ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 31, Number 2, Summer 2001

A GENERALIZATION OF A THEOREM OF COHN ON THE EQUATION $x^3 - Ny^2 = \pm 1$

F. LUCA AND P.G. WALSH

1. Introduction. In [**2**], Cohn investigated the solvability of the Diophantine equation

$$x^3 - Ny^2 = \pm 1. \tag{1.1}$$

Improving upon previous work of Stroeker [**5**], Cohn proved the following theorem.

Theorem A. *Let N denote a squarefree positive integer with no prime factor of the form $3k+1$. Then the equation $x^3 - Ny^2 = 1$ has no solutions in positive integers, and the equation $x^3 - Ny^2 = -1$ has no solutions in positive integers, unless $N \in \{1, 2\}$, in which case $(N, x, y) = (1, 2, 3)$ and $(N, x, y) = (2, 23, 78)$ are the only solutions.*

The interesting case in this theorem arises when the irreducible quadratic factors of $x^3 \pm 1$ take on values of the form $3z^2$, for otherwise the result is an immediate consequence of quadratic reciprocity. Cohn deals with this case in a very clever manner by determining all of the integer solutions to the respective equations

$$x^2 + x + 1 = 3z^2, \qquad x - 1 = 3Nw^2$$

and

$$x^2 - x + 1 = 3z^2, \qquad x + 1 = 3Nw^2,$$

which are equivalent respectively to

$$3N^2w^4 + 3Nw^2 + 1 = z^2 \tag{1.2}$$

1991 AMS *Mathematics Subject Classification.* 11D25, 11J86.
Received by the editors on October 22, 1999, and in revised form on December 7, 1999.

and

$$3N^2w^4 - 3Nw^2 + 1 = z^2. \tag{1.3}$$

We reformulate Cohn's theorem in terms of these Diophantine equations as follows.

Theorem B. *If N is a squarefree integer not divisible by any prime $p \equiv 1 \pmod 3$, then (1.2) has no positive integer solutions (w, z), and (1.3) has no positive integers solutions unless $N \in \{1, 2\}$, in which case $(N, w, z) = (1, 1, 1)$ and $(N, w, z) = (2, 2, 13)$ are the only solutions.*

The purpose of this paper is to exhibit a more general result concerning integer points on a large class of elliptic curves, which includes the particular curves considered by Cohn. Using a recent result of Bennett and the second author [**1**], we prove the following theorem. If a positive integer n is of the form $n = ma^2$ for some squarefree positive integer m and an integer a, we refer to m as the *squarefree class* of n and denote it by $m = \langle n\rangle$.

Theorem 1. *Let d be a positive integer with $d \equiv 3 \pmod 4$, and let $\varepsilon_d = T + U\sqrt{d} > 1$ denote the minimal solution to $X^2 - dY^2 = 1$. Assume that T is even. Let N denote a squarefree positive integer which is not divisible by any odd prime p with $(-d/p) = 1$. Then the Diophantine equation*

$$dN^2w^4 + dUNw^2 + (T/2)^2 = z^2 \tag{1.4}$$

has no solutions in positive integers (w, z). Also, the Diophantine equation

$$dN^2w^4 - dUNw^2 + (T/2)^2 = z^2 \tag{1.5}$$

has no solutions in positive integers (w, z), except only if $N = \langle U\rangle$, in which case

$$(w, z) = \left(\sqrt{\frac{U}{N}}, T/2\right)$$

is the only solution, and $N = \langle 2U \rangle$*, in which case*

$$(w, z) = \left(T\sqrt{\frac{2U}{N}}, (T/2)(4T^2 - 3) \right)$$

is the only solution.

We remark that the special case of $d = 3$ in Theorem 1 is precisely Theorem B. We also note that, if d in Theorem 1 is prime, then it immediately holds that the corresponding integer T is even, and so the assumption being made can be removed. To see this, suppose that T is odd. Then $T \pm 1 = 2du^2$ and $T \mp 1 = 2v^2$, and hence $u^2 - dv^2 = \pm 1$ for some positive integers u and v. Since $d \equiv 3 \pmod 4$, the only possibility is $u^2 - dv^2 = 1$, and this contradicts the minimality of the solution (T, U) to $X^2 - dY^2 = 1$.

General algorithmic procedures for completely solving a given quartic Diophantine equation of the form $y^2 = f(x)$ have been developed. Such methods are described explicitly in [**6**]. For a recent survey on quartic Diophantine equations, the reader may wish to consult [**7**], while for more applications of the results of [**1**], we refer the reader to [**8**] and [**9**].

2. Preliminary results. Throughout the paper we will make reference to the following notation. For a nonsquare positive integer d, let $T + U\sqrt{d}$ denote the minimal solution in positive integers to the Pell equation $X^2 - dY^2 = 1$, and for $k \geq 1$, let $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$. We interchangeably use T_1, respectively U_1, for T, respectively U, and vice versa. For more details on properties of terms in Lucas sequences, the reader is referred to [**4**].

