

ABOUT MORDELL'S DESCENT METHOD

FĂNEL TĂȘCHINĂ*

Abstract. *In this paper, a complete version of the descent method proposed by Mordell for finding the smallest solutions to Legendre's equation is described. The proofs given are for the Legendre equation arbitrary and without making transformations to bring the equation to the normal form, as has been done so far. Holzer's theorem and Williams' corollary can be obtained from the proved theorem, taking into account the corresponding equivalent equations.*

Keywords: Legendre; Diophantine equations

If the equation

$$(1) \quad ax^2 + by^2 + cz^2 = 0, \quad a, b, c \in \mathbb{Z}$$

is brought in the normal form in which a, b, c without squares, not all of the same sign and relatively prime in pairs, the necessary and sufficient conditions to have nontrivial solutions are

$-bc, -ac, -ab$ must be quadratic remainders modulo a, b , respectively c and were established by Legendre.

In 1950, Holzer[1] demonstrated using methods that go beyond the elementary framework that when the equation (1) in normal form, has nontrivial solutions, then there is a solution with

$$(2) \quad |x| \leq \sqrt{|bc|}, |y| \leq \sqrt{|ac|}, |z| \leq \sqrt{|ab|}.$$

In 1969, Mordell[2] presented an elementary proof of the Holzer theorem, based on his descent method, which we will call "The Mordell's Descent".

Starting from a wrong assumption, this method was taken up in 1988, with some modifications, by Williams[3], but in his proof for a corollary of Holzer's theorem, errors can be identified.

In the descent method proposed by Mordell there are two inaccuracies (not later corrected by Williams). Thus, no evidence is provided to refute the case: $Z = 0$ (when the descent is not obtained), which can result from the choice relation for Z . The other hand, in the case of the solution constructed with $(x, y, z) \neq 1$, through the descent process it is not possible to directly obtain the solution sought, as stated by the cited authors.

The need to correct the deficiencies highlighted justifies the revision of the descent method proposed by Mordell.

We will detail a new variant of the descent method proposed by Mordell, by proving a theorem that regards Legendre's equation as arbitrary and without making use of the normal form of the equation.

Without restricting generality, in the following we will consider the equivalent form of Legendre's equation $ax^2 + by^2 = cz^2$, $a, b, c \in \mathbb{Z}_+$.

Theorem. If the equation

* inbox.fanel@gmail.com, Vaslui, România

$$(3) \quad ax^2 + by^2 = cz^2, \quad a, b, c \in Z_+,$$

has nontrivial integer solutions, then there is a solution such that

$$(4) \quad |x| \leq \sqrt{bc}, |y| \leq \sqrt{ac}, |z| \leq \sqrt{ac}.$$

Proof. If (X, Y, Z) is a nontrivial solution of the equation (3), then the equation

$$(5) \quad ax^2 + by^2 = c_1z^2, \quad a, b, c_1 \in Z_+, \quad c_1 - \text{squares-free}, \quad c = c_1c_2^2,$$

has the nontrivial solution (X, Y, c_2Z) , respectively the solution

$$(6) \quad x_0 = \frac{X}{(X, Y, c_2Z)}, \quad y_0 = \frac{Y}{(X, Y, c_2Z)}, \quad z_0 = \frac{c_2Z}{(X, Y, c_2Z)}, \quad (x_0, y_0, z_0) = 1.$$

If $z_0^2 \leq ab$ then from the equation

$$(7) \quad ax_0^2 + by_0^2 = c_1z_0^2, \quad (x_0, y_0, z_0) = 1,$$

it is easy to deduce that we will have: $x_0^2 \leq bc_1, x_0^2 \leq ac_1$ and the solution (c_2x_0, c_2y_0, z_0) satisfies the conditions of the theorem statement.

If $z_0^2 > ab$ then we will proceed to obtain a new solution with $|z| < |z_0|$.

From $(x_0, y_0, z_0) = 1$ and $c_1 - \text{squares-free}$, then x_0, y_0 are coprimes. Therefore, exists $u, v \in Z, c_1 = vx_0 - uy_0$. After substitution in equation (7), we will obtain the system of equations

$$(8) \quad vz_0^2 - ax_0 = ty_0, \quad uz_0^2 + by_0 = tx_0, \quad t \in Z$$

and after solving in relation to x_0 and y_0 , we will get

$$(9) \quad dx_0 = tu + vb, \quad dy_0 = tv - ua, \quad dz_0^2 = t^2 + ab, \quad d \in Z$$

respectively,

$$(10) \quad dc_1 = au^2 + bv^2, \quad tc_1 = uax_0 + bvy_0.$$

By introducing a parameter $w \in Z, w \equiv d \pmod{2}$, we will build a new solution (x, y, z) with $z \neq 0$. We make the notations

$$(11) \quad \begin{cases} (d - w^2)c_1 = au^2 + bv^2 - c_1w^2 = 2p_0c_1 \\ (t - wz_0)c_1 = ax_0u + by_0v - c_1z_0w = q_0c_1 \end{cases}, \quad p_0, q_0 \in Z.$$

By multiplying the equations in (11) by z_0^2 , respectively by $(-2wz_0)$ and adding member by member, we obtain

$$(12) \quad 2z_0(p_0z_0 - q_0w) = (t - wz_0)^2 + ab.$$

The right member being non-zero, then $p_0z_0 - q_0w \neq 0$. If we will denoted this expression with z , we have

$$(13) \quad 2z_0z = (t - wz_0)^2 + ab.$$

By choosing the integers x and y from

$$(14) \quad uy - vx = -p_0c_1, \quad -x_0y + y_0x = q_0c_1,$$

It is easily verified that, for $w \equiv d \pmod{2}$, the triplet (x, y, z) with $z \neq 0$, given by the relations

(15) $x = p_0x_0 - q_0u, y = p_0y_0 - q_0v, z = p_0z_0 - q_0w$, checks the equation (7).

