Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
25 (2009), 155–164
www.emis.de/journals
ISSN 1786-0091

ON D SO THAT $x^2 - Dy^2$ REPRESENTS m AND $-m$ AND NOT -1

JOHN P. ROBERTSON

Abstract. For $m = 25$, 100, p, $2p$, $4p$, or $2p^2$, where p is prime, we show that there is at most one positive nonsquare integer D so that the form $x^2 - Dy^2$ primitively represents m and $-m$ and does not represent -1. We give support for a conjecture that for any $m > 1$ not listed above, there are infinitely many D so that the form $x^2 - Dy^2$ primitively represents m and $-m$ and does not represent -1.

1. Introduction

It is well known that if $F = x^2 - Dy^2$ represents m and -1, then F represents $-m$ [13, p. 14]. It is also well known that there are D and m so that F represents m and $-m$, but does not represent -1, for example $D = 34$, $m = 33$.

The article [11] shows that for any integer $m \neq 0$, ± 2 there are infinitely many D so that $x^2 - Dy^2$ primitively represents m, $-m$, and -1. In this article we show that for certain integers m there are only finitely many D so that $x^2 - Dy^2$ primitively represents m and $-m$, and does not represent -1. Based on empirical evidence, I conjecture that for any integer $m > 1$ that is not 25, 100, p, $2p$, $4p$, or $2p^2$, for p a prime, there are infinitely many D so that $x^2 - Dy^2$ primitively represents m and $-m$ and does not represent -1.

Given an integer m, call an integer $D > 0$, not a square, *good* if $x^2 - Dy^2$ primitively represents m and $-m$ and does not represent -1. For the following we give proofs or references in the literature:

- For $m = 2$, 4, 25, or 100 there are no good D.
- For $m = 8$, $D = 8$ is the only good D.
- For $m = p$, $2p$, or $4p$, for p an odd prime, there are no good D.
- For $m = 2p^2$, for p an odd prime, if there is no solution to $x^2 - 2p^2y^2 = -1$, there is a unique good D, namely $D = 2p^2$; otherwise there are no good D.

2000 *Mathematics Subject Classification.* 11D09, 11D85.
Key words and phrases. Generalized Pell equation, simultaneous Pell equations, representation.

- If $m = p^\alpha$, $2p^\alpha$, or $4p^\alpha$, p is an odd prime, $\alpha \in \mathbf{Z}$, $\alpha > 1$, and D is good, then $p^2|D$.

In addition, for the odd prime p we prove:

- If $p|D$ and F represents p and $-p$, then $D = p$.
- If $p|D$ and F represents $2p$ and $-2p$, then $D = 2p$.
- If $p|D$ and F primitively represents $4p$ and $-4p$, then $D = p$.

The following theorem, used below, is proved as part of [8, Theorem 2.3] (see also [7, Theorem 3.2] and [3, Lemma 1]). For completeness, we also give a proof.

Theorem 1. *If a, $b > 0$ are odd integers, v, $w \in \mathbf{N}$, and $av^2 - bw^2 = 4$ (resp. -4), then there are integers t, u so that $at^2 - bu^2 = 1$ (resp. -1).*

Proof. Either both v and w are even or both are odd. If both are even, then for $t = v/2$, $u = w/2$, t and u are integers and $at^2 - bu^2 = 1$ or -1. Now assume v and w are both odd. Then $v^2 \equiv w^2 \equiv 1 \pmod 8$. In the line below, all congruences are modulo 8.

$$av^2 - bw^2 \equiv 4 \implies a - b \equiv 4 \implies ab \equiv b^2 + 4b \equiv 1 + 4 = 5,$$

so $ab \equiv 5 \pmod 8$. Let $t = (av^3 + 3bvw^2)/8$ and $u = (3av^2w + bw^3)/8$. It is straightforward to check that $at^2 - bu^2 = 1$ or -1. To see that t is an integer, note that $av^3 + 3bvw^2 = v(av^2 + 3bw^2)$ and that

$$a(av^2 + 3bw^2) \equiv a(a + 3b) \equiv a^2 + 3ab \equiv 1 + 15 \equiv 0 \pmod 8.$$

Because $\gcd(a, 8) = 1$, 8 must divide $av^2 + 3bw^2$, and so t is an integer. A similar argument shows that u is an integer. □

2. $m = 2$, 4, OR 8

Henceforth, D denotes a positive nonsquare integer and F denotes the binary quadratic form $x^2 - Dy^2$. Also, m denotes an integer greater than 1 unless otherwise specified.

