ACTA ARITHMETICA
XXVI (1975)

# The cyclotomic numbers of order eleven*

by

PHILIP A. LEONARD (Tempe, Ariz.) and
KENNETH S. WILLIAMS (Vancouver, Canada)

**1. Introduction.** Let $e$ be an integer greater than 1 and let $p$ be a prime $\equiv 1 \pmod{e}$, say, $p = ef+1$. Let $g$ be a primitive root $(\bmod p)$. The number of solutions $(s, t)$ with $0 \leqslant s,\ t \leqslant f-1$ of the congruence

$$g^{es+h}+1 \equiv g^{et+k} \pmod{p}, \tag{1.1}$$

where $h$, $k$ are integers usually taken such that $0 \leqslant h,\ k \leqslant e-1$, is denoted by $(h, k)_e$. The numbers $(h, k)_e$ are called cyclotomic numbers of order $e$ and in addition to $h$, $k$ and $e$ depend upon $p$ and $g$. A central problem in the theory of cyclotomy is to evaluate the cyclotomic numbers in terms of the solutions of certain diophantine systems involving quadratic forms. The cases $e = 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 24$ and 30 have been treated by several authors (see for example Dickson ([2], [3] and [4]), Lehmer ([6], $e = 8$), Whiteman ([14], [15] and [16], $e = 10$, 12, 16), Muskat ([8] and [9], $e = 14, 24, 30$), Baumert and Fredricksen ([1], $e = 9, 18$), Muskat and Whiteman ([10], $e = 20$), and Leonard and Williams ([7], $e = 7$).

In this paper we give the first complete treatment of the case $e = 11$, and we begin by stating, for $e = 11$, some results from the theory of cyclotomy. All results are stated when $e = 11$ as this is the only case we consider. For more general results and proofs the reader is referred to Dickson [2], [3] and Storer [11].

Let $p$ be a prime of the form $p = 11f+1$, so that $f$ is even. The cyclotomic numbers $(h, k) = (h, k)_{11}$ are periodic in both $h$ and $k$ $(\bmod 11)$. They also have the following two well known properties:

$$(h, k) = (11-h, k-h) \tag{1.2}$$

and

$$(h, k) = (k, h). \tag{1.3}$$

* The research of both authors was supported by a grant (no. A7233) from the National Research Council of Canada. The second author's sabbatical leave at the University of British Columbia was supported by a N.R.C. travel grant (no. T 0259).

Using (1.2) and (1.3) we find that the $11 \times 11$ matrix whose entry in the $(h, k)$-place $(0 \leqslant h,\ k \leqslant 10)$ is $(h, k)$ is given by

$$(1.4) \qquad \begin{bmatrix} A & B & C & D & E & F & G & H & I & J & K \\ B & K & L & M & N & O & P & Q & R & S & L \\ C & L & J & S & T & U & V & W & X & T & M \\ D & M & S & I & R & X & Y & Z & Y & U & N \\ E & N & T & R & H & Q & W & Z & Z & V & O \\ F & O & U & X & Q & G & P & V & Y & W & P \\ G & P & V & Y & W & P & F & O & U & X & Q \\ H & Q & W & Z & Z & V & O & E & N & T & R \\ I & R & X & Y & Z & Y & U & N & D & M & S \\ J & S & T & U & V & W & X & T & M & C & L \\ K & L & M & N & O & P & Q & R & S & L & B \end{bmatrix}.$$

Thus the evaluation of the 121 cyclotomic numbers $(h, k)$ reduces to the determination of the 26 quantities $A, B, \ldots, Z$.

Let $\zeta = \exp(2\pi i/11)$, a primitive 11th root of unity. $Z[\zeta]$ is a unique factorization domain. Let $\pi$ be *any* prime factor of $p$ in $Z[\zeta]$. We order its conjugates by setting $\pi_k = \sigma_k(\pi)$, $1 \leqslant k \leqslant 10$, where $\sigma_k$ is the automorphism determined by $\sigma_k(\zeta) = \zeta^k$. We write $\left(\frac{\cdot}{\pi}\right)$ for the 11th power character defined by $\left(\frac{y}{\pi}\right) = \zeta^r$ if $y^{(p-1)/11} \equiv \zeta^r \pmod{\pi}$. This ordering is such that

$$\left(\frac{y}{\pi_k}\right) = \left(\frac{y}{\pi}\right)^k \quad \text{for} \quad k = 1, 2, \ldots, 10.$$

If $\left(\frac{g}{\pi}\right) = \zeta^l$ then, if $\bar{l}$ is any integer satisfying $l\bar{l} \equiv 1 \pmod{11}$, we have

$$\left(\frac{g}{\pi_{\bar{l}}}\right) = \left(\frac{g}{\pi}\right)^{\bar{l}} = \zeta^{l\bar{l}} = \zeta,$$

so replacing $\pi$ by $\pi_{\bar{l}}$ if necessary, we may assume without loss of generality that $\left(\frac{g}{\pi}\right) = \zeta$.

In the theory of cyclotomy the Jacobi sum plays a fundamental role. For any pair of integers $m, n$ we define the Jacobi sum of order 11 by

$$(1.5) \qquad J_\pi(m, n) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)^m \left(\frac{1+x}{\pi}\right)^n.$$

The Jacobi sum has the properties

$$(1.6) \qquad J_\pi(m, n) = J_\pi(n, m) = J_\pi(-m-n, n) = J_\pi(m, -m-n)$$

and, provided no one of the integers $m, n, m+n$ is divisible by 11,

$$J_\pi(m,n)\overline{J_\pi(m,n)} = p. \tag{1.7}$$

From (1.1) and (1.5) we have

$$J_\pi(m,n) = \sum_{h,k=0}^{10}(h,k)\left(\frac{g}{\pi}\right)^{mh+nk} = \sum_{h,k=0}^{10}(h,k)\zeta^{mh+nk}, \tag{1.8}$$

as $\left(\frac{g}{\pi}\right) = \zeta$. Taking $m = 1$ in (1.8) we obtain

$$J_\pi(1,n) = \sum_{i=0}^{10} B(i,n)\zeta^i, \tag{1.9}$$

where

$$B(i,j) = \sum_{h=0}^{10}(h, i-jh). \tag{1.10}$$

$B(i,j)$ is the Dickson–Hurwitz sum of order 11. It is defined for all integers $i$ and $j$ and has the properties (see for example [16])

$$B(i,j) = B(i, 10-j), \tag{1.11}$$

$$B(i,0) = \begin{cases} f-1, & i \equiv 0 \pmod{11}, \\ f, & i \not\equiv 0 \pmod{11}, \end{cases} \tag{1.12}$$

$$B(i,j) = B(i\bar{j}, \bar{j}), \tag{1.13}$$

if $j \not\equiv 0 \pmod{11}$ and $\bar{j}$ is any solution of the congruence $j\bar{j} \equiv 1 \pmod{11}$,

$$\sum_{i=0}^{10} B(i,j) = p-2. \tag{1.14}$$

Whiteman [16] has proved the important property

$$121(h,k) = -10(p-1)+\varepsilon(h)+11\sum_{v=0}^{10} B(vh+k, v), \tag{1.15}$$

where

$$\varepsilon(h) = \begin{cases} 0, & \text{if} \quad h \equiv 0 \pmod{11}, \\ 11, & \text{if} \quad h \not\equiv 0 \pmod{11}. \end{cases}$$

