On the Size of a Solution of Legendre's Equation

Kenneth S. Williams [1]

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada

Abstract. Using the ideas of Mordell [6], it is shown in a completely elementary way that if a, b, c are nonzero integers for which Legendre's equation $ax^2 + by^2 + cz^2 = 0$ is solvable in integers x, y, z not all zero, then there is a solution satisfying

$$0 < |a|x^2 + |b|y^2 + |c|z^2 \leq 2\frac{|abc|}{(a,b,c)^2}.$$

The estimate is best possible.

Let a, b, c be nonzero integers. A number of authors have considered the problem of estimating the size of a solution of Legendre's equation

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

when (1) is known to be solvable in integers x, y, z not all zero. Most of these authors restrict a, b, c to satisfy

$$\begin{cases} a, b, c \text{ not all of the same sign,} \\ a, b, c \text{ are all squarefree,} \\ (a,b) = (b,c) = (c,a) = 1, \end{cases} \tag{2}$$

in which case the equation (1) is said to be in normal form. When (1) is in normal form, the condition

$$-bc, -ca, -ab \text{ are quadratic residues of } a, b, c \text{ respectively} \tag{3}$$

is both necessary and sufficient for (1) to be solvable in integers x, y, z not all zero. In 1950 Holzer [3] proved, under the assumption that both (2) and (3) hold, that there is a solution of (1) satisfying

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ca|}, \quad |z| \leq \sqrt{|ab|}.$$

In the course of his proof Holzer appealed to a deep theorem of Hecke (the generalized prime number theorem). In 1951 Mordell [5] gave an elementary proof of an estimate weaker than that of Holzer also under the assumption of (2) and (3).

[1] Research supported by Natural Sciences and Engineering Research Council of Canada grant No. A7233.

This estimate was also found by Skolem in 1952 [7]. In 1958 Birch and Davenport proved a theorem [**1: eqn.** (4)] which gives the estimate

$$0 < |a|x^2 + |b|y^2 + |c|z^2 \leq 8\,|abc|$$

for the size of a solution of (1) under only the assumption that (1) is solvable. In 1959 Kneser [**4**], using deep methods, proved under the assumption of (2) and (3) that (1) has a non-trivial solution with

$$|z| \leq k(n)\sqrt{|ab|},$$

where n is a divisor of the least common multiple of 2 and abc and $k(n) < 1$ in certain cases. In Cassels' book [**2**] on the geometry of numbers, first published in 1959, it is proved [**2: p.102**] that under the assumption of (2) and (3) the equation (1) has a solution satisfying

$$0 < |a|x^2 + |b|y^2 + |c|z^2 < 4\,|abc|.$$

It is noted that this estimate can be improved to

$$0 < |a|x^2 + |b|y^2 + |c|z^2 < 2^{5/3}|abc|.$$

In 1969 Mordell [**6**] gave an elementary proof of Holzer's estimate under the assumption of (2) and (3). Unfortunately Mordell's argument is not quite complete as he does not prove that the integer z which he constructs is nonzero. It therefore seems worthwhile to provide the necessary details to complete Mordell's proof while at the same time removing the unnecessary restrictions that a, b, c be squarefree and coprime in pairs, so as to obtain the most general result of this type which is best possible. We prove in a completely elementary way the following theorem.

Theorem. *Let a, b, c be nonzero integers such that (1) is solvable in integers x, y, z not all zero. Then there is a solution of (1) in integers x, y, z not all zero satisfying*

$$|x| \leq \frac{\sqrt{|bc|}}{(a,b,c)}, \quad |y| \leq \frac{\sqrt{|ca|}}{(a,b,c)}, \quad |z| \leq \frac{\sqrt{|ab|}}{(a,b,c)}.$$

Using equation (1), it is easy to verify that the solution satisfies

$$0 < |a|x^2 + |b|y^2 + |c|z^2 \leq \frac{2\,|abc|}{(a,b,c)^2}.$$

The equation $x^2 + y^2 - z^2 = 0$ with solution $(x, y, z) = (1, 0, 1)$ shows that both these estimates are best possible.