From (13)

$$(16) \quad 2\frac{z}{z_0} = \left(\frac{t}{z_0} - w\right)^2 + \frac{ab}{z_0^2}, \quad w \equiv d \pmod{2}.$$

We will show that we can choose $w \equiv d \pmod{2}$ so that $\left|\frac{t}{z_0} - w\right| < 1$ after which it follows easily that for $z_0^2 > ab$ we will have: $|z| < |z_0|$.

From (9)

$$(17) \quad d = \left(\frac{t}{z_0}\right)^2 + \frac{ab}{z_0^2}.$$

We will have $d > 0$ and $\frac{t}{z_0} \notin Z \Rightarrow \frac{t}{z_0} = \left[\frac{t}{z_0}\right] + \left\{\frac{t}{z_0}\right\}$ respectively: $\left(\frac{t}{z_0} - w\right) \neq \pm 1$.

By solving the inequation $\left|\frac{t}{z_0} - w\right| < 1$, we will have $w \in \left\{\left[\frac{t}{z_0}\right], \left[\frac{t}{z_0}\right] + 1\right\}$.

Conditions of choice w for obtaining the descent when $z_0^2 > ab$ are

$$(18) \quad \left|\frac{t}{z_0} - w\right| < 1, \quad w \equiv d \pmod{2}.$$

If $\left|\frac{t}{z_0}\right| < 1$ then from (17) it follows that $d = 1$ and from (18) we get: $w = 1$ when $\frac{t}{z_0} > 0$ or $w = -1$ when $\frac{t}{z_0} < 0$.

If $\left|\frac{t}{z_0}\right| > 1$ then from (17) it follows that $d > 1$ and from $\left|\frac{t}{z_0} - w\right| < 1$: $w \in \left\{\left[\frac{t}{z_0}\right], \left[\frac{t}{z_0}\right] + 1\right\}$.

As a result, whatever the value for $d > 1$, one can choose the parity w so that $w \equiv d \pmod{2}$.

For the value chosen for w , as applicable, from (16) it follows that $|z| < |z_0|$.

Repeating the process starting from the constructed solutions, after a finite number of steps, we will obtain a solution with $\left(\frac{z}{(x,y,z)}\right)^2 \leq ab$.

It is clear that the solution: $\left(\frac{c_2x}{(x,y,z)}, \frac{c_2y}{(x,y,z)}, \frac{z}{(x,y,z)}\right)$ verifies the conditions in the statement of the theorem, the proof being complete.

Remarks: Holzer's Theorem are obtained from the Theorem for Legendre's equation brought to the form $a_0x^2 + b_0y^2 = c_0z^2$, in wich a_0, b_0, c_0 without squares and relatively prime in pairs and Wlliams' Corollary for Legendre's equation brought to the form:

$$a_1x^2 + b_1y^2 = c_1z^2, \text{ in wich } a_1 = \frac{a}{(a,b,c)}, b_1 = \frac{b}{(a,b,c)}, c_1 = \frac{c}{(a,b,c)}.$$

Example. Let the equation $30x^2 + 1729y^2 = z^2$ cu $x, y, z \in Z$, for which the solution is known: $(X, Y, Z) = (30, 29, 1217)$.

Determine a solution with $z^2 \leq ab$.

We apply the Mordell descent method from the description of the theorem for $(X, Y, Z) = (30, 29, 1217)$, $(X, Y, Z) = 1$, $a = 30$, $b = 1729$, $c = 1$, $c_1 = c_2 = c = 1$

Step 1. We take the solution $(x_0, y_0, z_0) = \left(\frac{x}{(x,y,z)}, \frac{x}{(x,y,z)}, \frac{x}{(x,y,z)}\right) = (30, 29, 1217)$;

Step 2. From $c_1 = x_0v - y_0u \Rightarrow u = 1 + 30k; v = 1 + 29k, k \in Z$. We take $u=1, v=1$;

Step 3. We calculate $d = \frac{au^2 + bv^2}{c_1}, t = \frac{aux_0 + by_0}{c_1}, [t/z_0] \Rightarrow d = 1759, t = 51041, [t/z_0] = 41$;

Step 4. We choose $w \in \{[t/z_0], [t/z_0] + 1\}$: $w \equiv d \pmod{2} \Rightarrow w = 41$;

Step 5. We calculate: $p_0 = \frac{d-w^2}{2}$ si $q_0 = t - wz_0 \Rightarrow p_0 = 39$ and $q_0 = 1144$;

Step 6. We determine the solution: $(x, y, z), |z| < |z_0|$ thus: $x = p_0x_0 - q_0u, y = p_0y_0 - q_0v, z = p_0z_0 - q_0w \Rightarrow x = 26, y = -13, z = 559, (x, y, z) = 13$;

Step 7. We check if $\left(\frac{z}{(x,y,z)}\right)^2 \leq ab \Rightarrow 43^2 < 30 * 1729$.

The solution sought is: $(x, y, z) = (2, -1, 43)$.

References

-
- ¹ L.Holzer, Minimal solutions of diophantine equations, *Canad. J. Math.* 2(1950) ,238-244
² L.J.Mordell, On the magnitude of the equation $ax^2 + by^2 - cz^2 = 0$, *J.Number Theory* 1(1969),1-3
³ Kenneth S. Williams, On the size of a solution of Legendre's equation, *Utilitas Mathematica* 34 (1988), 65-72.