FINDING THE FUNDAMENTAL SOLUTIONS OF $ax^2 + bxy + cy^2 = n$

K.R. MATTHEWS

ABSTRACT. Stolt defined an equivalence relation on the integer solutions of $x^2 - dy^2 = 4n$, $d > 0$ and non–square, n non–zero, that can result in a smaller number of equivalence classes than Nagell equivalence, which is the standard equivalence relation. We give a method of calculating class representatives called the Stolt fundamental solutions. This can then be used to solve the diophantine equation $ax^2 + bxy + cy^2 = N$, where $d = b^2 - 4ac > 0, a > 0$, and is not a perfect square and N is non–zero.

1. INTRODUCTION

Let $d > 0$ and n be integers, d non–square, n nonzero. We study the diophantine equation

$$x^2 - dy^2 = 4n. \tag{1}$$

This is relevant, because the equation $ax^2 + bxy + cy^2 = N$ reduces to $X^2 - dY^2 = 4aN$ under the transformation $X = 2ax + by, Y = y$.

Suppose (x, y) is an integer solution of (1). Then if (x', y') is defined by

$$x' + y'\sqrt{d} = (x + y\sqrt{d})(u + v\sqrt{d})/2, \tag{2}$$

equivalently

$$x' = (xu + dyv)/2, \quad y' = (xv + yu)/2, \tag{3}$$

where (u, v) is an integer solution of $u^2 - dv^2 = 4$, then (x', y') is also an integer solution of (1).

(The fact that x' and y' are integers follows from the congruences

$$x \equiv dy \pmod 2, \quad x' \equiv dy' \pmod 2, \quad u \equiv dv \pmod 2.)$$

Date: October 6, 2023.

Then (2) gives an equivalence relation on the set of integer solutions of (1) which we call *Stolt* equivalence.

The standard *Nagell* equivalence of solutions of (1) ([5, p. 204]) is defined by

$$x' + y'\sqrt{d} = (x + y\sqrt{d})(u + v\sqrt{d}), \tag{4}$$

where (u, v) is an integer solution of $u^2 - dv^2 = 1$.

LEMMA 1.1. ([6, Theorem 4]). *A necessary and sufficient condition for solutions* (x_1, y_1) *and* (x_2, y_2) *of* $x^2 - dy^2 = 4n$ *to be Stolt–equivalent is that* $x_1y_2 - x_2y_1 \equiv 0 \pmod{2|n|}$.

REMARK 1.1. This result is due to Stolt and is analogous to a similar criterion for Nagell–equivalence, where $2|n|$ is replaced by $4|n|$.

Let $\epsilon_1 = u_1 + v_1\sqrt{d}$, where (u_1, v_1) is the minimal positive integer solution to $u^2 - dv^2 = 1$.

Let $\epsilon_4 = (u_4 + v_4\sqrt{d})/2$, where (u_4, v_4) is the minimal positive integer solution to $u^2 - dv^2 = 4$.

Stolt ([6, Theorem 1]) gave a connection between the two types of equivalence classes in terms of ϵ_1 and ϵ_4.

THEOREM 1.1.

(i) *If* $d \equiv 1 \pmod 8$ *or* $d \equiv 2 \pmod 4$ *or* $d \equiv 3 \pmod 4$, *then* $\epsilon_1 = \epsilon_4$.

(ii) *If* $d \equiv 5 \pmod 8$, *then* $\epsilon_1 = \epsilon_4$ *if* v_4 *is even; whereas if* v_4 *is odd, then* $\epsilon_1 = \epsilon_4^3$.

(iii) *If* $d \equiv 0 \pmod 4$, *then* $\epsilon_1 = \epsilon_4$ *if* v_4 *is even; whereas if* v_4 *is odd, then* $\epsilon_1 = \epsilon_4^2$.

