Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
22 (2006), 143–148
www.emis.de/journals
ISSN 1786-0091

ON D SO THAT $x^2 - Dy^2 = \pm m$

JOHN P. ROBERTSON

ABSTRACT. We prove that for any integer $m \neq 0, \pm 2$, there are infinitely many positive integers D for which the form $x^2 - Dy^2$ primitively represents m, $-m$, and -1. We do this by constructing an infinite sequence of such D's associated with each m.

Also, when m is odd, we relate the existence of additional such D's to well-known conjectures.

1. Introduction

Below we will prove that for any integer $m \neq 0, \pm 2$, there are infinitely many positive integers D for which there are primitive solutions to each of the three equations

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

$$x^2 - Dy^2 = -m, \text{ and} \tag{2}$$

$$t^2 - Du^2 = -1. \tag{3}$$

A classical result has that the only integer D so that $x^2 - Dy^2$ represents both 2 and -2 is $D = 2$ [2, Satz 20, pp. 106-107].

In general, for a given $m \neq 0, \pm 2$, there seem to be many D in addition to those established by our main theorem below for which the three equations above have solutions. For example, for $m = 6$, the theorem will show that for $D = 2 \times 5^{2k+1}$ the three equations have solutions. That is, for $D < 1000$ the theorem finds $D = 10$ and $D = 250$. But, for $m = 6$ all three equations also have solutions for $D = 58$, 106, 202, 298, 394, 538, 586, 634, 778, 922, and 970.

The following Lemma is well known [5, p. 14].

Lemma 1. *If* (1) *has a primitive solution,* $r^2 - Ds^2 = \delta = \pm 1$, $v = rx + syD$, *and* $w = ry + sx$, *then* $v^2 - Dw^2 = \delta m$ *and* $\gcd(v, w) = 1$.

2000 *Mathematics Subject Classification.* 11D09, 11D85.

Key words and phrases. Generalized Pell equation, simultaneous Pell equations, representation.

Proof. First,

$$v^2 - Dw^2 = (rx + syD)^2 - D(ry + sx)^2 = (r^2 - Ds^2)(x^2 - Dy^2) = \delta m.$$

We have that $\gcd(v, w) = 1$ because

$$rv - sDw = r(rx + syD) - sD(ry + sx) = \delta x$$

and

$$rw - sv = r(ry + sx) - s(rx + syD) = \delta y,$$

so any common divisor of v and w would also divide both x and y. □

In particular, if (1) and (3) have solutions then (2) has a solution. But it is possible for (1) and (2) to have solutions while (3) does not have solutions. For example, $13^2 - 34 \cdot 2^2 = 33$ and $1^2 - 34 \cdot 1^2 = -33$, while $t^2 - 34u^2 = -1$ has no solutions.

2. Two preliminary lemmas

Our main result will be a consequence of the following two lemmas.

Lemma 2. *Suppose that* $a, M, t, u \in \mathbf{N}$, $t^2 - aMu^2 = -1$, *and* $\gcd(M, 6u) = 1$. *Then for every integer* $k \geq 0$ *there are integers* T_k *and* U_k *so that*

$$T_k^2 - aM^{2k+1}U_k^2 = -1 \tag{4}$$

and $\gcd(M, U_k) = 1$.

Proof. The lemma is trivial for $M = 1$ so assume $M \geq 5$. The lemma is true for $k = 0$ by hypothesis ($T_0 = t$, $U_0 = u$). Assume it's true for k; we'll show it for $k + 1$.

Set

$$R + SB = (T_k + U_k B)^M \tag{5}$$

where $B = \sqrt{aM^{2k+1}}$ and R and S are integers. We now show that $M|S$ and

$$\gcd(S/M, M) = 1.$$

Expanding (5), we have that

$$R + SB = T_k^M + MT_k^{M-1}U_k B + \binom{M}{2} T_k^{M-2}U_k^2 B^2 + \binom{M}{3} T_k^{M-3}U_k^3 B^3 + \cdots + U_k^M B^M,$$

so

$$S = MT_k^{M-1}U_k + \binom{M}{3} T_k^{M-3}U_k^3 B^2 + \binom{M}{5} T_k^{M-5}U_k^5 B^4 + \cdots + U_k^M B^{M-1}. \tag{6}$$

Because $B^2 = aM^{2k+1}$, each term on the right of (6) is divisible by M, so S/M is an integer. Additionally, we now show that each term on the right of (6) after the first is divisible by M^2. This should be clear for the third and subsequent terms, and for the second term when $k > 0$. When $k = 0$, the second term is $\binom{M}{3} t^{M-3} u^3 aM$. Because $\gcd(M, 6) = 1$, it follows that $M | \binom{M}{3}$, so M^2 divides this second term. Now $\gcd(T_k, M) = 1$ by (4) and $\gcd(U_k, M) = 1$ by hypothesis, so $T_k^{M-1} U_k$ is relatively prime to M and $S/M = T_k^{M-1} U_k + M \times$ (additional terms) is relatively prime to M. Because M is odd, it follows that

$$R^2 - aM^{2k+1} S^2 = \left(T_k^2 - aM^{2k+1} U_k^2\right)^M = (-1)^M = -1.$$

So, we can take $T_{k+1} = R$, and $U_{k+1} = S/M$, and we have

$$T_{k+1}^2 - aM^{2k+3} U_{k+1}^2 = -1$$

with $\gcd(M, U_{k+1}) = 1$. □

We need one more lemma.

