JOURNAL OF NUMBER THEORY 16, 100–105 (1983)

On Legendre's Equation $ax^2 + by^2 + cz^2 = 0$

RICHARD H. HUDSON

Department of Mathematics and Statistics, University of South Carolina, Columbia, South Carolina, 29208

AND

KENNETH S. WILLIAMS*

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6

Communicated by Hans Zassenhaus

Received January 19, 1981; revised May 20, 1981

Let a, b, c be nonzero integers having no prime factors $\equiv 3 \pmod 4$, not all of the same sign, abc squarefree, and for which Legendre's equation $ax^2 + by^2 + cz^2 = 0$ is solvable in nonzero integers x, y, z. A property is proved yielding a congruence which must be satisfied by any solution x, y, z.

Let a, b, c be three nonzero integers, not all of the same sign, and such that abc is squarefree. The Diophantine equation

$$ax^2 + by^2 + cz^2 = 0 \tag{1}$$

is named after Legendre, who proved in 1785 that it is solvable in integers x, y, z, not all zero, if and only if $-bc$, $-ca$, $-ab$ are quadratic residues of a, b, c, respectively (see for example [3, Theorem 3; 4, Theorem 113]). We shall consider solvable equations of form (1) in which a, b, c have no prime factors $\equiv 3 \pmod 4$. Clearly, without loss of generality, we may suppose throughout that $a > 0$, $b > 0$, $c < 0$.

Throughout this note, whenever n is a nonzero integer we use the notation n_1 to mean the odd integer $n/2^k$, where $2^k \parallel n$. Let p, q, r denote typical odd prime divisors of a, b, c respectively. As Eq. (1) is solvable, the Legendre

* Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7233.

0022-314X/83/010100–06\$03.00/0

symbols $(-bc/p)$, $(-ca/q)$, $(-ab/r)$, are all $+1$ and thus, as $p \equiv 1 \pmod 4$, the Dirichlet symbol

$$\left(\frac{-b^3c}{a_1}\right)_4 = \prod_{p|a} \left(\frac{-b^3c}{p}\right)_4, \tag{2}$$

and, similarly, the symbols $(-c^3a/b_1)_4$ and $(-a^3b/|c_1|)_4$ are well defined and take the values ± 1.

It is our purpose to evaluate the quantity

$$E(a,b,c) = \left(\frac{-b^3c}{a_1}\right)_4 \left(\frac{-c^3a}{b_1}\right)_4 \left(\frac{-a^3b}{|c_1|}\right)_4 \tag{3}$$

in terms of a nontrivial solution (x,y,z) of Legendre's equation (1). We note that

$$E(a,b,c)\,E(b,a,c) = +1$$

so that

$$E(a,b,c) = E(b,a,c). \tag{4}$$

We prove

THEOREM. *Let a, b, c be three nonzero integers having no prime factors $\equiv 3 \pmod 4$, not all the same sign, abc squarefree, and for which $ax^2+by^2+cz^2=0$ is solvable in nonzero integers x,y,z. Without loss of generality we may take $x>0$, $y>0$, $z>0$, $(x,y,z)=1$, and suppose that $a>0$, $b>0$, $c<0$. Then*

$$\begin{aligned} E(a,b,c) &= (-1)^{xy/2}(-1/z), && \text{if } 2\nmid abc,\\ &= (2/y)(-2/z), && \text{if } 2\mid a,\quad 2\nmid bc,\\ &= (2/x)(2/y)(-1/z_1), && \text{if } 2\nmid ab,\quad 2\mid c. \end{aligned} \tag{5}$$

(The case $2\mid b$, $2\nmid ac$, is obtained by interchanging a,b and x,y in the second line of (5).)

