ACTA ARITHMETICA
* (201*)

On fundamental solutions of binary quadratic form equations

by

Keith R. Matthews (Brisbane and Canberra),
John P. Robertson (Boca Raton, FL)
and Anitha Srinivasan (Madrid)

1. Introduction. We consider the integer solutions (u, v) of the equation

$$Au^2 + Buv + Cv^2 = N, \tag{1.1}$$

where A, B, C, N are integers, $A > 0$, $N \neq 0$ and $D = B^2 - 4AC > 0$ is nonsquare.

If (u, v) is an integer solution of (1.1) and

$$u_1 = \frac{u(x - By)}{2} - Cvy, \qquad v_1 = \frac{v(x + By)}{2} + Auy, \tag{1.2}$$

where (x, y) satisfies Pell's equation

$$x^2 - Dy^2 = 4, \tag{1.3}$$

then (u_1, v_1) is also an integer solution of (1.1). Equations (1.2) can be written concisely as

$$(2Au_1 + Bv_1) + v_1\sqrt{D} = \frac{x + y\sqrt{D}}{2}(2Au + Bv + v\sqrt{D}), \tag{1.4}$$

and give an equivalence relation on the set of integer solutions of (1.1).

Among all solutions (u, v) in an equivalence class K, we choose a *fundamental* solution where v is the least nonnegative value of v when (u, v) belongs to K. Let $u' = -(Au+Bv)/A$ be the conjugate solution to u. If u' is not integral or if (u', v) is not equivalent to (u, v), this determines (u, v). If u' is integral and (u', v) is equivalent to (u, v), where $u \neq u'$, we choose $u > u'$. There are finitely many equivalence classes, each indexed by a fundamental solution.

2010 *Mathematics Subject Classification*: Primary 11A55, 11D09, 11D45.
Key words and phrases: Diophantine equation, indefinite binary quadratic form, equivalence class, fundamental solution.

Definition 1.1. Suppose (x_1, y_1) is the least positive solution of the Pell equation (1.3). Then

$$(V, U) = \begin{cases} (\sqrt{AN(x_1-2)/D}, \sqrt{AN(x_1+2)}\,) & \text{if } N > 0, \\ (\sqrt{A|N|(x_1+2)/D}, \sqrt{A|N|(x_1-2)}\,) & \text{if } N < 0. \end{cases}$$

In [6], Stolt gave the following necessary condition for (u, v) to be a fundamental solution.

Proposition 1.2. *Suppose* (u, v) *is a fundamental solution of the Diophantine equation* (1.1). *Then* $0 \le v \le V$.

This was a generalization of Theorems 108 and 108a of Nagell [4], who dealt with the equation $u^2 - dv^2 = N$, using the Pell equation $x^2 - dy^2 = 1$.

We give a refinement of the Stolt bounds which completely characterizes the fundamental solutions.

Theorem 1.3. *Suppose* (x_1, y_1) *is the least positive solution of Pell's equation* (1.3).

(a) *If* $N > 0$, *then an integer pair* (u, v) *satisfying* (1.1) *is a fundamental solution if and only if one of the following holds:*
  (i) $0 < v < V$.
  (ii) $v = 0$ *and* $u = \sqrt{N/A}$.
  (iii) $v = V$ *and* $u = (U - BV)/(2A)$.

(b) *If* $N < 0$, *then an integer pair* (u, v) *satisfying* (1.1) *is a fundamental solution if and only if one of the following holds:*
  (i) $\sqrt{4A|N|/D} \le v < V$.
  (ii) $v = V$ *and* $u = (U - BV)/(2A)$.

Remark 1.4. We note that U is an integer if V is an integer. Indeed,

$$U^2V^2 = A^2N^2(x_1^2 - 4)/D = A^2N^2y_1^2,$$

so $U^2 = (ANy_1/V)^2$ and hence $U = A|N|y_1/V$; also $U^2 = A|N|(x_1 \pm 2)$. Hence U is a rational number whose square is an integer, and this implies that U is an integer.

Remark 1.5. The Stolt bounds are useful for brute-force searches for fundamental solutions, but the continued fraction method of Matthews [2] for finding primitive fundamental solutions is more efficient.