Proof of theorem: It suffices to prove the theorem when

$$(4) \qquad \begin{cases} a > 0\,,\ b > 0\,,\ c < 0\,, \\ (a,b,c) = 1\,. \end{cases}$$

Let r^2, s^2, t^2 denote the largest squares dividing a, b, c respectively, where $r > 0\,,\ s > 0\,,\ t > 0$, and set

$$(5) \qquad a = Ar^2\,,\ b = Bs^2\,,\ c = Ct^2\,,$$

so that A, B, C are squarefree integers such that

$$(6) \qquad A > 0\,,\ B > 0\,,\ C < 0\,,\ (Ar, Bs, Ct) = 1\,.$$

As $((A,B),(A,C)) = ((B,C),(B,A)) = ((C,A),(C,B)) = 1$, we may define integers $\alpha(>0), \beta(>0), \gamma(<0)$ by

$$(7) \qquad \alpha = \frac{A}{(A,B)(A,C)}\,, \quad \beta = \frac{B}{(B,C)(B,A)}\,, \quad \gamma = \frac{C}{(C,A)(C,B)}\,.$$

Clearly α, β, γ are squarefree and we have

$$(8) \qquad (\alpha,\beta) = (\beta,\gamma) = (\gamma,\alpha) = 1$$

and

$$(9) \qquad \begin{cases} (\alpha, A, B) = (\alpha, B, C) = (\alpha, C, A) = 1\,, \\ (\beta, A, B) = (\beta, B, C) = (\beta, C, A) = 1\,, \\ (\gamma, A, B) = (\gamma, B, C) = (\gamma, C, A) = 1\,. \end{cases}$$

Next, we define integers $k(>0), l(>0), m(<0)$ by

$$(10) \qquad k = \alpha(B,C)\,, \quad l = \beta(C,A)\,, \quad m = \gamma(A,B)\,.$$

It is easy to check that

$$(11) \qquad (k,l) = (l,m) = (m,k) = 1$$

and

$$(12) \qquad k, l, m \text{ squarefree.}$$

Now let x_0, y_0, z_0 be a solution of (1) in integers not all zero, so that

$$(13) \qquad ax_0^2 + by_0^2 + cz_0^2 = 0\,.$$

In view of (4) and (13) we must have $z_0 \neq 0$. From (5), (7) and (13) we deduce

$$(14)\quad \alpha(A,B)(A,C)r^2x_0^2 + \beta(B,C)(B,A)s^2y_0^2 + \gamma(C,A)(C,B)t^2z_0^2 = 0.$$

Thus we have

$$(15)\qquad (A,B)\,|\,\gamma(C,A)(C,B)t^2z_0^2.$$

As $(A,B,C) = (A,B,t) = (A,B,\gamma) = 1$ and (A,B) is squarefree, we deduce from (15) that $(A,B)|z_0$. Similarly we can show that $(B,C)|x_0$, $(C,A)|y_0$. Thus there are integers $X,Y,Z(\neq 0)$ such that

$$(16)\qquad x_0 = (B,C)X, \quad y_0 = (C,A)Y, \quad z_0 = (A,B)Z.$$

Putting these expressions for x_0, y_0, z_0 into (14), and cancelling the factor (A,B) $(B,C)(C,A)$, we obtain

$$(17)\qquad kr^2X^2 + ls^2Y^2 + mt^2Z^2 = 0.$$

Now define integers $X_0, Y_0, Z_0(\neq 0)$ by

$$(18)\qquad X_0 = \frac{rX}{(rX,sY,tZ)}, \quad Y_0 = \frac{sY}{(rX,sY,tZ)}, \quad Z_0 = \frac{tZ}{(rX,sY,tZ)}.$$

From (17) and (18) we see that

$$(19)\qquad kX_0^2 + lY_0^2 + mZ_0^2 = 0$$

and

$$(20)\qquad (X_0,Y_0,Z_0) = 1.$$

Moreover, appealing to (11), (12), (19) and (20), we deduce

$$(21)\quad \begin{cases} (X_0,Y_0) = (Y_0,Z_0) = (Z_0,X_0) = 1, \\ (X_0,m) = (Y_0,m) = (X_0,l) = (Z_0,l) = (Y_0,k) = (Z_0,k) = 1. \end{cases}$$

