International Journal of Algebra, Vol. 1, 2007, no. 6, 293 - 302

Diophantine Equations and Congruences

R. A. Mollin

Department of Mathematics and Statistics
University of Calgary, Calgary, Alberta, Canada, T2N 1N4
http://www.math.ucalgary.ca/˜ ramollin/
ramollin@math.ucalgary.ca

Abstract

We present conditions for quadratic Diophantine equations of the form $ax^2 - by^2 = \pm 1$, (where $1 < a < b$ are integers) for which there are no solutions (x, y), yet for which there are solutions modulo n for all $n \geq 1$. This generalizes work in the literature which follow as very special cases.

Mathematics Subject Classification: Primary: 11D09, 11R11, 11A55; Secondary: 11R29

Keywords: quadratic Diophantine equations, continued fractions, central norms, fundamental units, modular solvability

1 Introduction

Texts on the fundamentals of number theory, such as [3, p. 208] and [9, p. 207], discuss the Diophantine equation $2x^2 - 219y^2 = -1$ which has no integer solutions x, y, yet for which $2x^2 - 219y^2 \equiv -1 \pmod{n}$ has integer solutions for all moduli $n \in \mathbb{N}$. In [9], Nagell is credited with having proved the modular solvability as a deduction from a deeper theorem presented in [8]. However, in none of [3], [8] or [9] is there any connection with the real reason underlying this phenomenon, namely the underlying continued fraction expansions of certain quadratic surds and related central norms which we will explain in the next section. More recently such results for $px^2 - by^2 = -1$ were generalized in [1] when $p = 2$, and for a general prime p in [5], but only in the latter are the underlying continued fraction reasons provided. It is the intention herein to generalize to the case where $a > 1$ is any natural number.

2 Notation and Preliminaries

We will consider the simple continued fraction expansion of $\sqrt{D}$, where $D > 0$ is not a perfect square, and whose period length we denote by $\ell = \ell(\sqrt{D})$ and whose partial quotients we denote by q_j for $j \geq 0$, where $q_0 = \lfloor \sqrt{D} \rfloor$ (the *floor* of $\sqrt{D}$), and $q_1 q_2, \ldots, q_{\ell-1}$ is a palindrome.

The jth *convergent* of α for $j \geq 0$ are given by,

$$\frac{A_j}{B_j} = \langle q_0; q_1, q_2, \ldots, q_j \rangle,$$

where

$$A_j = q_j A_{j-1} + A_{j-2},$$
$$B_j = q_j B_{j-1} + B_{j-2},$$

with $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$. The *complete quotients* are given by, $(P_j + \sqrt{D})/Q_j$, where $P_0 = 0$, $Q_0 = 1$, and for $j \geq 1$,

$$P_{j+1} = q_j Q_j - P_j, \tag{2.1}$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor,$$

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}.$$

We will also need the following facts (which can be found in most introductory texts in number theory, such as [3]. Also, see [2] for a more advanced exposition).

$$A_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j. \tag{2.2}$$

In particular,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell, \tag{2.3}$$

and it follows that $(x_0, y_0) = (A_{\ell-1}, B_{\ell-1})$ is the fundamental solution of the Pell Equation $x^2 - Dy^2 = (-1)^\ell$.

When ℓ is even, $P_{\ell/2} = P_{\ell/2+1}$, so by Equation (2.1),

$$Q_{\ell/2} \mid 2P_{\ell/2},$$

where $Q_{\ell/2}$ is called the *central norm*, (via Equation (2.2)), where

$$Q_{\ell/2} \mid 2D. \tag{2.4}$$

In the following (which we need in the next section), and all subsequent results, the notation for the A_j, B_j, Q_j and so forth apply to the above-developed notation for the continued fraction expansion of $\sqrt{D}$.

Proof of the following elementary number-theoretic results may be found in most introductory texts on the subject such as [3], for instance.