The groundwork for our evaluation of the cyclotomic numbers of order 11 was laid by Dickson in [2] and [3]. His work leads us to consider the diophantine system

$$1200p = 12x_1^2+33x_2^2+55x_3^2+110x_4^2+330x_5^2+ \\ +660(x_6^2+x_7^2+x_8^2+x_9^2+x_{10}^2), \tag{1.16}$$

$$(1.17)\quad 45x_2^2+5x_3^2+20x_4^2-540x_5^2+720x_6^2-720x_{10}^2-288x_1x_5+30x_2x_3-$$
$$-120x_2x_4-72x_2x_5+200x_3x_4-360x_3x_5+360x_4x_5+1440x_6x_7-$$
$$-1440x_6x_8+1440x_7x_8-1440x_7x_9+1440x_8x_9-1440x_8x_{10}+$$
$$+2880x_9x_{10}=0,$$

$$(1.18)\quad 45x_2^2-35x_3^2-80x_4^2+720x_9^2-720x_{10}^2-144x_1x_4-144x_1x_5+$$
$$+150x_2x_3-96x_2x_4-216x_2x_5+160x_3x_4+120x_3x_5+240x_4x_5+$$
$$+2880x_6x_7-1440x_6x_9+1440x_7x_8-1440x_7x_{10}+1440x_8x_9+$$
$$+1440x_8x_{10}+1440x_9x_{10}=0,$$

$$(1.19)\quad 45x_2^2+5x_3^2+20x_4^2-540x_5^2+720x_7^2-720x_{10}^2-96x_1x_3-48x_1x_4-$$
$$-144x_1x_5+126x_2x_3+108x_2x_4-36x_2x_5+20x_3x_4-60x_3x_5+$$
$$+600x_4x_5+1440x_6x_7+1440x_6x_8-1440x_6x_{10}+1440x_7x_8+$$
$$+1440x_7x_{10}+2880x_8x_9+1440x_9x_{10}=0,$$

$$(1.20)\quad 27x_2^2+35x_3^2-40x_4^2-360x_5^2+720x_8^2-720x_{10}^2-72x_1x_2-24x_1x_3-$$
$$-48x_1x_4-144x_1x_5+114x_2x_3+48x_2x_4+144x_2x_5+320x_3x_4+$$
$$+1440x_6x_7+1440x_6x_9+1440x_6x_{10}+2880x_7x_8+1440x_7x_9+$$
$$+1440x_8x_9+1440x_9x_{10}=0,$$

$$(1.21)\quad x_3+2x_4+2x_5\equiv 0 \pmod{11},$$

$$(1.22)\quad x_2-x_4+3x_5\equiv 0 \pmod{11},$$

and we are able to determine the number of integral simultaneous solutions $(x_1, \ldots, x_{10})$ of this system. The following theorem giving the nature of the solutions is proved in § 4 after we prove some lemmas in § 2 and § 3.

THEOREM 1. *For a prime* $p \equiv 1 \pmod{11}$, *there are exactly* 64 *integral solutions* $(x_1, \ldots, x_{10})$ *of the system* (1.16)–(1.22). *Of these* 64 *solutions*, 4 *trivial solutions are given by*

$$(1.23)\quad \pm(\pm 5a, 0, 0, 0, 0, b, -b, b, b, b),$$

*where* $4p = a^2+11b^2$, $a \equiv 9 \pmod{11}$. *Amongst the remaining* 60 *non-trivial solutions we can find* 3 *solutions*

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

*such that all 60 solutions are given by*

(1.24)

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

*for* $i = 1, 2, 3$ *and* $k = 0, 1, 2, \ldots, 9$.

Theorem 1 is proved by establishing a one-to-one correspondence between solutions $\pm(x_1, \ldots, x_{10})$ of (1.16)–(1.22) and those elements $K$ of $Z[\zeta]$ which satisfy the conditions $K\bar{K} = p$ and $K \equiv -1 \pmod{(1-\zeta)^2}$.

There are four possibilities for $K$ with $K\bar{K} = p$:

(I) $K \sim \sigma_k(\pi_1\pi_3\pi_4\pi_6\pi_9)$ for some $k = 1, 2, \ldots, 10$,

or

(II) $K \sim \sigma_k(\pi_1\pi_2\pi_4\pi_6\pi_8)$ for some $k = 1, 2, \ldots, 10$,

or

(III) $K \sim \sigma_k(\pi_1\pi_2\pi_3\pi_5\pi_7)$ for some $k = 1, 2, \ldots, 10$,

or

(IV) $K \sim \sigma_k(\pi_1\pi_3\pi_4\pi_5\pi_9)$ for some $k = 1, 2, \ldots, 10$.

It is proved in § 2 (Lemma 1) that if $K \in Z[\zeta]$ is such that $K\bar{K} = p$ then $K$ has a unique normalized associate satisfying the same condition. Let $K_1$ (resp., $K_2$; $K_3$) be the unique normalized associate of $\pi_1\pi_3\pi_4\pi_6\pi_9$ (resp., $\pi_1\pi_2\pi_4\pi_6\pi_8$; $\pi_1\pi_2\pi_3\pi_5\pi_7$) and let $\pm(x_{1i}, \ldots, x_{10i})$ $(i = 1, 2, 3)$ be the solutions of (1.16)–(1.22) corresponding to $K_i$ $(i = 1, 2, 3)$ given by the correspondence in Lemma 5. The conjugates of $K_i$ $(i = 1, 2, 3)$ give rise to the 60 solutions (1.24). These solutions are distinct as in cases (I), (II), (III) the conjugates are distinct. The trivial solutions arise from case (IV) where the conjugates are not distinct.

The quantities $K_1$ and $K_2$ are (see § 2, Lemma 1) the Jacobi sums $J_\pi(1, 1)$ and $J_\pi(1, 2)$ respectively. (On the other hand $K_3$ is not a Jacobi sum.) Using this information we are able to compute the Dickson–Hurwitz sums $B(i, j)$ in terms of the solutions $(x_{11}, \ldots, x_{10\,1}) = (x_1, \ldots, x_{10})$ and $(x_{12}, \ldots, x_{10\,2}) = (y_1, \ldots, y_{10})$ corresponding to the Jacobi sums $J_\pi(1, 1)$ and $J_\pi(1, 2)$. The cyclotomic numbers of order 11 are computed using these values and the result of Whiteman given in (1.15). We have

THEOREM 2. *Let $p$ be a prime $\equiv 1 \pmod{11}$ and let $g$ be a primitive root $\pmod p$. Let $\pi$ be the unique (up to associates) prime factor of $p$ in $Z[\zeta]$, $\zeta = \exp(2\pi i/11)$, such that $\left(\frac{g}{\pi}\right) = \zeta$. Let $(x_1, \ldots, x_{10})$ and $(y_1, \ldots, y_{10})$ be the solutions of (1.16)–(1.22) corresponding to $J_\pi(1, 1)$ and $J_\pi(1, 2)$ respectively. Then the cyclotomic numbers of order 11 are given by (1.4) and Table 1.*

