SOLVING THE DIOPHANTINE EQUATION $ax^2 + bxy + cy^2 + dx + ey + f = 0$

KEITH MATTHEWS

1. Introduction

This note originates from studying the paper [11, pp. 38–40] where a new method of solving the general quadratic diophantine equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{1}$$

is given in the case where (1) represents an hyperbola. This was an improvement on a classical method of Lagrange mentioned in [11, p. 39]. We use a transformation due to Legendre [8]).

In our note, we give a variation of the method of [11] due to John Robertson, which uses a transformation of variables where the centre of the hyperbola becomes the origin.

The rest of the note is a standard treatment of the special cases that correspond to an ellipse, parabola, or two straight lines, possibly coincident.

The output of parabola case was improved by Chi Chon Lei.

The underlying algorithm has been coded as BCMath program [3].

An earlier computer program for solving (1) due to Dario Alpern is available at [4]. This sometimes yields redundant families.

2. The cases

Let $D = b^2 - 4ac$. We assume not all of a, b, c are zero.

Case 1. $D = 0$. We use completion of the square, as in Hua's book [7, p. 278]. We can assume $a \neq 0$ (by interchanging x and y, as one of a and c is nonzero) and multiply (1) by $4a$ to get an equivalent equation:

$$(2ax + by)^2 + 4adx + 4aey + 4af = 0. \tag{2}$$

Let $t = 2ax + by$. Then (2) becomes

$$(t + d)^2 = uy + v. \tag{3}$$

where $u = 2(bd - 2ae)$ and $v = d^2 - 4af$.

(i) Assume $u = 0$. Then (3) becomes $(t + d)^2 = v$. Let $h = \gcd(2a, b)$.
If $v = 0$, then equation (3) becomes $2ax + by + d = 0$ and we have a line of integer solutions $(2a/h)x + (b/h)y = d/h$ for (1) if h divides d, but no integer solution if h does not divide d.

Date: 11th May 2015, amended 18th July 2017, 29th November 2019, 15th December 2019, 5th January 2020, 9th January 2020, 27th January 2020.

If $v < 0$ or $v > 0$ and v is nonsquare, there is no integer solution of (1).

Next assume $v = g^2, g > 0$. Then $t + d = \pm g$, i.e.,

$$2ax + by = \pm g - d$$

and we have the following possibilities:

(a) If h divides $g - d$, we have a line of integer solutions of (1):

$$(2a/h)x + (b/h)y = (g - d)/h.$$

(b) If h divides $g + d$, we have a line of integer solutions of (1):

$$(2a/h)x + (b/h)y = (-g - d)/h.$$

(c) Neither $g - d$ nor $g + d$ is divisible by h. Then there is no integer solution of (1).

(ii) Assume $u \neq 0$. Then (3) gives rise to the congruence

$$T^2 \equiv v \pmod{|u|}, \tag{4}$$

where $T = t + d$ and $t = 2ax + by$.

If there are no solutions of (4), then there are no integer solutions of (1). Otherwise let $T_1, \ldots, T_c$ be the solutions in the range $-|u|/2 < T_i \leq |u|/2$. Then

$$t = T_i - d + uk, \ k \text{ an integer.}$$

Then equation (3) gives

$$y = r + sk + uk^2, \tag{5}$$

where $r = (T_i^2 - v)/u$ and $s = 2T_i$. Also

$$2ax + by = t = T_i - d + ku,$$

or equivalently

$$2ax = T_i - d - br + (u - bs)k - buk^2. \tag{6}$$

Now $-bu/2a$ is an integer. For $bu = 2b(bd - 2ae) = 2b^2d - 4bae$ and since $b^2 = 4ac$, we see that $-bu/2a = 2be - 4cd$, an integer. Also

$$u - bs \equiv 0 \pmod{2a} \tag{7}$$

$$T_i - d - br \equiv 0 \pmod{2a}. \tag{8}$$

Hence

$$x = \frac{T_i - d - br}{2a} + \frac{u - bs}{2a}k - \frac{bu}{2a}k^2. \tag{9}$$

Conversely, if the congruences (7) and (8) hold for a solution T_i of (4), then x given by (9) and y given by (5), with k arbitrary, will give an integer solution of (1).

The solutions will either lie on a parabola or two parallel lines, or a single line.