Theorem 2.1 *Let $c \in \mathbb{Z}$ be odd and let $\alpha \in \mathbb{N}$. Then each of the following holds.*

1. *There exists an $z \in \mathbb{Z}$ with*

$$c \equiv z^2 \pmod{2^\alpha}$$

if and only if

$$c \equiv 1 \pmod{\gcd(2^\alpha, 8)}.$$

2. *If p is an odd prime not dividing c and $\alpha \in \mathbb{N}$, then there exists an $z \in \mathbb{Z}$ such that*

$$c \equiv z^2 \pmod{p^\alpha}$$

if and only if the following Legendre symbol equality holds

$$\left(\frac{c}{p}\right) = 1.$$

3. *If $u, v, w \in \mathbb{Z}$ and p is an odd prime dividing neither u nor $v^2 - 4uw$, then the following Legendre symbol equaity holds*

$$\sum_{x=0}^{p-1} \left(\frac{ux^2 + vx + w}{p}\right) = -\left(\frac{u}{p}\right).$$

Theorem 2.2 *Suppose that $D = ab$ is a positive integer that is not a perfect square, where $1 < a < b$ and $\ell = \ell(\sqrt{D})$ is even. Then whenever*

$$ax^2 - by^2 = \pm 1$$

has a solution we have

1. $A_{\ell-1} \equiv (-1)^{\ell/2} \pmod{2b}$,

   and

2. $Q_{\ell/2} = a$.

in the simple continued fraction expansion of $\sqrt{D}$.

Proof. This is a consequence of a more far-reaching result in [4] where detailed criteria for ℓ to be even, in terms of solvability of Diophantine equations such as the above, are provided. □

3 Congruences & Quadratic solvability

In what follows the notation from the previous section is in force.

Theorem 3.1 *Suppose that $1 < a < b$ are integers such that each of the following conditions hold.*

1. $a \equiv 7 \pmod{8}$.
2. *b is a quadratic residue modulo a.*
3. *$-a$ is a quadratic residue modulo b.*
4. *$A_{\ell-1} \not\equiv (-1)^{\ell/2} \pmod{2b}$, where $\ell = \ell(\sqrt{ab})$ is the period length of the simple continued fraction expansion of $\sqrt{ab}$ with ab not a perfect square.*

Then

$$ax^2 - by^2 = -1 \tag{3.5}$$

has no solutions $x, y \in \mathbb{Z}$, whereas

$$ax^2 - by^2 \equiv -1 \pmod{n} \tag{3.6}$$

has solutions $x, y \in \mathbb{Z}$ for all $n \in \mathbb{N}$.

Proof. Since $a \equiv 3 \pmod{4}$, then by Equation (2.3), with $D = ab$, ℓ must be even. Therefore, since $A_{\ell-1} \not\equiv (-1)^{\ell/2} \pmod{2b}$, we may invoke Theorem 2.2 to conclude that Equation (3.18) is not solvable for any $x, y \in \mathbb{Z}$.

Now we show that Equation (3.19) is solvable for all $n \in \mathbb{N}$. Clearly if $n = 1$, it is solvable for any $x, y \in \mathbb{Z}$. By the Chinese remainder Theorem, it suffices to prove the result for $n > 1$ when n is a prime power.

If $n = 2^\alpha$, for $\alpha \in \mathbb{N}$ then, given that $a \equiv -1 \pmod{8}$, then by part 1 of Theorem 2.1, there exists $z \in \mathbb{Z}$ such that $-a \equiv z^2 \pmod{2^\alpha}$. Let z^{-1} be an integer which is a multiplicative inverse of z modulo 2^α, and set $x = z^{-1}$, and $y = 0$. Then

$$ax^2 - by^2 \equiv az^{-2} \equiv -1 \pmod{2^\alpha}.$$

Suppose that $n = p^\alpha$ where p is an odd prime dividing a and $\alpha \in \mathbb{N}$. Part 2 of the hypothesis allows us to invoke part 2 of Theorem 2.1, so there exists $z \in \mathbb{Z}$ such that $b \equiv z^2 \pmod{p^\alpha}$. If we set $x = 0$ and $y = z^{-1}$ where z^{-1} is a multiplicative inverse of z modulo p^α, then