In § 6 we introduce two so-called Jacobsthal–Whiteman sums $\varphi^1(a)$ and $\varphi^2(a)$, defined by (6.1), in terms of which we can express $(x_1, x_2, \ldots, x_{10})$ and $(y_1, y_2, \ldots, y_{10})$ as follows (see [13], equations (7.3), (9.5), and [7], equations (1.6), for similar results for $e = 3$, 5 and 7):

$$
\begin{aligned}
x_1 &= -\big(1+\varphi^1(4)\big),\\
11x_2 &= \varphi^1(4g)+\varphi^1(4g^2)+\varphi^1(4g^3)+\varphi^1(4g^4)-4\varphi^1(4g^5)-4\varphi^1(4g^6)+\\
&\qquad +\varphi^1(4g^7)+\varphi^1(4g^8)+\varphi^1(4g^9)+\varphi^1(4g^{10}),\\
11x_3 &= \varphi^1(4g)+\varphi^1(4g^2)+\varphi^1(4g^3)-3\varphi^1(4g^4)-3\varphi^1(4g^7)+\\
&\qquad +\varphi^1(4g^8)+\varphi^1(4g^9)+\varphi^1(4g^{10}),\\
11x_4 &= \varphi^1(4g)+\varphi^1(4g^2)-2\varphi^1(4g^3)-2\varphi^1(4g^8)+\varphi^1(4g^9)+\varphi^1(4g^{10}),\\
11x_5 &= \varphi^1(4g)-\varphi^1(4g^2)-\varphi^1(4g^9)+\varphi^1(4g^{10}),\\
11x_6 &= \varphi^1(4g)-\varphi^1(4g^{10}),\\
11x_7 &= \varphi^1(4g^2)-\varphi^1(4g^9),\\
11x_8 &= \varphi^1(4g^3)-\varphi^1(4g^8),\\
11x_9 &= \varphi^1(4g^4)-\varphi^1(4g^7),\\
11x_{10} &= \varphi^1(4g^5)-\varphi^1(4g^6).
\end{aligned}
\tag{1.25}
$$

The corresponding formulae for the $y_i$ are obtained by replacing each $x_i$ by $y_i$ and each $\varphi^1(4g^i)$ by $\varphi^2(4g^i)$ in (1.25) above.

Finally in § 7 we illustrate the ideas of the paper by a simple example.

**2. Technical lemmas.** The element $1-\zeta$, $\zeta = \exp(2\pi i/11)$, is a prime in $Z[\zeta]$ as its norm is the rational prime 11.

DEFINITION. An element $K \in Z[\zeta]$, $\zeta = \exp(2\pi i/11)$, is said to be *normalized* if

$$K \equiv -1 \pmod{(1-\zeta)^2}.$$

Clearly $K = \sum_{i=1}^{10} a_i \zeta^i \in Z[\zeta]$ is normalized if and only if

$$\sum_{i=1}^{10} a_i \equiv -1 \pmod{11}, \qquad \sum_{i=1}^{10} i a_i \equiv 0 \pmod{11}.$$

We will be particularly interested in those $K \in Z[\zeta]$ for which $K\bar{K} = p$.

LEMMA 1. (i) *If $K \in Z[\zeta]$ is such that $K\bar{K} = p$ then $K$ possesses a unique normalized associate $K_1$ such that $K_1\bar{K}_1 = p$.*

## Table of cyclotomic numbers of order eleven

**TABLE 1**

| Cyclotomic Numbers | 1 | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ | $x_8$ | $x_9$ | $x_{10}$ | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | $y_6$ | $y_7$ | $y_8$ | $y_9$ | $y_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 121 $A$ | $p-32$ | $-3$ | | | | | | | | | | $-6$ | | | | | | | | | |
| 14520 $B$ | $120p-1200$ | 36 | 99 | 165 | 330 | 330 | 1320 | $-660$ | | | | 72 | 198 | 330 | | | 1320 | 1320 | $-1320$ | | |
| 14520 $C$ | $120p-1200$ | 36 | 99 | $-55$ | 220 | $-660$ | | 1320 | | $-660$ | | 72 | $-132$ | $-220$ | 220 | $-660$ | | 1320 | | 1320 | 1320 |
| 14520 $D$ | $120p-1200$ | 36 | $-66$ | 110 | $-440$ | | | | 1320 | | 660 | 72 | $-132$ | 220 | $-220$ | $-660$ | | 1320 | 1320 | | $-1320$ |
| 14520 $E$ | $120p-1200$ | 36 | 99 | $-275$ | $-220$ | | | | 660 | 1320 | | 72 | 198 | $-110$ | $-220$ | 660 | $-1320$ | | $-1320$ | 1320 | |
| 14520 $F$ | $120p-1200$ | 36 | $-231$ | 55 | 110 | 330 | 660 | | | | 1320 | 72 | $-132$ | $-220$ | 220 | 660 | $-1320$ | | | $-1320$ | 1320 |
| 14520 $G$ | $120p-1200$ | 36 | $-231$ | 55 | 110 | 330 | $-660$ | | | | $-1320$ | 72 | $-132$ | $-220$ | 220 | 660 | 1320 | | | 1320 | $-1320$ |
| 14520 $H$ | $120p-1200$ | 36 | 99 | $-275$ | $-220$ | | | | $-660$ | $-1320$ | | 72 | 198 | $-110$ | $-220$ | 660 | 1320 | | 1320 | $-1320$ | |
| 14520 $I$ | $120p-1200$ | 36 | $-66$ | 110 | $-440$ | | | | $-1320$ | | $-660$ | 72 | $-132$ | 220 | $-220$ | $-660$ | | $-1320$ | $-1320$ | | 1320 |
| 14520 $J$ | $120p-1200$ | 36 | 99 | $-55$ | 220 | $-660$ | | $-1320$ | | 660 | | 72 | $-132$ | $-220$ | 220 | $-660$ | | $-1320$ | | $-1320$ | $-1320$ |
| 14520 $K$ | $120p-1200$ | 36 | 99 | 165 | 330 | 330 | $-1320$ | 660 | | | | 72 | 198 | 330 | | | $-1320$ | $-1320$ | 1320 | | |
| 14520 $L$ | $120p+120$ | $-96$ | 66 | 110 | $-440$ | | | | | | | 72 | $-132$ | $-220$ | 220 | 660 | | | | | |
| 14520 $M$ | $120p+120$ | 36 | $-66$ | $-110$ | 110 | 330 | 660 | | | 660 | $-660$ | $-60$ | | $-220$ | $-440$ | | | | 1320 | | 660 |
| 14520 $N$ | $120p+120$ | 36 | $-66$ | $-110$ | 110 | $-330$ | | 660 | | 660 | 660 | $-60$ | $-165$ | 165 | 330 | 330 | 1320 | $-660$ | | | |
| 14520 $O$ | $120p+120$ | 36 | $-66$ | 110 | $-110$ | $-330$ | | 660 | 660 | | $-660$ | $-60$ | 165 | $-165$ | | $-660$ | | | $-660$ | $-1320$ | |
| 14520 $P$ | $120p+120$ | $-96$ | 66 | $-330$ | | | | | | | | 72 | $-132$ | 220 | $-220$ | $-660$ | | | | | |
| 14520 $Q$ | $120p+120$ | 36 | $-66$ | 110 | $-110$ | $-330$ | | $-660$ | $-660$ | | 660 | $-60$ | 165 | $-165$ | | $-660$ | | | 660 | 1320 | |
| 14520 $R$ | $120p+120$ | 36 | $-66$ | $-110$ | 110 | $-330$ | | $-660$ | | $-660$ | $-660$ | $-60$ | $-165$ | 165 | 330 | 330 | $-1320$ | 660 | | | |
| 14520 $S$ | $120p+120$ | 36 | $-66$ | $-110$ | 110 | 330 | $-660$ | | | $-660$ | 660 | $-60$ | | $-220$ | $-440$ | | | | $-1320$ | | $-660$ |
| 14520 $T$ | $120p+120$ | $-96$ | $-264$ | | | | | | | | | 72 | 198 | 330 | | | | | | | |
| 14520 $U$ | $120p+120$ | 36 | 99 | $-55$ | $-110$ | 330 | 660 | | 660 | $-660$ | | $-60$ | 165 | 55 | 440 | | | $-1320$ | | 660 | |
| 14520 $V$ | $120p+120$ | 36 | 99 | 165 | | | 660 | 660 | $-660$ | | | $-60$ | $-165$ | 165 | $-330$ | 330 | $-660$ | | | | $-1320$ |
| 14520 $W$ | $120p+120$ | 36 | 99 | 165 | | | $-660$ | $-660$ | 660 | | | $-60$ | $-165$ | 165 | $-330$ | 330 | 660 | | | | 1320 |
| 14520 $X$ | $120p+120$ | 36 | 99 | $-55$ | $-110$ | 330 | $-660$ | | $-660$ | 660 | | $-60$ | 165 | 55 | 440 | | | 1320 | | $-660$ | |
| 14520 $Y$ | $120p+120$ | $-96$ | 66 | 110 | 220 | $-660$ | | | | | | 72 | 198 | $-110$ | $-220$ | 660 | | | | | |
| 14520 $Z$ | $120p+120$ | $-96$ | 66 | 110 | 220 | 660 | | | | | | 72 | $-132$ | $-220$ | 220 | $-660$ | | | | | |