Chi Chon Lei has observed that equations (9) and (5) can be rewritten as

$$x = -\frac{bu}{2a}\left(k - \frac{1}{2b} + \frac{T_i}{u}\right)^2 + \frac{u^2 - 4bdu + 4b^2v}{8abu}, \tag{10}$$

$$y = u\left(k + \frac{T_i}{u}\right)^2 - \frac{v}{u}. \tag{11}$$

It can happen that there exists an $N > 1$ dividing $|u|$ for which the m solutions of congruence (4) which satisfy (7) and (8) break up into arithmetic progressions of N integers with common difference $|u|/N$.

The advantage of writing the solutions in form (10) and (11) is that it allows us to merge the families corresponding to the integers in each arithmetic progression into one family, since everything outside the brackets n (10) and (11) does not depend on T_i, and k can be replaced by k/N in the general solution coreponding to any one of the T_i in a progression.

For example, in the equation $9x^2 - 12xy + 4y^2 + 3x + 2y - 12 = 0$, we have $u = -144, v = 441$ and the $m = 8$ solutions are

$$3, 27, 21, 45, -27, -51, -45, -69.$$

With $N = 2$ and $|u|/N = 72$, these can be grouped into 4 arithmetic progressions, with common difference 72:

$$\{3, -69\}, \{27, -45\}, \{21, -51\}, \{45, -27\},$$

and we end up with the 4 solution families of Example 4 below.

Chi Chon Lei provided an even more spectacular example with the equation $x^2 - 20xy + 100y^2 - 8x - 16y + 12 = 0$, where an initial 32 families of solutions are converted to two families:

$$x = 15n^2 + 17n + 6, \quad y = \frac{n}{2}(3n + 1), \tag{12}$$

$$x = 15n^2 + 7n + 2, \quad y = \frac{n}{2}(3n - 1). \tag{13}$$

Here $u = 384, v = 16, N = 16$ and we have two arithmetic progressions with common difference $|u|/N = 24$:

$$-172, -148, -124, -100, -76, -52, -28, -4, 20, 44, 68, 92, 116, 140, 164, 188,$$
$$-188, -164, -140, -116, -92, -68, -44, -20, 4, 28, 52, 76, 100, 124, 148, 172.$$

Case 2. $D \neq 0$. We multiply (1) by D^2 and translate the origin to (α, β), where

$$\alpha = 2cd - be, \beta = 2ae - bd,$$

using the transformation of Legendre ([8, p. 105])

$$Dx = X + \alpha, Dy = Y + \beta,$$

to get the equation

$$aX^2 + bXY + cY^2 = k, \tag{14}$$

where

$$k = -D(ae^2 - bed + cd^2 + fD).$$

Let $g = \gcd(a, b, c)$. Clearly g divides D and hence k, so we replace (a, b, c, k) by $(a/g, b/g, c/g, k/g)$ in (14). (Pointed out by Sander Verdonschot 26/08/2022.)

(a) Assume $k = 0$ and D not a square. Then the only integer solution of (14) is $(X, Y) = (0, 0)$ and so $Dx = \alpha$ and $Dy = \beta$. Hence if $D|\alpha$ and $D|\beta$, we have the unique solution $(x, y) = (\alpha/D, \beta/D)$, whereas if D does not divide α or D does not divide β, there is no integer solution of (1).

(b) Assume $D < 0$ and $k \neq 0$. Then (1) describes an ellipse. We use the recent algorithm of Matthews ([10]) to find all integer solutions (X_i, Y_i) of $aX^2 + bXY + cY^2 = k$. If D divides $X_i + \alpha$ and D divides $Y_i + \beta$, we get a corrresponding integer solution of (1):

$$(x, y) = ((X_i + \alpha)/D, (Y_i + \beta)/D).$$

(c) Assume $D = g^2, g > 0$.

