R + S + T)x_3 - Tx_4\} &\equiv \lambda w\{(2R - 2T)x_1 + (35R + 42S + 70T)x_5 + (-21R - 84S - 42T)x_6\}, \\ 42\{(R + T)x_2 - (R + S + T)x_3 - Rx_4\} &\equiv \mu w\{(-2R + 2S)x_1 + (70R + 35S + 42T)x_5 + (-42R - 21S - 84T)x_6\}, \\ 42\{(R + S)x_2 - (R + S + T)x_3 - Sx_4\} &\equiv \nu w\{(-2S + 2T)x_1 + (42R + 70S + 35T)x_5 + (-84R - 42S - 21T)x_6\},\end{aligned} \tag{5.10}$$

where $\lambda = \pm 1$, $\mu = \pm 1$, $\nu = \pm 1$. Note there are $8 = 2^3$ choices for (λ, μ, ν). We can rule out the two possibilities $(\lambda, \mu, \nu) = \varepsilon(1, 1, 1)$, where $\varepsilon = \pm 1$, since in this case (5.10) gives (using (5.3), (5.4), (5.5))

$$42x_2 \equiv \varepsilon w\{-2x_1 + 7x_5 - 63x_6\},$$

$$42x_3 \equiv \varepsilon w\{-2x_1 - 35x_5 + 21x_6\},$$

$$42x_4 \equiv \varepsilon w\{2x_1 - 28x_5 - 42x_6\},$$

which is impossible by Lemma 2 (E) as $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a non-trivial solution. Taking $(\lambda, \mu, \nu) = \varepsilon(1, 1, -1)$ (resp., $\varepsilon(1, -1, 1)$, $\varepsilon(-1, 1, 1)$) in (5.10) and solving the congruences for x_2, x_3, x_4 using (5.3), (5.4) (5.5), we obtain (5.6) (resp., (5.7), (5.8)). We note that (5.7) is obtained from (5.6) by the mapping $R \to T$, $S \to R$, $T \to S$, equivalently $r \to r^3$, and (5.8) is obtained from (5.6) by the mapping $R \to S$, $S \to T$, $T \to R$, equivalently $r \to r^2$.

6. Number of non-trivial solutions—proof of Theorem 3

Let $(x_1, x_2, x_3, x_4, x_5, x_6)$ be any non-trivial solution of (1.1)–(1.4). By Lemma 3 it must satisfy (5.6), (5.7) or (5.8). By replacing r by r^2 or r^3 if necessary we may suppose it satisfies (5.6). Further by replacing $(x_1, x_2, x_3, x_4, x_5, x_6)$ by the solution $(x_1, -x_2, -x_3, -x_4, x_5, x_6)$ if necessary we may suppose it satisfies (5.6) with $\varepsilon = +1$. Now let $(y_1, y_2, y_3, y_4, y_5, y_6)$ be another non-trivial solution of (1.1)–(1.4). By Lemma 6 it must satisfy one of the six triples of congruences given by (5.6), (5.7), and (5.8). We will show that if $(y_1, y_2, y_3, y_4, y_5, y_6)$ satisfies

(i) (5.6) with $\varepsilon = +1$ then $(y_1, y_2, y_3, y_4, y_5, y_6) = (x_1, x_2, x_3, x_4, x_5, x_6)$,

(ii) (5.6) with $\varepsilon = -1$ then

$$(y_1, y_2, y_3, y_4, y_5, y_6) = (x_2, -x_2, -x_3, -x_4, x_5, x_6),$$

(iii) (5.7) with $\varepsilon = +1$ then

$$(y_1, y_2, y_3, y_3, y_5, y_6) = (x_1, -x_4, x_2, -x_3, -\tfrac{1}{2}(x_5 - 3x_6), -\tfrac{1}{2}(x_5 + x_6)),$$

(iv) (5.7) with $\varepsilon = -1$ then

$$(y_1, y_2, y_3, y_4, y_5, y_6) = (x_1, x_4, -x_2, x_3, -\tfrac{1}{2}(x_5 - 3x_6), -\tfrac{1}{2}(x_5 + x_6)),$$

(v) (5.8) with $\varepsilon = +1$ then

$$(y_1, y_2, y_3, y_4, y_5, y_6) = (x_1, x_3, -x_4, -x_2, -\tfrac{1}{2}(x_5 + 3x_6), \tfrac{1}{2}(x_5 - x_6)),$$

