

# The Number of Bounded Solutions of Norm-Form Equations Via Pell Equations and Ambiguous Classes of Solutions\*

R.A. Mollin

## Abstract

We find the number of solutions of norm-form equations  $x^2 - Dy^2 = c$  for positive non-square integers  $D$ , which are less than a certain bound related to Pell's equations  $x^2 - Dy^2 = \pm 1$  and based upon the ambiguous classes of solutions to the norm-form. This generalizes recent results in the literature.

## 1 Introduction

In previous work, such as [4]–[5], we found criteria for the solutions of norm-form equations in terms of continued fractions. However, more recently, work by Pihko in [2] focused on the number of solutions less than a certain bound, defined below. We completely generalize these results and show how this is related to ambiguous classes, also defined below, which is not mentioned in [2], but really reveals the underlying reasons for this phenomenon to occur. Of course, the Pell equations and norm-form equations have a long and distinguished history, which can be found, for instance in Dixon's work [1].

---

\*Mathematics Subject Classification 2000: Primary: ; Secondary: Key words and phrases: Pell's Equation, Norm-Form Equations, Quadratic Extensions, Classes of Solutions.

## 2 Norm-Form Equations

Let  $(T, U)$  be the fundamental solution of

$$x^2 - Dy^2 = 1 \tag{2.1}$$

and let  $(t, u)$  be the fundamental solution of

$$x^2 - Dy^2 = -1 \tag{2.2}$$

where  $D$  is a positive nonsquare integer. Also, set  $T_i + U_i\sqrt{D} = (T + U\sqrt{D})^i$  and  $t_i + u_i\sqrt{D} = (t + u\sqrt{D})^i$  for any integer  $i$ .

Let  $c > 1$  and  $N \geq 1$  be fixed integers. We call a solution  $(a, b)$  of  $x^2 - Dy^2 = \pm c$  to be *trivial* if  $c \mid a^2$ . In what follows, we only consider positive solutions that are *nontrivial*, namely those for which  $c$  does not divide  $a^2$ .

Define  $F(D, c, N)$  to be the number of positive solutions of

$$x^2 - Dy^2 = c \tag{2.3}$$

which are smaller than  $(T_N\sqrt{c}, U_N\sqrt{c})$ , and  $f(D, c, N)$  to be the number of positive solutions of

$$x^2 - Dy^2 = -c \tag{2.4}$$

that are smaller than  $(t_N\sqrt{c}, u_N\sqrt{c})$ .

**Theorem 2.1** *Let  $\mathcal{S}$  be the set of all solutions of Equation (2.3) that are less than  $(T_N\sqrt{c}, U_N\sqrt{c})$ .*

1. *Then if  $\mathcal{S}$  has no element from an ambiguous classes of solutions, then  $2 \mid F(D, c, N)$ .*
2. *If Equation (2.2) has solutions, then  $F(D, c, N) = 2f(D, c, N)$ .*

*Proof.* To establish part 1, we first show the following.

**Claim 2.1** *If  $(a, b)$  is a solution of Equation (2.3), then  $(a, b) \in \mathcal{S}$  if and only if  $(aT_N - U_NbD, aU_N - T_Nb) \in \mathcal{S}$ .*

Suppose that  $(a, b) \in \mathcal{S}$ . Since

$$N((a - b\sqrt{D})(T_N + U_N\sqrt{D})) = (a^2 - b^2D)(T_N^2 - U_N^2D) = c,$$

then

$$(a - b\sqrt{D})(T_N + U_N\sqrt{D}) = (aT_N - U_NbD) + (aU_N - T_Nb)\sqrt{D}$$

is a solution of (2.3). Thus, we need only show that

$$0 < aT_N - U_NbD < T_N\sqrt{c}, \quad (2.5)$$

and

$$0 < aU_N - T_Nb < U_N\sqrt{c}. \quad (2.6)$$

To this end, we first establish the following

**Claim 2.2** *If  $aU_N - T_Nb < U_N\sqrt{c}$ , then  $aT_N - U_NbD < T_N\sqrt{c}$ .*

From the fact that  $(aT_N - U_NbD, aU_N - T_Nb)$  is a solution of (2.3), we have,

$$(aT_N - U_NbD)^2 = (aU_N - T_Nb)^2D + c < U_N^2Dc + c = (U_N^2 + 1)c = T_N^2c,$$

so

$$|aT_N - U_NbD| < T_N\sqrt{c},$$

which secures Claim 2.2.