(i) Assume $a \neq 0$. Then on multiplying by $4a$, equation (14) becomes

$$(2aX + (b + g)Y)(2aX + (b - g)Y) = 4ak.$$

Let $g_1 = \gcd(2a, b + g), g_2 = \gcd(2a, b - g)$.
Sander Verdonschot has pointed out (29/08/2022) that $g_1 g_2$ divides $4ak$; in fact $g_1 g_2$ divides $4aD$.
For $g_1|2a$ and $g_2|b-g$, so $g_1 g_2|2a(b-g)$. Similarly $g_1 g_2|2a(b+g)$. Hence

$$g_1 g_2||2a(b - g) + 2a(b + g) = 4ab,$$

and consequently $g_1 g_2|4ab^2$. We also have

$$g_1 g_2|(b + g)(b - g) = b^2 - g^2 = b^2 - (b^2 - 4ac) = 4ac,$$

so $g_1 g_2|16a^2 c$. Hence $g_1 g_2|(4ab^2 - 16a^2 c) = 4aD$.
Hence we now have to solve

$$\left(\frac{2a}{g_1}X + \frac{(b + g)}{g_1}Y\right)\left(\frac{2a}{g_2}X + \frac{(b - g)}{g_2}Y\right) = \frac{4ak}{g_1 g_2}.$$

We consider the cases $k = 0$ and $k \neq 0$ separately:
First the case $k = 0$. We get two equations $2aX + (b \pm g)Y = 0$.
Using $Dx = X + \alpha$ and $Dy = Y + \beta$, these in turn give two equations

$$2aDx + (b + g)Dy = 2a\alpha + (b + g)\beta \tag{15}$$

$$2aDx + (b - g)Dy = 2a\alpha + (b - g)\beta. \tag{16}$$

If Dg_1 does not divide $2a\alpha + (b+g)\beta$, then equation (15) does not lead to a solution for (x, y).
If Dg_1 divides $2a\alpha + (b+g)\beta$, then we get the line of integer solutions:

$$(2a/g_1)x + ((b+g)/g_1)y = (2a\alpha + (b+g)\beta)/Dg_1.$$

Similarly for (16).
Secondly, consider the case $k \neq 0$. We are dealing with an equation of the form

$$(A_1X + B_1Y)(A_2X + B_2Y) = 4ak/(g_1g_2),$$

where $A_1 = 2a/g_1, A_2 = 2a/g_2, B_1 = (b+g)/g_1, B_2 = (b-g)/g_2$. We have to examine all divisors d_i of $4ak/(g_1g_2)$ and test for integer solutions (X, Y) of

$$A_1X + B_1Y = d_i \tag{17}$$

$$A_2X + B_2Y = 4ak/(g_1g_2d_i). \tag{18}$$

If there are no integer solutions of the system of equations (17) and (18) for any i, then there are no integer solutions of (1).
However if there is an i such that (17) and (18) have integer solutions (X, Y), then each such solution, we have to check if D divides $X+\alpha$ and $Y+\beta$, in which case we get an integer solution of (1):

$$(x, y) = ((X + \alpha)/D, (Y + \beta)/D).$$

(ii) Assume $a = 0$. Then (14) becomes $Y(bX + cY) = k$. Again we consider the cases $k \neq 0$ and $k = 0$ separately. Let $h = \gcd(b, c)$. First assume $k \neq 0$. If h does not divide k, then (1) has no integer solutions.
If h divides k, we get the equation

$$Y((b/h)X + (c/h)Y) = k/h.$$

We then have to examine all divisors d_i of k/h and solve the system

$$Y = d_i$$
$$(b/h)X + (c/h)Y = k/(hd_i)$$

in integers.
Secondly, assume $k = 0$. Then (3) becomes $Y(bX + cY) = 0$, i.e.,

$$(Dy + \beta)(bDx + cDy + b\alpha + c\beta) = 0.$$

.
If D divides β, we get one family of integer solutions of (1), namely $y = \beta/D$, with x arbitrary. Let $g' = \gcd(b, c)$ and $t = b\alpha + c\beta$.

If $g'D$ does not divide t, there are no integer solutions of (1).
If $g'D$ divides t, we get a line of integer solutions of (1):

$$(b/g')x + (c/g')y + t/Dg' = 0.$$

(d) Assume $D > 0$ and nonsquare and $k \neq 0$. Then (1) describes an hyperbola. This case is discussed in detail at [13].

3. Examples

(1) $x^2 - 15y^2 = 61$. [7, p. 285]. Ans. $x + y\sqrt{15} = \pm(11 \pm 2\sqrt{15})(4 + \sqrt{15})^n$.
(2) $3x^2 - 8xy + 7y^2 - 4x + 2y - 109 = 0$. Exercise (a), [7, p. 286].

