PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 1, May 1975

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

$$16p = x^2 + 125w^2 + 50u^2 + 50v^2 \tag{1}$$

with the side condition

$$xw = v^2 - u^2 - 4uv, \tag{2}$$

where p is any prime $\equiv 1 \pmod 5$. 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

$$kp = c_1x^2 + c_2w^2 + c_3u^2 + c_4v^2, \qquad c_1, c_2, c_3, c_4 > 0, \tag{3}$$

p any odd prime $\equiv a \pmod e$, with the side condition

$$d_1xw = d_2v^2 + d_3u^2 + d_4uv, \tag{4}$$

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 insure 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 $p \equiv a \pmod e$, (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).

(5) $$c_4 = c_3,$$

(6) $$d_3 = -d_2,$$

(7) $$c_1c_2(4d_2^2 + d_4^2) = c_3^2d_1^2,$$

(8) c_1c_2 is a quadratic residue of p,

(9) $[-1 \pm 2sd_2/(c_3d_1)]c_1/c_3$ are quadratic residues of p,

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

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

$$d_2^2(v^2 - u^2)^2 = (d_1xw - d_4uv)^2,$$

(10) $$d_2^2(v^2 + u^2)^2 = (d_1xw - d_4uv)^2 + 4d_2^2u^2v^2.$$

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

(11) $$c_3(v^2 + u^2) \equiv -c_1x^2 - c_2w^2.$$

Substitute (11) into (10):

$$d_2^2(-c_1x^2 - c_2w^2)^2 \equiv c_3^2(d_1xw - d_4uv)^2 + 4c_3^2d_2^2u^2v^2,$$

$$d_2^2(c_1x^2 - c_2w^2)^2 \equiv (c_3^2d_1^2 - 4c_1c_2d_2^2)x^2w^2$$

$$- 2c_3^2d_1d_4xwuv + c_3^2(d_4^2 + 4d_2^2)u^2v^2$$

$$\equiv x^2w^2c_1c_2d_4^2 - 2xwuvc_3^2d_4d_1 + u^2v^2c_3^4d_1^2/(c_1c_2),$$

upon two applications of (7),

$$\equiv (xwc_1c_2d_4 - uvc_3^2d_1)^2/(c_1c_2).$$

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

(12) $$c_3^2d_1uv \equiv c_1c_2d_4xw + sd_2(c_1x^2 - c_2w^2).$$

Add $2/(c_3d_1)$ times (12) to (11):

$$c_3(v^2 + 2uv + u^2) \equiv c_1x^2(-1 + 2sd_2/(c_3d_1)) + 2xwc_1c_2d_4/(c_3d_1) + c_2w^2(-1 - 2sd_2/(c_3d_1)). \tag{13}$$

In view of (9), define

$$m^2 \equiv [-1 + 2sd_2/(c_3d_1)]c_1/c_3, \qquad t^2 \equiv [-1 - 2sd_2/(c_3d_1)]c_1/c_3. \tag{14}$$

$$m^2t^2 \equiv [1 - 4c_1c_2d_2^2/(c_3^2d_1^2)]c_1^2/c_3^2 \equiv [sc_1d_4/(c_3^2d_1)]^2,$$

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

$$mt \equiv sc_1d_4/(c_3^2d_1). \tag{15}$$

The congruences

$$m^2 + t^2 \equiv -2c_1/c_3, \qquad m^2 - t^2 \equiv 4sc_1d_2/(c_3^2d_1) \tag{16}$$

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

$$v^2 + 2uv + u^2 \equiv x^2m^2 + 2xwmts/c_1 + w^2t^2c_2/c_1;$$

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

Similarly, subtracting $2/(c_3d_1)$ times (12) from (11) yields, after simplification,

$$v^2 - 2uv + u^2 \equiv x^2t^2 - 2xwmts/c_1 + w^2m^2c_2/c_1;$$

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

Thus

$$(v + u)(v - u) \equiv q_1q_2[(c_1x^2 - c_2w^2)sd_4 - 4xwc_1c_2d_2]/(c_3^2d_1),$$