Next we show that if $|Z_0| > \sqrt{kl}$ then we can construct from the solution (X_0,Y_0,Z_0) of (19) another solution (X_1,Y_1,Z_1) of (19) with $0 < |Z_1| < |Z_0|$. Set

$$(22)\qquad d = \begin{cases} \frac{m}{2}, & \text{if } m \equiv 0 \pmod 2, \\ m, & \text{if } m \equiv 1 \pmod 2, \end{cases}$$

and let u, v be integers satisfying

$$Y_0 u - X_0 v = d. \tag{23}$$

This is possible in view of (21). From (21) and (22) we deduce that

$$(Y_0, d) = 1. \tag{24}$$

Next we choose an integer w such that

$$\begin{cases} \left|w + \frac{kX_0u + lY_0v}{mZ_0}\right| \le \frac{1}{2}, & \text{if } m \equiv 0 \pmod 2, \\ \left|w + \frac{kX_0u + lY_0v}{mZ_0}\right| \le 1, \ w \equiv ku + lv \pmod 2, & \text{if } m \equiv 1 \pmod 2. \end{cases} \tag{25}$$

From (22), (23) and (25) we see that

$$(kX_0u + lY_0v + mZ_0w)^2 + kl(Y_0u - X_0v)^2 < \theta dmZ_0^2, \tag{26}$$

where

$$\theta = \begin{cases} 1, & \text{if } m \equiv 0 \pmod 2, \\ 2, & \text{if } m \equiv 1 \pmod 2. \end{cases} \tag{27}$$

Next we observe that by (19) and (23) we have

$$\begin{cases} (kX_0u + lY_0v)Y_0 \equiv (kX_0^2 + lY_0^2)v \equiv -mZ_0^2 v \equiv 0 \pmod d, \\ (ku^2 + lv^2)Y_0^2 \equiv (kX_0^2 + lY_0^2)v^2 \equiv -mZ_0^2 v^2 \equiv 0 \pmod d, \end{cases}$$

and so, by (24), we have

$$kX_0u + lY_0v \equiv ku^2 + lv^2 \equiv 0 \pmod d. \tag{28}$$

From (27) and (28) we see that we can define integers X_1, Y_1, Z_1 by

$$\begin{cases} \theta dX_1 = X_0(ku^2 + lv^2 + mw^2) - 2u(kX_0u + lY_0v + mZ_0w), \\ \theta dY_1 = Y_0(ku^2 + lv^2 + mw^2) - 2v(kX_0u + lY_0v + mZ_0w), \\ \theta dZ_1 = Z_0(ku^2 + lv^2 + mw^2) - 2w(kX_0u + lY_0v + mZ_0w). \end{cases} \tag{29}$$

It is easily verified from (19) and (29) that

$$kX_1^2 + lY_1^2 + mZ_1^2 = 0. \tag{30}$$

Moreover we have (using (19), (26) and (29))

$$\begin{aligned} \theta dm|Z_0||Z_1| &= m|Z_0||-\theta dZ_1| \\ &= m|Z_0||2w(kX_0u + lY_0v + mZ_0w) - Z_0(ku^2 + lv^2 + mw^2)| \\ &= |(kX_0u + lY_0v + mZ_0w)^2 + kl(Y_0u - X_0v)^2| \\ &< \theta dmZ_0^2, \end{aligned}$$

so that

$$(31)\qquad |Z_1| < |Z_0|.$$

Next we show that $Z_1 \neq 0$. Suppose on the contrary that $Z_1 = 0$. Then, from (30) (as $k > 0$, $l > 0$, $m < 0$), we have $X_1 = Y_1 = 0$ and so (29) gives

$$(32)\qquad X_0(ku^2 + lv^2 + mw^2) = 2u(kX_0u + lY_0v + mZ_0w),$$

$$(33)\qquad Y_0(ku^2 + lv^2 + mw^2) = 2v(kX_0u + lY_0v + mZ_0w),$$

$$(34)\qquad Z_0(ku^2 + lv^2 + mw^2) = 2w(kX_0u + lY_0v + mZ_0w),$$

Multiplying (32), (33), (34) by kX_0, lY_0, mZ_0 respectively and adding the resulting equations, we obtain

$$(35)\quad (kX_0^2 + lY_0^2 + mZ_0^2)(ku^2 + lv^2 + mw^2) = 2(kX_0u + lY_0v + mZ_0w)^2.$$