(ii) *If no one of the integers* $m, n, m+n$ *is divisible by* 11, $J_\pi(m, n)$ *is a normalized element of* $Z[\zeta]$ *such that* $J_\pi(m, n)\overline{J_\pi(m, n)} = p$.

(iii) *The unique normalized associate* $K_1$ *of* $K = \pi_1\pi_3\pi_4\pi_6\pi_9$ (*resp.*, $K = \pi_1\pi_2\pi_4\pi_6\pi_8$) *is* $K_1 = J_\pi(1, 1)$ (*resp.*, $K_2 = J_\pi(1, 2)$).

Proof. (i) This result is contained in the work of Dickson ([3], p. 375).

(ii) By (1.5) and (1.7) $J_\pi(m, n)$ is an element of $Z[\zeta]$ such that $J_\pi(m, n)\overline{J_\pi(m, n)} = p$. Now clearly

$$\sum_{x=1}^{p-2}\left\{\left(\frac{x}{\pi}\right)^m - 1\right\}\left\{\left(\frac{x+1}{\pi}\right)^n - 1\right\} \equiv 0 \pmod{(1-\zeta)^2},$$

so that $J_\pi(m, n) \equiv -p \equiv -1 \pmod{(1-\zeta)^2}$, proving that $J_\pi(m, n)$ is normalized.

(iii) This is a result of Kummer (see for example [3], p. 376).

LEMMA 2. *If* $K = \sum_{i=1}^{10} a_i\zeta^i \in Z[\zeta]$ *is normalized and such that* $K\overline{K} = p$ *then*

$$\sum_{i=1}^{10} i^2 a_i \equiv 0, \qquad \sum_{i=1}^{10} i^4 a_i \equiv 0 \pmod{11}.$$

Proof. As $K$ is normalized we have

$$(K+1)(\overline{K}+1) \equiv 0 \pmod{(1-\zeta)^4},$$

giving, as

$$K\overline{K} = p \equiv 1 \pmod{11 \sim (1-\zeta)^{10}}, \qquad K+\overline{K} \equiv -2 \pmod{(1-\zeta)^4},$$

that is

$$\sum_{i=1}^{5}(a_i + a_{11-i})(\zeta^i + \zeta^{11-i} - 2) \equiv 0 \pmod{(1-\zeta)^4}. \tag{2.1}$$

Now we set $\beta = \zeta + \zeta^{10} - 2$ so that

$$\begin{aligned}
\beta^2 &\sim (1-\zeta)^4,\\
\zeta^2 + \zeta^9 - 2 &= 4\beta + \beta^2,\\
\zeta^3 + \zeta^8 - 2 &= 9\beta + 6\beta^2 + \beta^3,\\
\zeta^4 + \zeta^7 - 2 &= 16\beta + 20\beta^2 + 8\beta^3 + \beta^4,\\
\zeta^5 + \zeta^6 - 2 &= 25\beta + 50\beta^2 + 35\beta^3 + 10\beta^4 + \beta^5.
\end{aligned}$$

Hence (2.1) becomes

$$\sum_{i=1}^{5} b_i\beta^i \equiv 0 \pmod{\beta^2}, \tag{2.2}$$

where

$$
\begin{aligned}
b_1 &= (a_1+a_{10})+4(a_2+a_9)+9(a_3+a_8)+16(a_4+a_7)+25(a_5+a_6),\\
b_2 &= (a_2+a_9)+6(a_3+a_8)+20(a_4+a_7)+50(a_5+a_6),\\
b_3 &= (a_3+a_8)+8(a_4+a_7)+35(a_5+a_6),\\
b_4 &= (a_4+a_7)+10(a_5+a_6),\\
b_5 &= (a_5+a_6).
\end{aligned}
\tag{2.3}
$$

From (2.2) we have $b_1 \equiv 0 \pmod{\beta}$, implying $b_1 \equiv 0 \pmod{11}$, as the norm of $\beta$ in $Z[\zeta]$ is $-11$. Hence from (2.3) we have

$$
\begin{aligned}
(a_1+a_{10})+4(a_2+a_9)+9(a_3+a_8)+16(a_4+a_7)+25(a_5+a_6)\\
\equiv 0 \pmod{11},
\end{aligned}
\tag{2.4}
$$

which is

$$
\sum_{i=1}^{10} i^2 a_i \equiv 0 \pmod{11},
\tag{2.5}
$$

as required. Now (2.5), together with the fact that $K$ is normalized, gives

$$
K \equiv -1 \pmod{(1-\zeta)^3},
$$

so that as above we have

$$
K+\bar{K} \equiv -2 \pmod{(1-\zeta)^6},
$$

that is

$$
\sum_{i=1}^{5} (a_i+a_{11-i})(\zeta^i+\zeta^{11-i}-2) \equiv 0 \pmod{(1-\zeta)^6},
$$

or

$$
\sum_{i=1}^{5} b_i \beta^i \equiv 0 \pmod{\beta^3}.
\tag{2.6}
$$

Now, as $b_1 \equiv 0 \pmod{11 \sim \beta^5}$, (2.6) gives $b_2 \equiv 0 \pmod{\beta}$, implying as before $b_2 \equiv 0 \pmod{11}$. Hence from (2.3) we have

$$
(a_2+a_9)+6(a_3+a_8)+20(a_4+a_7)+50(a_5+a_6) \equiv 0 \pmod{11}.
\tag{2.7}
$$

Thus taking (2.4) plus 12 times (2.7) we obtain

$$
\begin{aligned}
(a_1+a_{10})+16(a_2+a_9)+81(a_3+a_8)+256(a_4+a_7)+625(a_5+a_6)\\
\equiv 0 \pmod{11},
\end{aligned}
$$

which is

$$
\sum_{i=1}^{10} i^4 a_i \equiv 0 \pmod{11},
$$

as required. This completes the proof of Lemma 2.