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

$$v^2 - u^2 \equiv q_1q_2[uvd_4/d_2 - xwc_1c_2(d_4^2 + 4d_2^2)/(c_3^2d_1d_2)]$$

$$\equiv q_1q_2[d_4uv - d_1xw]/d_2,$$

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

$$v^2 - u^2 \equiv -q_1q_2(v^2 - u^2).$$

Hence if $v^2 \not\equiv u^2$, $q_2 = -q_1$. If $v^2 \equiv u^2$, 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

$$2v \equiv x(m-t) + w(t+m)s/c_1,$$

$$2u \equiv x(m+t) + w(t-m)s/c_1. \tag{17}$$

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

$$(x, w, u, v), (x', w', u', v') \tag{18}$$

be two solutions. We have

$$4vv' \equiv xx'(m-t)^2 + ww'(t+m)^2c_2/c_1 + (xw' + x'w)(m^2 - t^2)s/c_1.$$

$$4uu' \equiv xx'(m+t)^2 + ww'(t-m)^2c_2/c_1 + (xw' + x'w)(t^2 - m^2)s/c_1.$$

$$uu' + vv' \equiv (xx' + ww'c_2/c_1)(m^2 + t^2)/2 \equiv (-c_1xx' - c_2ww')/c_3,$$

by (16). Hence

$$\text{if } A = |c_1xx' + c_2ww' + c_3uu' + c_3vv'|, \text{ then } A \equiv 0 \pmod{p}. \tag{19}$$

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

$$\begin{aligned}(kp)^2 = A^2 &+ c_1c_2(xw' - x'w)^2 + c_1c_3(xu' - x'u)^2 + c_1c_3(xv' - x'v)^2 \\ &+ c_2c_3(wu' - w'u)^2 + c_2c_3(wv' - w'v)^2 + c_3^2(uv' - u'v)^2.\end{aligned} \tag{20}$$

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

$$xw' = x'w, \quad xu' = x'u, \quad xv' = x'v. \tag{21}$$

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) $D \nmid x$. 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 $p \equiv 1 \pmod 5$, and (1) and (2) are satisfied, choose r such that $\operatorname{ord}_p r = 5$. Set

$$m \equiv (2r - r^2 + r^3 - 2r^4)/25, \qquad t \equiv (r + 2r^2 - 2r^3 - r^4)/25,$$

$$s \equiv 5(r - r^2 - r^3 + r^4), \qquad s^2 \equiv 125.$$

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, Theorem 8]. Set

$$m \equiv (r - r^2 + r^3 - r^4)/5, \qquad t \equiv (r + r^2 - r^3 - r^4)/5,$$

$$mt \equiv -(r - r^2 - r^3 + r^4)/25 \equiv -s/25, \qquad s^2 \equiv 5.$$

If $p \equiv 1 \pmod{16}$, then $k = 1$, $c_1 = 1$, $c_2 = c_3 = c_4 = 8$, $d_1 = d_2 = -d_3 = 1$, $d_4 = 2$ [3, p. 236]. (Uniqueness is mentioned there.) 8 is a quadratic residue of p. Choose r so that $\operatorname{ord}_p r = 16$. Then

$$s \equiv 2(r^2 + r^{14}), \quad m \equiv (r + r^7)/4, \quad t \equiv -(r^3 + r^5)/4.$$

$$s^2 \equiv 4(r^4 + 2 + r^{12}) \equiv 8.$$

$$m^2 \equiv (r^2 + 2r^8 + r^{14})/16 \equiv -1/8 + s/32.$$

$$t^2 \equiv (r^6 + 2r^8 + r^{10})/16 \equiv (-r^{14} - 2 - r^2)/16 \equiv -1/8 - s/32.$$

$$mt \equiv -(r^4 + r^6 + r^{10} + r^{12})/16 \equiv s/32.$$

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

If $p \equiv 7 \pmod{16}$, 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 $r^{16} = 1$ 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

$$s^2 = r^4 + 2 + r^{12} = 2,$$

$$m^2 = (r^2 - 2 + r^{14})/4 = -1/2 + s/4,$$

$$t^2 = (r^6 - 2 + r^{10})/4 = -1/2 - s/4, \quad mt = -s/4.$$

Uniqueness is established.

