ON THE UNIQUENESS OF SOLUTIONS OF CERTAIN DIOPHANTINE EQUATIONS

JOSEPH B. MUSKAT AND YUN-CHENG ZEE

ABSTRACT. An arithmetic proof by L. E. Dickson of the uniqueness of the integral solutions of a certain quaternary quadratic form is generalized to include several similar forms which have appeared recently in cyclotomy.

In his exposition of cyclotomy of order 5, Dickson studied the quaternary quadratic form

\[ 16p = x^2 + 125w^2 + 50u^2 + 50v^2 \]

with the side condition

\[ xw = v^2 - u^2 - 4uv, \]

where \( p \) is any prime \( \equiv 1 \) (mod 5). He gave an arithmetic proof, and an algebraic proof, that (1) and (2) have essentially a unique integral solution. There are eight related solutions; if \((x, w, u, v)\) is a solution, so are \((x, w, -u, -v), (x, -w, v, -u), \) and \((x, -w, -v, u)\). The other four are obtained from these by reversing all the signs [1, Theorem 8].

In recent studies of cyclotomy there have appeared several other examples of forms

\[ kp = c_1x^2 + c_2w^2 + c_3u^2 + c_4v^2, \quad c_1, c_2, c_3, c_4 > 0, \]

\( p \) any odd prime \( \equiv a \) (mod \( e \)), with the side condition

\[ d_1xw = d_2v^2 + d_3u^2 + d_4uv, \]

where all coefficients are relatively prime to \( p \). The symbols \( x, w, u \) and \( v \) denote rational linear combinations of coefficients of Jacobi sums (if \( a = 1 \)) or Eisenstein sums; \( k \) is taken to be greater than 1 where necessary to ensure that \( x, w, u \) and \( v \) are integers. Thus for each pair \((e, a)\) to be considered here, there are integers \( c_1, c_2, c_3, c_4, d_1, d_2, d_3, d_4 \) (which depend only on \( e \) and \( a \)) such that for every \( p \equiv a \) (mod \( e \)), (3) and (4) are solvable in integers.

Received by the editors November 15, 1973 and, in revised form, February 15, 1974.

AMS (MOS) subject classifications (1970). Primary 10B05, 10C05.

Key words and phrases. Cyclotomy, quaternary quadratic form.
In this paper, we generalize Dickson's arithmetic proof to show that a number of these forms have essentially unique integral solutions.

First we express $u$ and $v$ linearly in terms of $x$ and $w$. All congruences will be modulo $p$.

Assume that the following five restrictions are satisfied by the coefficients in (3) and (4).

1. $c_4 = c_3$,
2. $d_3 = -d_2$,
3. $c_1 c_2 \left(4d_2^2 + d_4^2\right) = c_3^2 d_1^2$,
4. $c_1 c_2$ is a quadratic residue of $p$,
5. $[-1 \pm 2sd_2/(c_3 d_1)] c_1/c_3$ are quadratic residues of $p$,

where $s$ satisfies $s^2 \equiv c_1c_2$.

Transpose the last term in (4), apply (6), and square:

$$d_2^2(v^2 - u^2)^2 = (d_1 xw - d_4 uv)^2,$$

(10) $$d_2^2(v^2 + u^2)^2 = (d_1 xw - d_4 uv)^2 + 4d_2^2 u^2 v^2.$$

Transpose (3), regarded as a congruence (mod $p$), and apply (5):

(11) $$c_3(v^2 + u^2) = -c_1 x^2 - c_2 w^2.$$

Substitute (11) into (10):

$$d_2^2(-c_1 x^2 - c_2 w^2)^2 = c_3^2 (d_1 xw - d_4 uv)^2 + 4c_2^2 d_2^2 u^2 v^2,$$

$$d_2^2(c_1 x^2 - c_2 w^2)^2 = (c_3^2 d_1^2 - 4c_1 c_2 d_2^2)x^2 w^2$$

$$- 2c_2^2 d_1 d_4 xwu + c_3^2 (d_4^2 + 4d_2^2) u^2 v^2$$

$$\equiv x^2 w^2 c_1 c_2 d_4^2 - 2xwuvc_3^2 d_4 d_1 + u^2 v^2 c_3^2 d_1^2/(c_1 c_2),$$

upon two applications of (7),

$$\equiv (xwc_1 c_2 d_4 - uvc_3^2 d_1)^2/(c_1 c_2).$$

Take the square root and separate $uv$, choosing the sign of $s$ appropriately:

$$c_3 d_1 uv \equiv c_1 c_2 d_4 xw + sd_2(c_1 x^2 - c_2 w^2).$$
Add $2/(c_3 d_1)$ times (12) to (11):