If $\epsilon_1 = \epsilon_4$, *the Stolt and Nagell equivalence classes are the same. However if* $\epsilon_1 = \epsilon_4^2$ *(resp.* ϵ_4^3*), each Stolt class consists of two (resp. three) Nagell classes.*

A *Stolt fundamental solution* is the solution in a class with the minimal non-negative y. If there are two solutions in a class with the same minimal

non-negative y, then the solution with $x > 0$ is taken as the fundamental solution.

If $d \equiv 1 \pmod 8$ or $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, then the Stolt and Nagell fundamental solutions are identical. However when $d \equiv 5 \pmod 8$ or $d \equiv 0 \pmod 4$, if $\epsilon_1 \neq \epsilon_4$, one has to determine which Nagell fundamental solutions belong to the same Stolt class. This can be done by first finding the Nagell fundamental solutions using the LMM (Lagrange-Mollin-Matthews) continued fraction–based algorithm in [2], and using Lemma 1.1 to select the Stolt fundamental solutions.

The Stolt fundamental solutions can also be computed for small d and n using the following result, which is similar to Theorem 4.1 of [4], which characterises the Nagell fundamental solutions.

THEOREM 1.2. *Let (x_1, y_1) be the least positive solution of $x^2 - dy^2 = 4$. An integer pair (u, v) satisfying (1) is an SFS, if and only if one of the following holds:*

(a) *If $n > 0$,*
  (i) $0 < v < y_1\sqrt{\frac{n}{x_1+2}}$,
  (ii) $v = 0$ *and* $u = \sqrt{4n}$,
  (iii) $v = y_1\sqrt{\frac{n}{x_1+2}}$ *and* $u = \sqrt{n(x_1+2)}$.

(b) *If $n < 0$, then*
  (i) $\sqrt{\frac{|4n|}{d}} \leq v < y_1\sqrt{\frac{|n|}{x_1-2}}$,
  (ii) $v = y_1\sqrt{\frac{|n|}{x_1-2}}$ *and* $u = \sqrt{|n|(x_1-2)}$.

EXAMPLE 1.1. The equation $x^2 - 28y^2 = 72$. We have $\epsilon_1 = \epsilon_4^2$. There are six Nagell fundamental solutions $(\pm 10, 1), (\pm 18, 3), (\pm 38, 7)$ and three Stolt fundamental solutions $(\pm 10, 1), (18, 3)$, as

$$(10, 1) \sim (-38, 7), (-10, 1) \sim (38, 7), (18, 3) \sim (-18, 3),$$

and $(10, 1), (-10, 1)$ and $(18, 3)$ are not Stolt equivalent.

EXAMPLE 1.2. The equation $x^2-13y^2 = 48$. We have $\epsilon_1 = \epsilon_4^3$. There are six Nagell fundamental solutions $(\pm 10, 2), (\pm 16, 4), (\pm 94, 26)$ and two Stolt fundamental solutions $(\pm 10, 2)$, as

$$(10, 2) \sim (-16, 4) \sim (94, 26), (-10, 2) \sim (16, 4) \sim (-94, 26),$$

and $(10, 2)$ and $(-10, 2)$ are not Stolt equivalent.

2. The diophantine equation $ax^2 + bxy + cy^2 = N$

Stolt [7] defined equivalence for the diophantine equation

$$ax^2 + bxy + cy^2 = N, \tag{5}$$

where $D = b^2 - 4ac > 0$ and not a perfect square.

If (x, y) is an integer solution of (5) and (x', y') is defined by

$$2ax' + by' + y'\sqrt{D} = \frac{(u + v\sqrt{D})}{2}(2ax + by + y\sqrt{D}), \tag{6}$$

where (u, v) is an integer solution of $u^2 - dv^2 = 4$, then (x', y') is also an integer solution of (5) and (6) gives an equivalence relation on the set of integer solutions of (5).

Note that this equivalence reduces to Nagell equivalence when $a = 1, b = 0, c = -d, d > 0$ and nonsquare.

