

# A LOOK AT MORDELL'S PROOF: CAN WE FIND A SMALLER Z?

LAURA M. NUNLEY

ABSTRACT. L. J. Mordell published a proof of Holzer's theorem in 1969 [1]. This theorem states that if the equation  $ax^2 + by^2 + cz^2 = 0$  taken in the normal form has an integral solution, then a solution exists in which the following inequalities hold:

$$|x| \leq (|bc|)^{1/2} \quad |y| \leq (|ca|)^{1/2} \quad |z| \leq (|ab|)^{1/2}$$

It is widely accepted that there are gaps in Mordell's proof. However, Cochrane and Mitchell claim that Williams filled in these gaps in 1988 [2], while Cochrane and Mitchell gave a new elementary proof of Holzer's theorem ten years later [3]. Here, we shall exposit Mordell's proof and attempt to fill in the gaps which he mistakenly overlooked.

Mordell begins his paper by discussing Legendre's exploration in his classic work of nontrivial solutions to the equation

$$(1) \quad ax^2 + by^2 + cz^2 = 0,$$

in which he says that the equation can be reduced to a normal form in which the following conditions hold:

- i.  $a, b, c$  do not all have the same sign. If they did, then the only solution would be the trivial one  $(0, 0, 0)$ .
- ii.  $a, b, c$  are all squarefree. Suppose not. Then we can get another solution by letting  $a = a_1^2 a_2$ .

$$\begin{aligned} ax^2 + by^2 + cz^2 &= 0 \\ \Rightarrow a_2(a_1x)^2 + by^2 + cz^2 &= 0. \end{aligned}$$

- iii.  $a, b, c$  are relatively prime in pairs. If they were not, then suppose  $d|a$  and  $d|b$ ,  $d > 1$ . Then

$$\begin{aligned} ax^2 + by^2 + cz^2 &= 0 \\ \Rightarrow ax^2 + by^2 &= -cz^2 \\ \Rightarrow \frac{a}{d}x^2 + \frac{b}{d}y^2 &= -\frac{c}{d}z^2 \end{aligned}$$

If  $d|c$ , then divide out and reduce it to an equation with no common divisors. If  $d \nmid c$ , then the only solution is the trivial one  $(0, 0, 0)$ .

Legendre 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).

Mordell begins by saying we can suppose  $a > 0$ ,  $b > 0$ ,  $c < 0$ . Then the above congruences are equivalent to the following inequalities:

$$(2) \quad |x| \leq (b|c|)^{1/2} \quad |y| \leq (|c|a)^{1/2} \quad |z| \leq (ab)^{1/2}.$$

We see that the first two inequalities follow from the third. Since  $c < 0$ ,

$$\begin{aligned} |z| \leq (ab)^{1/2} &\Rightarrow ax^2 + by^2 + c((ab)^{1/2}) < 0 \\ (3) \quad &\Leftrightarrow ax^2 + by^2 + abc < 0 \end{aligned}$$

From this, we can get two inequalities, giving us the result that we desire. First, since  $\frac{-by^2}{a} < 0$  and  $-\frac{abc}{a} > 0$ ,

$$(3) \Rightarrow x^2 < \frac{-by^2 - abc}{a} = \frac{-by^2}{a} - \frac{abc}{a} < b(-c) \Rightarrow |x| < (b|c|)^{1/2}.$$

Secondly, since  $\frac{-ax^2}{b} < 0$  and  $-\frac{abc}{b} > 0$ ,

$$(3) \Rightarrow y^2 < \frac{-ax^2 - abc}{b} = \frac{-ax^2}{b} - \frac{abc}{b} < a(-c) \Rightarrow |y| < (a|c|)^{1/2}.$$

We can also see that we have strict inequality unless two of the  $a, b, c$  are equal to one. To see this, let's suppose  $|x| = (b|c|)^{1/2}$ . Then  $b|c|$  is a perfect square only if  $b = |c| = 1$  since  $b, c$  are squarefree.

Now, what Mordell shows in his paper is that if a solution  $(x_0, y_0, z_0)$  exists with  $\gcd(x_0, y_0) = 1$  and  $|z_0| > (ab)^{1/2}$ , we can find another solution  $(x, y, z)$  with  $|z| < |z_0|$ . Then (2) follows since the other inequalities follow from this one.

Let's prove it!