$$c_3(v^2 + 2uv + u^2) = c_1 x^2(-1 + 2sd_2/(c_3 d_1))$$

(13)

$$+ 2xwc_1 c_2 d_4/(c_3 d_1) + c_2 w^2(-1 - 2sd_2/(c_3 d_1)).$$

In view of (9), define

$$m \equiv [-1 + 2sd_2/(c_3 d_1)] c_1/c_3,$$

(14)

$$t \equiv [-1 - 2sd_2/(c_3 d_1)] c_1/c_3.$$

$$m^2 + t^2 = [1 - 4c_1 c_2 d_1^2/(c_3 d_1^2)] c_1/c_3^2 \equiv [sc_1 d_4/(c_3 d_1)]^2,$$

by (7). Having picked $m$, choose the sign of $t$ so that

$$mt = sc_1 d_4/(c_3 d_1).$$

The congruences

$$m^2 + t^2 \equiv -2c_1/c_3, \quad m^2 - t^2 \equiv 4sc_1 d_2/(c_3 d_1)$$

(16)

are noted here for later reference. Now (13) can be written as

$$v^2 + 2uv + u^2 \equiv x^2 m^2 + 2xwmt/c + w^2 t^2/c_1;$$

$$v + u \equiv q_1(xm + wts/c_1), \quad q_1^2 = 1.$$

Similarly, subtracting $2/(c_3 d_1)$ times (12) from (11) yields, after simplification,

$$v^2 - 2uv + u^2 \equiv x^2 t^2 - 2xwmts/c + w^2 m^2/c_1;$$

$$v - u \equiv q_2(xt - wms/c_1), \quad q_2^2 = 1.$$

Thus

$$(v + u)(v - u) \equiv q_1 q_2 [(c_1 x^2 - c_2 w^2)sd_4 - 4xwc_1 c_2 d_2]/(c_3 d_1),$$

by (15) and (16). Apply (12) and regroup:

$$v^2 - u^2 \equiv q_1 q_2 [uvd_4/d_2 - xwc_1 c_2 (d_4^2 + 4d_2^2)/(c_3 d_1 d_2)]$$

$$\equiv q_1 q_2 [d_4 uv - d_1 xw]/d_2,$$

by (7). Now apply (4) and (6):

$$v^2 - u^2 \equiv q_1 q_2 (v^2 - u^2).$$

Hence if $v^2 \neq u^2$, $q_2 = -q_1$. If $v^2 = u^2$, one of $q_1$ and $q_2$ can be chosen arbitrarily; choose that one so that $q_2 = -q_1$. (The latter situation actually occurs.) In either case,
2v \equiv q_1 [x(m - t) + w(t + m)s/c_1],
2u \equiv q_1 [x(m + t) + w(t - m)s/c_1].

But \( q_1 \) can be discarded, for the effect of changing the sign of \( q_1 \) can be achieved by changing the signs of both \( m \) and \( t \). Thus

\[ 2v \equiv x(m - t) + w(t + m)s/c_1, \]
\[ 2u \equiv x(m + t) + w(t - m)s/c_1. \]

(17)

Thus there are two signs to be chosen, those of \( s \) and \( m \).

Let \((x, w, u, v)\) be a solution of (3) and (4). \((-x, -w, -u, -v)\) is another. Changing the signs of \( m \) and \( t \) gives two more, \((x, w, -u, -v)\) and \((-x, -w, u, v)\). Changing the sign of \( s \) interchanges \( m^2 \) with \( t^2 \), and the sign of the product \( mt \) is changed (see (14) and (15)). Thus replacing \( s, w, m, t \) by \(-s, -w, t, -m\) in (17) gives the solution \((x, -w, v, -u)\). The other three solutions are obtained by changing the signs of \( m \) and \( t \) or \( x \) and \( w \).

Fix the signs of \( s \) and \( m \) in (17) and let

\[ (x, w, u, v), (x', w', u', v') \]

be two solutions. We have

\[ 4uv' = xx'(m - t)^2 + ww'(t + m)^2c_2/c_1 + (xw' + x'w)(m^2 - t^2)s/c_1. \]
\[ 4uu' = xx'(m + t)^2 + ww'(t - m)^2c_2/c_1 + (xw' + x'w)(t^2 - m^2)s/c_1. \]

\[ uu' + vv' = (xx' + ww'c_2/c_1)(m + t)/2 = (-c_1xx' - c_2ww')/c_3, \]
by (16). Hence

\[ (19) \quad \text{if } A = |c_1xx' + c_2ww' + c_3uu' + c_3vv'|, \text{ then } A \equiv 0 \pmod{p}. \]

Multiply together the representations of \( kp \) given in (3) corresponding to the two solutions in (18):

\[ (kp)^2 = A^2 + c_1c_2(xw' - x'w)^2 + c_1c_3(xu' - x'u)^2 + c_1c_3(xv' - x'v)^2 \]
\[ + c_2c_3(wu' - w'u)^2 + c_2c_3(wv' - w'v)^2 + c_2^2(uv' - u'v)^2. \]

(20)

This implies that \( A \leq kp \).

