ACTA ARITHMETICA
138.4 (2009)

# On the number of large integer points on elliptic curves

by

P. G. Walsh (Ottawa)

**1. Introduction.** We are interested in the number and size of integer points on certain families of plane curves of genus 1. Such is the work of Evertse and Silverman [2], wherein it is shown that for any $\epsilon > 0$, the number of integer solutions to an equation of the form

$$y^2 = f(x) = x^3 + bx^2 + cx + d,$$

with $b, c, d \in \mathbb{Z}$ and discriminant $\Delta(f)$ nonzero, is bounded by $c(\epsilon)|\Delta(f)|^{1/2+\epsilon}$ for some effectively computable $c(\epsilon) > 0$. The results we present here are substantially more restrictive, however they are quite different, and do improve upon the results in [2] in certain cases.

The results presented here are based on a recent theorem of Akhtari [1], which we now state.

Theorem A (Akhtari, 2008). *Let $F(x, y)$ be a reduced binary quartic form with integer coefficients, which is irreducible over $\mathbb{Q}$, and which splits over $\mathbb{R}$. If $J_F = 0$, then the inequality $|F(x, y)| \leq h$ has at most twelve integer solutions $(x, y)$ with*

$$|y| \geq \frac{h^{3/4}}{(3I)^{1/8}}.$$

All of the conditions in Theorem A will be fully explained in the paper. The particular condition $J_F = 0$ forces us to be quite restrictive in our applications to cubic and quartic curves.

In what follows, $D > 1$ and $N$ will denote positive squarefree integers, $k < 0$ will denote a negative squarefree integer coprime to $D$. We will be interested in the quartic equation

$$X^2 - DY^4 = k, \tag{1.1}$$

2000 *Mathematics Subject Classification*: Primary 11D25; Secondary 11B39.
*Key words and phrases*: elliptic curve, quadratic field, Thue equation.

DOI: 10.4064/aa138-4-2

and the cubic equation

$$Y^2 = X^3 - NX. \tag{1.2}$$

Notation. For a nonzero integer $k$, let $\omega(k)$ denote the number of distinct prime factors of $k$. Also, $n(D,k)$ denotes the number of classes of coprime solutions $(x,y)$ to the quadratic equation $x^2 - Dy^2 = k$, which will be defined in Section 3. Finally, for a squarefree positive integer $D > 1$, we let $\epsilon_D$ denote the minimal unit greater than 1 in $\mathbb{Z}[\sqrt{D}]$ of positive norm. We present our results in terms of $\epsilon_D$, since this allows us to explicitly show how the bounds we obtain depend on this unit. Moreover, this unit can often be quite small, and one can therefore obtain practical upper bounds. In general, however, it is known that this unit can be very large. In fact, the best result known to this author is $\epsilon_D < e^{D^{1/2}(\log(4D)+2)}$ (see [4]).

Theorem 1.1. *There are at most* $48n(D,k)$ *integer solutions to* (1.1) *with*

$$|Y| > \frac{2^{5/4}|k|^{39/4}\epsilon_D^{45/4}}{D^{13/4}}.$$

The value of $n(D,k)$ is not altogether very well understood, but generally depends on the arithmetic of the field $\mathbb{Q}(\sqrt{D})$. In the worst possible case, one has $n(D,k) \le 2^{\omega(k)}$, and so if $k$ has few distinct prime factors, then $n(D,k)$ is small.

Corollary 1.1. *There are at most* $48 \cdot 2^{\omega(k)}$ *integer solutions to* (1.1) *with*

$$|Y| > \frac{2^{5/4}|k|^{39/4}\epsilon_D^{45/4}}{D^{13/4}}.$$

Let $N$ denote a squarefree positive integer. An integer solution to the equation $Y^2 = X^3 - NX = X(X^2 - N)$, with $X = Dy^2$ and $X^2 - N = Dx^2$, gives rise to a positive integer solution $(x,y)$ to the equation $x^2 - Dy^4 = -N/D$, where $D \mid N$. In this case, if either $D < 0$ or $D = 1$, then the positive integers $x$ and $y$ must be relatively small. If $D > 1$, we can appeal to Corollary 1.1, which yields the following application to cubic curves of the form (1.2).

Theorem 1.2. *There are at most* $48\sum_{D\mid N} 2^{\omega(D)}$ *integer solutions to* (1.2) *with*

$$|X| > \max_{D\mid N,\, D>1} \frac{2^{5/2}|N/D|^{39/2}\epsilon_D^{45/2}}{D^{11/2}}.$$

Apart from the small solutions, below the quantitative bound in Theorem 1.2, Theorem 1.2 compares favourably with the results in [2] in the case where $N$ has few prime factors.

**2. Generalized Pythagorean triples.** The following lemma appears in [7]. We will later need to make reference to it, and to some of the variables contained in the proof, and so we provide all the details for completeness.

