JOURNAL OF NUMBER THEORY 1, 1–3 (1969)

On the Magnitude of the Integer Solutions of the Equation $ax^2+by^2+cz^2=0$

L. J. MORDELL

Cambridge University, Cambridge, England

Communicated May 3, 1968

A simple elementary proof is given of Holzer's theorem, namely, that if the equation $ax^2 + by^2 + cz^2 = 0$, taken in the normal form is solvable in integers, then a solution exists with

$$|x| \le (|bc|)^{\frac{1}{2}}, \quad |y| \le (|ca|)^{\frac{1}{2}}, \quad |z| \le (|ab|)^{\frac{1}{2}}.$$

Legendre has discussed in his classic work the question of a nontrivial integer solution of the equation

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

The equation can be reduced to a normal form in which a, b, c do not all have the same sign, are all square free, and relatively prime in pairs. He proved that the solvability of the congruences

$$bX^2+c \equiv 0 \pmod a, \quad cY^2+a \equiv 0 \pmod b, \quad aZ^2+b \equiv 0 \pmod c$$

is a necessary and sufficient condition for the existence of integer solutions of (1). Many other proofs have been given.

In recent years, attention has been paid to the problem of finding an estimate for the magnitude of a solution, the equation being supposed solvable. We may suppose that $a > 0$, $b > 0$, $c < 0$. In 1950, Holzer [*1*] proved that a solution exists for which

$$|x| \le (b|c|)^{\frac{1}{2}}, \quad |y| \le (|c|a)^{\frac{1}{2}}, \quad |z| \le (ab)^{\frac{1}{2}}, \tag{2}$$

and obviously the first two inequalities follow from the third. Clearly the inequality signs may be removed unless two of the a, b, c are equal to one. His proof depends upon a deep result on prime numbers in arithmetic progressions in a quadratic field. In 1951, I gave an elementary proof [*2*] of a cruder estimate. This was also found later by Skolem [*3*]. Then Kneser [*4*] in 1959 established a result of the form

$$|z| \le k(ab)^{\frac{1}{2}}, \tag{3}$$

where in many cases $k < 1$. I notice that the estimate (2) can be proved in a most elementary way from first principles. I show that if a solution (x_0, y_0, z_0) exists with $(x_0, y_0) = 1$ and $|z_0| > (ab)^{\frac{1}{2}}$, we can find another solution (x, y, z) with $|z| < |z_0|$. Then (2) follows.

Put

$$x = x_0+tX, \quad y = y_0+tY, \quad z = z_0+tZ,$$

where X, Y, Z, are integers to be determined later. Then

$$(aX^2+bY^2+cZ^2)t+2(ax_0X+by_0Y+cz_0Z) = 0.$$

Hence, on neglecting a denominator, we have an integer solution, say (x, y, z), given by

$$\left.\begin{aligned} \delta z &= z_0(aX^2+bY^2+cZ^2)-2Z(ax_0X+by_0Y+cz_0Z), \\ \delta x &= x_0(aX^2+bY^2+cZ^2)-2X(ax_0X+by_0Y+cz_0Z), \\ \delta y &= y_0(aX^2+bY^2+cZ^2)-2Y(ax_0X+by_0Y+cz_0Z), \end{aligned}\right\} \tag{4}$$

where δ is a common divisor of the three expressions on the right.

We show that if

$$\delta/c, \qquad \delta/(Xy_0-Yx_0),$$

then x, y, z are integers.

From

$$ax_0^2+by_0^2+cz_0^2 = 0,$$

it easily follows that $(\delta, abx_0y_0) = 1$. From (4) it suffices to show that

$$P = ax_0X+by_0Y \equiv 0 \pmod{\delta}, \quad Q = aX^2+bY^2 \equiv 0 \pmod{\delta}.$$

Then $\quad P \equiv Y(ax_0^2+by_0^2)/y_0 \equiv 0 \pmod{\delta}, \quad$ since $X \equiv x_0Y/y_0 \pmod{\delta}$.

Also $Q \equiv (ax_0^2+by_0^2)Y^2/y_0^2 \equiv 0 \pmod{\delta}$. From (4) we find

$$\frac{-\delta z}{cz_0} = \left(Z+\frac{ax_0X+by_0Y}{cz_0}\right)^2+\frac{ab}{c^2z_0^2}(y_0X-x_0Y)^2. \tag{5}$$

We take X, Y as any solution of $y_0X-x_0Y = \delta$. We may suppose that $z_0^2 > ab$. First let c be even. We take $\delta = \frac{1}{2}c$, and Z so that

$$\left|Z+\frac{ax_0X+by_0Y}{cz_0}\right| \le \frac{1}{2}.$$

Then from (5),

$$\frac{1}{2}\left|\frac{z}{z_0}\right| < \frac{1}{4}+\frac{1}{4} \quad \text{and} \quad |z| < |z_0|. \tag{6}$$

Hence on continuing the process we have a solution with $z^2 \le ab$. Secondly, let c be odd. We now impose the condition

$$aX+bY+cZ \equiv 0 \pmod{2}.$$

This defines the parity of Z. Since δ is odd, the three expressions on the right-hand side of (4) are divisible by 2δ, and so we now have (5) with δ replaced by 2δ. We take $\delta = c$ and Z with assigned parity so that

$$\left(Z + \frac{ax_0 X + by_0 Y}{cz_0}\right) \leq 1.$$

Then instead of (5), we have

$$2\left|\frac{z}{z_0}\right| < 1+1 \quad \text{and} \quad |z| < |z_0|.$$

This completes the proof.

References

1. Holzer, L. Minimal solutions of diophantine equations. *Can. J. Math.* **2** (1950), 238–244.
2. Mordell, L. J. On the equation $ax^2 + by^2 - cz^2 = 0$. *Monatshefte für Math.* **53** (1951), 323–327.
3. Skolem, T. On the Diophantine equation $ax^2 + by^2 - cz^2 = 0$. *Rendiconti die matematica delle sue applicazione* **5**, 11 (1952), 88–102.
4. Kneser, M. Kleine Lösungen der diophantischen Gleichung $ax^2 + by^2 = cz^2$. *Abhand. Math. Sem. Hamburg* **23** (1959), 163–173.