Ans. $D = -20, (2, 5), (2, -3), (14, 9), (-10, -7)$.

(3) $3xy + 2y^2 - 4x - 3y - 12 = 0$. Exercise (b), [7, p. 286].

Ans. $D = 9$,

$$(5, 2), (-3, 6), (-1, 4), (-13, 20), (-13, 1),$$
$$(-1, -1), (-3, 0), (5, -8), (2, -4), (24, -36).$$

(4) $9x^2 - 12xy + 4y^2 + 3x + 2y - 12 = 0$. Exercise (c), [7, p. 286].

Ans. $D = 0$. Four families:

$$x = 2 - 2t - 24t^2, x = 0 + 14t - 24t^2, x = 1 + 10t - 24t^2, x = -3 - 22t - 24t^2,$$
$$y = 3 + 3t - 36t^2, y = -2 + 27t - 36t^2, y = 0 + 21t - 36t^2, y = -2 - 27t - 36t^2.$$

(5) $x^2 - 8xy - 17y^2 + 72y - 75 = 0$. Exercise (d), [7, p. 286].

Ans. $D = 132$. Two families: With $F + G\sqrt{33} = -(23 + 4\sqrt{33})^n$ and

$$11x = 70F + 297G + 48, \quad 11x = -62F - 231G + 48,$$
$$11y = F + 66G + 12, \quad 11y = F - 66G + 12,$$

with representatives $(-2, 1)$ and $(10, 1)$, respectively.

(6) $x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$. Art. 221, [6, p. 220–221].

Ans. $D = 60$. One solution is $(-1, 0)$ with general solution

$$(x, y)^t = ((-1)^m U^m(-8, 2)^t + (3, -2)^t)/5, m \in \mathbb{Z},$$

where $U = \begin{pmatrix} 0 & -1 \\ 1 & 8. \end{pmatrix}$. A solution was given by Gauss, namely

$$5x = 2t + 3$$
$$5y = -8t + 30u - 2,$$

where $t^2 - 15u^2 = 1$ and $t \equiv 1 \pmod 5$.

(7) $x^2 + 2xy + y^2 + x + y - 6 = 0$.

Ans. $D = -31$. Six solutions: $(31, 10), (-31, -10), (-17, -19), (17, 19), (46, -10), (-46, 10)$.
Note. Faisant does not list four of these solutions.

(8) $3x^2 - 22xy + 25y^2 = 81$. Exercise III.6, [5, p. 115].

Ans. $D = 184$. Five families of solutions:

$$x = -658F - 4463G, \quad x = -2F - 47G, \quad x = -156F + 1059G$$
$$y = -111F - 753G, \quad y = F - 17G, \quad y = -111F + 753G,$$

$$x = 54F + 369G, \quad x = -12F + 93G,$$
$$y = 9F + 63G, \quad y = -9F + 63G,$$

with $F + G\sqrt{46} = \pm(24335 + 1794\sqrt{46})^m$. Note. Faisant has an incorrect answer $(-111, -156)$ instead of $(-156, -111)$.

(9) $2x^2 + 8xy - y^2 - 4x + 10y - 7 = 0$. Ans. $(-1, 1)$.

References

[1] `http://www.numbertheory.org/php/patz.html`
[2] `http://www.numbertheory.org/php/binarygen.html`
[3] `http://www.numbertheory.org/gnubc/patz`
[4] `http://www.alpertron.com.ar/QUAD.HTM`
[5] A. Faisant, *L'équation diophantinne du second degré*, Hermann, 1991.
[6] C.F. Gauss, *Disquisitiones Arithmeticae*.
[7] Hua Loo Keng, *Introduction to Number Theory*, Springer 1982.
[8] A-M. Legendre, *Théorie des nombres*, Tome II, Edition 3, 1830.
[10] `https://cs.uwaterloo.ca/journals/JIS/VOL17/Matthews/matt10.html`
[11] R.E. Sawilla, A.K. Silvester, H.C. Williams, *LNCS* 5011, 37–59, 2008.
[12] Th. Skolem, *Diophantische Gleichungen*, Chelsea New York 1950.
[13] K.R. Matthews, J.P. Robertson, *On solving a binary quadratic diophantine equation* (to appear, Rocky Mountain Math. Journal 2021).