Lemma 3. *Assume that $D_1, t, u \in \mathbf{N}$ and $t^2 - D_1 u^2 = -1$. Given relatively prime integers x_1, y_1, define integers x_i, y_i for $i > 1$ by*

$$x_i + y_i \sqrt{D_1} = (x_1 + y_1 \sqrt{D_1})(t + u\sqrt{D_1})^{i-1}. \tag{7}$$

Then for any integer $n \geq 0$,

$$x_{4n+1} \equiv x_1 \pmod{D_1},$$
$$y_{4n+1} \equiv y_1 - 4ntux_1 \pmod{D_1}, \text{ and}$$
$$\gcd(x_{4n+1}, y_{4n+1}) = 1.$$

Proof. Because $t^2 \equiv -1 \pmod{D_1}$, we have $t^3 \equiv -t \pmod{D_1}$ and $t^4 \equiv 1 \pmod{D_1}$. Now

$$\begin{aligned} x_{4n+1} + y_{4n+1}\sqrt{D_1} &= (x_1 + y_1\sqrt{D_1})(t + u\sqrt{D_1})^{4n} \\ &\equiv (x_1 + y_1\sqrt{D_1})(t^{4n} + 4nt^{4n-1}u\sqrt{D_1}) \\ &\equiv x_1 t^{4n} + (y_1 t^{4n} + x_1 4nt^{4n-1}u)\sqrt{D_1} \pmod{D_1}. \end{aligned}$$

Since $t^{4n} \equiv 1 \pmod{D_1}$ and $t^{4n-1} \equiv -t \pmod{D_1}$, the first two conclusions of the Lemma follow. By repeated application of Lemma 1 we have that $(t + u\sqrt{D_1})^{4n}$ expanded can be written as $v + w\sqrt{D_1}$ where $v^2 - D_1 w^2 = (-1)^{4n} = 1$. From this and another application of Lemma 1 to (7) we get that $\gcd(x_{4n+1}, y_{4n+1}) = 1$. □

3. Main proof

Our result will be an application of the following theorem.

Theorem 1. *If*

$a, m, M, x, y, t, u \in \mathbf{N}$,
$x^2 - aMy^2 = m$ *is a primitive solution with* $\gcd(M, x) = 1$, *and*
$t^2 - aMu^2 = -1$ *with* $\gcd(M, 6u) = 1$,

then for every integer $k \geq 0$ *there is a primitive solution to* $x^2 - aM^{2k+1}y^2 = m$ *with* $\gcd(M, x) = 1$ *and there is a primitive solution to* $x^2 - aM^{2k+1}y^2 = -m$.

Proof. By Lemma 2, for every $k \geq 0$ there are solutions to

$$t^2 \; - \; aM^{2k+1}u^2 \; = \; -1$$

with $\gcd(M, u) \; = \; 1$.

We proceed by induction on k. The case $k = 0$ holds by hypothesis. Now, using the notation of Lemma 3, assume we have $x_1^2 - aM^{2k+1}y_1^2 = m$ with $\gcd(M, x_1) = \gcd(x_1, y_1) = 1$. In Lemma 3, take $D_1 = aM^{2k+1}$, so $y_{4n+1} \equiv y_1 - 4ntux_1 \pmod{M}$. Because M is odd, $\gcd(4, M) = 1$. That $\gcd(t, M) = 1$ is a consequence of $t^2 - aM^{2k+1}u^2 = -1$. That $\gcd(u, M) = 1$ is given by Lemma 2. So $\gcd(4tux_1, M) = 1$. We conclude that there is an n so that $y_1 \equiv 4ntux_1 \pmod{M}$, and so $M | y_{4n+1}$. Taking $r = x_{4n+1}$ and $s = y_{4n+1}/M$, we have $r^2 - aM^{2k+3}s^2 = m$. Because $\gcd(x_1, M) = 1$, by inductive hypotheses, and $r = x_{4n+1} \equiv x_1 \pmod{M}$, it follows that $\gcd(r, M) = 1$. Finally, $\gcd(r, s) = 1$ because $\gcd(x_{4n+1}, y_{4n+1}) = 1$.

Because there is a primitive solution to

$$x^2 - aM^{2k+1}y^2 = m$$

and a solution to

$$x^2 - aM^{2k+1}y^2 = -1$$

it follows from Lemma 1 that there is a primitive solution to

$$x^2 - aM^{2k+1}y^2 = -m.$$

□

Our main result is

Theorem 2. *For any integer* $m \neq 0, \pm 2$, *there are infinitely many positive integers* D *so that there are primitive solutions to* (1), (2) *and* (3).