Proof. We just treat the case $2\nmid abc$, as the proofs in the other two cases are similar. As abc is squarefree and $(x,y,z)=1$, we have

$$(x,y) = (y,z) = (z,x) = 1,$$

$$(a,b) = (b,c) = (c,a) = 1,$$

$$(a,yz) = (b,zx) = (c,xy) = 1.$$

Since $a \equiv b - c \equiv 1 \pmod 4$, we deduce from (1) that z is odd and one of x and y is even and the other odd. We begin by supposing that x is even and y is odd. We have from (1)

$$\left(\frac{-b^3c}{p}\right)_4 = \left(\frac{-b^3cz^4}{p}\right)_4 = \left(\frac{b^4y^2z^2}{p}\right)_4 = \left(\frac{yz}{p}\right),$$

so that

$$(-b^3c/a)_4 = (yz/a). \tag{6}$$

Similarly, we obtain

$$\left(\frac{-c^3a}{b}\right)_4 = \left(\frac{zx}{b}\right), \qquad \left(\frac{-a^3b}{|c|}\right)_4 = \left(\frac{xy}{|c|}\right). \tag{7}$$

Putting (6) and (7) together, we get

$$E(a, b, c) = \left(\frac{yz}{a}\right)\left(\frac{zx}{b}\right)\left(\frac{xy}{|c|}\right). \tag{8}$$

As x is even, we have $x = 2^k x_1$, where $k \geqslant 1$ and x_1 is odd. By the law of quadratic reciprocity, we have

$$\begin{aligned} &\left(\frac{yz}{a}\right) = \left(\frac{a}{y}\right)\left(\frac{a}{z}\right), \qquad \left(\frac{zx}{b}\right) = \left(\frac{2}{b}\right)^k \left(\frac{b}{z}\right)\left(\frac{b}{x_1}\right), \\ &\left(\frac{xy}{|c|}\right) = \left(\frac{2}{|c|}\right)^k \left(\frac{|c|}{x_1}\right)\left(\frac{|c|}{y}\right). \end{aligned} \tag{9}$$

From (1) we have

$$ax^2 \equiv -by^2 \pmod z, \qquad by^2 \equiv -cz^2 \pmod{x_1}, \qquad cz^2 \equiv -ax^2 \pmod y,$$

so that

$$\left(\frac{a}{z}\right) = \left(\frac{-b}{z}\right), \qquad \left(\frac{b}{x_1}\right) = \left(\frac{|c|}{x_1}\right), \qquad \left(\frac{|c|}{y}\right) = \left(\frac{a}{y}\right). \tag{10}$$

Putting (8)–(10) together, we obtain

$$E(a, b, c) = \left(\frac{2}{b\,|c|}\right)^k \left(\frac{-1}{z}\right). \tag{11}$$

Finally, from (1), we have

$$a2^{2k} + b + c \equiv 0 \qquad \pmod 8,$$

so that

$$b\,|c| = -bc \equiv ac2^{2k} + 1 \equiv 1 \pmod 8, \quad \text{if} \quad k \geqslant 2,$$
$$\equiv 5 \pmod 8, \quad \text{if} \quad k = 1,$$

giving

$$(2/b\,|c|)^k = 1, \quad \text{if} \quad k \geqslant 2,$$
$$= -1, \quad \text{if} \quad k = 1,$$

that is

$$(2/b\,|c|)^k = (-1)^{x/2} = (-1)^{xy/2}. \tag{12}$$

Equations (11) and (12) yield (5) in this case.

If x is odd and y is even, by interchanging a and b the above derivation applies and we have

$$E(b, a, c) = (-1)^{xy/2}(-1/z).$$

The result now follows from (4).

If p and q are distinct primes congruent to 1 (mod 4) satisfying $(p/q) = +1$, Scholz [5] (see also [2]) has shown that

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_p}{q}\right),$$

where ε_p is the fundamental unit (>1) of the real quadratic field $Q(\sqrt{p})$ and, in the Legendre symbol (ε_p/q), $\sqrt{p}$ is interpreted as an integer (mod q). Using this law in conjunction with our theorem, we obtain alternative expressions for (ε_p/q). We prove

