TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2013) 37: 733 – 738

doi:10.3906/mat-1204-40

Algorithm to solve certain ternary quartic Diophantine equations

László SZALAY*
Institute of Mathematics, University of West Hungary, H-9400 Sopron, Ady E. utca 5. Hungary

Received: 19.04.2012 • **Accepted:** 17.07.2012 • **Published Online:** 26.08.2013 • **Printed:** 23.09.2013

Abstract: In this paper, we develop an algorithm to solve completely the Diophantine equation $F(x,y)=z^2$, where the quartic inhomogeneous polynomial $F(x,y)$ with integer coefficients satisfies certain technical conditions. The procedure is an extension of the version of Runge's method given by Poulakis.

Key words: Diophantine equation, Runge method, inhomogeneous ternary equation

1. Introduction

Let

$$G(x,y)=\sum_{i=0}^{k}\sum_{j=0}^{n}c_{ij}x^iy^j\in\mathbb{Z}[x,y]$$

denote an irreducible polynomial over $\mathbb{Q}$. Runge [5] showed that if the so-called *Runge's condition* holds, then the equation

$$G(x,y)=0 \tag{1}$$

has only finitely many solutions in $x\in\mathbb{Z}$ and $y\in\mathbb{Z}$ (for details see, for example [9]). In this case Hilliker and Strauss [2], and later Walsh [9], gave explicit upper bounds for the size of the solutions (x,y). Unfortunately, these bounds are usually too large to test all possible candidates for solutions of (1). Beukers and Tengely [1] suggested a practical algorithm for finding the solutions if the coefficients and $\deg(G)$ are not too large.

The present paper is devoted to solving the Diophantine equation

$$F(x,y)=z^2 \tag{2}$$

in integers x,y, and z, where the inhomogeneous quartic polynomial

$$F(x,y)=\sum_{i+j\le 4}a_{ij}x^iy^j\in\mathbb{Z}[x,y] \tag{3}$$

satisfies a few strict technical conditions. In order to sketch the crucial idea of the method, we first consider a specific case of (1), given by the equation

$$y^2=f(x)\,, \tag{4}$$

*Correspondence: laszalay@emk.nyme.hu
2010 *AMS Mathematics Subject Classification:* 11D25.

where $f(x)$ is a polynomial of degree four with integer coefficients and nonzero discriminant. Tzanakis [8] described a procedure for computing the integer solutions to (4). His method is based on some estimates on linear forms in elliptic logarithms. If $f(x)$ is monic and not a perfect square, Poulakis [4] provided an elegant method for solving (4). His algorithm was generalized by Szalay [6], [7]. Their methods use an elementary approach for applying Runge's method.

The present paper extends the idea of Poulakis to certain quartic Diophantine equations with three variables and suggests an algorithm to solve them in general. Although the application of the method is limited by the configuration (and obviously by the size) of the coefficient, there are advantages in its usage. First, it handles non-homogeneous polynomials $F(x,y)$ of degree four in (2). We note that only a few papers have dealt with the non-homogeneous case. For instance, Mordell in [3] showed that the equation $z^2 = U_1^2 + U_2U_3$ has an infinite number of solutions, where $U_r = a_rx^2 + h_rxy + b_ry^2 + f_rx + g_ry \in \mathbb{Z}[x,y]$ $(r = 1,\ 2,\ 3)$ and $h_r > 4a_rb_r$.

In this paper we assume that $F(x,y)$ can be written in the form $B^2(x,y) + C(x,y)$ with $B(x,y) = U_1(x,y) + j_1 \in \mathbb{Q}[x,y]$ and the linear polynomial $C(x,y) \in \mathbb{Q}[x,y]$. Furthermore we take $h_1^2 < 4a_1b_1$.

Another advantage of our approach is that the procedure can be implemented by computer, allowing us to get all solutions after inserting the coefficients and checking the conditions of the method.

Now we clarify the exact type of equations which can be solved by our algorithm.