In order to prove that the two solutions in (18) are essentially the same, one first verifies that (5) through (9) are satisfied. This includes actually exhibiting \( m \) and \( t \). Having thereby justified the expressions for \( u \) and \( v \) given in (17), one then seeks to show that \( A = kp \), so that

\[ (21) \quad xu' = x'u, \quad xu = x'u, \quad xv' = x'v. \]
In every case to be considered here, the greatest common divisor \( D \) of \( c_2 \) and \( c_3 = c_4 \) does not divide \( k \), and \( c_1 = 1 \). Then according to (3) \( D \neq x \). Hence \( x \neq 0 \), so that (21) implies \( w/x = w'/x', \ u/x = u'/x', \ v/x = v'/x' \). Thus if \( A = kp \), then \( x' = \pm x, \ w' = \pm w, \ u' = \pm u \) and \( v' = \pm v \). That \( c_1 x \) is not divisible by \( D \) implies, furthermore, that in (19), \( A \neq 0 \). Consequently, if \( k = 1 \), it suffices to verify that (5) through (9) hold.

Although the notation here is modeled after that of Dickson, there are differences. If \( p \equiv 1 \) (mod 5), and (1) and (2) are satisfied, choose \( r \) such that \( \text{ord}_p r = 5 \). Set
\[
m \equiv (2r - r^2 + r^3 - 2r^4)/25, \quad t \equiv (r + 2r^2 - 2r^3 - r^4)/25, \quad s \equiv 5(r - r^2 - r^3 + r^4), \quad s^2 \equiv 125.
\]

There is also the form having \( k = 1, \ c_1 = 1, \ c_2 = c_3 = c_4 = 5, \ d_1 = d_2 = - d_3 = - d_4 = 1 \) \[2, \text{Theorem 8}\]. Set
\[
m \equiv (r - r^2 + r^3 - r^4)/5, \quad t \equiv (r^2 - r^3 - r^4)/5, \quad \]
\[
m t \equiv -(r - r^2 + r^3 - r^4)/5 \equiv -s/25, \quad s^2 \equiv 5.
\]

If \( p \equiv 1 \) (mod 16), then \( k = 1, \ c_1 = 1, \ c_2 = c_3 = c_4 = 8, \ d_1 = d_2 = - d_3 = - d_4 = 2 \) \[3, \text{p. 236}\]. (Uniqueness is mentioned there.) \( 8 \) is a quadratic residue of \( p \). Choose \( r \) so that \( \text{ord}_p r = 16 \). Then
\[
s \equiv 2(r^2 + r^{14}), \quad m \equiv (r + r^7)/4, \quad t \equiv -(r^3 + r^5)/4, \quad s^2 \equiv 4(r^4 + 2 + r^{12}) \equiv 8, \quad m^2 \equiv (r^2 + 2r^8 + r^{14})/16 \equiv -1/8 + s/32, \quad t^2 \equiv (r^6 + 2r^8 + r^{10})/16 \equiv (-r^{14} - 2 - r^2)/16 \equiv -1/8 - s/32, \quad mt \equiv -(r^4 + r^6 + r^{10} + r^{12})/16 \equiv s/32.
\]

Hence (9), (14), and (15) are satisfied, and the proof of uniqueness is complete.

If \( p \equiv 7 \) (mod 16), there is a form with \( k = 1, \ c_1 = 1, \ c_2 = c_3 = c_4 = 2, \ d_1 = 2, d_2 = - d_3 = 1, d_4 = - 2 \) \[2, (6.1), (6.2)\]. \( 2 \) is a quadratic residue of \( p \). Choose \( r \in GF(p^2) \) such that \( r^8 = 1 \) but \( r^8 \neq 1 \). Then \( s = r^2 + r^{14}, \ m = (r + r^7)/2 \) and \( t = (r^3 + r^5)/2 \) all lie in the ground field. Also
\[
s^2 \equiv r^4 + 2 + r^{12} = 2, \quad m^2 \equiv (r^2 - 2 + r^{14})/4 = -1/2 + s/4, \quad t^2 \equiv (r^6 - 2 + r^{10})/4 = -1/2 - s/4, \quad mt = - s/4.
\]

Uniqueness is established.