The next lemma gives us information about the solutions of (1.16)–(1.22).

LEMMA 3. *For any solution* $(x_1, \ldots, x_{10})$ *of* (1.16)–(1.22) *we have*

$$x_1 + x_2 + x_{10} \equiv 0 \pmod 2, \tag{2.8}$$

$$x_3 + x_4 + x_8 + x_9 \equiv 0 \pmod 2, \tag{2.9}$$

$$x_5 + x_6 + x_7 \equiv 0 \pmod 2, \tag{2.10}$$

$$x_4 - x_5 + 2x_7 + 2x_8 \equiv 0 \pmod 4, \tag{2.11}$$

$$x_2 - x_3 + 4x_9 + 4x_{10} \equiv 0 \pmod 8, \tag{2.12}$$

$$x_3 - x_4 \equiv 0 \pmod 3, \tag{2.13}$$

$$x_1 - x_2 \equiv 0 \pmod 5, \tag{2.14}$$

$$x_6 + 2x_7 + 3x_8 + 4x_9 + 5x_{10} \equiv 0 \pmod{11}. \tag{2.15}$$

Proof. Reducing (1.16)–(1.20) modulo 32 we obtain

$$12x_1^2 + x_2^2 + 23x_3^2 + 14x_4^2 + 10x_5^2 + 20(x_6^2 + x_7^2 + x_8^2 + x_9^2 + x_{10}^2) \equiv 16 \pmod{32}, \tag{2.16}$$

$$13x_2^2 + 5x_3^2 + 20x_4^2 + 4x_5^2 + 16x_6^2 + 16x_{10}^2 + 30x_2x_3 + 8x_2x_4 + 24x_2x_5 + 8x_3x_4 + 24x_3x_5 + 8x_4x_5 \equiv 0 \pmod{32}, \tag{2.17}$$

$$13x_2^2 + 29x_3^2 + 16x_4^2 + 16x_9^2 + 16x_{10}^2 + 16x_1x_4 + 16x_1x_5 + 22x_2x_3 + 8x_2x_5 + 24x_3x_5 + 16x_4x_5 \equiv 0 \pmod{32}, \tag{2.18}$$

$$13x_2^2 + 5x_3^2 + 20x_4^2 + 4x_5^2 + 16x_7^2 + 16x_{10}^2 + 16x_1x_4 + 16x_1x_5 + 30x_2x_3 + 12x_2x_4 + 28x_2x_5 + 20x_3x_4 + 4x_3x_5 + 24x_4x_5 \equiv 0 \pmod{32}, \tag{2.19}$$

$$27x_2^2 + 3x_3^2 + 24x_4^2 + 24x_5^2 + 16x_8^2 + 16x_{10}^2 + 24x_1x_2 + 8x_1x_3 + 16x_1x_4 + 16x_1x_5 + 18x_2x_3 + 16x_2x_4 + 16x_2x_5 \equiv 0 \pmod{32}. \tag{2.20}$$

Taking (2.16) modulo 2 we obtain $x_2 - x_3 \equiv 0 \pmod 2$. Using this and (2.16) taken modulo 4 we obtain

$$x_4 - x_5 \equiv 0 \pmod 2. \tag{2.21}$$

Next taking (2.18) modulo 8 we obtain $5x_2^2 + 5x_3^2 + 6x_2x_3 \equiv 0 \pmod 8$, which gives

$$x_2 - x_3 \equiv 0 \pmod 4. \tag{2.22}$$

Reducing (2.16) modulo 8 we obtain

$$4x_1^2 + x_2^2 + 7x_3^2 + 6x_4^2 + 2x_5^2 + 4(x_6^2 + x_7^2 + x_8^2 + x_9^2 + x_{10}^2) \equiv 0 \pmod 8. \tag{2.23}$$

From (2.22) we have $x_2^2+7x_3^2 \equiv 0 \pmod 8$ and from (2.21) we have $6x_4^2+2x_5^2 \equiv 0 \pmod 8$, so that (2.23) becomes

$$x_1+x_6+x_7+x_8+x_9+x_{10} \equiv 0 \pmod 2. \tag{2.24}$$

Subtracting (2.19) from (2.17) we obtain

$$16x_6^2+16x_7^2+16x_1x_4+16x_1x_5+28x_2x_4+28x_2x_5+20x_3x_4+20x_3x_5+16x_4x_5 \equiv 0 \pmod{32}. \tag{2.25}$$

Appealing to (2.21) and (2.22) we have

$$28x_2x_4+28x_2x_5+20x_3x_4+20x_3x_5 \equiv 0 \pmod{32},$$

$$16x_1x_4+16x_1x_5+16x_4x_5 \equiv 16x_5^2 \pmod{32},$$

so that (2.25) gives $x_5+x_6+x_7 \equiv 0 \pmod 2$, which is (2.10).

Adding (2.18) and (2.20) we obtain

$$x_2^2+x_4^2+3x_5^2+2x_8^2+2x_9^2+3x_1x_2+x_1x_3+x_2x_3+2x_2x_4+3x_2x_5+3x_3x_5+2x_4x_5 \equiv 0 \pmod 4. \tag{2.26}$$

Appealing to (2.21) and (2.22) we have

$$x_4^2+3x_5^2+2x_4x_5 \equiv 2x_4^2 \pmod 4,$$

$$x_2^2+3x_1x_2+x_1x_3+x_2x_3+2x_2x_4+3x_2x_5+3x_3x_5 \equiv 2x_3^2 \pmod 4,$$

so that (2.26) gives $x_3+x_4+x_8+x_9 \equiv 0 \pmod 2$, which is (2.9).

From (2.9), (2.10), (2.21) and (2.24) we have

$$\begin{aligned} x_1+x_2+x_{10} &\equiv x_1+x_3+x_4+x_5+x_{10} \pmod 2 \\ &\equiv (x_1+x_6+x_7+x_8+x_9+x_{10})+(x_5+x_6+x_7)+(x_3+x_4+x_8+x_9) \\ &\equiv 0 \pmod 2, \end{aligned}$$

which proves (2.8.)

Adding (2.19) and (2.20) we obtain

$$2x_2^2+2x_3^2+3x_4^2+7x_5^2+4x_7^2+4x_8^2+6x_1x_2+2x_1x_3+4x_2x_3+7x_2x_4+3x_2x_5+5x_3x_4+x_3x_5+6x_4x_5 \equiv 0 \pmod 8.$$

Using (2.21) in the form $x_4 = x_5+2l$, and also (2.22), this congruence gives

$$x_7^2+x_8^2+3l^2 \equiv 0 \pmod 2,$$

that is,

$$x_7+x_8+l \equiv 0 \pmod 2$$

or

$$x_4-x_5+2x_7+2x_8 \equiv 0 \pmod 4,$$

which is (2.11).