2. The sets S and T. Let S be the set of integer solutions (u, v) of $Au^2 + Buv + Cv^2 = N$ that satisfy the conditions of Theorem 1.3. Also let T denote the set of fundamental solutions. Let R denote the real number points (u, v) of the hyperbola $Au^2 + Buv + Cv^2 = N$ that satisfy the conditions

(a) $0 < v < V$, or $(u,v) = (\sqrt{N/A}, 0)$, or $(u,v) = ((U - BV)/(2A), V)$, if $N > 0$.
(b) $\sqrt{4A|N|/D} \le v < V$, or $(u,v) = ((U - BV)/(2A), V)$, if $N < 0$.

Then Theorem 1.3 states that S consists of the integer points of R.

The bold sections of Figures 1 and 2 depict R, where $\circ$ and $\bullet$ denote points omitted and points left in, respectively.

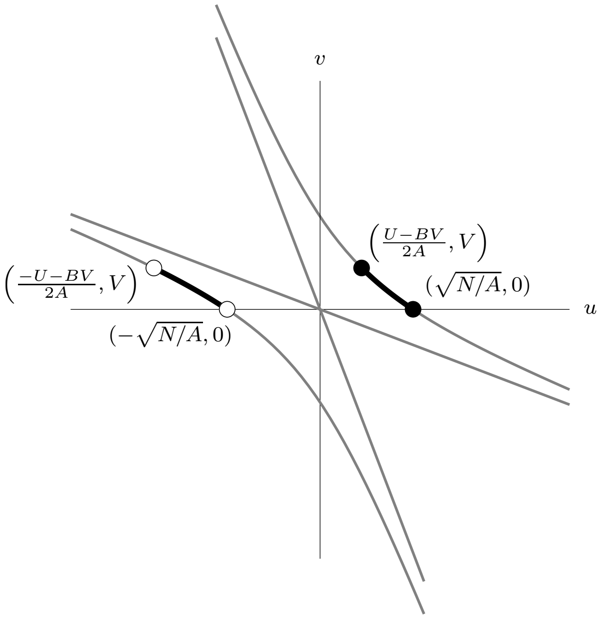

Fig. 1. Region R: $Au^2 + Buv + Cv^2 = N$, $A, N > 0$

Lemma 2.1 (Stolt [6, p. 383]). *Solutions* (u,v) *and* (u_1, v_1) *of* (1.1) *are equivalent if and only if the following congruences hold:*

$$2Auu_1 + B(uv_1 + u_1v) + 2Cvv_1 \equiv 0 \pmod{|N|}, \tag{2.1}$$

$$vu_1 - uv_1 \equiv 0 \pmod{|N|}. \tag{2.2}$$

Remark 2.2. Stolt also proved that (2.2) implies (2.1).

Proposition 2.3. *We have* $T \subseteq S$.

Proof. Suppose (u,v) is a fundamental solution. Then by Proposition 1.2, $0 \le v \le V$.

(i) If $v = V$, then $u = (U - BA)/(2A)$ or $(-U - BA)/(2A)$. However we see by Lemma 2.1 that these solutions are equivalent, so $u = (U - BA)/(2A)$.

(ii) If $N > 0$ and $v = 0$, then $u = \pm\sqrt{N/A}$. However $(-\sqrt{N/A}, 0)$ and $(\sqrt{N/A}, 0)$ are equivalent, so $u = \sqrt{N/A}$.