By Claim 2.2, it suffices to show that (2.6) holds and  $aT_N - U_NbD > 0$  in order to secure the sufficiency of Claim 2.1.

We have that

$$\begin{aligned} (aU_N + T_Nb)(aU_N - T_Nb) &= a^2U_N^2 - T_N^2b^2 = (b^2D + c)U_N^2 - T_N^2b^2 = \\ &= (DU_N^2 - T_N^2)b^2 + cU_N^2 = U_N^2c - b^2 > 0 \end{aligned}$$

since  $b < U_N\sqrt{c}$ . Hence,  $aU_N - T_Nb > 0$ . Suppose that  $aU_N - T_Nb \geq U_N\sqrt{c}$ . Then we get the contradiction,

$$U_N^2c > U_N^2c - b^2 = (aU_N + T_Nb)(aU_N - T_Nb) \geq (aU_N)(U_N\sqrt{c}) \geq U_N^2c, \quad (2.7)$$

where the first inequality follows from  $b > 0$ , and last inequality follows from the fact that  $a^2 > a^2 - b^2D = c$ . This secures (2.6). Lastly, we establish that  $aT_N - U_NbD > 0$ . Suppose that  $aT_N - U_NbD < 0$ . Then

$$\begin{aligned} 0 > (aT_N - U_NbD)(aT_N + U_NbD) &= a^2T_N^2 - U_N^2b^2D^2 = a^2(U_N^2D + 1) - U_N^2b^2D^2 \\ &= U_N^2D(a^2 - b^2D) + a^2 = U_N^2Dc + a^2 > 0. \end{aligned}$$

This contradiction secures the sufficiency of Claim 2.1.

To prove the necessity of Claim 2.1, we apply the sufficiency to  $(a', b') = (aT_N - U_NbD, aU_N - T_Nb) \in \mathcal{S}$ . Thus,  $(a'T_N - U_Nb'D, a'U_N - T_Nb') \in \mathcal{S}$ . However,

$$\begin{aligned} a'T_N - U_Nb'D &= (aT_N - U_NbD)T_N - U_N(aU_N - T_Nb) = \\ aT_N^2 - T_NU_NbD - aU_N^2D + U_NT_NbD &= a(T_N^2 - U_N^2D) = a, \end{aligned}$$

and

$$\begin{aligned} a'U_N - T_Nb' &= (aT_N - U_NbD)U_N - T_N(aU_N - T_Nb) = \\ aT_NU_N - U_N^2bD - aT_NU_N + T_N^2b &= (T_N^2 - U_N^2D)b = b. \end{aligned}$$

This secures Claim 2.1.

**Claim 2.3**

$$a = aT_N - U_NbD, \tag{2.8}$$

*if and only if*

$$b = aU_N - T_Nb. \tag{2.9}$$

If (2.8) holds, then  $aT_N = aT_N^2 - T_NU_NDb$ , so

$$aT_N - a = aT_N^2 - a - T_NU_NDb = a(T_N^2 - 1) - T_NU_NDb = aU_N^2D - T_NU_NDb.$$

Thus,  $(aT_N - a)/(U_ND) = aU_N - T_Nb$ . However, since (2.8) holds, then  $(aT_N - a)/(U_ND) = b$ . If Equation (2.9) holds, then  $a = (b + T_Nb)/U_N = b(T_N + 1)/U_N$ , so

$$\begin{aligned} aT_N - U_NbD &= \frac{b(T_N + 1) - U_N^2bd}{U_N} = \frac{bT_N^2 + bT_N - U_N^2bD}{U_N} = \\ \frac{b(T_N^2 - U_N^2D) + bT_N}{U_N} &= \frac{b + bT_N}{U_N} = \frac{b(T_N + 1)}{U_N} = a, \end{aligned}$$

which establishes Claim 2.3.