$$ax^2 - by^2 \equiv -bz^{-2} \equiv -1 \pmod{p^\alpha}.$$

Now let $n = p^\alpha$ for $c \in \mathbb{N}$ where p is an odd prime not dividing a. If the Legendre symbol equality $\left(\frac{-a}{p}\right) = 1$ holds, then by part 2 of Theorem 2.1, there exists $z \in \mathbb{Z}$ such that $-a \equiv z^2 \pmod{p^\alpha}$. Let $x = a^{-1}z$ and $y = 0$ where a^{-1} is a multiplicative inverse of a modulo p^α. Then

$$ax^2 - by^2 \equiv a \cdot a^{-2}z^2 \equiv -1 \pmod{p^\alpha}.$$

Lastly, there is the case where the Legendre symbol equality $\left(\frac{-a}{p}\right) = -1$ holds. Since part 3 of the hypothesis holds, we may invoke part 3 of Theorem 2.1, so there exists $t \in \mathbb{Z}$ such that

$$\left(\frac{1 - bt^2}{p}\right) = -1.$$

Therefore,

$$\left(\frac{abt^2 - a}{p}\right) = 1.$$

Thus, by part 2 of Theorem 2.1, there is an integer z such that $abt^2 - a \equiv z^2 \pmod{p^\alpha}$. Let $y = t$ and $x = a^{-1}z$ where a^{-1} is an integer that is a multiplicative inverse of a modulo p^α. Hence,

$$ax^2 - by^2 \equiv a^{-1}z^2 - bt^2 \equiv a^{-1}(abt^2 - a) - bt^2 \equiv -1 \pmod{p^\alpha}.$$

This completes all cases and secures the proof. $\square$

The following illustrates both theorem 3.1 and the techniques in the proof for construction of solutions modulo n.

Example 3.1 *We maintain the notation of Theorem 3.1 and its proof in this example. Let* $a = 119 \cdot 17$ *and* $b = 128 = 2^7$*. In this case, if* $\ell = \ell(\sqrt{ab}) = \ell(8\sqrt{238}) = 16$ *and*

$$A_{\ell-1} = A_{15} = 272051137 \equiv 193 \not\equiv \pm 1 \pmod{2b}.$$

Hence, the Diophantine equation

$$119x^2 - 128y^2 = -1$$

has no solutions. However, since $-a \equiv 3^3 \pmod{b}$ *and* $b \equiv 3^2 \pmod{a}$*, then*

$$119x^2 - 128y^2 \equiv -1 \pmod{n} \tag{3.7}$$

has solutions for all $n \in \mathbb{N}$*. Now we show how solutions may be constructed for Equation* (3.8)*. Select a value of* n *at random, say,* $n = 2^3 \cdot 7^2 \cdot 5^4 \cdot 11^2$*. We construct solutions via the Chinese Remainder Theorem as in the proof of Theorem 3.1. Since* $-a \equiv -119 \equiv 1^2 = z^2 \pmod{2^3}$*, then*

$$ax^2 - by^2 = 119 \cdot 1^2 - 128 \cdot 0^2 \equiv az^{-2} \equiv -1 \pmod{2^3}. \tag{3.8}$$

Since $7|a$, $b \equiv 128 \equiv 18^2 = z^2 \pmod{7^2}$, *and* $z^{-1} = 30$ *is a multiplicative inverse of* z *modulo* 7^2, *then we have*

$$ax^2 - by^2 = 119 \cdot 0^2 - 128 \cdot 30^2 \equiv -1 \pmod{7^2}. \tag{3.9}$$

Since 5 *does not divide* a *and* $-a \equiv 141^2 = z^2 \pmod{5^4}$, *while* $a^{-1} = 604$ *is a multiplicative inverse of* a *modulo* 5^4, *then*

$$119 \cdot (604 \cdot 141)^2 - 128 \cdot 0^2 = a(a^{-1}z)^2 - b \cdot 0^2 \equiv -1. \tag{3.10}$$