Equivalently

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = U \begin{pmatrix} x \\ y \end{pmatrix}, \tag{7}$$

where

$$U = \begin{pmatrix} \frac{u-bv}{2} & -cv \\ av & \frac{u+bv}{2} \end{pmatrix}. \tag{8}$$

The equivalence class containing (x, y) is then given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \pm U^n \begin{pmatrix} x \\ y \end{pmatrix}, n \in \mathbb{Z}. \tag{9}$$

LEMMA 2.1. ([7, Theorem 5]). *A necessary and sufficient condition for solutions* (x_1, y_1) *and* (x_2, y_2) *of* $ax^2+bxy+cy^2 = N$ *to be equivalent is that* $x_1y_2 - x_2y_1 \equiv 0 \pmod{|N|}$.

Among all solutions (x, y) in an equivalence class K, we choose a *fundamental* solution where y is the least nonnegative value of y when (x, y) belongs to K. Let $x' = -(ax + by)/a$ be the conjugate solution to x in the equation $ax^2 + bxy + cy^2 = N$. If x' is not integral or if (x', y) is not equivalent to (x, y), this determines (x, y). If x' is integral and (x', y) is equivalent to (x, y), we replace x by x', if $x' > x$. There are finitely many equivalence classes, each indexed by a fundamental solution.

These were also discussed in [4], where inequalities derived by Stolt [7] were shown to determine the fundamental solutions.

The transformation

$$X = 2ax + by, Y = y \tag{10}$$

transforms equation (5) into equation (11).

$$X^2 - Dy^2 = 4aN, \tag{11}$$

If there are no integer solutions of (11), then there are no integer solutions of (5).

In what follows, we assume that (11) has an integer solution and that $a > 0$.

THEOREM 2.1. *Let* $(\alpha_1, \beta_1), \ldots, (\alpha_h, \beta_h)$ *be the Stolt fundamental solutions of* (11) *such that* $2a$ *divides* $\alpha_i - b\beta_i$. *Then* $(\frac{\alpha_1 - b\beta_1}{2a}, \beta_1), \ldots, \frac{\alpha_h - b\beta_h}{2a}, \beta_h)$ *are the fundamental solutions of* (5).

REMARK 2.1. The equivalence class of solutions (x, y) of (5) determined by the fundamental solution $(\frac{\alpha_i - b\beta_i}{2a}, \beta_i)$ is given by

$$x = \left(\frac{\alpha_i - b\beta_i}{2a}u + \frac{D\beta_i - b\alpha_i}{2a}v\right)/2, \tag{12}$$

$$y = (\beta_i u + \alpha_i v)/2, \tag{13}$$

Proof. (i) Let (x, y) satisfy $ax^2+bxy+cy^2 = N$. Then $(X, Y) = (2ax+by, y)$ satisfies $X^2 - DY^2 = 4aN, D = b^2 - 4ac$, and hence

$$(2ax + by, y) \sim (\alpha_i, \beta_i) \text{ for some } i, 1 \le i \le h,$$

$$(2ax + by)\beta_i - y\alpha_i \equiv 0 \pmod{2a|N|}$$

$$x\beta_i - y\left(\frac{\alpha_i - b\beta_i}{2a}\right) \equiv 0 \pmod{|N|}$$

and $(x, y) \sim \left(\frac{\alpha_i - b\beta_i}{2a}, \beta_i\right)$.

(ii) The solutions $(\frac{\alpha_i - b\beta_i}{2a}, \beta_i), 1 \le i \le h$ are inequivalent.