**Claim 2.4** *If  $(a, b) \in \mathcal{S}$ , then  $a = aT_N - U_NbD$  if and only if  $(a, b)$  is element from an ambiguous class of solutions.*

If  $a = aT_N - U_NbD$ , then by Claim 2.9,  $b = aU_N - T_Nb$ , so

$$(a + b\sqrt{D})(-T_N + U_N\sqrt{D}) = -aT_N + bU_ND + (U_Na - T_Nb)\sqrt{D} = -a + b\sqrt{D},$$

so  $(a, b)$  and  $(-a, b)$  are in the a same class.

If  $(a, b) \in \mathcal{S}$  is an element from an ambiguous class, then there is an integer  $N$  such that  $\pm(T_N + U_N\sqrt{D})$  is a unit with  $\pm(T_N + U_N\sqrt{D})(a + b\sqrt{D}) = -a + b\sqrt{D}$ . However, if we have the plus sign then this is not possible since for  $N > 0$ , the constant term is positive, and for  $N < 0$  the constant term is positive by Claim 2.1. Thus, we must have the negative sign. In this case  $N > 0$  is not possible since then the coefficient of  $\sqrt{D}$  is negative. Hence only  $N < 0$  is possible and the negative sign, for which we get that  $a = T_N - U_NbD$ , which proves Claim 2.4.

By hypothesis, Claim 2.4 tells us that

$$\text{if } (a, b) \in \mathcal{S} \text{ then } (aT_N - U_NbD, aU_N - T_Nb) \notin \mathcal{S} \text{ when } a = aT_N - U_NbD.$$

However, by Claim 2.1 one of them is in  $\mathcal{S}$  if and only if the other is in  $\mathcal{S}$ . Hence, elements of  $\mathcal{S}$  may be paired with distinct elements of  $\mathcal{S}$  in a one-to-one fashion. In other words,  $2 \mid F(D, c, N) = |\mathcal{S}|$ , which completes part 1.

Now we establish part 2. If  $\mathcal{T}$  is the set of all solutions of Equation (2.4) that are less than  $(t_N\sqrt{c}, u_N\sqrt{c})$ , then  $|\mathcal{T}| = f(D, c, N)$ .

**Claim 2.5** *If  $(a, b) \in \mathcal{S}$ , then  $(A, B) \in \mathcal{T}$  where  $A = |t_Na - u_NDb|$  and  $B = u_Na - t_Nb$ .*

Since

$$N((t_N + u_N\sqrt{D})(a - b\sqrt{D})) = N(A + B\sqrt{D}) = -c,$$

then  $(A, B)$  is a solution of Equation (2.4). Also, by Equation (2.12),

$$\begin{aligned} B = u_Na - t_Nb &= \frac{b(1 - u_N^2D) + 2t_Nu_Na - t_N^2b}{2t_N} = \\ &= \frac{b + 2t_Nu_Na - (t_N^2 + u_N^2D)b}{2t_N} = \frac{b + U_Na - T_Nb}{2t_N}. \end{aligned}$$

Therefore, if  $(a, b) \in \mathcal{S}$ ,  $b > 0$ , then by Claim 2.1,  $U_N a - T_N b > 0$ , so  $B > 0$ . Assume that  $B = u_N a - t_N b \geq u_N \sqrt{c}$ . Then

$$u_N^2 a^2 \geq t_N^2 b^2 + u_N^2 c + 2t_N u_N b \sqrt{c} = t_N^2 b^2 + u_N b \sqrt{c} + u_N^2 (a^2 - b^2 D).$$

Therefore, by Equation (2.12),

$$u_N^2 b^2 D - t_N^2 b^2 \geq U_N b \sqrt{c} b,$$

so  $b \geq U_N \sqrt{c}$  contradicting that  $(a, b) \in \mathcal{S}$ , so we have shown that

$$0 < B < u_N \sqrt{c}.$$

It remains to show that  $0 < A < t_N \sqrt{c}$  to establish Claim 2.5. If  $A = 0$ , then  $c \mid a^2$  contradicting that we have a nontrivial solution, so  $A > 0$ . Also, by the above,  $A^2 = B^{\circledast} D - c < D u_N^2 c - c = c(D u_N^2 - 1) = c t_N^2$ . Thus,  $A < t_N \sqrt{c}$ , which secures Claim 2.5.