Lastly, since 11 *does not divide* a *and* $-a = -119$ *is a quadratic nonresidue modulo* 1, *then we select* $t = 2$ *since the following Legendre symbol equality holds*

$$-1 = \left(\frac{1 - bt^2}{11}\right) = \left(\frac{1 - 128 \cdot 2^2}{11}\right).$$

Moreover, since $a^{-1} = 60$ *is a multiplicative inverse of* a *modulo* 11^2, *and* $abt^2 - a \equiv 208^2 = z^2 \pmod{11^2}$, *then*

$$119 \cdot (60 \cdot 208)^2 - 128 \cdot 2^2 = a(a^{-1}z)^2 - b \cdot t^2 \equiv -1 \pmod{11^2}. \tag{3.11}$$

Now we put together the equations (3.8)–(3.11) *via the Chinese Remainder Theorem to secure the values of* x *and* y *that are solutions to equation* (3.7).

$$x \equiv 1 \cdot 7^2 \cdot 5^4 \cdot 11^2 \cdot (7^{-2} \cdot 5^{-4} \cdot 11^{-2} \pmod{2^3}) + 7^2 \cdot 2^3 \cdot 5^4 \cdot 11^2 \cdot (2^{-3} \cdot 5^{-4} \cdot 11^{-2} \pmod{7^2}) +$$
$$164 \cdot 2^3 \cdot 7^2 \cdot 11^2 \cdot (2^{-3} \cdot 7^{-2} \cdot 11^{-2} \pmod{5^4}) + 17 \cdot 2^3 \cdot 7^2 \cdot 5^4 \cdot (2^{-3} \cdot 7^{-2} \cdot 5^{-4} \pmod{11^2}) \equiv$$
$$7^2 \cdot 5^4 \cdot 11^2 \cdot 1 \cdot 1 \cdot 1 + 7^2 \cdot 2^3 \cdot 5^4 \cdot 11^2 \cdot 43 \cdot 4 \cdot 32 + 164 \cdot 2^3 \cdot 7^2 \cdot 11^2 \cdot 547 \cdot 574 \cdot 31 +$$
$$17 \cdot 2^3 \cdot 7^2 \cdot 5^4 \cdot 106 \cdot 42 \cdot 115 \equiv 24978289 \pmod{n},$$

and

$$y \equiv 2^3 \cdot 7^2 \cdot 5^4 \cdot 11^2 \cdot (7^{-2} \cdot 5^{-4} \cdot 11^{-2} \pmod{2^3}) + 30 \cdot 2^3 \cdot 5^4 \cdot 11^2 \cdot (2^{-3} \cdot 5^{-4} \cdot 11^{-2} \pmod{7^2}) +$$
$$5^4 \cdot 2^3 \cdot 7^2 \cdot 11^2 \cdot (2^{-3} \cdot 7^{-2} \cdot 11^{-2} \pmod{5^4}) + 2 \cdot 2^3 \cdot 7^2 \cdot 5^4 \cdot (2^{-3} \cdot 7^{-2} \cdot 5^{-4} \pmod{11^2}) \equiv$$
$$2^3 \cdot 7^2 \cdot 5^4 \cdot 11^2 \cdot 1 \cdot 1 \cdot 1 + 30 \cdot 2^3 \cdot 5^4 \cdot 11^2 \cdot 43 \cdot 4 \cdot 32 + 5^4 \cdot 2^3 \cdot 7^2 \cdot 11^2 \cdot 547 \cdot 574 \cdot 31 +$$
$$2 \cdot 2^3 \cdot 7^2 \cdot 5^4 \cdot 106 \cdot 42 \cdot 115 \equiv 8160000 \pmod{n},$$

where $n = 29645000$. *Thus, we have*

$$ax^2 - by^2 = 119 \cdot 24978289^2 - 128 \cdot 8160000^2 \equiv -1 \pmod{29645000}$$

as we set out to accomplish.

Immediate from Theorem 3.1 is the following result, which, in turn, was a generalization of [5, Theorem 4, p. 357].