2. Background

Consider the polynomial (3) again, and suppose that there exist polynomials $B(x,y) = ax^2 + bxy + cy^2 + dx + ey + f \in \mathbb{Q}[x,y]$ $(a, c > 0)$ and $C(x,y) = ux + vy + w \in \mathbb{Q}[x,y]$ such that

$$F(x,y) = B^2(x,y) + C(x,y). \tag{5}$$

If $4ac - b^2 > 0$ also holds, then we can describe an algorithm for finding all the solutions to the equation

$$z^2 = F(x,y) \tag{6}$$

with integer unknowns x, y, and z.

The algorithm depends on the following theorem. Let δ denote the smallest positive integer such that both $2\delta B(x,y)$ and $\delta^2 C(x,y)$ are polynomials with integer coefficients. We define

$$\begin{aligned} P_1(x,y) &= 2\delta B(x,y) + 1 - \delta^2 C(x,y) \text{ and} \\ P_2(x,y) &= 2\delta B(x,y) - 1 + \delta^2 C(x,y). \end{aligned}$$

Obviously, $P_r(x,y) \in \mathbb{Z}[x,y]$, when $r = 1, 2$.

Theorem 1 *If $(x,y,z) \in \mathbb{Z}^3$ is a solution of $z^2 = F(x,y)$, then $P_1(x,y) > 0$ and $P_2(x,y) > 0$ implies $C(x,y) = 0$.*

By Theorem 1, it is obvious that for any solution of (6) that does not satisfy $C(x,y) = 0$, then either $P_1(x,y) \leq 0$ or $P_2(x,y) \leq 0$ must hold. Since $4\delta^2(4ac - b^2) > 0$, then the quadratic equation

$$P_1(x,y) = 2\delta ax^2 + 2\delta bxy + 2\delta cy^2 + (2\delta d - \delta^2 u)x + (2\delta e - \delta^2 v)y + (2\delta f + 1 - \delta^2 w) = 0$$

(with real x and y) corresponds to an ellipse in the xy-plane with finitely many integer points inside. Similarly, the case $P_2(x,y)=0$ also determines an ellipse. Thus we only need to check equation (6) for the inner points of the ellipses. Clearly, this verification may provide some sporadic solutions besides the family of infinitely many solutions derived from $C(x,y)=0$ (see Example 1). Note that the case for $C(x,y)=0$ does not always have integer solutions since $C(x,y)\in\mathbb{Q}[x,y]$ (see Example 2).

Proof Following Poulakis' idea in [4], we suppose that $P_1(x,y)>0$ and $P_2(x,y)>0$ hold for some integer solution (x,y,z) of equation (6). Consequently,

$$-2\delta B(x,y)+1<\delta^2 C(x,y)<2\delta B(x,y)+1,$$

and equivalently

$$\underbrace{\delta^2B^2(x,y)-2\delta B(x,y)+1}_{(\delta B(x,y)-1)^2}<\underbrace{\delta^2B^2(x,y)+\delta^2C(x,y)}_{\delta^2F(x,y)}<\underbrace{\delta^2B^2(x,y)+2\delta B(x,y)+1}_{(\delta B(x,y)+1)^2}.$$

Since $\delta^2F(x,y)=(\delta z)^2$, the three consecutive squares imply $z^2=B^2(x,y)$, which leads immediately to $C(x,y)=0$. □

3. Conditions

Now we determine the conditions under which it is possible to have the decomposition $F(x,y)=B^2(x,y)+C(x,y)$. Later the algorithm must check the existence of these conditions. Therefore we compare the coefficients of $F(x,y)$ and $B^2(x,y)$ for the terms having degree at least two. This will provide a sufficient condition, where the linear polynomial $C(x,y)$ will satisfy the equality in equation (5) with $F(x,y)$ and $B^2(x,y)$ for the terms having degree at most one.

We first take the case with degree four. Given variables a_{ij}, the subsystem

$$a_{40}=a^2,\quad a_{31}=2ab,\quad a_{22}=2ac+b^2,\quad a_{13}=2bc,\quad a_{04}=c^2 \tag{7}$$

is usually overdetermined in a, b, and c. Thus the system (7) can specify the coefficients a_{ij} $(i+j=4)$ for which $F(x,y)=B^2(x,y)+C(x,y)$ may exist. Clearly, if there are such rationals a, b and c, then $a>0$ and $c>0$ are positive integers; and b is also an integer.