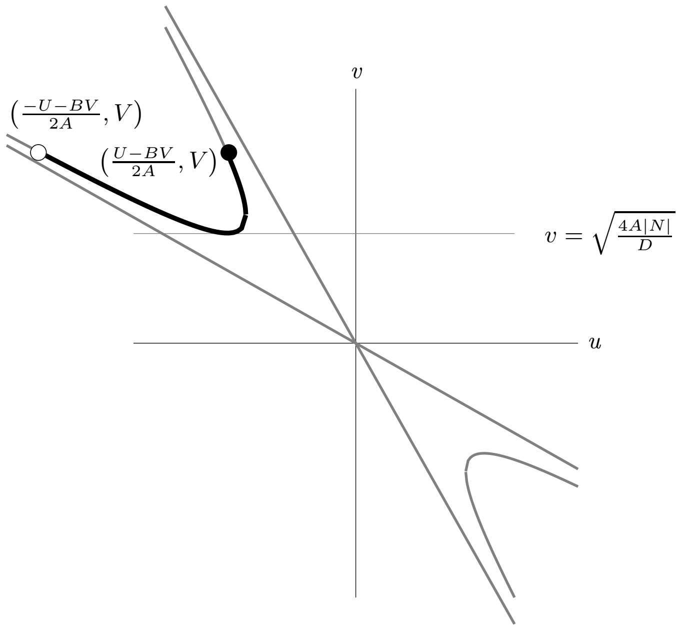

Fig. 2. Region R: $Au^2 + Buv + Cv^2 = N$, $A > 0$, $N < 0$

(iii) If $N < 0$, then $(2Au + Bv)^2 + 4A|N| = Dv^2$ and this implies that $v \geq \sqrt{4A|N|/D}$. ■

3. The proof of $S = T$. Proposition 3.1 below implies that distinct points of S belong to distinct equivalence classes, which in turn have distinct fundamental solutions, so it follows that $|S| \leq |T|$. But by Proposition 2.3, we have $T \subseteq S$. Hence $S = T$.

PROPOSITION 3.1. *Suppose (u, v) and (u_1, v_1) are distinct equivalent solutions of equation* (1.1) *where $0 \leq v, v_1 \leq V$. Then one of the following holds:*

(i) *$N > 0$, $v = v_1 = 0$ and $u = -u_1 = \pm\sqrt{N/A}$;*
(ii) *$v = v_1 = V$ and $u = (\epsilon U - BV)/(2A)$, $u_1 = (-\epsilon U - BV)/(2A)$, where $\epsilon = \pm 1$.*

Proof. We have

$$(2Au + Bv + v\sqrt{D})(2Au_1 + Bv_1 - v_1\sqrt{D})$$
$$= 2A(2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1) + 2A(vu_1 - uv_1)\sqrt{D}.$$

Hence as (x_1, y_1) is the least solution of (1.3), we have

$$\left(\frac{2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1}{N}\right)^2 - D\left(\frac{vu_1 - uv_1}{N}\right)^2 = 4,$$

where $(2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1)/N$ and $(vu_1 - uv_1)/N$ are integers by Lemma 2.1. Therefore

(a) $vu_1 - uv_1 = 0$ and $|2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1| = 2|N|$, or
(b) $|2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1| \geq |N|x_1$.

Case (a). Suppose $vu_1 = uv_1$. Then $u \neq 0$, as $u = 0$ implies $vu_1 = 0$. Now $v = 0$ and equation (1.1) would imply $N = 0$; also $u_1 = 0$ implies $v = v_1$, and so $(u, v) = (u_1, v_1)$. Similarly $u_1 \neq 0$. Hence $v_1/u_1 = v/u$ and

$$\frac{N}{u^2} = A + B\frac{v}{u} + C\left(\frac{v}{u}\right)^2 = A + B\frac{v_1}{u_1} + C\left(\frac{v_1}{u_1}\right)^2 = \frac{N}{{u_1}^2}.$$

So $u = \pm u_1$ and $v = v_1$. Consequently, $u = -u_1$, $v = 0$ and $Au^2 = N$. Hence $N > 0$ and $u = \pm\sqrt{N/A}$.

Case (b). Suppose $|2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1| \geq |N|x_1$. Then if $v \leq V$, we have

$$\begin{aligned}(2Au + Bv)^2 &= 4AN + Dv^2 \leq 4AN + DV^2 \\ &= \begin{cases} 4AN + AN(x_1 - 2) = AN(x_1 + 2) = U^2 & \text{if } N > 0, \\ 4AN + A|N|(x_1 + 2) = A|N|(x_1 - 2) = U^2 & \text{if } N < 0. \end{cases}\end{aligned}$$