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 and  $t \neq 0, t \in \mathbb{Q}$ . Then, by substitution, we get

$$\begin{aligned} 0 &= a(x_0 + tX)^2 + b(y_0 + tY)^2 + c(z_0 + tZ)^2 \\ \Rightarrow 0 &= ax_0^2 + 2ax_0tX + at^2X^2 + by_0^2 + 2by_0tY + bt^2Y^2 + cz_0^2 + 2cz_0tZ + ct^2Z^2 \end{aligned}$$

Regrouping and by our hypothesis that  $(x_0, y_0, z_0)$  is a solution, then we get

$$\begin{aligned} \Rightarrow 0 &= (aX^2 + bY^2 + cZ^2)t^2 + 2t(ax_0X + by_0Y + cz_0Z) + ax_0^2 + by_0^2 + cz_0^2 \\ \Rightarrow 0 &= (aX^2 + bY^2 + cZ^2)t + 2(ax_0X + by_0Y + cz_0Z) \end{aligned}$$

since  $t \neq 0$ . If we solve for  $t$  here, we see that we get

$$t = \frac{-2(ax_0X + by_0Y + cz_0Z)}{aX^2 + bY^2 + cZ^2}$$

Plugging this into our formulas for  $x, y, z$ , we get the following equations, where  $\delta = aX^2 + bY^2 + cZ^2$ :

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

Next, Mordell shows that  $x, y, z$  are integers if

$$\delta|c \quad \text{and} \quad \delta|y_0X - x_0Y.$$

Suppose  $\delta|c$  and  $\delta|y_0X - x_0Y$ . It is claimed that  $\gcd(\delta, abx_0y_0) = 1$ . To show this, suppose that there is some prime  $p$  such that  $p|\delta$  and  $p|abx_0y_0$ . Since  $\delta|c$  and  $a, b, c$  are pairwise relatively prime,  $p|x_0y_0$ . Suppose  $p|x_0$ . Then by the equation  $ax_0^2 + by_0^2 + cz_0^2 = 0$ , we see that  $p|by_0^2$ . But  $p \nmid b$ , so  $p|y_0^2 \xrightarrow{\text{Euclid's Lemma}} p|y_0$ , which is a contradiction since we assumed that  $\gcd(x_0, y_0) = 1$ .

Next, we verify that from equation (4), it suffices to show that

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

Given these two congruences, taking (4) mod  $\delta$ , we get three true equivalences because  $\delta|c$ , making  $x, y, z$  integers, as desired.

$$\begin{array}{ll} \delta z \equiv z_0(Q + cZ^2) - 2Z(P + cz_0Z) & \delta x \equiv x_0(Q + cZ^2) - 2X(P + cz_0Z) \\ 0 \equiv z_0cZ^2 - 2cz_0Z^2 & 0 \equiv x_0cZ^2 - 2Xcz_0Z \\ 0 \equiv -cz_0Z^2 & 0 \equiv cZ(x_0 - 2z_0X) \\ 0 \equiv 0 & 0 \equiv 0 \end{array}$$

$$\begin{array}{ll} \delta y \equiv y_0(Q + cZ^2) - 2Y(P + cz_0Z) \\ 0 \equiv y_0cZ^2 - 2Ycz_0Z \\ 0 \equiv cZ(y_0Z - 2z_0Y) \\ 0 \equiv 0 \end{array}$$

Since  $\delta|y_0X - x_0Y$ , we have that  $y_0X - x_0Y \equiv 0 \pmod{\delta}$  and  $X \equiv \frac{x_0Y}{y_0} \pmod{\delta}$ . By substitution, we have  $P \equiv \frac{Y(ax_0^2 + by_0^2)}{y_0} \equiv 0 \pmod{\delta}$ , and  $Q \equiv \frac{(ax_0^2 + by_0^2)Y^2}{y_0^2} \equiv 0 \pmod{\delta}$ . Now, to get a useful equation, we manipulate equation (4) in a clever way:

$$\begin{aligned} \delta z &= z_0(aX^2 + bY^2 + cZ^2) - 2Z(ax_0X + by_0Y + cz_0Z) \\ \frac{\delta z}{cz_0} &= \frac{aX^2 + bY^2}{c} + Z^2 - 2Z\left(\frac{ax_0X + by_0Y}{cz_0}\right) - 2Z^2 \\ \frac{-\delta z}{cz_0} &= Z^2 + 2Z\left(\frac{ax_0X + by_0Y}{cz_0}\right) - \frac{aX^2 + bY^2}{c} \\ \frac{-\delta z}{cz_0} &= \left(Z + \frac{ax_0X + by_0Y}{cz_0}\right)^2 - \frac{aX^2 + bY^2}{c} - \left(\frac{ax_0X + by_0Y}{cz_0}\right)^2 \\ \frac{-\delta z}{cz_0} &= \left(Z + \frac{ax_0X + by_0Y}{cz_0}\right)^2 - \frac{1}{c^2z_0^2}(aX^2cz_0^2 + bY^2cz_0^2 + a^2x_0^2X^2 + b^2y_0^2Y^2 + 2abx_0y_0XY) \end{aligned}$$