**Claim 2.6** *If  $(A, B) \in \mathcal{T}$ , then both*

$$(a, b) = (-t_N A + u_N D B, t_N B - u_N A) \in \mathcal{S} \quad (2.10)$$

and

$$(a', b') = (t_N A + u_N D B, u_N A + t_N B) \in \mathcal{S}. \quad (2.11)$$

Let  $(A, B) \in \mathcal{T}$ . Since

$$N(t_N + u_N \sqrt{D})(-A + B \sqrt{D}) = N(-t_N A + u_N D B + (u_N A + t_N B) \sqrt{D}) = c,$$

and

$$N(t_N + u_N \sqrt{D})(A + B \sqrt{D}) = N(t_N A + u_N D B + (u_N A + t_N B) \sqrt{D}) = c,$$

then  $(a, b)$  and  $(a', b')$  are solutions of Equation (2.3). Thus, to establish (2.10)–(2.11), it suffices to show that

$$0 < a, a' < T_N \sqrt{c} \text{ and } 0 < b, b' < U_N \sqrt{c}.$$

Clearly,  $a' > 0$  and  $b' > 0$ . Also, since  $(A, B) \in \mathcal{T}$ , then

$$b' = u_N A + t_N B < u_N t_N \sqrt{c} + t_N u_N \sqrt{c} = 2u_N t_N \sqrt{c} = U_N \sqrt{c},$$

since

$$T_N + U_N\sqrt{D} = (t_N + u_N\sqrt{D})^2 = t_N^2 + u_N^2D + 2u_Nt_N\sqrt{D}. \quad (2.12)$$

Therefore,

$$(a')^2 = D(b')^2 + c < DU_N^2c + c = c(DU_N^2 + 1) = cT_N^2.$$

Thus, we have established (2.11).

To establish (2.10), we employ Claim 2.1. Assume first that

$$aT_N - U_NbD \geq \sqrt{c}T_N.$$

Therefore,

$$a^2T_N^2 + U_N^2b^2D^2 - 2T_NU_NbD \geq cT_N^2.$$

However,

$$\begin{aligned} a^2T_N^2 + U_N^2b^2D^2 - 2T_NU_NbD &= a^2T_N^2 + b^2(T_N^2 - 1)D - 2T_NU_NbD = \\ T_N^2(a^2 - b^2D) - b^2D - 2T_NU_NbD &= T_N^2c - b^2D - 2T_NU_NbD < T_N^2c, \end{aligned}$$

a contradiction. Hence,

$$aT_N - U_NbD < \sqrt{c}T_N. \quad (2.13)$$

Now assume that  $aU_N - T_Nb \geq \sqrt{c}U_N$ . Therefore, we get a contradiction in exactly the same fashion as the argument in (2.7).

If  $aT_N - U_NbD < 0$ , then

$$\begin{aligned} 0 > aT_N^2 - U_N^2b^2D^2 &= a^2T_N^2 - b^2D(T_N^2 - 1) = aT_N^2 - b^2DT_N^2 + b^2D = \\ T_N^2(a^2 - b^2D) + b^2D &= cT_N^2 + b^2D > 0, \end{aligned}$$

a contradiction. Hence, by Claim 2.1, we have (2.10) and so Claim 2.6.

Let  $\mathcal{S}_1$  be the set of all positive solutions  $(a, b)$  of Equation (2.3) such that  $(A, B) = (t_Na - u_NDb, u_Na - t_Nb) \in \mathcal{T}$ , and let  $\mathcal{S}_2$  be the set of all solutions  $(a', b')$  of Equation (2.3) such that  $(A, B) = (u_NDb' - t_Na', u_Na' - t_Nb') \in \mathcal{T}$ . If  $(a, b) = (a', b') \in \mathcal{S}_1 \cap \mathcal{S}_2$ , then  $t_Na - u_NDb = u_NDb - t_Na$ , which means that  $t_Na = u_NDb$ . Therefore,

$$c = a^2 - b^2D = \left( \frac{u_NDb}{t_N} \right)^2 - b^2D = \frac{u_N^2D^2b^2 - t_N^{\textcircled{a}}b^2D}{t_N^2} =$$