Perron [10, p. 96] proves the next theorem.

Theorem 2. *If F represents 2 and -2 then $D = 2$ and F represents -1.*

Theorem 3. *If F primitively represents 4 and -4 then F represents -1.*

Proof. Considerations modulo 16 show that if F primitively represents 4 and -4, then $D \equiv 5 \pmod 8$ and x and y are odd. The theorem then follows from Theorem 1. See also [8, Theorem 2.3] and [7, Theorem 3.2]. □

Note that it is not sufficient that F primitively represent -4. For example, $x^2 - 8y^2$ primitively represents -4 ($2^2 - 8 \cdot 1^2 = -4$), but does not represent -1. In fact, if $D = 4k^2 + 4$, then $x^2 - Dy^2$ primitively represents -4 (take $y = 1$), but does not represent -1 (because $4|D$). Additional such D include 52, 116, 164, 212, 232, 244, 292, 296, ...

Theorem 4. *If F primitively represents 8 and -8 then either $D = 8$ or F represents -1.*

Consider first the case where D is even. Let $v_1^2 - Dw_1^2 = 8$ and $v_2^2 - Dw_2^2 = -8$ where $\gcd(v_1, w_1) = \gcd(v_2, w_2) = 1$. Then $2|v_1$ and $2|v_2$, so $4|D$, $(v_1/2)^2 - (D/4)w_1^2 = 2$, and $(v_2/2)^2 - (D/4)w_2^2 = -2$. By Theorem 2, $D/4 = 2$, and $D = 8$.

Before considering the case where D is odd, we establish two lemmas and another theorem.

Lemma 1. *If the complete quotients for the continued fraction expansion of $\sqrt{D}$ are denoted $(P_i + \sqrt{D})/Q_i$ for $i \in \mathbf{Z}$, $i \geq 0$, where $P_i \in \mathbf{Z}$, $Q_i \in \mathbf{N}$, $P_0 = 0$, and $Q_0 = 1$, then Q_i and Q_{i+1} cannot both be even.*

Proof. Substituting $Q_{i+1}a_{i+1} - P_{i+1}$ for P_{i+2} in $Q_{i+2} = Q_i - a_{i+1}(P_{i+2} - P_{i+1})$ [10, p. 70] gives

$$Q_i = Q_{i+1}a_{i+1}^2 + Q_{i+2} - 2P_{i+1}a_{i+1}.$$

If Q_{i+1} and Q_{i+2} are even, then Q_i must be even, and working backwards we get $Q_0 = 1$ is even, a contradiction. □

Lemma 2. *For $D \equiv 1 \pmod 8$ and $(P_i + \sqrt{D})/Q_i$ as in Lemma 1, in any period of the continued fraction expansion of $\sqrt{D}$, there are at most two i so that $Q_i = 8$.*

Proof. For $i \geq 1$, $(P_i + \sqrt{D})/Q_i$ is a reduced quadratic irrational [10, pp. 75 and 83], so

$$-1 < (P_i - \sqrt{D})/Q_i < 0$$

and

$$\sqrt{D} - Q_i < P_i < \sqrt{D}. \tag{1}$$

Now assume $Q_i = 8$. As $D - P_i^2 = Q_iQ_{i-1} = 8Q_{i-1}$ [10, p. 69], P_i is odd. From (1), there is at most one P_i in each of the residue classes 1, 3, 5, 7 modulo 8. Let $D = 8k + 1$. For k even, if $P_i \equiv 1$ or $7 \pmod 8$ then $Q_{i-1} = (D - P_i^2)/8$ is even, while if $P_i \equiv 3$ or $5 \pmod 8$ then Q_{i-1} is odd. For k odd, if $P_i \equiv 1$ or $7 \pmod 8$ then Q_{i-1} is odd, while if $P_i \equiv 3$ or $5 \pmod 8$ then Q_{i-1} is even. Because Q_{i-1} must be odd, there are at most two possible values for P_i when $Q_i = 8$. □