COROLLARY. *Let p and q be distinct primes such that one of the following holds:*

$$p \equiv q \equiv 1 \pmod 4, \quad (p/q) = +1, \tag{a}$$
$$p \equiv 1 \pmod 8, \quad q \equiv 1 \pmod 4, \quad (p/q) = +1, \tag{b}$$
$$p \equiv q \equiv 1 \pmod 8, \quad (p/q) = +1; \tag{c}$$

so that, by Legendre's theorem, there are positive integers x, y, z such that

$$px^2 + qy^2 - z^2 = 0, \quad \textit{in case } (a)$$
$$px^2 + 2qy^2 - z^2 = 0, \quad \textit{in case } (b),$$
$$px^2 + qy^2 - 2z^2 = 0, \quad \textit{in case } (c).$$

Then

$$\left(\frac{\varepsilon_p}{q}\right) = (-1)^{xy/2}\left(\frac{-1}{z}\right), \qquad \textit{in case (a)},$$
$$= \left(\frac{2}{p}\right)_4\left(\frac{2}{x}\right)\left(\frac{-2}{z}\right), \qquad \textit{in case (b)},$$
$$= \left(\frac{2}{p}\right)_4\left(\frac{2}{q}\right)_4\left(\frac{2}{x}\right)\left(\frac{2}{y}\right)\left(\frac{-1}{z_1}\right), \qquad \textit{in case (c)}.$$

Proof. We have (using (3))

$$E(p, q, -1) = \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4, \qquad \text{in case (a)},$$
$$E(p, 2q, -1) = \left(\frac{2}{p}\right)_4\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4, \qquad \text{in case (b)},$$
$$E(p, q, -2) = \left(\frac{2}{p}\right)_4\left(\frac{2}{q}\right)_4\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4, \qquad \text{in case (c)}.$$

The corollary now follows by appealing to Scholz's law and the theorem.

We remark that this note was suggested by certain results in the literature (for example [1, 2]). These results may be deduced from the above theorem or its corollary. We give just one example, namely [2, Theorem 4]. The assumption in [2] that $p^v = e^2 - 4qf^2$ means that $px^2 + qy^2 - z^2 = 0$ is solvable with $x = p^{(v-1)/2}$, $y = 2f$, $z = e$. (In [2] it is assumed that $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$ are primes such that $(p/q) = +1$, v is odd, and e, f are positive coprime integers.) By the corollary (case (a)) we have

$$(\varepsilon_p/q) = (-1)^f(-1/e),$$

which becomes Lehmer's result

$$(\varepsilon_p/q) = (-1/e)$$

under the further assumption $p \equiv 1 \pmod 8$.

We close with a simple numerical example.

Example. By Legendre's criterion the equation

$$5x^2 + 29y^2 - 109z^2 = 0 \tag{13}$$

is solvable in integers x, y, z not all zero. Let (x, y, z) be a primitive solution of (13) with $x > 0$, $y > 0$, $z > 0$. Clearly x, y, z satisfy

$$x \equiv 0 \pmod 4, \qquad y \equiv z \equiv 1 \pmod 2,$$

or

$$x \equiv z \equiv 1 \pmod 2, \qquad y \equiv 0 \pmod 4,$$

so that, in both cases, we have $xy \equiv 0 \pmod 4$. Since $E(5, 29, -109) = +1$, by the Theorem each primitive solution (x, y, z) of (13) with $x > 0$, $y > 0$, $z > 0$ must have $z \equiv 1 \pmod 4$. The solution $x = 28$, $y = 661$, $z = 341$ shows that z may have prime factors $\equiv 3 \pmod 4$.

References

1. P. Kaplan, Sur le 2-groupe des classes d'idéaux des corps quadratiques, *J. Reine Angew. Math.* **283/284** (1976), 313–363.
2. E. Lehmer, On some special quartic reciprocity laws, *Acta Arith.* **21** (1972), 367–377.
3. L. J. Mordell, "Diophantine Equations," Academic Press, New York, 1969.
4. T. Nagell, "Introduction to Number Theory," Almqvist & Wiksells, Stockholm, 1951.
5. A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, *Math. Z.* **39** (1934), 95–111.