Using (2.22) in the form $x_2 = x_3 + 4m$, and also (2.21), in (2.18) we obtain

$$x_9^2 + x_{10}^2 + m^2 \equiv 0 \pmod 2,$$

that is

$$x_9 + x_{10} + m \equiv 0 \pmod 2,$$

or

$$x_2 - x_3 + 4x_9 + 4x_{10} \equiv 0 \pmod 8,$$

which is (2.12).

(2.13) follows by reducing (1.17) modulo 3.

Reducing (1.16)–(1.20) modulo 5 we obtain

$$\begin{aligned}(x_1+x_2)(x_1-x_2) &\equiv x_5(x_1-x_2) \equiv (x_4+x_5)(x_1-x_2) \equiv (4x_3+2x_4+x_5)(x_1-x_2)\\ &\equiv (2x_2+x_3+2x_4+x_5)(x_1-x_2) \equiv 0 \pmod 5.\end{aligned}$$

If $x_1 - x_2 \equiv 0 \pmod 5$ then we have

$$x_5 \equiv x_4 \equiv x_3 \equiv x_2 \equiv x_1 \equiv 0 \pmod 5,$$

which is a contradiction. This proves (2.14).

Finally from (1.21) and (1.22) we have

$$3x_2 + 4x_3 + 5x_4 + 6x_5 \equiv 0 \pmod{11}. \tag{2.27}$$

Also by computing $3(1.17) + 4(1.18) + (1.19) + 5(1.20)$ modulo 11 we obtain

$$(x_6 + 2x_7 + 3x_8 + 4x_9 + 5x_{10})^2 + 3x_1(3x_2 + 4x_3 + 5x_4 + 6x_5) \equiv 0 \pmod{11}. \tag{2.28}$$

Thus from (2.27) and (2.28) we have (2.15).

This completes the proof of Lemma 3.

The next lemma, which is just stated here, is a result of Dickson. It relates the factorization $p = K\bar{K}$ in $Z[\zeta]$ to representability of $1200p$ as a sum of squares. For a proof the reader is referred to [3].

LEMMA 4. *Let* $K = \sum_{i=1}^{10} a_i \zeta^i \in Z[\zeta]$, *and set*

$$\begin{aligned}A_1 &= a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_6 + a_6a_7 + a_7a_8 + a_8a_9 + a_9a_{10},\\ A_2 &= a_1a_3 + a_2a_4 + a_3a_5 + a_4a_6 + a_5a_7 + a_6a_8 + a_7a_9 + a_8a_{10} + a_{10}a_1,\\ A_3 &= a_1a_4 + a_2a_5 + a_3a_6 + a_4a_7 + a_5a_8 + a_6a_9 + a_7a_{10} + a_9a_1 + a_{10}a_2,\\ A_4 &= a_1a_5 + a_2a_6 + a_3a_7 + a_4a_8 + a_5a_9 + a_6a_{10} + a_8a_1 + a_9a_2 + a_{10}a_3,\\ A_5 &= a_1a_6 + a_2a_7 + a_3a_8 + a_4a_9 + a_5a_{10} + a_7a_1 + a_8a_2 + a_9a_3 + a_{10}a_4.\end{aligned}$$

*Then we have* $K\bar{K} = p$ *if and only if*

$$
\begin{aligned}
(2.29)\quad 1200p = {} & 12(a_1+a_2+a_3+a_4+a_5+a_6+a_7+a_8+a_9+a_{10})^2 + \\
& +33(a_1+a_2+a_3+a_4-4a_5-4a_6+a_7+a_8+a_9+a_{10})^2 + \\
& +55(a_1+a_2+a_3-3a_4-3a_7+a_8+a_9+a_{10})^2 + \\
& +110(a_1+a_2-2a_3-2a_8+a_9+a_{10})^2 + \\
& +330(a_1-a_2-a_9+a_{10})^2 + \\
& +660\{(a_1-a_{10})^2+(a_2-a_9)^2+(a_3-a_8)^2+(a_4-a_7)^2 + \\
& \qquad +(a_5-a_6)^2\}
\end{aligned}
$$

*and*

$$(2.30)\qquad A_1 = A_2 = A_3 = A_4 = A_5.$$

**3. Solutions of the diophantine system.** In this section we provide the main step in the proof of Theorem 1, by relating factorizations of $p$ in $Z[\zeta]$ to solutions of (1.16)–(1.22).

LEMMA 5. *There is a one-to-one correspondence between normalized elements* $K \in Z[\zeta]$ *satisfying* $K\bar{K} = p$ *and solutions* $\pm(x_1, \ldots, x_{10})$ *of* (1.16)–(1.22).

Proof. Let $K = \sum_{i=1}^{10} a_i \zeta^i$ be a normalized element of $Z[\zeta]$ satisfying $K\bar{K} = p$. We define integers $x_1, \ldots, x_{10}$ by

$$
\begin{aligned}
x_1 &= a_1+a_2+a_3+a_4+a_5+a_6+a_7+a_8+a_9+a_{10}, \\
x_2 &= a_1+a_2+a_3+a_4-4a_5-4a_6+a_7+a_8+a_9+a_{10}, \\
x_3 &= a_1+a_2+a_3-3a_4-3a_7+a_8+a_9+a_{10}, \\
x_4 &= a_1+a_2-2a_3-2a_8+a_9+a_{10}, \\
x_5 &= a_1-a_2-a_9+a_{10}, \qquad (3.1) \\
x_6 &= a_1-a_{10}, \\
x_7 &= a_2-a_9, \\
x_8 &= a_3-a_8, \\
x_9 &= a_4-a_7, \\
x_{10} &= a_5-a_6.
\end{aligned}
$$

Note that as $K$ is normalized we have $x_1 = \sum_{i=1}^{10} a_i \equiv -1 \pmod{11}$. Equation

(2.29) of Lemma 4 shows that (1.16) holds. Inverting the system (3.1) we obtain

$$
\begin{aligned}
120a_1 &= 12x_1+3x_2+5x_3+10x_4+30x_5+60x_6,\\
120a_2 &= 12x_1+3x_2+5x_3+10x_4-30x_5 \qquad +60x_7,\\
120a_3 &= 12x_1+3x_2+5x_3-20x_4 \qquad\quad +60x_8,\\
120a_4 &= 12x_1+3x_2-15x_3 \qquad\qquad +60x_9,\\
120a_5 &= 12x_1-12x_2 \qquad\qquad\quad +60x_{10},\\
120a_6 &= 12x_1-12x_2 \qquad\qquad\quad -60x_{10},\\
120a_7 &= 12x_1+3x_2-15x_3 \qquad\qquad -60x_9,\\
120a_8 &= 12x_1+3x_2+5x_3-20x_4 \qquad\quad -60x_8,\\
120a_9 &= 12x_1+3x_2+5x_3+10x_4-30x_5 \qquad -60x_7,\\
120a_{10} &= 12x_1+3x_2+5x_3+10x_4+30x_5-60x_6.
\end{aligned} \tag{3.2}
$$

Substituting these values for $a_1, \ldots, a_{10}$ into the conditions (2.30)

$$A_1-A_2 = A_1-A_3 = A_1-A_4 = A_1-A_5 = 0$$

given by Lemma 4, we obtain (1.17)–(1.20). Finally by Lemma 2 we have

$$\sum_{i=1}^{10} i^2 a_i \equiv \sum_{i=1}^{10} i^4 a_i \equiv 0 \pmod{11}, \tag{3.3}$$

and substituting the values for $a_1, \ldots, a_{10}$ given by (3.2) into (3.3) we obtain (1.21) and (1.22).