Now consider the following form for $p \equiv 1 \pmod{60}$:

$k = c_1 = 1, \quad c_2 = 45, \quad c_3 = c_4 = 15, \quad d_1 = d_2 = -d_3 = -d_4 = 1$

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

$$s \equiv 3(r - r^2 - r^3 + r^4),$$

$$m \equiv (R + R^{11})(r - r^2 + r^3 - r^4)/15,$$

$$t \equiv (R + R^{11})(r + r^2 - r^3 - r^4)/15, \qquad s^2 \equiv 9 \cdot 5 \equiv 45,$$

$$m^2 \equiv (R^2 + 2 + R^{10})(r^2 + r^4 + r^6 + r^8 - 4 - 2r^3 + 2r^4 + 2r - 2r^2)/225$$

$$\equiv 3(-1 - 4 + 2s/3)/225 \equiv -1/15 + 2s/225.$$

Similarly,

$$t^2 \equiv -1/15 - 2s/225, \qquad mt \equiv 3(-r + r^2 + r^3 - r^4)/225 \equiv -s/225,$$

Uniqueness is proved.

Finally we present a form for which we have been unable to establish uniqueness. If $p \equiv 1 \pmod{13}$, then $k = 16$, $c_1 = 1$, $c_2 = 13$, $c_3 = c_4 = 26$, $d_1 = 1$, $d_2 = -d_3 = 3$, $d_4 = -4$ [4, Theorem 1]. 13 is a quadratic residue of p. Choose r so that $\operatorname{ord}_p r = 13$. 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 $s \equiv y_0 + y_2 - y_1 - y_3$, $m \equiv (y_0 - y_2)/13$, $t \equiv (y_1 - y_3)/13$. From the multiplication table for the periods

y_0	$y_1 + 2y_2$			
y_1	$-1 - y_2$	$y_2 + 2y_3$		
y_2	$3 + y_1 + y_3$	$-1 - y_3$	$y_3 + 2y_0$	
y_3	$-1 - y_1$	$3 + y_0 + y_2$	$-1 - y_0$	$y_0 + 2y_1$
	y_0	y_1	y_2	y_3

it is easy to verify that

$$s^2 \equiv 20 + 7(y_0 + y_1 + y_2 + y_3) \equiv 13,$$

$$m^2 \equiv (-6 + 2y_0 - y_1 + 2y_2 - y_3)/13^2$$

$$\equiv (-6\tfrac{1}{2} + 3s/2)/13^2 \equiv -1/26 + 3s/338,$$

$$t^2 \equiv -1/26 - 3s/338,$$

$$mt \equiv (y_0 - y_2)(y_1 - y_3)/13^2 \equiv (-y_0 + y_1 - y_2 + y_3)/13^2 \equiv -s/13^2.$$

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 (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

1. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.

2. R. E. Giudici, J. B. Muskat and S. F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc. 171 (1972), 317–347. MR 46 #5249.

3. H. Hasse, *Der 2^n-te Potenzcharakter von 2 im Körper der 2^n-ten Einheitswurzeln*, Rend. Circ. Mat. Palermo (2) 7 (1958), 185–244. MR 21 #4143.

4. Y. C. Zee, *The Jacobi sums of orders thirteen and sixty and related quadratic decompositions*, Math. Z. 115 (1970), 259–272. MR 41 #6812.

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

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