The following was proved by Cohn in [**3**] and will be used to prove Theorem 1.

Lemma 1. *If* $T_k = x^2$ *for some integer* x*, then* $k = 1$ *or* $k = 2$*. Moreover, if* T_1 *and* T_2 *are both squares, then* $T + U\sqrt{d} = 169 + 4\sqrt{1785}$.

An immediate corollary to Lemma 1 and the previously cited work in [**1**] is the following, which forms the basis to prove Theorem 1.

Lemma 2. *If $T_k/T_1 = x^2$ for some positive integer x, then $k = 1$.*

Proof. First note that, for T_k/T_1 to be an integer, k must be odd. By Lemma 1, it follows that there are integers b, u, v with $b > 1$ and squarefree, such that $T_k = bu^2$ and $T_1 = bv^2$. By the main result of [**1**], this implies that $k = 1$.

Lemma 3. *If p is an odd prime divisor of some term T_k, then $(-d/p) = 1$.*

Proof. As $T_k^2 - 1 = dU_k^2$, it follows that there are positive integers a, b, r, s such that $T_k - 1 = ra^2$ and $T_k + 1 = sb^2$, where either $d = rs$ and $U_k = ab$, or $4d = rs$ and $U_k = 2ab$. In either case, $2T_k = ra^2 + sb^2$, and so if p is a prime factor of T_k, then $ra^2 \equiv -sb^2 \pmod p$. Since $\gcd(T_k, U_k) = 1$, we have that $\gcd(p, b) = 1$ and so $(ra(2^\delta b)^{-1})^2 \equiv -d \pmod p$, where $\delta \in \{0, 1\}$, proving the lemma.

Lemma 4. *For all $k \geq 1$, $U_{2k+1} - U_1 = 2U_kT_{k+1}$ and $U_{2k+1} + U_1 = 2T_kU_{k+1}$.*

Proof. We prove the first equality, as the second is proved in the same manner. Using basic properties of solutions to Pell equations, we have the following

$$\begin{aligned}
U_{2k+1} - U_1 &= T_{2k}U_1 + T_1U_{2k} - U_1 \\
&= (2T_k^2 - 2)U_1 + 2T_1T_kU_k \\
&= 2dU_k^2U_1 + 2T_1T_kU_k \\
&= U_k(2dU_kU_1 + 2T_1T_k) \\
&= 2U_kT_{k+1}.
\end{aligned}$$

3. Proof of Theorem 1. We first consider (1.4). Let $s = (dU_1 - 1)/2$ and $r = (d+1)/4$; then from (1.4) it is easily deduced, with $x = dNw^2 + s$, that $x^2 + x + r = dz^2$, and hence

$$(2z)^2 - d\left(\frac{2x+1}{d}\right)^2 = 1.$$

Therefore, $U_l = (2x+1)/d$ for some $l \geq 1$, and since $T_l = 2z$, it follows that l is odd. Let $l = 2k+1$, then from the definition of s and of x,

$$dU_{2k+1} - dU_1 = 2x + 1 - 2s - 1 = 2(x-s) = 2dNw^2,$$

and hence $U_{2k+1} - U_1 = 2Nw^2$. By Lemma 4, this implies that

$$U_k T_{k+1} = Nw^2. \tag{3.1}$$

Assume first that k is odd. In this case we claim that $\gcd(U_k, T_{k+1}) = 1$. To see this, by the definition of the sequences $\{T_k\}$ and $\{U_k\}$, one has the relation $U_k = U_{k+1}T_1 - T_{k+1}U_1$, and so if p divides both U_k and T_{k+1}, then p divides either U_{k+1} or p divides T_1. The former case is clearly not possible, and so p divides T_1. Since T_1 divides U_2, p divides $\gcd(U_k, U_2) = U_{\gcd(k,2)} = U_1$, a contradiction proving the claim.

By our assumption on the prime factors of N, together with Lemma 3, (3.1) shows that $T_{k+1} = v^2$ or $T_{k+1} = 2v^2$ for some integer v. Since $k+1$ is even, T_{k+1} is odd, and so only the case $T_{k+1} = v^2$ can occur. By Lemma 1, $k+1 = 2$, and so $T_2 = v^2$. But $T_2 = 2T_1^2 - 1$, and so $v^2 - 2T_1^2 = -1$, forcing T_1 to be odd, contradicting the hypothesis that T_1 is even.