Conversely let $\pm(x_1, \ldots, x_{10})$ be a solution of (1.16)–(1.22). By Lemma 3 we may define integers $a_1, \ldots, a_{10}$ by

$$
\begin{aligned}
120\lambda a_1 &= 12x_1+3x_2+5x_3+10x_4+30x_5+60x_6,\\
120\lambda a_2 &= 12x_1+3x_2+5x_3+10x_4-30x_5+60x_7,\\
120\lambda a_3 &= 12x_1+3x_2+5x_3-20x_4+60x_8,\\
120\lambda a_4 &= 12x_1+3x_2-15x_3+60x_9,\\
120\lambda a_5 &= 12x_1-12x_2+60x_{10},\\
120\lambda a_6 &= 12x_1-12x_2-60x_{10},\\
120\lambda a_7 &= 12x_1+3x_2-15x_3-60x_9,\\
120\lambda a_8 &= 12x_1+3x_2+5x_3-20x_4-60x_8,\\
120\lambda a_9 &= 12x_1+3x_2+5x_3+10x_4-30x_5-60x_7,\\
120\lambda a_{10} &= 12x_1+3x_2+5x_3+10x_4+30x_5-60x_6,
\end{aligned} \tag{3.4}
$$

where $\lambda = \pm 1$. Clearly $\lambda \sum_{i=1}^{10} a_i = x_1$, and since $(x_1, \ldots, x_{10})$ satisfies (1.16)

we have $x_1 \equiv \pm 1 \pmod{11}$. Thus we take $\lambda = -1$, if $x_1 \equiv 1 \pmod{11}$, and $\lambda = +1$, if $x_1 \equiv -1 \pmod{11}$, so that

$$\sum_{i=1}^{10} a_i \equiv -1 \pmod{11}. \tag{3.5}$$

We then set $K = \sum_{i=1}^{10} a_i \zeta^i$ so that $K \in Z[\zeta]$. By Lemma 4 we have $K\bar{K} = p$, as (3.4) implies that (2.29) and (2.30) are satisfied. Now from (3.4) we have

$$\lambda \sum_{i=1}^{10} i a_i \equiv x_6 + 2x_7 + 3x_8 + 4x_9 + 5x_{10} \pmod{11}, \tag{3.6}$$

so that Lemma 3 gives

$$\sum_{i=1}^{10} i a_i \equiv 0 \pmod{11}. \tag{3.7}$$

Hence by (3.5) and (3.7) $K$ is a *normalized* element of $Z[\zeta]$ satisfying $K\bar{K} = p$.

This completes the proof of Lemma 5.

**4. Proof of Theorem 1.** The integers $K$ of $Z[\zeta]$ such that $K\bar{K} = p$ have been described in § 1. Applying to Lemma 1, we let $K_1 = J_\pi(1, 1)$, $K_2 = J_\pi(1, 2)$ and $K_3$ denote, respectively, the unique normalized associates of

$$\pi_1\pi_3\pi_4\pi_6\pi_9, \quad \pi_1\pi_2\pi_4\pi_6\pi_8, \quad \text{and} \quad \pi_1\pi_2\pi_3\pi_5\pi_7$$

satisfying $K_i\bar{K}_i = p$, $i = 1, 2, 3$. By Lemma 5, each $K_i$ gives rise to solutions $\pm(x_{1i}, x_{2i}, \ldots, x_{10i})$ of (1.16)–(1.22). The conjugates of each $K_i$ give rise to the 20 solutions given in (1.24). (These solutions are distinct as the conjugates are distinct.) Thus $K_1$, $K_2$ and $K_3$ account for 60 solutions of (1.16)–(1.22).

It remains to consider the conjugates and associates of $\pi_1\pi_3\pi_4\pi_5\pi_9$. As this algebraic integer is left fixed by the automorphism $\sigma_3$ of $Q(\zeta)$, it is an integer of $Q(\sqrt{-11})$, so that

$$\pi_1\pi_3\pi_4\pi_5\pi_9 = \tfrac{1}{2}(a + b\sqrt{-11}), \tag{4.1}$$

where $a$ and $b$ are integers such that $a \equiv b \pmod 2$. As $4p = a^2 + 11b^2$, we have $a \equiv 2$ or $9 \pmod{11}$.

Considering (4.1) and the Gaussian sum

$$\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x = \zeta - \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 - \zeta^6 - \zeta^7 - \zeta^8 + \zeta^9 - \zeta^{10} = \sqrt{-11} \tag{4.2}$$

we have

$$\pi_1\pi_3\pi_4\pi_5\pi_9 = \sum_{i=1}^{10} c_i\zeta^i,$$

where

$$c_1 = c_3 = c_4 = c_5 = c_9 = \tfrac{1}{2}(b-a), \qquad c_2 = c_6 = c_7 = c_8 = c_{10} = -\tfrac{1}{2}(b+a)$$

Now $\sum_{i=1}^{10} c_i = -5a$, $\sum_{i=1}^{10} ic_i \equiv 0 \pmod{11}$, so that

$$(4.3) \qquad \begin{cases} -\pi_1\pi_3\pi_4\pi_5\pi_9 \text{ is normalized if } a \equiv 2 \pmod{11}, \\ +\pi_1\pi_3\pi_4\pi_5\pi_9 \text{ is normalized if } a \equiv 9 \pmod{11}. \end{cases}$$

The normalized element (4.3) and its conjugate give rise to the 4 solutions.

$$\begin{cases} \pm(5a,0,0,0,0,-b,b,-b,-b,-b); \pm(5a,0,0,0,0,b,-b,b,b,b), \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad a \equiv 2 \pmod{11}, \\ \pm(-5a,0,0,0,0,b,-b,b,b,b); \pm(-5a,0,0,0,0,-b,b,-b,-b,-b). \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad a \equiv 9 \pmod{11}. \end{cases}$$

By Lemma 5 every solution of (1.16)–(1.22) arises in this way so the total number of solutions is $60+4 = 64$, and this completes the proof of Theorem 1.

**5. Evaluation of the cyclotomic numbers of order eleven — proof of Theorem 2.** We let $(x_1, \ldots, x_{10})$ (resp., $(y_1, \ldots, y_{10})$) where $x_1 \equiv -1 \pmod{11}$ (resp., $y_1 \equiv -1 \pmod{11}$), be the solution of (1.16)–(1.22) corresponding to $J_\pi(1,1)$ (resp., $J_\pi(1,2)$) so that $J_\pi(1,1) = \sum_{i=1}^{10} a_i\zeta^i$ (resp., $J_\pi(1,2) = \sum_{i=1}^{10} a_i'\zeta^i$), where the $a_i$ are given in terms of the $x_i$ by (3.2) (resp., the $a_i'$ are given in terms of the $y_i$ by (3.2) modified in the obvious way). Moreover from (1.9) we have

$$(5.1) \qquad a_i = B(i,1) - B(0,1), \qquad a_i' = B(i,2) - B(0,2).$$

Now by (1.14) we have

$$x_1 = \sum_{i=1}^{10} a_i = \sum_{i=1}^{10} B(i,1) - 10B(0,1) = p - 2 - 11B(0,1)$$

so that

$$(5.2) \qquad 11B(0,1) = p - 2 - x_1.$$

Similarly we have

$$(5.3) \qquad 11B(0,2) = p - 2 - y_1.$$

Then from (5.1), (5.2) and (5.3) we can compute immediately $B(i,1)$ and $B(i,2)$ for $i = 0, 1, 2, \ldots, 10$ in terms of the $x_i$ and $y_i$. The values

of $B(0, 0)$ and $B(1, 0)$ follow immediately from (1.12). These 24 values of the $B(i, j)$ enable us to calculate all the Dickson–Hurwitz sums $B(i, j)$ in view of (1.11) and (1.13). Using these values in (1.15) we obtain the cyclotomic numbers of order 11 as given in Table 1.