Now consider the following form for \( p \equiv 1 \) (mod 60):
\[ k = c_1 = 1, \quad c_2 = 45, \quad c_3 = c_4 = 15, \quad d_1 = d_2 = -d_3 = -d_4 = 1 \]

[4, Theorem 2]. Choose \( z \) such that \( \text{ord}_p z = 60 \). Set \( r \equiv z^{12}, R \equiv z^5 \). Then

\[
\begin{align*}
  s & = 3(r - r^2 - r^3 + r^4), \\
  m & = (R + R^{11})(r - r^2 + r^3 - r^4)/15, \\
  t & = (R + R^{11})(r + r^2 - r^3 - r^4)/15, \\
  s^2 & = 9 - 5 = 45, \\
  m^2 & = 9 \cdot 5 = 45, \\
  t^2 & = (R^2 + 2 + R^{10})(r^2 + r^4 + r^6 + r^8 - 4 - 2r^3 + 2r^4 + 2r - 2r^2)/225 \\
  & = 3(-1 - 4 + 2s/3)/225 \equiv -1/15 + 2s/225.
\end{align*}
\]

Similarly,

\[
\begin{align*}
  t^2 & \equiv -1/15 - 2s/225, \\
  mt & = 3(-r + r^2 + r^3 - r^4)/225 \equiv -s/225,
\end{align*}
\]

Uniqueness is proved.

Finally we present a form for which we have been unable to establish uniqueness. If \( p \equiv 1 \pmod{13} \), then \( k = 16, c_1 = 1, c_7 = 13, c_3 = c_4 = 26, d_1 = 1, d_2 = -d_3 = 3, d_4 = -4 \) [4, Theorem 1]. 13 is a quadratic residue of \( p \). Choose \( r \) so that \( \text{ord}_p r = 13 \). Define the periods \( y_0 \equiv r + r^3 + r^9, y_1 \equiv r^2 + r^6 + r^5, y_2 \equiv r^4 + r^{12} + r^{10}, y_3 \equiv r^8 + r^{11} + r^7 \) [1, p. 392]. Then \( s = y_0 + y_2 - y_1 - y_3, m \equiv (y_0 - y_2)/13, t \equiv (y_1 - y_3)/13 \). From the multiplication table for the periods

\[
\begin{array}{|c|c|c|c|c|}
\hline
  y_0 & y_1 + 2y_2 & -1 - y_2 & y_2 + 2y_3 & 3 + y_1 + y_3 \\
\hline
  y_1 & -1 - y_2 & y_2 + 2y_3 & -1 - y_3 & y_3 + 2y_0 \\
\hline
  y_2 & 3 + y_1 + y_3 & -1 - y_3 & y_3 + 2y_0 & -1 - y_1 \\
\hline
  y_3 & -1 - y_1 & 3 + y_0 + y_2 & -1 - y_0 & y_0 + 2y_1 \\
\hline
\end{array}
\]

it is easy to verify that

\[
\begin{align*}
  s^2 & \equiv 20 + 7(y_0 + y_1 + y_2 + y_3) \equiv 13, \\
  m^2 & \equiv (-6 + 2y_0 - y_1 + 2y_2 - y_3)/13^2 \\
  & \equiv (-6 + 3s/2)/13^2 \equiv -1/26 + 3s/338, \\
  t^2 & \equiv -1/26 - 3s/338, \\
  mt & \equiv (y_0 - y_2)(y_1 - y_3)/13^2 \equiv (-y_0 + y_1 - y_2 + y_3)/13^2 \equiv -s/13^2.
\end{align*}
\]
Since in this case \( k = 16 \), completing a proof of uniqueness requires showing that \( A = 16p \). In other words, by (19), if \( A = Mp \), \( M \) cannot assume any of the integer values from 1 to 15. Regarding (3) as a congruence \((\text{mod } 2)\) gives \( x \equiv w \pmod{2} \) and \( x' \equiv w' \pmod{2} \). Hence \( xx' + 13ww' \) is even, so \( M \) is even, by (19). According to (20), \( M^2 \equiv 16^2 \pmod{13} \). These conditions exclude all possible values of \( M \) except 10. We have been unable to eliminate this possibility.

A computer search of all primes \( p \equiv 1 \pmod{13}, p < 10,000 \), revealed no instance of nonunique solutions. We wish to thank the University of Pittsburgh Computer Center for granting access to its IBM 7090/1401 system, partially supported by National Science Foundation grant G-11309.

This research was partially supported by National Science Foundation grants GP-5308 and GP-8973. The second author also received support under a Faculty Research Grant, California State University, Fullerton.

REFERENCE


DEPARTMENT OF MATHEMATICS, BAR-ILAN UNIVERSITY, RAMAT-GAN, ISRAEL

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, FULLERTON, CALIFORNIA 92634