Proof. Given m, Table 1 gives a and M and shows that for these a and M there are solutions to $x^2 \; - \; aMy^2 \; = \; m$ and $t^2 \; - \; aMu^2 \; = \; -1$ that satisfy the hypotheses of Lemma 2 and Theorem 1. Because $M > 1$ for $m \neq 0$, ± 2, Lemma 2 and Theorem 1 show that for any of the infinitely many different $D = aM^{2k+1}$, $x^2 - Dy^2$ primitively represents m, $-m$, and -1. □

4. Conjectures

We show that for odd m that there are infinitely many primes p so that $x^2 - py^2$ represents $+m$, $-m$, and -1 would follow from some well-known conjectures. To start, we show:

Lemma 4. *For* $D > 0$ *an odd integer and* $(P_i + \sqrt{D})/Q_i$ *the complete quotients for the continued fraction expansion of* $\sqrt{D}$ *(so* $P_0 = 0$ *and* $Q_0 = 1$*), it is not possible for both* Q_i *and* Q_{i+1} *to be even.*

Representations of m and -1

m	a	M	x	y	t	u
$m \equiv 0 \pmod 4$	1	$\left(\frac{m}{2}\right)^2 + 1$	$\frac{m}{2} + 1$	1	$\frac{m}{2}$	1
$m \equiv 2 \pmod 4$	2	$\frac{\left(\frac{m}{2}\right)^2+1}{2}$	$\frac{m}{2} + 1$	1	$\frac{m}{2}$	1
$m \equiv 1 \pmod 2$	1	$m^2 + 4$	$\frac{m^2-m+2}{2}$	$\frac{m-1}{2}$	$\frac{m^3+3m}{2}$	$\frac{m^2+1}{2}$

TABLE 1. $x^2 - aMy^2 = m$ and $t^2 - aMu^2 = -1$

Proof. First, $D = P_i^2 + Q_iQ_{i-1}$ [1, p. 251, eq. 5.3.13] and D is odd, so if Q_i is even, then P_i must be odd.

Now, suppose Q_i and Q_{i+1} are both even. We will show that Q_{i+2} must be even, and so all Q_k with $k \geq i$ must be even. Since we know there are arbitrarily large j so that $Q_j = 1$ [1, p. 250] [4, p. 48], this contradiction will prove the Lemma.

If Q_i and Q_{i+1} are both even, then P_i and P_{i+1} are both odd. Also, P_{i+2} is odd because $P_{i+2} = Q_{i+1}a_{i+1} - P_{i+1}$ [1, p. 251, eq. 5.3.12]. From

$$Q_{i+2} = Q_i - a_{i+1}(P_{i+2} - P_{i+1})$$

we have that Q_{i+2} is even because Q_i and $P_{i+2} - P_{i+1}$ are even. $\square$

Next we show

Lemma 5. *If $p = n^2 + m^2$ where p is prime, m and n are integers, and $m > 2$ is odd, then the form $x^2 - py^2$ represents both $+m$ and $-m$.*

Proof. Clearly $p \equiv 1 \pmod 4$, so the length ℓ of the period of the continued fraction expansion of $\sqrt{p}$ is odd and

$$p = P_{(\ell+1)/2}^2 + Q_{(\ell+1)/2}^2$$

where $(P_i + \sqrt{D})/Q_i$ are the complete quotients for the continued fraction expansion of $\sqrt{p}$ [4, pp. 70-71]. Since $Q_{(\ell+1)/2} = Q_{(\ell-1)/2}$ (by the palindromic properties of the continued fraction expansion of $\sqrt{p}$ [1, Cor. 5.3.1, p. 242]), $Q_{(\ell+1)/2}$ must be odd. Because p can be written as a sum of squares in an essentially unique way, $Q_{(\ell+1)/2} = Q_{(\ell-1)/2} = m$. It follows that the form $x^2 - py^2$ represents both $+m$ and $-m$ [1, Thm. 5.3.4, p. 246]. $\square$

It is conjectured that for m odd there are infinitely many n so that $p = n^2 + m^2$ is prime [3, Conjectures B (Bouniakowsky), B1, B2, and Schinzel's Conjecture H, pp. 307-312]. That there are infinitely many primes p so that $x^2 - py^2$ represents both $+m$ and $-m$ would follow from the truth of any of these conjectures.

Acknowledgements The author would like to thank Professor R. A. Mollin for his encouragement of this research.

References

[1] R. A. Mollin. *Fundamental number theory with applications*. CRC Press, Boca Raton, 1998.

[2] O. Perron. *Die Lehre von den Kettenbrüchen*. Chelsea Publishing Co., New York, N. Y., 1950. 2d ed.

[3] P. Ribenboim. *The book of prime number records*. Springer-Verlag, New York, 1988.

[4] A. M. Rockett and P. Szüsz. *Continued fractions*. World Scientific Publishing Co. Inc., River Edge, NJ, 1992.

[5] A. Weil. *Number Theory, an approach through history from Hammurapi to Legendre*. Birkhäuser, Boston, 2001.

Received December 12, 2005.

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