Now assume that k is even, $k = 2m$. Then

$$\begin{aligned} 2Nw^2 &= U_{2m}T_{2m+1} = U_2(U_{2m}/U_2)T_1(T_{2m+1}/T_1) \\ &= 2T_1U_1(U_{2m}/U_2)T_1(T_{2m+1}/T_1) \end{aligned}$$

from which it follows that there is another integer y for which

$$Ny^2 = U_1(U_{2m}/U_2)(T_{2m+1}/T_1).$$

In a manner similar to the above case, it is easy to show that $\gcd(U_1(U_{2m}/U_2), (T_{2m+1}/T_1)) = 1$. Therefore, by the assumption on the prime factors of N, together with Lemma 3, it follows that $T_{2m+1}/T_1 = v^2$ for some integer v. We deduce from Lemma 2 that $m = 0$, hence $k = 0$, and so $U_k = U_0 = 0$, which shows that $w = 0$. Thus, (1.4) has no solutions in positive integers.

We now consider (1.5). Let s and r be defined as above; then with $x = dNw^2 - s$, we find that (1.5) yields $x^2 - x + r = dz^2$, and hence

$$(2z)^2 - d\left(\frac{2x-1}{d}\right)^2 = 1.$$

Therefore, $U_{2k+1} = (2x-1)/d$ for some $k \geq 0$. If $k = 0$, then $dU_1 = 2x-1$, and from the definition of s this entails that $dNw^2 = x+s = dU_1$, that is, $N = \langle U_1 \rangle$. It follows that $w = \sqrt{U_1/N}$ and $z = T_1/2$.

Henceforth assume that $k \geq 1$. From the definitions of s and x, $U_{2k+1} + U_1 = 2Nw^2$, and so an application of Lemma 4 gives

$$T_k U_{k+1} = Nw^2. \tag{3.2}$$

Assume first that k is even; then, as argued above, $\gcd(T_k, U_{k+1}) = 1$. By the assumption on the prime factors of N together with Lemma 1, Lemma 3 and the fact that T_k is odd, we find that $T_2 = v^2$ for some integer v. But this implies that T_1 is odd, which contradicts our hypothesis on T_1.

Assume now that k is odd. Then

$$Nw^2 = T_1(T_k/T_1)2T_1U_1(U_{k+1}/U_2)$$

and it follows that

$$N(w/T_1)^2 = (T_k/T_1)2U_1(U_{k+1}/U_2). \tag{3.3}$$

As argued in an earlier case $\gcd((T_k/T_1), 2U_1(U_{k+1}/U_2)) = 1$, and so it follows from the assumption on the prime factors of N, together with Lemma 3, that T_k/T_1 is a square. Therefore, we conclude from Lemma 2 that $k = 1$. Thus, (3.3) becomes $N(w/T_1)^2 = 2U_1$, from which we obtain $N = \langle 2U_1 \rangle$, $w = T_1\sqrt{2U_1/N}$, and $z = (T_1/2)(4T_1^2-3)$.

REFERENCES

1. M.A. Bennett and P.G. Walsh, *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proc. Amer. Math. Soc. **127** (1999),

2. J.H.E. Cohn, *The Diophantine equations* $x^3 = Ny^2 \pm 1$, Quart. J. Math. Oxford **42** (1991), 27–30.

3. ———, *The Diophantine equation* $x^4 - Dy^2 = 1$, II, Acta Arith. **78** (1997), 401–403.

4. D.H. Lehmer, *An extended theory of Lucas functions*, Ann. Math. **31** (1930), 419–448.

5. R.J. Stroeker, *On the Diophantine equation* $x^3 - Dy^2 = 1$, Nieuw Arch. Wisk. **24** (1976), 231–255.

6. N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, Acta Arith. **75** (1996), 165–190.

7. P.G. Walsh, *Diophantine equations of the form* $aX^4 - bY^2 = \pm 1$, *Proc. ICM Satellite Conf. in Graz on Analytic Number Theory and Diophantine Analysis* (R. Tichy, ed.), 1998, to appear.

8. ———, *A note on a theorem of Ljunggren and the Diophantine equations* $x^2 - kxy^2 + y^4 = 1, 4$, Arch. Math. **73** (1999), 119–125.

9. ———, *The Diophantine equation* $X^2 - db^2Y^4 = 1$, Acta Arith. **87** (1998), 179–188.

MATHEMATICAL INSTITUTE, CZECH ACADEMY OF SCIENCES, ŽITNÁ 25, 115 67 PRAHA 1, CZECH REPUBLIC
E-mail address: `luca@matserv.math.cas.cz`

Current address: INSTITUTO DE MATEMATICAS UNAM, CAMPUS MORELIA, APARTADO POSTAL 61-3 (XANGARI) CP 58 089, MORELIA, MICHOACAN, MEXICO

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OTTAWA, 585 KING EDWARD ST., OTTAWA, ONTARIO, CANADA K2H-5V9
E-mail address: `gwalsh@mathstat.uottawa.ca`