Hence in both subcases, we have $|2Au + Bv| \leq U$. Also

$$\begin{aligned}|N|x_1 &\leq |2Auu_1 + B(uv_1 + vu_1) + 2Cvv_1| \\ &= \left|\frac{(2Au + Bv)(2Au_1 + Bv_1) - Dvv_1}{2A}\right| \\ &\leq \frac{|(2Au + Bv)(2Au_1 + Bv_1)| + Dvv_1}{2A} \\ &\leq \frac{U^2 + DV^2}{2A} = \frac{A|N|(x_1 \mp 2) + A|N|(x_1 \pm 2)}{2A} = |N|x_1.\end{aligned}$$

It follows that $v = v_1 = V$ and $|2Au + Bv| = U = |2Au_1 + Bv|$. Hence $2Au + Bv = \epsilon U$ and $2Au_1 + Bv = -\epsilon U$, where $\epsilon = \pm 1$. This gives $u = (\epsilon U - BV)/(2A)$ and $u_1 = (-\epsilon U - BV)/(2A)$. ∎

4. The equation $u^2 - dv^2 = N$. We deal with the special case of equation (1.1) studied by Nagell in his paper [3] and book [4], and by Chebyshev [7], namely the equation

$$u^2 - dv^2 = N. \tag{4.1}$$

Here $A = 1$, $B = 0$ and $C = -d$, where $d > 0$ is not a perfect square and N is nonzero. Then $D = 4d$, and the equivalence relation (1.2) between two integer solutions $(u, v), (u_1, v_1)$ of equation (4.1) simplifies to

$$u_1 + v_1\sqrt{d} = (u + v\sqrt{d})(x + y\sqrt{d}), \tag{4.2}$$

where (x, y) satisfies Pell's equation

$$x^2 - dy^2 = 1. \tag{4.3}$$

The definition of a fundamental solution (u, v) in a class K is simpler here, as v is the least nonnegative value of v, and if (u, v) and $(-u, v)$, $u > 0$, belong to the same class, we choose (u, v). Then Theorem 1.3 simplifies to:

THEOREM 4.1. *Suppose (x_0, y_0) is the least positive solution of Pell's equation* (4.3).

(a) *If $N > 1$, then an integer pair (u, v) satisfying* (4.1) *is a fundamental solution if and only if one of the following holds:*
  (i) $0 < v < y_0\sqrt{N/(2(x_0+1))}$.
  (ii) $v = 0$ *and* $u = \sqrt{N}$.
  (iii) $v = y_0\sqrt{N/(2(x_0+1))}$ *and* $u = \sqrt{N(x_0+1)/2}$.

(b) *If $N < 0$, then an integer pair (u, v) satisfying* (4.1) *is a fundamental solution if and only if one of the following holds:*
  (i) $\sqrt{|N|/D} \le v < y_0\sqrt{|N|/(2(x_0-1))}$.
  (ii) $v = y_0\sqrt{|N|/(2(x_0-1))}$ *and* $u = \sqrt{|N|(x_0-1)/2}$.

REMARK 4.2. The restriction $N > 1$ is imposed because there is only one fundamental solution $(1, 0)$ when $N = 1$, and in this case tradition has reserved the name *fundamental solution* for the least positive solution (x_0, y_0) of the Pell equation (4.3).

Let R_0 be the real number points (u, v) on the hyperbola $u^2 - Dv^2 = N$ that satisfy the conditions

(a) $0 < v < V_0$, or $(u, v) = (\sqrt{N}, 0)$, or $(u, v) = (U_0, V_0)$, if $N > 1$,
(b) $\sqrt{|N|/D} \le v < V_0$, or $(u, v) = (U_0, V_0)$, if $N < 0$,

where

$$(U_0, V_0) = \begin{cases} \left(\sqrt{\dfrac{N(x_0+1)}{2}},\ y_0\sqrt{\dfrac{N}{2(x_0+1)}}\right) & \text{if } N > 1, \\ \left(\sqrt{\dfrac{|N|(x_0-1)}{2}},\ y_0\sqrt{\dfrac{|N|}{2(x_0-1)}}\right) & \text{if } N < 0. \end{cases}$$

The bold sections of Figures 3 and 4 depict R_0, where $\circ$ and $\bullet$ denote points omitted and points left in, respectively. Then Theorem 4.1 states that S_0, the set of fundamental solutions, consists of the integer points of R_0.