**6. Evaluation of solutions in terms of Jacobsthal–Whiteman sums.** In this section we follow ideas of Whiteman [12], [16] in order to give explicit formulae for the solutions $(x_1, \ldots, x_{10})$ and $(y_1, \ldots, y_{10})$ of (1.16)–(1.22) in terms of which the cyclotomic numbers of order eleven have been given. In order to do this we need a sum considered by Whiteman which generalizes the familar Jacobsthal sum. We define the Jacobsthal–Whiteman sum $\varphi^n(a)$ of order 11 as follows: for any positive integer $n$ and any integer $a$ we let $N_n(a)$ denote the number of solutions $y$, $0 \leqslant y \leqslant p-1$, for which $y^{n+1}+y^n \equiv a \pmod p$ and set

$$\varphi^n(a) = \sum_{x=0}^{p-1} N_n(\tilde{4}ax^{11}) - (p+1), \tag{6.1}$$

where $\tilde{4}$ denotes the inverse of 4 modulo $p$. When $n = 1$, $\varphi^1(a) = \varphi_{11}(a)$ — the familar Jacobsthal sum, as in this case

$$N_1(b) = 1 + \left(\frac{1+4b}{p}\right)$$

so that

$$\varphi^1(a) = \sum_{x=1}^{p-1}\left(\frac{1+ax^{11}}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)^{10}\left(\frac{1+a\bar{x}^{11}}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{\bar{x}}{p}\right)\left(\frac{x^{11}+a}{p}\right) = \varphi_{11}(a).$$

Whiteman [16] has noted that the number of solutions $(x, y)$ of the congruence

$$y^{n+1}+y^n \equiv x^{11}g^v \pmod p \qquad (v \text{ fixed};\ 0 \leqslant x, y \leqslant p-1)$$

is equal to $2+11B(v, n)$ so that

$$2+11B(v, n) = \sum_{x=0}^{p-1} N_n(g^v x^{11}) = p+1+\varphi^n(4g^v)$$

giving

$$11B(v, n) = \varphi^n(4g^v)+p-1. \tag{6.2}$$

Taking $n = 1, 2$ and $v = 0, 1, \ldots, 10$ in (6.2) and using (3.1) and (5.1) we obtain the expressions given in (1.25).

**7. Example.** We take $p = 23$. The $\varphi(22) = 10$ primitive roots (mod 23) are $g = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$. We will just determine the

cyclotomic numbers of order 11 when $g = 5$. We first compute the number of solutions of $x^2+x \equiv a$ and $x^3+x^2 \equiv a \pmod{23}$. We obtain

| $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_1(a)$ | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 1 | 2 | 2 | 2 | 2 | 0 |
| $N_2(a)$ | 2 | 2 | 1 | 1 | 1 | 3 | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 0 | 3 | 1 | 1 | 1 |

Using the above values and (6.1) we obtain the values of $\varphi^1(4g^v)$ and $\varphi^2(4g^v)$, for $g = 5$ and $v = 0, 1, \ldots, 10$, as given below

| $\varphi^1(4)$ | $\varphi^1(4g)$ | $\varphi^1(4g^2)$ | $\varphi^1(4g^3)$ | $\varphi^1(4g^4)$ | $\varphi^1(4g^5)$ | $\varphi^1(4g^6)$ | $\varphi^1(4g^7)$ | $\varphi^1(4g^8)$ | $\varphi^1(4g^9)$ | $\varphi^1(4g^{10})$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $-22$ | 0 | 22 | 0 | 0 | 22 | $-22$ | 11 | 0 | 0 | $-22$ |
| $\varphi^2(4)$ | $\varphi^2(4g)$ | $\varphi^2(4g^2)$ | $\varphi^2(4g^3)$ | $\varphi^2(4g^4)$ | $\varphi^2(4g^5)$ | $\varphi^2(4g^6)$ | $\varphi^2(4g^7)$ | $\varphi^2(4g^8)$ | $\varphi^2(4g^9)$ | $\varphi^2(4g^{10})$ |
| 11 | 11 | 0 | 0 | 22 | 0 | $-11$ | $-22$ | $-22$ | 11 | $-11$ |

From (1.25) we find that the solutions $(x_1, x_2, \ldots, x_{10})$ and $(y_1, y_2, \ldots, y_{10})$ are given by

| $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ | $x_8$ | $x_9$ | $x_{10}$ | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | $y_6$ | $y_7$ | $y_8$ | $y_9$ | $y_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 21 | 1 | $-3$ | 0 | $-4$ | 2 | 2 | 0 | $-1$ | 4 | $-12$ | 3 | $-1$ | 5 | $-1$ | 2 | $-1$ | 2 | 4 | 1 |

Then from Table 1 we obtain the cyclotomic numbers as given below:

| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

These values are easily checked by direct calculation.

## References


[1] L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. 21 (1967), pp. 204–219.

[2] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem, I, II*, Amer. J. Math. 57 (1935), pp. 391–424, 463–474.

[3] — *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), pp. 363–380.

[4] — *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. 38 (1935), pp. 187–200.

[5] E. Lehmer, Abstract: *On the quintic character of* 2, Bull. Amer. Math. Soc. 55 (1949), pp. 62–63.

[6] — *On the number of solutions of* $u^k+D \equiv w^2 \pmod{p}$, Pacific J. Math. 5 (1955), pp. 103–118.

[7] P. A. Leonard and K. S. Williams, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc. (to appear).

[8] J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. 11 (1966), pp. 263–279.

[9] — *Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. 134 (1969), pp. 483–502.

[10] — and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta. Arith. 17 (1970), pp. 185–216.

[11] T. Storer, *Cyclotomy and Difference Sets*, Chicago 1967.

[12] A. L. Whiteman, *Theorems on quadratic partitions*, Proc. Nat. Acad. Sci. U.S.A. 36 (1950), pp. 60–65.

[13] — *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), pp. 89–99.

[14] — *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), pp. 401–413.

[15] — *The cyclotomic numbers of order twelve*, Acta Arith. 6 (1960), pp. 53–76.

[16] — *The cyclotomic numbers of order ten*, Proc. Symp. Appl. Math. 10 (1960) pp. 95–111.

DEPARTMENT OF MATHEMATICS
ARIZONA STATE UNIVERSITY
Tempe, Arizona, U.S.A.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BRITISH COLUMBIA
Vancouver, B. C., Canada

*Received on 7. 8. 1973* (454)