From [9, Theorem 7.24] we have

Theorem 5. *If*

$N \in \mathbf{Z}$, $|N| < \sqrt{D}$,
$x^2 - Dy^2$ primitively represents N,
ℓ is the length of the period of the continued fraction expansion of $\sqrt{D}$,
$(P_i + \sqrt{D})/Q_i$ is as in Lemma 1, and
A_i/B_i are the convergents of the continued fraction expansion of $\sqrt{D}$,

then there is an $1 \le i \le \ell$ *so that* $A_{i-1}^2 - DB_{i-1}^2 = (-1)^{i-1}Q_i = N$. *In particular,* $Q_i = |N|$.

Now we return to the proof of Theorem 4 for D odd. The odd $D < 64$ for which F represents 8 and -8 are $D = 17$ and 41, and for both of these F represents -1. When D is odd, x and y must also both be odd, so $x^2 \equiv y^2 \equiv 1 \pmod 8$. From

$$1 \equiv x^2 \equiv Dy^2 \equiv D \pmod 8$$

we have that that $D \equiv 1 \pmod 8$.

Now assume $D > 64$ is not a square and $D \equiv 1 \pmod 8$. Let P_i and Q_i be as in Lemma 1, and let $a_i = \left\lfloor (P_i + \sqrt{D})/Q_i \right\rfloor$ be the i-th convergent in the continued fraction expansion of $\sqrt{D}$. Let ℓ be the length of the period of this continued fraction expansion, so $Q_\ell = 1$ and $P_{i+\ell} = P_i$ and $Q_{i+\ell} = Q_i$ for $i \ge 1$.

If $x^2 - Dy^2$ primitively represents ± 8, then by Theorem 5, $Q_j = 8$ for some $1 \le j \le \ell$. By palindromic properties of the sequence $\{Q_i\}$, we also have that $Q_{\ell-j} = 8$ [10, p. 81]. Because at most two $Q_i = 8$ in any period of the continued fraction expansion of $\sqrt{D}$, there are no $1 \le i \le \ell$ so that $Q_i = 8$ other than $i = j$ and $i = \ell - j$. If $x^2 - Dy^2$ does not represent -1, then ℓ is even, and $(-1)^{i-1} = (-1)^{\ell-i-1}$, so $x^2 - Dy^2$ represents exactly one of 8 or -8. This completes the proof of Theorem 4.

As an aside, we note that methodology similar to that used to prove Theorem 4 can be used to prove Theorems 2 and 3. For $D \ge 5$, D odd, there is exactly one reduced quadratic irrational $(P + \sqrt{D})/2$ (namely with $P = \lfloor \sqrt{D} \rfloor$ or $P = \lfloor \sqrt{D} \rfloor - 1$, whichever is odd). For $D \equiv 1 \pmod 4$ there are exactly two reduced quadratic irrationals $(P + \sqrt{D})/4$.

3. $m = p$, $2p$, $4p$, or $2p^2$ for p an odd prime

The following extends [6, Cor. 3.2]. See also [7, 8].

Theorem 6. *If* $v^2 - Dw^2 = \delta p^\alpha$ *and* $r^2 - Ds^2 = -\delta p^\alpha$, *where* $v, w, r, s \in \mathbf{Z}, \alpha \in \mathbf{N}$, *p is an odd prime,* $\gcd(v, w) = \gcd(r, s) = 1$, *and* $\delta = 1$, 2, *or* 4, *then*

If $\alpha = 1$ *then* $x^2 - Dy^2$ *represents* -1.
If $\alpha > 1$ *then either* $x^2 - Dy^2$ *represents* -1 *or* $p^2 | D$.

Proof. For any α, $\gcd(w, p) = \gcd(s, p) = 1$ because otherwise $p|v$ or $p|r$.