$$\frac{b^2 D(u_N^{\textcircled{a}} D - t_N^2)}{t_N^2} = \frac{-b^2 D}{t_N^2},$$

so  $t_N^2 c = -b^2 D$ . Thus,  $c \mid b^2 D$ , so  $c \mid a^2$ , which contradicts that we have a nontrivial solution. Hence  $\mathfrak{S}_1 \cap \mathfrak{S}_2 = \emptyset$ . Moreover, by Claim 2.6,  $\mathfrak{S}_1 \cup \mathfrak{S}_2 \subseteq \mathfrak{S}$  and by Claim 2.5,  $\mathfrak{S} \subseteq \mathfrak{S}_1 \cup \mathfrak{S}_2$ , so  $\mathfrak{S} = \mathfrak{S}_1 \cup \mathfrak{S}_2$ . Thus,  $F(D, c, N) = 2f(D, c, N)$ . Note, as well that by Claim 2.5,  $F(D, c, N) = 0$  if and only if  $f(D, c, N) = 0$ . This secures the entire result.  $\square$

**Corollary 2.1** ([2, Theorem 1, p. 402])

*If  $c = n^2 > 1$  for  $n \in \mathbb{N}$  and  $2(T_N + 1)$  is not a perfect square, then  $2 \mid F(D, c, N)$ .*

*Proof.* We begin with the following key result. If  $(a, b) \in \mathfrak{S}$ , then

**Claim 2.7**  $2(T_N + 1) = z^2$  for some  $z \in \mathbb{N}$  if and only if  $2b^2(T_N + 1) = U_N^2 n^2$ .

By Claims 2.3–2.4,  $\mathfrak{S}$  has an element in an ambiguous class if and only if  $b = aU_N - T_N b$ , and this holds if and only if  $aU_N = b + T_N b = (T_N + 1)b$  if and only if  $U_N^2 a^2 = (T_N + 1)^2 b^2$  if and only if

$$U_N^2 n^2 = [(T_N + 1)^2 - DU_N^2] b^2 = (T_N^2 - DU_N^2 + 2N + 1) b^2 = 2b^2(T_N + 1),$$

so  $2(T_N + 1) = U_N^2 n^2 / b^2 = z^2$ . Thus, by Theorem 2.1, if  $2(T_N + 1)$  is not a perfect square, then  $2 \mid F(D, c, N)$   $\square$

**Corollary 2.2** [Pihko, [2, Theorem 2, p. 402]]

*If  $c = n^2 > 1$  for some  $n \in \mathbb{N}$  and Equation (2.2) has solutions then  $2(T_N + 1)$  is not a perfect square.*

*Proof.* By Claim 2.7,  $2(T_N + 1) = z^2$  for some  $z \in \mathbb{N}$  if and if  $2b^2(T_N + 1) = U_N^2 z^2$ . Hence, by Equation (2.12),  $U_N^2 n^2 = 2b^2(T_N + 1) = 2b^2(t_N^2 + u_N^2 D + 1) = 2b^2(2t_N^2 + 2) = 4(t_N^2 + 1)$ , which cannot be a perfect square.  $\square$

In [2, p.405], classes of radicands  $D$  are cited where  $2(T_N + 1)$  is not a perfect square. However, it is not mentioned that these are special cases of the well-known and studied *Richud-Degert* types,  $D = m^2 + r$  where  $r \mid 4m$ , see [3], for instance.

However, by Theorem 2.1, we can say much more than Corollary 2.2.

**Corollary 2.3** *If Equation (2.2) has solutions, then  $\mathcal{S}$  has no element from an ambiguous class.*

**Acknowledgements:** The author's research is supported by NSERC Canada grant # A8484.

## References

- [1] L.E. Dixon, **Theory of Numbers Vol. II**, Chelsea, (1992).
- [2] J. Pihko, *Even and Odd Remarks on Pell's Equation*, JP Jour. Algebra, Number Theory and Appl., **5** (2005), 401–411.
- [3] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, New York, London, Tokyo (1996).
- [4] R.A. Mollin, *All Solutions of the Diophantine Equation*, Far East J. Math. Sci., Special Volume (1998), Part III, 257–293.
- [5] R.A. Mollin, *Norm Form Equations and Continued Fractions*, Acta Math. Univ. Comenianae **LXXIV** (2005), 273–278.

Department of Mathematics and Statistics  
University of Calgary  
Calgary, Alberta  
Canada, T2N 1N4  
URL: <http://www.math.ucalgary.ca/~ramollin/>  
E-mail: [ramollin@math.ucalgary.ca](mailto:ramollin@math.ucalgary.ca)