REMARK 4.3. Tsangaris [8, 9] proved that if (u, v) satisfies the bounds of Chebyshev and Nagell, then v is the least nonnegative value of v in the class determined by (u, v). His claim that (u, v) is a fundamental solution is

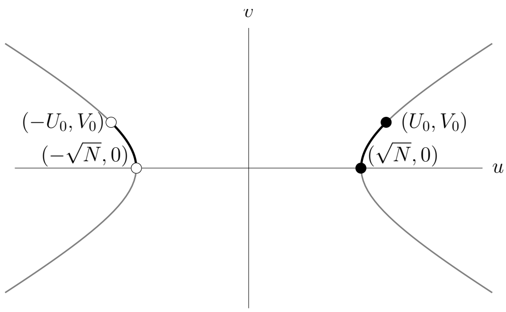

Fig. 3. Region R_0: $u^2 - Dv^2 = N$, $N > 0$

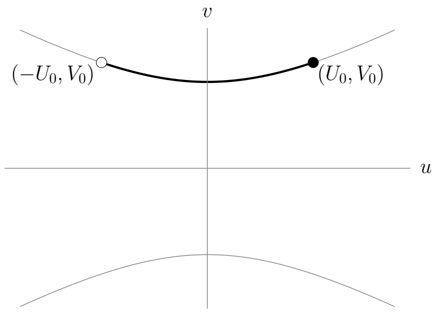

Fig. 4. Region R_0: $u^2 - Dv^2 = N$, $N < 0$

not quite correct if $u \neq 0$ and (u, v) and $(-u, v)$ are in the same class, for then only $(|u|, v)$ is a fundamental solution.

5. Numerical examples. The first four are from Stolt's paper [6, p. 389].

EXAMPLE 5.1. $209u^2 + 29uv + v^2 = 31$. Here $D = 5$, $(x_1, y_1) = (3, 1)$ and $\sqrt{N/A} = \sqrt{31/209} = 0.38\ldots$ and $V = 35.99\ldots$. Hence the fundamental solutions lie in the range $1 \leq v \leq 35$. We find solutions $(-2, 23)$ and $(-2, 35)$.

EXAMPLE 5.2. $u^2 + 3uv + v^2 = 5$. Here $D = 5$, $(x_1, y_1) = (3, 1)$, $\sqrt{N/A} = \sqrt{5} = 2.23\ldots$ and $V = 1$, $U = 5$, $(U - BV)/(2A) = 1$, and $(1, 1)$ is a fundamental solution with $1 \leq v \leq 1$. In fact $(1, 1)$ is a solution.

EXAMPLE 5.3. $3u^2 + 7uv + 3v^2 = -13$. Here $D = 13$, $(x_1, y_1) = (11, 3)$ and $\sqrt{4A|N|/D} = \sqrt{12} = 3.46\ldots$, $V = 6.24\ldots$, and the fundamental solutions lie in the range $4 \leq v \leq 6$. We find one solution $(-8, 5)$.

EXAMPLE 5.4. $2u^2 + 5uv + v^2 = 16$. Here $D = 17$, $(x_1, y_1) = (66, 16)$ and $\sqrt{N/A} = \sqrt{8} = 2.82\ldots$, $V = 10.97\ldots$, and the fundamental solutions lie in the range $1 \leq v \leq 10$, with solutions $(-6, 2), (1, 2), (-10, 4), (0, 4), (-1, 7)$.

EXAMPLE 5.5. $121u^2+73uv+11v^2 = 5$. Here $D = 5$, $(x_1, y_1) = (3, 1)$ and $\sqrt{N/A} = \sqrt{5/121} = 0.20\ldots$, $V = 11$, $U = 55$, $(U - BV)/(2A) = -3.09\ldots$, and the fundamental solutions lie in the range $1 \le v \le 10$. We find one solution $(-1, 4)$.

EXAMPLE 5.6. $121u^2 + 73uv + 11v^2 = -1$. Here $D = 5$, $(x_1, y_1) = (3, 1)$ and $\sqrt{4A|N|/D} = 9.83\ldots$, $V = 11$, $U = 11$, $(U - BV)/(2A) = -3.27\ldots$, and the fundamental solutions lie in the range $10 \le v \le 10$. We find one solution $(-3, 10)$.