If $\alpha > 1$ and $p|D$ then $p|v$, so $p^2 | v^2 - \delta p^\alpha = Dw^2$, and $p^2 | D$. For the rest of the proof we assume that either $\alpha = 1$ or $p \nmid D$.

We have

$$v^2 \equiv Dw^2 \pmod{p^\alpha} \text{and} r^2 \equiv Ds^2 \pmod{p^\alpha}$$

so

$$(vw^{-1})^2 \equiv (rs^{-1})^2 \equiv D \pmod{p^\alpha}$$

and

$$vw^{-1} \equiv \pm rs^{-1} \pmod{p^\alpha}$$

because the equation $X^2 \equiv D \pmod{p^\alpha}$ has at most two solutions when either $\alpha = 1$ or $\gcd(D, p) = 1$. Choose signs so that

$$vw^{-1} \equiv rs^{-1} \pmod{p^\alpha}.$$

Then $vs \equiv rw \pmod{p^\alpha}$ and (multiply by v, substitute Dw^2 for v^2, cancel a w) $vr \equiv Dws \pmod{p^\alpha}$.

If $\delta = 1$, then for $x = (vr - Dws)/p^\alpha$, $y = (vs - rw)/p^\alpha$, we have that $x^2 - Dy^2 = -1$.

If $\delta = 2$, then w and s are odd and, by considerations modulo 16, $D \equiv 2 \pmod 8$ and v and r are even, so $x = (vr - Dws)/2p^\alpha$ and $y = (vs - rw)/2p^\alpha$ are both integers, and we have that $x^2 - Dy^2 = -1$.

If $\delta = 4$, then v, w, r, s, and D are all odd, and $D \equiv 5 \pmod 8$ (by considerations modulo 16) so $x = (vr - Dws)/4p^\alpha$, $y = (vs - rw)/4p^\alpha$ are both integers or both half integers and $x^2 - Dy^2 = -1$. If x and y are half-integers, then for $X + Y\sqrt{D} = (x + y\sqrt{D})^3$, X and Y are integers and $X^2 - DY^2 = -1$ [3, Lemma 1]. □

Corollary 1. *If $m = 2p^2$ where p is an odd prime, and F represents m and $-m$, and does not represent -1, then $D = 2p^2$.*

Proof. By Theorem 6, if F does not represent -1 then $p^2 | D$. We then have that $x^2 - (D/p^2)y^2$ represents 2 and -2. By Theorem 2, $D/p^2 = 2$, so $D = 2p^2$. □

Whether $F = x^2 - 2p^2y^2$ represents -1 depends on p. If $p \equiv 3 \pmod 4$ then F does not represent -1. If $p \equiv 5 \pmod 8$ then F does represent -1 [10, p. 97], [1, p. 39]. If $p \equiv 1 \pmod 8$ then F might or might not represent -1. For example, $x^2 - 2 \cdot 17^2 y^2$ does not represent -1, while $x^2 - 2 \cdot 137^2 y^2$ represents -1.

4. $m = 25$ OR 100

First we establish a lemma that will be useful.

Lemma 3. *If F represents -1 (resp. -4) then either:*

There are $x, y \in \mathbf{Z}$ with $5|y$ and $x^2 - Dy^2 = -1$ (resp. -4), or
$5|y$ for every $x, y \in \mathbf{Z}$ so that $x^2 - Dy^2 = 1$ (resp. 4).

Proof. If $\{x_1, y_1\}$ is the minimal positive integral solution to $x^2 - Dy^2 = -1$ then all positive integral solutions $\{x_n, y_n\}$ to $x^2 - Dy^2 = \pm 1$ are given by

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n, \tag{2}$$

where $n \in \mathbf{N}$, $x_n^2 - Dy_n^2 = 1$ when n is even, and $x_n^2 - Dy_n^2 = -1$ when n is odd [9, p. 356].

By the binomial theorem we have that

$$y_n = \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2i+1} x_1^{n-2i-1} y_1^{2i+1} D^i. \tag{3}$$

An immediate consequence is that if n is even, then $x_1 | y_n$. Thus, if $x_1 \equiv 0 \pmod 5$ then $5|y$ for every solution to $x^2 - Dy^2 = 1$.