(vi) (5.8) with $\varepsilon = -1$ then

$$(y_1, y_2, y_3, y_4, y_5, y_6) = (x_1, -x_3, x_4, x_2, -\tfrac{1}{2}(x_5 + 3x_6), \tfrac{1}{2}(x_5 - x_6)),$$

completing the proof of the theorem. As cases (i)–(vi) are very similar we will only give the details for case (i). In this case we have from (5.6), with $\varepsilon = +1$,

$$2058\{2x_1y_1 + 42(x_2y_2 + x_3y_3 + x_4y_4) + 343(x_5y_5 + 3x_6y_6)\}$$
$$\equiv 4116x_1y_1 - 7\{(10R - 2S + 6T)x_1 + (49R + 49S - 147T)x_5$$
$$+ (147R + 147S + 147T)x_6\}\{(10R - 2S + 6T)y_1$$
$$+ (49R + 49S - 147T)y_5 + (147R + 147S + 147T)y_6\}$$
$$- 7\{(6R + 10S - 2T)x_1 + (147R + 49S + 49T)x_5$$
$$+ (147R - 147S - 147T)x_6\}\{(6R + 10S - 2T)y_1$$
$$+ (147R + 49S + 49T)y_5 + (147R - 147S - 147T)y_6\}$$
$$- 7\{(2R - 6S - 10T)x_1 + (98R + 98T)x_5 + (294S)x_6\}$$
$$\{(2R - 6S - 10T)y_1 + (98R + 98T)y_5 + (294S)y_6\}$$
$$+ 705894x_5y_5 + 2117682x_6y_6 \equiv 0 \pmod{p},$$

appealing to equations (5.3)–(5.5), so that

$$A = 2x_1y_1 + 42(x_2y_2 + x_3y_3 + x_4y_4) + 343(x_5y_5 + 3x_6y_6) \tag{6.1}$$

satisfies

$$A \equiv 0 \pmod{p}, \quad \text{say} \quad A = Bp. \tag{6.2}$$

Next as $x_1 \equiv y_1 \equiv 1 \pmod 7$ we have from (6.1) and (6.2),

$$B \equiv 2 \pmod 7. \tag{6.3}$$

Also taking (1.1), (1.2), (1.3) modulo 3 it is easy to show that

$$x_1 \equiv -x_5 \pmod 3$$

(similarly $y_1 \equiv -y_5 \pmod 3$) so that

$$B \equiv 0 \pmod 3. \tag{6.4}$$

Again from (1.1), (1.2), (1.3) working modulo 8 we find

$$x_1 \equiv x_2 + x_3 + x_4 \pmod 2, \quad x_5 \equiv x_2 + 3x_3 + 2x_4 \pmod 4,$$
$$x_6 \equiv x_2 + x_3 \pmod 2,$$

with similar congruences for y_1, y_5, y_6 in terms of y_2, y_4, y_4, so that

$$B \equiv 0 \pmod 4. \tag{6.5}$$

Equations (6.3), (6.4), (6.5) give $B \equiv 72 \pmod{84}$, say $B = 84C + 72$. Finally the inequality

$$|2x_1y_1 + 42(x_2y_2 + x_3y_3 + x_4y_4) + 343(x_5y_5 + 3x_6y_6)|$$
$$\leq \{(2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2))(2y_1^2 + 42(y_2^2 + y_3^2 + y_4^2)$$
$$+ 343(y_5^2 + 3y_6^2)\}^{1/2}$$

gives

$$|A| \leq 72p, \quad |B| = |84C + 72| \leq 72,$$

so that $C = 0$, or -1, that is, $A = 72p$ or $A = -12p$. We next rule out the possibility $A = -12p$. To do this we consider a number of cases depending on the residue of $p \pmod{49}$ and on the residues of $x_2 - 5x_4$ and $y_2 - 5y_4 \pmod 7$. In view of the symmetry in the x_i and y_i there are $7 \times 28 = 196$ cases. We give just one of these. Suppose that $p \equiv 43 \pmod{49}$ and $x_2 - 5x_4 \equiv 2 \pmod 7$, $y_2 - 5y_4 \equiv 4 \pmod 7$. Then, as $(x_1, \cdots, x_6)$ and $(y_1, \cdots, y_6)$ are solutions of (1.1)–(1.4) we have

$$x_2 + 2x_3 + 3x_4 \equiv 0 \pmod 7, \quad y_2 + 2y_3 + 3y_4 \equiv 0 \pmod 7,$$

so that

$$x_3 \equiv 3x_4 + 6 \pmod 7, \quad y_3 \equiv 3y_4 + 5 \pmod 7,$$

giving

$$x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv 3 \pmod 7,$$

$$x_2^2 + x_3^3 + x_4^2 \equiv 5 \pmod 7, \quad y_2^2 + y_3^2 + y_4^2 \equiv 6 \pmod 7.$$