Hence, by (19), we deduce

$$(36)\qquad kX_0u + lY_0v + mZ_0w = 0.$$

Then, from (32) and (33), we have

$$(37)\qquad (ku^2 + lv^2 + mw^2)X_0 = (ku^2 + lv^2 + mw^2)Y_0 = 0.$$

As $(X_0, Y_0) = 1$ we must have

$$(38)\qquad ku^2 + lv^2 + mw^2 = 0.$$

Then, we obtain by (19), (36) and (38)

$$\begin{aligned} kl(Y_0u - X_0v)^2 &= (kX_0^2 + lY_0^2)(ku^2 + lv^2) - (kX_0u + lY_0v)^2 \\ &= (-mZ_0^2)(-mw^2) - (-mZ_0w)^2 \\ &= 0, \end{aligned}$$

which contradicts $Y_0u - X_0v = d \neq 0$.

We have shown that from the solution (X_0, Y_0, Z_0) of $kX_0^2 + lY_0^2 + mZ_0^2 = 0$ with $|Z_0| > \sqrt{kl}$ we can construct another solution (X_1, Y_1, Z_1) with $0 < |Z_1| < |Z_0|$. If $|Z_1| > \sqrt{kl}$ we can repeat the process on (X_1, Y_1, Z_1) to obtain another solution (X_2, Y_2, Z_2) with $0 < |Z_2| < |Z_1|$. Continuing this process, after a finite number of steps, we obtain a solution (X_n, Y_n, Z_n) $(n \geq 0)$ of $kX_n^2 + lY_n^2 + mZ_n^2 = 0$ with

$$(39)\qquad 0 < |Z_n| \leq \sqrt{kl}.$$

We define integers x, y, z, with $z \neq 0$, by

$$x = st(B,C)X_n, \quad y = rt(C,A)Y_n, \quad z = rs(A,B)Z_n. \tag{40}$$

Then we have, appealing to (5), (7), (10), (39), (40),

$$\begin{aligned}
ax^2 + by^2 + cz^2 &= Ar^2s^2t^2(B,C)^2X_n^2 + Br^2s^2t^2(C,A)^2Y_n^2 \\
&\quad + Cr^2s^2t^2(A,B)^2Z_n^2 \\
&= r^2s^2t^2(A,B)(B,C)(C,A)(\alpha(B,C)X_n^2 + \beta(C,A)Y_n^2 \\
&\quad + \gamma(A,C)Z_n^2) \\
&= r^2s^2t^2(A,B)(B,C)(C,A)(kX_n^2 + lY_n^2 + mZ_n^2) \\
&= 0
\end{aligned}$$

and

$$\begin{aligned}
0 < |z| &= rs(A,B)|Z_n| \\
&\leq rs(A,B)\sqrt{kl} \\
&= rs(A,B)\sqrt{(B,C)(C,A)\alpha\beta} \\
&= \sqrt{ab}.
\end{aligned}$$

This proves that (x, y, z) is a nontrivial solution of (1) satisfying the inequalities stated in the theorem. This completes the proof of the theorem.

REFERENCES

1. B.J. Birch and H. Davenport, *Quadratic equations in several variables*, Proc. Cambridge Philos. Soc. **54** (1958), 135–138.
2. J.W. Cassels, "An Introduction to the Geometry of Numbers," Springer-Verlag, New York, 1971. (Second Printing).
3. L. Holzer, *Minimal solutions of diophantine equations*, Canad. J. Math. **2** (1950), 238–244.
4. M. Kneser, *Kleine Lösungen der diophantischen Gleichung* $ax^2 + by^2 = cz^2$, Math. Sem. Univ. Hamburg **23** (1959), 163–173.
5. L.J. Mordell, *On the equation* $ax^2 + by^2 - cz^2 = 0$, Montash. Math. **55** (1951), 323-327.
6. L.J. Mordell, *On the magnitude of the integer solutions of the equation* $ax^2 + by^2 + cz^2 = 0$, J. Number Theory **1** (1969), 1–3.
7. T. Skolem, *On the diophantine equation* $ax^2 + by^2 + cz^2 = 0$, Univ. Roma. 1st. Naz. Alta Mat. Rend. Mat. e Appl. **(5) 11** (1952), 88–100.