If $x_1 \equiv 1$ or $4 \pmod 5$ then $Dy_1^2 = x_1^2 + 1 \equiv 2 \pmod 5$, and, by (3)

$$y_3 = y_1(3x_1^2 + Dy_1^2) \equiv y_1(3+2) \equiv 0 \pmod 5.$$

Hence $x_3^2 - Dy_3^2 = -1$ and $5|y_3$.

If $x_1 \equiv 2$ or $3 \pmod 5$ then $Dy_1^2 = x_1^2 + 1 \equiv 0 \pmod 5$, and, by (3)

$$y_5 = y_1(5x_1^4 + 10x_1^2 y_1^2 D + y_1^4 D^2) \equiv y_1(0+0+0) \equiv 0 \pmod 5.$$

Hence $x_5^2 - Dy_5^2 = -1$ and $5|y_5$.

Similar arguments apply when F represents -4, but note that (2) is replaced by

$$\frac{1}{2}(x_n + y_n\sqrt{D}) = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n.$$

□

This lemma can also be proved by applying the theory of linear recurrence relations to the sequence of solutions to Pell equations [4, 5].

We will use this to show

Theorem 7. *If F primitively represents 25 and -25 (resp. 100 and -100), then F represents -1.*

Proof. First consider the case where F represents 25 and -25. By Theorem 6 if F does not represent -1, then $25|D$. Therefore, for any primitive solution to $x^2 - Dy^2 = 25$, $5|x$ and $5 \nmid y$. Thus, for $D_1 = D/25$, $x^2 - D_1 y^2 = 1$ has solutions so that $5 \nmid y$. Since $x^2 - D_1 y^2 = -1$ has solutions, by Lemma 3 it has solutions so that $5|y$. But then $x^2 - D(y/5)^2 = -1$, so F does represent -1.

Virtually the same argument works when F represents 100 and -100. □

5. Additional results

The following theorem [12, Theorem 8] is used in the proof of Theorem 9.

Theorem 8. *If $a, b \in \mathbf{N}$, $x^2 - aby^2$ represents -1, and $ax^2 - by^2$ represents 1 or -1, then $a = 1$ or $b = 1$.*

Theorem 9. *Let F primitively represent δp and $-\delta p$ where p is an odd prime, $p|D$, and $\delta \in \{1, 2, 4\}$. Then*

(a) if $\delta = 1$ or 4 then $D = p$.

(b) if $\delta = 2$ then $D = 2p$.

Proof. For any x and y so that $x^2 - Dy^2 = \pm\delta p$, we have that $p|x$, so the form $px^2 - (D/p)y^2$ represents δ and $-\delta$. Also, by Theorem 6, $x^2 - Dy^2$ represents -1.

When $\delta = 1$, Theorem 8 tells us that $D/p = 1$, and $D = p$.

When $\delta = 2$, D/p is even (as we show below), so for any x and y so that $px^2 - (D/p)y^2 = \pm 2$, we have that x is even. It follows that the form $2px^2 - (D/2p)y^2$ represents 1 and -1, so by Theorem 8, $D/2p = 1$, and $D = 2p$.

To see that D/p must be even when $\delta = 2$, suppose D/p were odd. Then for any representation of 2 by $px^2 - (D/p)y^2$, x and y would have the same parity. If they were both even, we would have $4|px^2 - (D/p)y^2$, but $4 \nmid 2$, so both must be odd. Then $x^2 \equiv y^2 \equiv 1 \pmod 8$ and $p - D/p \equiv 2 \pmod 8$. A similar argument using the fact that $px^2 - (D/p)y^2$ represents -2 shows that $p - D/p \equiv -2 \pmod 8$. Because $2 \not\equiv -2 \pmod 8$, D/p must be even.