Using the fact that  $cz_0^2 = -ax_0^2 - by_0^2$ , and letting  $L = \left(Z + \frac{ax_0X + by_0Y}{cz_0}\right)^2$  we see that

$$\begin{aligned} \frac{-\delta z}{cz_0} &= L - \frac{1}{c^2z_0^2}(aX^2(-ax_0^2 - by_0^2) + bY^2(-ax_0^2 - by_0^2) + a^2x_0^2X^2 + b^2y_0^2Y^2 + 2abx_0y_0XY) \\ \frac{-\delta z}{cz_0} &= L - \frac{1}{c^2z_0^2}(-a^2x_0^2X^2 - aby_0^2Y^2 - abx_0^2Y^2 - b^2y_0^2Y^2 + a^2x_0^2X^2 + b^2y_0^2Y^2 + 2abx_0y_0XY) \\ \frac{-\delta z}{cz_0} &= L + \frac{ab}{c^2z_0^2}(y_0^2X^2 - 2x_0y_0XY + x_0^2Y^2) \\ \frac{-\delta z}{cz_0} &= L + \frac{ab}{c^2z_0^2}(y_0X - x_0Y)^2 \end{aligned}$$

Thus, we have

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

Now, take  $X, Y$  as any solution of  $y_0X - x_0Y = \delta$ . From our assumption that  $|z_0| > (ab)^{1/2}$ , we can assume that  $z_0^2 > ab$ . Now there are two cases.

First, let  $c$  be even. In this case, take  $\delta = \frac{1}{2}c$ , and choose  $Z$  so that

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

Then from equation (5) we have

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

If  $|z| > ab$ , then repeat this process until you find a  $z$  that will give  $z^2 \leq ab$ .

In the second case, let  $c$  be odd. Now, we impose the condition that

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

Because  $a, b, X, Y$  are chosen already and  $c$  is odd, then  $Z \equiv aX + bY \pmod{2}$ . Also,  $\delta$  is odd because  $\delta|c$ , so all three of the right-hand sides of the equations in (4) are divisible by  $2\delta$ . This is easy to see because the terms with the 2s are divisible by 2, and they are divisible by  $\delta$  because  $P = ax_0X + by_0Y \equiv 0 \pmod{\delta}$ , and  $\delta|c$ . Similarly, the first terms are divisible by  $\delta$ . However, since we have imposed the condition that  $aX + bY + cZ \equiv 0 \pmod{2}$ , since  $\forall n \in \mathbb{Z}, n \equiv n^2 \pmod{2}$ , we have that  $aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{2}$  also. Thus, we can take (5) and replace  $\delta$  by  $2\delta$ . Take  $\delta = c$  and choose  $Z$  with the desired parity so that

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

Then instead of (6) we have

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

While Mordell claimed that this completes his proof, we have yet to show that this new solution is nontrivial (i.e. not  $(0, 0, 0)$ ). To do this, it suffices to check that  $z \neq 0$ . If  $z = 0$ , then from equation (5), since both of the terms of the right-hand side are positive ( $a, b > 0$ ), they both must equal 0 also. This is absurd since  $y_0X - x_0Y = \delta \neq 0$ . So  $z \neq 0$  or else we would get a contradiction. Therefore, we have found a nontrivial integral solution  $(x, y, z)$  to the equation  $ax^2 + by^2 + cz^2 = 0$ .  $\square$

#### REFERENCES

- [1] Mordell, L. J. On the Magnitude of the Integer Solutions of the Equation  $ax^2 + by^2 + cz^2 = 0$ . *Journal of Number Theory* 1 (1969), 1-3.
- [2] Williams, Kenneth S. On the size of a solution of Legendre's equation. *Utilitas Mathematica* 34 (1988), 65-72.
- [3] Cochrane, T. & Mitchell, P. Small Solutions of the Legendre Equation. *Journal of Number Theory* 70(1) (1998), 62-66.