Corollary 3.1 ([7, Theorem 2, p. 1627])

Let p be a prime and c a positive integer with $\ell = \ell(\sqrt{pc})$, such that $p \equiv 7 \pmod 8$, $c \equiv 1 \pmod p$, c is not divisible by any primes q such that the Legendre symbol equality $(\frac{-p}{q}) = -1$ holds, and in the simple continued fraction expansion of $\sqrt{pc}$, $A_{\ell-1} \not\equiv \pm 1 \pmod{2c}$. Then the Diophantine equation,

$$px^2 - cy^2 = -1 \tag{3.12}$$

has no solutions (x, y), but

$$px^2 - cy^2 \equiv -1 \pmod n \tag{3.13}$$

has a solution (x, y) for all $n \geq 1$.

The following analogue of Theorem 3.1 is presented without proof since the arguments are the same.

Theorem 3.2 *Suppose that a and b are integers with $1 < a < b$ and $\ell(\sqrt{ab})$ is even where ℓ is the period length of the simple continued fraction expansion of $\sqrt{ab}$ with ab not a perfect square. Furthermore assume that each of the following holds.*

1. *$a \equiv 1 \pmod 8$.*
2. *$-b$ is a quadratic residue modulo a.*
3. *a is a quadratic residue modulo b.*
4. *$A_{\ell-1} \not\equiv (-1)^{\ell/2} \pmod{2b}$.*

Then

$$ax^2 - by^2 = 1 \tag{3.14}$$

has no solutions $x, y \in \mathbb{Z}$, whereas

$$ax^2 - by^2 \equiv 1 \pmod n \tag{3.15}$$

has solutions $x, y \in \mathbb{Z}$ for all $n \in \mathbb{N}$.

An illustration of Theorem 3.2 is the following.

Example 3.2 *If* $a = 25$ *and* $b = 44$, *then clearly* $a \equiv 1 \pmod 8$, a *is a quadratic residue modulo* b, *and* $-b = -44 \equiv 9^2 \pmod a$. *Moreover,* $A_{\ell-1} = A_1 = 199 \not\equiv \pm 1 \pmod{2b}$. *Hence,* $25x^2 - 44y^2 = 1$ *has no solutions. However, it has solutions modulo all* $n \in \mathbb{N}$. *For instance,* $25 \cdot 229^2 - 44 \cdot 390^2 \equiv 1 \pmod{3 \cdot 7^2 \cdot 13}$.

Immediate from Theorem 3.2 is the following result which, in turn, generalized [5, Theorem 4, p. 357].

Corollary 3.2 ([7, Theorem 3, p. 1630])

Let p *be a prime and* c *a positive integer with* $\ell = \ell(\sqrt{pc})$, *such that either* $p \equiv 1 \pmod 8$, $c \equiv -1 \pmod p$, $\ell(\sqrt{pc})$ *even, and* c *is not divisible by any primes* q *such that the Legendre symbol equality* $(\frac{p}{q}) = -1$ *holds. Also,* $A_{\ell-1} \not\equiv \pm 1 \pmod{2c}$ *in the simple continued fraction expansion of* $\sqrt{pc}$. *Then the Diophantine equation,*

$$px^2 - cy^2 = 1 \tag{3.16}$$

has no solutions (x, y), *but*

$$px^2 - cy^2 \equiv 1 \pmod n \tag{3.17}$$

has a solution (x, y) *for all* $n \geq 1$.

Remark 3.1 *A key feature of the discussion in the paper on global versus local solutions of quadratic Diophantine equations has a feature which we have not yet explicitly mentioned, namely the* central norm (*see* display (2.4))). *In other words, we have not exploited part 2 of Theorem 2.2 yet. The following consequences of Theorems 3.1–3.2 do make use of that fact.*

Corollary 3.3 ([7, Corollary 1, p. 1630]). *Suppose that* p *and* q *are odd primes where* $p \equiv 7 \pmod 8$, $2q \equiv 1 \pmod p$ *and* $pc = p^2q^2 + 2pq = p(pq^2 + 2q)$, *with* c *not divisible by any prime* r *for which* $-p$ *is a quadratic nonresidue. Then Equation* (3.12) *has no solutions but Equation* (3.13) *has a solution for all* $n \geq 1$.