When $\delta = 4$, the form $px^2 - (D/p)y^2$ represents 4 and -4. By considerations modulo 16 we have $p(D/p) = D \equiv 5 \pmod 8$, and in particular D/p is odd. Then by Theorem 1 the form $px^2 - (D/p)y^2$ represents 1 and -1, so by Theorem 8, $D/p = 1$, and $D = p$. □

6. A conjecture

We begin with some theorems needed to prove the main theorem in this section. Theorem 9 in [4] says, in part

Theorem 10. *If $\{x_i, y_i\}$ is the sequence of positive solutions to $x^2 - Dy^2 = 1$ (where $\{x_1, y_1\}$ is the smallest positive solution), $q > 3$ is a prime, $q|D$, and $q \nmid y_1$, then $q \nmid y_i$ for $i < q$ and $q \| y_q$.*

Theorem 10 in the same paper [4] is

Theorem 11. *If q is an odd prime, $\alpha, \lambda \in \mathbf{N}$, $\{x_i, y_i\}$ is as in Theorem 10, κ is the smallest index i so that $q^\alpha | y_i$, $q^\alpha \| y_\kappa$, and $\gcd(q, \chi) = 1$, then $q^{\alpha+\lambda} \| y_{\chi\kappa q^\lambda}$.*

We have as an immediate consequence

Corollary 2. *If $q > 3$ is an odd prime, $\alpha \in \mathbf{N}$, $\{x_i, y_i\}$ is as in Theorem 10, $q|D$, and $q \nmid y_1$, then $q^\alpha \| y_{p^\alpha}$.*

The following theorem provides support for the conjecture below.

Theorem 12. *If*

$x_1, y_1, t, u \in \mathbf{N}$,
$m \in \mathbf{Z}$,
$x_1^2 - Dy_1^2 = m$ *with* $\gcd(x_1, y_1) = 1$,
$x^2 - Dy^2$ *does not represent* -1,
$t^2 - Du^2 = 1$,
$q > 3$ *is an odd prime,* $q|D$, *and* $q \nmid ux_1$,

then, for all integers $k \geq 0$, $x^2 - Dq^{2k}y^2$ primitively represents m and does not represent -1.

Proof. By Corollary 2, for any k there are t_k, u_k so that

$$t_k^2 - Dq^{2k}u_k^2 = 1 \tag{4}$$

and $\gcd(q, u_k) = 1$.

By hypothesis, the theorem is this true for $k = 0$. We assume the theorem for k and show it for $k + 1$. Let

$$x_1^2 - Dq^{2k}y_1^2 = m \tag{5}$$

be a positive primitive solution with $q \nmid x_1$, and define x_{2n+1}, y_{2n+1} by

$$x_{2n+1} + y_{2n+1}\sqrt{Dq^{2k}} = (t_k + u_k\sqrt{Dq^{2k}})^{2n}(x_1 + y_1\sqrt{Dq^{2k}}). \tag{6}$$

Then

$$\begin{aligned} &x_{2n+1} + y_{2n+1}\sqrt{Dq^{2k}} \\ &\qquad \equiv (t_k^{2n} + 2nt_k^{2n-1}u_k\sqrt{Dq^{2k}})(x_1 + y_1\sqrt{Dq^{2k}}) \pmod q, \end{aligned} \tag{7}$$

and

$$x_{2n+1} + y_{2n+1}\sqrt{Dq^{2k}} \equiv x_1 + (2nt_ku_kx_1 + y_1)\sqrt{Dq^{2k}} \tag{8}$$

because $q|D$, $t_k^{2n} \equiv 1 \pmod q$, and $t_k^{2n-1} \equiv t_k \pmod q$. From this we have that

$$x_{2n+1} \equiv x_1 \pmod q \tag{9}$$

and

$$y_{2n+1} \equiv 2nt_ku_kx_1 + y_1 \pmod q. \tag{10}$$

By hypothesis, $\gcd(2t_ku_kx_1, q) = 1$, so there is an n so that

$$2nt_ku_kx_1 + y_1 \equiv 0 \pmod q, \tag{11}$$

and so $q|y_{2n+1}$. We then have

$$x_{2n+1}^2 - Dq^{2k+2}\left(\frac{y_{2n+1}}{q}\right)^2 = m \tag{12}$$

with $\gcd(x_{2n+1}, q) = 1$ (by (9)).