EXAMPLE 5.7 (Lagrange [5, pp. 471–485]). The equation is $u^2 - 46v^2 = 210$. Here $d = 46$, $(x_0, y_0) = (24335, 3588)$, $\sqrt{N} = 14.49\ldots$, $V_0 = 235.67\ldots$, so the fundamental solutions lie in the range $1 \le v \le 235$. We find solutions

$$(\pm 16, 1),\ (\pm 76, 11),\ (\pm 292, 43),\ (\pm 536, 79).$$

EXAMPLE 5.8 (Frattini [1, p. 179]). The equation is $u^2 - 13v^2 = -12$. Here $d = 13$, $(x_0, y_0) = (649, 180)$, $\sqrt{|N|/D} = 0.95\ldots$ and $V_0 = 17.32\ldots$. Hence the fundamental solutions lie in the range $1 \le v \le 17$. We find solutions

$$(\pm 1, 1),\ (\pm 14, 4),\ (\pm 25, 7).$$

EXAMPLE 5.9. $u^2 - 96v^2 = 4$. Here $d = 96$, $(x_0, y_0) = (49, 5)$, $\sqrt{N} = 2$, $V_0 = 1$, $U_0 = 10$, and $(\sqrt{N}, 0) = (2, 0)$ and $(U_0, V_0) = (10, 1)$ are the fundamental solutions.

EXAMPLE 5.10. $u^2 - 96v^2 = -96$. Here $d = 96$, $(x_0, y_0) = (49, 5)$, $\sqrt{|N|/d} = 1$, $V_0 = 5$, $U_0 = 48$, and $(0, \sqrt{|N|/d}) = (0, 1)$ and $(U_0, V_0) = (48, 5)$ are the fundamental solutions. No further solutions lie in the range $1 \le v \le 4$.

References

[1] G. Frattini, *Dell'analisi indeterminata di secondo grado*, Periodico di Mat. 6 (1891) 169–180.

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

[3] T. Nagell, *Bemerkung über die diophantische Gleichung $u^2 - Dv^2 = C$*, Arch. Math. (Basel) 3 (1952), 8–9.

[4] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981.

[5] J.-A. Serret (ed.), *Oeuvres de Lagrange*, tome 2, Gauthier-Villars, Paris, 1868.

[6] B. Stolt, *On a Diophantine equation of the second degree*, Ark. Mat. 3 (1957), 381–390.

[7] P. Tchebichef, *Sur les formes quadratiques*, J. Math. Pures Appl. 16 (1851), 257–282.

[8] P. G. Tsangaris, *Prime numbers and cyclotomy—primes of the form $x^2 + (x + 1)^2$*, Ph.D. thesis, Athens Univ., Athens, 1984.

[9] P. G. Tsangaris, *Fermat–Pell equation and the numbers of the form $w^2 + (w + 1)^2$*, Publ. Math. Debrecen 47 (1995), 127–138.

Keith R. Matthews
Department of Mathematics
University of Queensland
Brisbane 4072, Australia
and
Centre for Mathematics and its Applications
Australian National University
Canberra, ACT 0200, Australia
E-mail: keithmatt@gmail.com

John P. Robertson
Actuarial and Economic Services Division
National Council on Compensation Insurance
Boca Raton, FL 33487, U.S.A.
E-mail: jpr2718@gmail.com

Anitha Srinivasan
Department of Mathematics
Saint Louis University – Madrid campus
Avenida del Valle 34
28003 Madrid, Spain
E-mail: rsrinivasan.anitha@gmail.com

Received on 6.1.2015 (8048)

Abstract (will appear on the journal's web site only)

We show that, with suitable modification, the upper bound estimates of Stolt for the fundamental integer solutions of the Diophantine equation $Au^2 + Buv + Cv^2 = N$, where $A > 0$, $N \neq 0$ and $B^2 - 4AC$ is positive and nonsquare, in fact characterize the fundamental solutions. As a corollary, we get a corresponding result for the equation $u^2 - dv^2 = N$, where d is positive and nonsquare, in which case the upper bound estimates were obtained by Nagell and Chebyshev.