Then from (1.1) we deduce

$$x_1 \equiv 36 \pmod{49}, \quad y_1 \equiv 1 \pmod{49}, \quad x_1 y_1 \equiv 36 \pmod{49},$$

so that $A \equiv 2 \pmod{49}$. Generally we find that

$$\begin{aligned}
A &\equiv 9, 16, 23, 44 \pmod{49} && \text{if } p \equiv 1 \pmod{49},\\
A &\equiv 9, 23, 30, 37 \pmod{49} && \text{if } p \equiv 8 \pmod{49},\\
A &\equiv 2, 23, 37, 44 \pmod{49} && \text{if } p \equiv 15 \pmod{49},\\
A &\equiv 2, 9, 16, 37 \pmod{49} && \text{if } p \equiv 22 \pmod{49},\\
A &\equiv 2, 16, 23, 30 \pmod{49} && \text{if } p \equiv 29 \pmod{49},\\
A &\equiv 16, 30, 37, 44 \pmod{49} && \text{if } p \equiv 36 \pmod{49},\\
A &\equiv 2, 9, 30, 44 \pmod{49} && \text{if } p \equiv 43 \pmod{49},
\end{aligned}$$

so that as

$$-12p \equiv 37, 2, 16, 30, 44, 9, 23 \quad \text{if} \quad p \equiv 1, 8, 15, 22, 29, 36, 42 \pmod{49}$$

respectively, we cannot have $A = -12p$.

Thus $A = 72p$ and the identity

$$\begin{aligned}
(72p)^2 = A^2 &+ 84(x_1 y_2 - x_2 y_2)^2 + 84(x_1 y_3 - x_3 y_1)^2 + 84(x_1 y_4 - x_4 y_1)^2\\
&+ 686(x_1 y_5 - x_5 y_1)^2 + 2058(x_1 y_6 - x_6 y_1)^2\\
&+ 1764(x_2 y_3 - x_3 y_2)^2 + 1764(x_2 y_4 - x_4 y_2)^2\\
&+ 14406(x_2 y_5 - x_5 y_2)^2 + 43218(x_2 y_6 - x_6 y_2)^2\\
&+ 1764(x_3 y_4 - x_4 y_3)^2 + 14406(x_3 y_5 - x_5 y_3)^2
\end{aligned}$$

$$+ 43218(x_3 y_6 - x_6 y_3)^2 + 14406(x_4 y_5 - y_5 y_4)^2$$
$$+ 43218(x_4 y_6 - x_6 y_4)^2 + 352947(x_5 y_6 - x_6 y_5)^2,$$

then gives $x_1 y_2 - x_2 y_1 = \cdots = x_5 y_6 - x_6 y_5 = 0$. Now as

$$x_1 \equiv y_1 \equiv 1 \pmod 7 \quad \text{we have} \quad x_1 \neq 0, \quad y_1 \neq 0,$$

so that

$$x_i/x_1 = y_i/y_1 \quad (i = 2, 3, 4, 5, 6). \tag{6.6}$$

Hence from (1.1) we have

$$\begin{aligned} 72p/x_1^2 &= 2 + 42((x_2/x_1)^2 + (x_3/x_1)^2 + (x_4/x_1)^2) + 343((x_5/x_1)^2 + 3(x_6/x_1)^2) \\ &= 2 + 42((y_2/y_1)^2 + (y_3/y_1)^2 + (y_4/y_1)^2) + 343((y_5/y_1)^2 + 3(y_6/y_1)^2) \\ &= 72p/y_1^2, \end{aligned}$$

so that $x_1^2 = y_1^2$. As $x_1 \equiv y_1 \equiv 1 \pmod 7$ we must have $x_1 = y_1$ and so from (6.6) we also have $x_i = y_i$ $(i = 2, 3, 4, 5, 6)$, proving that

$$(x_1, \cdots, x_6) = (y_1, \cdots, y_6)$$

as required.

This completes the proof of Theorem 2.

References

1. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., vol. 57 (1935), pp. 391–424.
2. K. Ireland and M. I. Rosen, *Elements of number theory*, Bogden and Quigley, New York, 1972.
3. P. A. Leonard and K. S. Williams, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc., to appear.
4. ———, *The septic character of* 2, 3, 5, *and* 7, Pacific J. Math., to appear.
5. ———, *A diophantine system of Dickson*, Rendiconti Accademia Nationale dei Lincei to appear.
6. A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math., vol. 74 (1952), pp. 89–99.

Carleton University
Ottawa, Ontario, Canada
University of British Columbia
Vancouver, British Columbia, Canada