For

$$\left(\frac{\alpha_i - b\beta_i}{2a}, \beta_i\right) \sim \left(\frac{\alpha_j - b\beta_j}{2a}, \beta_j\right)$$

$$\implies \frac{(\alpha_i - b\beta_i)}{2a}\beta_j - \frac{(\alpha_j - b\beta_j)}{2a}\beta_i \equiv 0 \pmod{|N|}$$

$$\implies \alpha_i\beta_j - \alpha_j\beta_i \equiv 0 \pmod{2a|N|}$$

$$\implies (\alpha_i, \beta_i) \sim (\alpha_j, \beta_j).$$

(iii) Let $(x, y), y \ge 0$ belong to the equivalence class K of solutions of $ax^2 + bxy + cy^2 = N$ determined by $\left(\frac{\alpha_i - b\beta_i}{2a}, \beta_i\right)$. Then $(X, Y) = (2ax + by, y)$ belongs to the equivalence class K' of solutions of $X^2 - DY^2 = 4aN$ determined by (α_i, β_i). Hence $y \ge \beta_i$.

Let (x', y) be the conjugate solution to $(x, y) = \left(\frac{\alpha_i - b\beta_i}{2a}, \beta_i\right)$.

Then

$$x' = -\frac{(ax + by)}{a} = \frac{-2ax - 2by}{2a} = \frac{-(\alpha_i - b\beta_i) - 2b\beta_i}{2a} = -\frac{\alpha_i + b\beta_i}{2a}.$$

If x' is not an integer, or (x', y) is not equivalent to (x, y), then (x, y) is a fundamental solution for K. But if (x', y) is an integer solution of K, then

(x', y) maps to $(-\alpha_i, \beta_i)$ and (x, y) maps to (α_i, β_i) and these are equivalent solutions of K'. Hence $\alpha_i \geq 0$ and $-(\alpha_i + b\beta_i)/2a \leq (\alpha_i - b\beta_i)/2a$. Hence $x' \leq x$ and (x, y) is a fundamental solution of K.

□

3. Examples

EXAMPLE 3.1. ([3, p. 266–267]). The equation $42x^2+62xy+21y^2 = 585$. Here $D = 316$. This equation becomes $X^2 - 316Y^2 = 98280$ under the transformation $X = 84x + 62y, Y = y$. This has ten Stolt fundamental solutions: (314,1), (-634,31), (634,31), (-314,1), (-318,3), (1578,87), (1266,69), (-1266,69), (-1578,87), (318,3), of which only $(314, 1), (-318, 3), (-1266, 69)$ and $(-1578, 87)$ satisfy the condition that 84 divides $\alpha - 62\beta$. These give the following four solution families of the equation $42x^2+62xy+21y^2 = 585$:

(i) $(\alpha_1, \beta_1) = (314, 1)$: Fundamental solution $(3, 1)$.

$$x = (3u - 228v)/2$$

$$y = (u + 314v)/2.$$

(ii) $(\alpha_2, \beta_2) = (-318, 3)$: Fundamental solution $(-6, 3)$.

$$x = (-6u + 246v)/2$$

$$y = (3u - 318v)/2.$$

(iii) $(\alpha_3, \beta_3) = (-1266, 69)$: Fundamental solution $(-66, 69)$.

$$x = (-66u + 1194v)/2$$

$$y = (69u - 1266v)/2.$$

(iv) $(\alpha_4, \beta_4) = (-1578, 87)$: Fundamental solution $(-83, 87)$

$$x = (-83u + 1492v)/2$$

$$y = (87u - 1578v)/2.$$

Here $u^2 - 316v^2 = 4$.

EXAMPLE 3.2. The equation $2x^2 + 5xy + y^2 = 16$. Here $D = 17$. This becomes $X^2 - 17Y^2 = 128$ under the transformation $X = 4x + 5y, Y = y$. There are 6 Stolt fundamental solutions:

$$(31, 7), (-31, 7), (14, 2), (-14, 2), (20, 4), (-20, 4),$$

and only 5 for which 4 divides $\alpha - 5\beta$:

$$(31, 7), (14, 2), (-14, 2), (20, 4), (-20, 4).$$

(i) $(\alpha_1, \beta_1) = (31, 7)$: Fundamental solution $(-1, 7)$.

$$x = (-u - 9v)/2$$
$$y = (7u + 31v)/2.$$

(ii) $(\alpha_2, \beta_2) = (14, 2)$: Fundamental solution $(-6, 2)$.