Proof. By [2, Theorem 3.2.1, p. 78], $\ell = \ell(\sqrt{pc}) = 2$ and $Q_{\ell/2} = 2pq$. Thus, by part 2 of Theorem 2.2, Equation (3.12) has no solutions. Hence, by Theorem 3.1, Equation (3.13) has a solution for all $n \geq 1$. $\square$

Similarly the following follows from Theorem 3.2.

Corollary 3.4 ([7, Corollary 2, p. 1631]). *Suppose that p and q are odd primes where $p \equiv 1 \pmod 8$, $2q \equiv 1 \pmod p$ and $pc = p^2q^2 - 2pq = p(pq^2 - 2q)$, with c not divisible by any prime r for which p is a quadratic nonresidue. Then Equation* (3.16) *has no solutions but Equation* (3.17) *has a solution for all $n \geq 1$.*

We conclude with a result for even a, the proof of which is omitted since it is entirely analogous to the above.

Theorem 3.3 *Suppose that $1 < a < b$ are integers such that each of the following conditions hold.*

1. *$a = 2^{\beta}c$, where $\beta, c \in \mathbb{N}$ and $c \equiv 1 \pmod 8$.*
2. *$b \equiv 2^{\beta} + 1 \pmod 8$ and b is a quadratic residue modulo c.*
3. *$-a$ is a quadratic residue modulo b.*
4. *$A_{\ell-1} \not\equiv (-1)^{\ell/2} \pmod{2b}$, where $\ell = \ell(\sqrt{ab})$ is the period length of the simple continued fraction expansion of $\sqrt{ab}$ with ab not a perfect square.*

Then

$$ax^2 - by^2 = -1 \tag{3.18}$$

has no solutions $x, y \in \mathbb{Z}$, whereas

$$ax^2 - by^2 \equiv -1 \pmod n \tag{3.19}$$

has solutions $x, y \in \mathbb{Z}$ for all $n \in \mathbb{N}$.

Immediate from this is the following result by Kimura and Williams.

Corollary 3.5 ([1, Theorem, p. 911]*) Let $a > 1$ divisible only by primes congruent to* 1 *or* 3 *modulo* 8*. Then*

$$2x^2 - (2a^4 + a^2)y^2 = -1$$

has no integer solutions, whereas

$$2x^2 - (2a^4 + a^2)y^2 \equiv -1 \pmod n$$

has integer solutions for all $n \in \mathbb{N}$.

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

References

[1] N. Kimura and K.S. Williams, *Infinitely many insolvable Diophantine equations* $f(x_1, x_2) = 0$ *such that* $f(x_1, x_2) \equiv 0 \pmod{m}$ *is solvable for every* m, Amer. Math. Monthly **111** (2004), 909–913.

[2] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, New York, London, Tokyo (1996).

[3] R.A. Mollin, **Fundamental Number Theory with Applications**, CRC Press, Boca Raton, New York, London, Tokyo (1998).

[4] R.A. Mollin, *A continued fraction approach to the Diophantine equation* $ax^2 - by^2 = \pm 1$, JP Journal Algebra, Number Theory, and Appl. **4** (2004), 159–207.

[5] R.A. Mollin, *Infinitely many quadratic diophantine equations solvable everywhere locally, but not solvable globally*, JP Journal Algebra, Number Theory and Appl. **4**, 353– 362

[6] R.A. Mollin, *Norm Form Equations and Continued Fractions*, Acta Math. Univ. Comenianae, **LXXIV** (2005), 273–278.

[7] R.A. Mollin, *Global Versus Local Solvability of Quadratic Diophantine Equations*, International Math. Forum **1** (2006), 1625–1633.

[8] T. Nagell, *On a special class of Diophantine equations of the second degree*, Ark. Mat. **3** (1954), 51–65.

[9] W. Sierpiński, **Elementary Theory of Numbers**, North-Holland (PWN), Amsterdam, New York, Oxford (1988).

Received: December 8, 2006