If system (7) is satisfied by some integers a, b, and c, then considering the terms of degree three in (5), we need rational numbers d and e such that

$$a_{30}=2ad,\quad a_{21}=2ae+2bd,\quad a_{12}=2be+2cd,\quad a_{03}=2ce. \tag{8}$$

The first and last equation give $d=a_{30}/(2a)$ and $e=a_{03}/(2c)$, respectively. Clearly, the second and third equation of (8) must also be fulfilled. Thus

$$a_{21}=\frac{a}{c}\,a_{03}+\frac{b}{a}\,a_{30}\quad\text{and}\quad a_{11}=\frac{b}{c}\,a_{03}+\frac{c}{a}\,a_{30} \tag{9}$$

are necessarily integers. We observe that the congruences

$$a^2\,a_{03}+bc\,a_{30}\equiv 0\pmod{ac},\qquad ab\,a_{03}+c^2\,a_{30}\equiv 0\pmod{ac}$$

are soluble in a_{03} and a_{30}, and therefore their solutions ensure the existence of the integers a_{21} and a_{12} having the form given in (9).

After clarifying the coefficients a_{ij} linked to the terms of degree four and three, we turn our attention to the last subsystem

$$a_{20} = d^2 + 2af, \quad a_{11} = 2de + 2bf, \quad a_{02} = e^2 + 2cf. \tag{10}$$

Using the middle equation, clearly $f = (a_{11} - 2de)/(2b)$. Then we must check the first and last equations.

In summary, we have shown that the polynomial $F(x, y)$ must satisfy several conditions in order to have the decomposition described in (5).

4. Examples

We are now ready to establish the algorithm needed to solve equation (6). We verify the conditions that determine $B(x, y)$ and $C(x, y)$ in (5). We establish the value for δ and obtain $P_1(x, y)$ and $P_2(x, y)$. Then we solve $C(x, y) = 0$ in integers (x, y). Finally, we examine the inner points of the ellipses corresponding to $P_1(x, y) = 0$ and $P_2(x, y) = 0$, respectively. The following two examples illustrate our methodology.

Example 1. Equation (6) is taken as

$$\begin{aligned} z^2 \;=\; & F(x, y) = x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + y^4 - 4x^3 - 2x^2y - 2xy^2 + 2y^3 \\ & +8x^2 + 5y^2 - 88x + 17y + 1. \end{aligned}$$

Then we obtain

$$\begin{aligned} B(x, y) &= x^2 + xy + y^2 - 2x + y + 2, \\ C(x, y) &= -80x + 13y - 3, \\ \delta &= 1, \\ P_1(x, y) &= x^2 + xy + y^2 + 78x - 12y + 6, \\ P_2(x, y) &= x^2 + xy + y^2 - 82x + 14y - 2. \end{aligned}$$

The requirement $C(x, y) = 0$ provides solutions $x = 18 - 13t$, $y = 111 - 80t$ $(t \in \mathbb{Z})$. Besides this family of infinite cardinality, there exist 23 exceptional solutions given in Table 1.

Table 1. The sporadic solutions to the equation of Example 1.

x	-25	-23	-14	-8	-6	-5	-4	-3	-1	0	4	7
y	11	19	19	-5	-1	-5	11	3	-1	0	-8	-2
z	536	522	342	144	60	84	116	26	10	1	27	6

x	7	7	11	19	22	25	32	36	42	54	61
y	-1	10	-21	-38	-16	10	-21	-48	0	-48	-38
z	18	216	288	1008	327	936	708	1753	1681	2473	2688

Figure 1 shows the ellipses $P_1(x, y) = 0$, $P_2(x, y) = 0$, the straight line $C(x, y) = 0$, two points $(t = 1, 2)$ on $C(x, y) = 0$, and the 23 exceptional solutions belonging to the ellipses (some of them are located on the curve $P_2(x, y) = 0$).