$$x = (-6u + 26v)/2$$
$$y = (2u - 14v)/2.$$

(iii) $(\alpha_3, \beta_3) = (-14, 2)$: Fundamental solution $(1, 2)$.

$$x = (u - 9v)/2$$
$$y = (2u + 14v)/2.$$

(iv) $(\alpha_4, \beta_4) = (20, 4)$: Fundamental solution $(-10, 4)$.

$$x = (-10u + 42v)/2$$
$$y = (4u - 20v)/2.$$

(v) $(\alpha_5, \beta_5) = (-20, 4)$: Fundamental solution $(0, 4)$.

$$x = (0u - 8v)/2$$
$$y = (4u + 20v)/2.$$

Here $u^2 - 17v^2 = 4$.

EXAMPLE 3.3. ([3, p. 267]) The equation $19x^2 - 85xy + 95y^2 = -671$. Here $D = 5$. This becomes $X^2 - 5Y^2 = -50996$ under the transformation $X = 38x - 85y, Y = y$. There are eight Stolt fundamental solutions (α, β):

$$(\pm 3, 101), (\pm 32, 102), (\pm 72, 106), (\pm 103, 111).$$

Only four satisfy the condition that 38 divides $\alpha + 85\beta$ and these give the following four solution families of the equation $19x^2 - 85xy + 95y^2 = -671$:

(i) $(\alpha_1, \beta_1) = (3, 101)$: Fundamental solution $(226, 101)$.

$$x = (226u + 20v)/2$$
$$y = (101u + 3v)/2.$$

(ii) $(\alpha_1, \beta_1) = (32, 102)$: Fundamental solution $(229, 102)$.

$$x = (229u + 85v)/2$$
$$y = (102u + 32v)/2.$$

(iii) $(\alpha_1, \beta_1) = (72, 106)$: Fundamental solution $(239, 106)$.

$$x = (239u + 175v)/2$$
$$y = (106u + 72v)/2.$$

(iv) $(\alpha_1, \beta_1) = (103, 111)$: Fundamental solution $(251, 111)$.

$$x = (251u + 245v)/2$$
$$y = (111u + 103v)/2.$$

Here $u^2 - 5v^2 = 4$.

EXAMPLE 3.4. ([1, pp. 93–94]) The equation $x^2 - 5xy + y^2 = -3$. Here $D = 21$. This becomes $X^2 - 21Y^2 = -12$ under the transformation $X = 2x - 5y, Y = y$. This has one Stolt fundamental solution $(3, 1)$. It

satisfies the condition that 2 divides $\alpha + 5\beta$, resulting in the solution family for the equation $x^2 - 5xy + y^2 = -3$:

$$x = 2u + 9v$$

$$y = (u + 3v)/2,$$

where $u^2 - 21v^2 = 4$.

4. Acknowledgment

I am indebted to John Robertson for his contribution to Section 1.

References

[1] T Andreescu and D. Andrica, *Quadratic Diophantine equations*, Springer 2015.

[2] K.R Matthews, *The Diophantine equation* $x^2 - Dy^2 = N, D > 0$, Expositiones Mathematicae, 18 (2000), 323–331.

[3] K.R. Matthews, *The Diophantine equation* $ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0$, Journal de Théorie des Nombres de Bordeaux, 14 (2002) 257–270.

[4] K.R. Matthews, J.P. Robertson and A. Srinivasan, *On fundamental solutions of binary quadratic form equations*, Acta Arith. 169 (2015), 291–299.

[5] T. Nagell, *Number Theory*, Chelsea, New York 1981.

[6] B. Stolt, *On the Diophantine equation* $u^2 - Dv^2 = 4N$, Ark. för Mat. 2 (1951), 1–23.

[7] B. Stolt, *On a Diophantine equation of the second degree*, Ark. för Mat. 3 (1956), 381–390.