To show that this is a primitive solution, it suffices to show that

$$\gcd(x_{2n+1}, y_{2n+1}) = 1.$$

Define t, u by

$$t + u\sqrt{Dq^{2k}} = (t_k + u_k\sqrt{Dq^{2k}})^{2n}$$

so by (6)

$$x_{2n+1} + y_{2n+1}\sqrt{Dq^{2k}} = (t + u\sqrt{Dq^{2k}})(x_1 + y_1\sqrt{Dq^{2k}})$$

where

$$t^2 - u^2Dq^{2k} = 1.$$

Then

$$x_{2n+1} = tx_1 + uy_1Dq^{2k}$$

and

$$y_{2n+1} = ux_1 + ty_1$$

so

$$\begin{aligned}(13)\quad & tx_{2n+1} - uD^{2k}y_{2n+1} \\ &= t^2x_1 + tuy_1Dq^{2k} - (tuy_1Dq^{2k} + u^2x_1Dq^{2k}) \\ &= (t^2 - u^2Dq^{2k})x_1 = x_1.\end{aligned}$$

Similarly,

$$ty_{2n+1} - ux_{2n+1} = y_1.$$

Hence any common factor of x_{2n+1} and y_{2n+1} divides both x_1 and y_1, so x_{2n+1} and y_{2n+1} are relatively prime. □

For $1 < m \leq 15000$, m not equal to 25, 100, p, $2p$, $4p$, $2p^2$, for p prime, there is a $D < 500000$ and $q|D$ so that the conditions of the theorem apply for m and $-m$.

Based on this, and other empirical evidence, I conjecture that for any integer $m > 1$ that is not 25, 100, p, $2p$, $4p$, or $2p^2$, for p a prime, there are infinitely many D so that $x^2 - Dy^2$ primitively represents m and $-m$ and does not represent -1.

References

[1] B. D. Beach and H. C. Williams. A numerical investigation of the Diophantine equation $x^2 - dy^2 = -1$. In *Proceedings of the Third Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1972)*, pages 37–68, Boca Raton, Fla., 1972. Florida Atlantic Univ.

[2] L. E. Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality.* AMS Chelsea Publishing, 1999.

[3] P. Kaplan and K. S. Williams. Pell's equations $X^2 - mY^2 = -1, -4$ and continued fractions. *J. Number Theory*, 23(2):169–182, 1986.

[4] D. H. Lehmer. On the multiple solutions of the Pell equation. *Ann. of Math. (2)*, 30(1-4):66–72, 1928/29.

[5] D. H. Lehmer. An extended theory of Lucas' functions. *Ann. of Math. (2)*, 31(3):419–448, 1930.

[6] R. A. Mollin. A simple criterion for solvability of both $X^2-DY^2 = c$ and $x^2-Dy^2 = -c$. *New York J. Math.*, 7:87–97 (electronic), 2001.

[7] R. A. Mollin, K. Cheng, and B. Goddard. The Diophantine equation $AX^2 - BY^2 = C$ solved via continued fractions. *Acta Math. Univ. Comenian. (N.S.)*, 71(2):121–138, 2002.

[8] R. A. Mollin and A. J. van der Poorten. Continued fractions, Jacobi symbols, and quadratic Diophantine equations. *Canad. Math. Bull.*, 43(2):218–225, 2000.

[9] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers.* John Wiley & Sons Inc., New York, fifth edition, 1991.

[10] O. Perron. *Die Lehre von den Kettenbrüchen. Bd I. Elementare Kettenbrüche.* B. G. Teubner Verlagsgesellschaft, Stuttgart, 1954. 3te Aufl.

[11] J. P. Robertson. On D so that $x^2 - Dy^2 = \pm m$. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)*, 22(2):143–148 (electronic), 2006.

[12] D. T. Walker. On the diophantine equation $mX^2 - nY^2 = \pm 1$. *Amer. Math. Monthly*, 74:504–513, 1967.

[13] A. Weil. *Number theory*. Modern Birkhäuser Classics. Birkhäuser Boston Inc., Boston, MA, 2007. An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition.

Received on August 31, 2007; accepted on August 03, 2009

Actuarial and Economic Services Division,
National Council on Compensation Insurance,
Boca Raton, FL 33487, USA
E-mail address: `jpr2718@gmail.com`