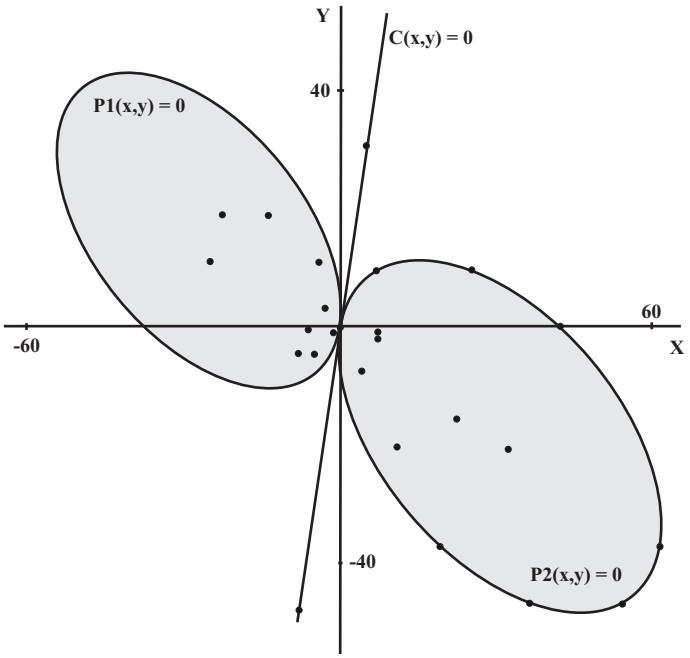

Figure 1. Solutions to the equation of Example 1.

Example 2. Equation (6) is taken as

$$\begin{aligned} z^2 &= F(x,y) = x^4 + 4x^3y + 14x^2y^2 + 20xy^3 + 25y^4 + x^3 + 3x^2y + 7xy^2 + 5y^3 \\ &\quad +x^2 + 2xy + 4y^2 + 13x - 17y + 2 = 0. \end{aligned}$$

Then we obtain

$$\begin{aligned} B(x,y) &= x^2 + 2xy + 5y^2 + \frac{1}{2}x + \frac{1}{2}y + \frac{3}{8}, \\ C(x,y) &= \frac{101}{8}x - \frac{139}{8}y + \frac{119}{64}, \\ \delta &= 8, \\ P_1(x,y) &= 16x^2 + 32xy + 80y^2 - 800x + 1120y - 112, \\ P_2(x,y) &= 16x^2 + 32xy + 80y^2 + 816x - 1104y + 124. \end{aligned}$$

Clearly, there is no integer solution derived from $C(x,y) = 0$. But there exist four exceptional solutions if one scans the inner points of the ellipses:

$$(x,y,z) = (-25,11,673),\ (-13,-1,193),\ (-8,2,48),\ (-3,1,1).$$

References

[1] Beukers, F., Tengely, Sz.: An implementation of Runge's method for Diophantine equations. arXiv:math/0512418v1.

[2] Hilliker, D. E., Strauss, E. G.: Determination of bounds for the solutions to those Diophantine equations that satisfy the hypotheses of Runges theorem. Trans. Amer. Math. Soc. 280, 637-657 (1983).

[3] Mordell, L., J.: On some ternary quartic Diophantine equations. Elem. Math. 31, 89-90 (1966).

[4] Poulakis, D.: A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$. Elem. Math. 54, 32-36 (1999).

[5] Runge, C.: Über ganzzahlige Lösungen von Gleichungen zwissen zwei Veränderlichen. J. Reine Angew. Math. 100, 425-435 (1887).

[6] Szalay, L.: Fast algorithm for solving superelliptic equations of certain types. Acta Acad. Paed. Agriensis 27, 19-24 (2000).

[7] Szalay, L.: Superelliptic equations of the form $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$. Bull. Greek Math. Soc. 46, 23-33 (2002).

[8] Tzanakis, N.: Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. Acta Arithm. 75, 165-190 (1996).

[9] Walsh, P. G.: A quantitative version of Runge's theorem on Diophantine equations. Acta Arithm. 62, 157-172 (1992).