LEMMA 2.1. *Let $a, b, c$ be nonzero integers with $(a, b, c) = 1$, and such that the Diophantine equation*

$$ax^2 + by^2 + cz^2 = 0 \tag{2.1}$$

*has a solution in integers $x, y, z$ not all zero. Then there are integers $R_1, S_1, T_1, R_2, S_2, T_2, z_1$, depending only on $a, b, c$, satisfying the relations*

$$R_1T_2 + R_2T_1 = 2S_1S_2 \tag{2.2}$$

*and*

$$S_1^2 - R_1T_1 = -bcz_1^2, \qquad S_2^2 - R_2T_2 = -acz_1^2, \tag{2.3}$$

*and a nonzero integer $\delta$, depending only on $a, b, c$, such that for every nonzero solution $(x, y, z)$ of* (2.1), *there exist integers $Q, u, v$ and a divisor $P$ of $\delta$ so that*

$$Px = Q(R_1u^2 - 2S_1uv + T_1v^2), \qquad Py = Q(R_2u^2 - 2S_2uv + T_2v^2).$$

*The integers $R_1, R_2, T_1, T_2$ satisfy $R_1T_2 - R_2T_1 = 0$, and furthermore, if* $\gcd(x, y, z)$ *is bounded, then an upper bound for $Q$ can be determined.*

*Proof.* We follow Tzanakis' arguments in [7]. First put $a = a_0A^2, b = b_0B^2, c = c_0C^2$ with $a_0, b_0, c_0$ squarefree, so that (2.1) becomes

$$a_0(Ax)^2 + b_0(By)^2 + c_0(Cz)^2 = 0. \tag{2.4}$$

Let $d = (a_0, b_0), e = (a_0, c_0), f = (b_0, c_0)$. Then by hypothesis it follows that

$$(d, e) = (d, f) = (e, f) = 1$$

and

$$a_0 = dea_1, \quad b_0 = dfb_1, \quad c_0 = efc_1, \quad Ax = fX, \quad By = eY, \quad Cz = dZ,$$

for integers $a_1, b_1, c_1, X, Y, Z$. Now (2.4) becomes

$$a_1fX^2 + b_1eY^2 + c_1dZ^2 = 0, \tag{2.5}$$

which has coefficients which are pairwise relatively prime and squarefree. By hypothesis, (2.5) has a nonzero solution $(x_1, y_1, z_1)$, which will be used in what follows. We may now appeal to formula 20 on p. 225 of [6], where it is proved that there exist coprime integers $u, v$ such that the solutions to (2.5) take the form

$$\begin{aligned} d_1\frac{X}{Q} &= -a_1fx_1u^2 - 2b_1ey_1uv + b_1ex_1v^2, \\ d_1\frac{Y}{Q} &= a_1fy_1u^2 - 2a_1fx_1uv - b_1ey_1v^2, \\ \pm d_1\frac{Z}{Q} &= a_1fz_1u^2 + b_1ez_1v^2, \end{aligned}$$

with $d_1$ representing the greatest common divisor of the three expressions on the right-hand sides and $Q = \gcd(X, Y, Z)$. Multiplying the first relation by $fBC$, and recalling that $fX = Ax$, it follows that

$$d_1ABCx = Q(-a_1f^2BCx_1u^2 - 2b_1efBCy_1uv + b_1efBCx_1v^2),$$

which we rewrite as

$$Px = Q(R_1u^2 - 2S_1uv + T_1v^2). \tag{2.6}$$

Similarly, multiplying the second relation by $eAC$, and recalling that $eY = By$, it follows that

$$d_1ABCy = Q(a_1efACy_1u^2 - 2a_1efACx_1uv - b_1e^2ACy_1v^2),$$

which we rewrite as

$$Py = Q(R_2u^2 - 2S_2uv + T_2v^2). \tag{2.7}$$

It is readily verified that $R_1, S_1, T_1, R_2, S_2, T_2$, as defined in (2.6) and (2.7), satisfy the relations (2.2) and (2.3). Also, as proved in [7], $P = d_1ABC$ is a divisor of $\delta = 2a_1b_1c_1d_1efABCz_1^3$. To see that $R_1T_2 - R_2T_1 = 0$, observe that the above expressions for these values show that $R_1T_2 = R_2T_1 = a_1b_1e^2f^2ABC^2x_1y_1$. Finally, as noted in [7], if $M$ represents an upper bound for $\gcd(x, y, z)$, then $Q \le M \cdot \gcd(A, B, C)$.

We will need to have an upper bound for the smallest nontrivial solution to the equation $ax^2 + by^2 + cz^2 = 0$. A discussion on this topic is given in Chapter 7 of [5], however we will use the quantitative result due to Holzer [3].

LEMMA 2.2. *Let $a, b, c$ denote nonzero, pairwise coprime squarefree integers. If equation* (2.1) *has a nontrivial solution, then there is at least one nontrivial solution* $(x, y, z)$ *with*

$$|x| < \sqrt{|bc|}, \quad |y| < \sqrt{|ac|}, \quad |z| < \sqrt{|ab|}.$$

**3. Pellian equations.** In this section, we make some brief definitions and remarks on solutions to Pellian equations, which will be used later in the paper. In particular, we provide the necessary background on the equation

$$X^2 - DY^2 = k. \tag{3.1}$$

For further details, the reader is referred to Section 58 in Chapter VI of [6].

Let $D$ denote a nonsquare positive integer, and let

$$\epsilon_D = T + U\sqrt{D}$$

denote the minimal unit greater than 1 in the ring $\mathbb{Z}[\sqrt{D}]$ with positive norm. We note that both $T$ and $U$ are positive integers. Let $k$ denote a nonzero integer, and assume that $x_0, y_0$ are nonzero integers satisfying (3.1). Let $\alpha = x_0 + y_0\sqrt{D}$, and for $i \in \mathbb{Z}$, define

$$x_i + y_i\sqrt{D} = \alpha \cdot \epsilon^i. \tag{3.2}$$

Then each pair $x_i, y_i$ is a solution to (3.1), and the set of all such solutions is referred to as the *class* of solutions to (3.1) associated to $x_0, y_0$. As noted in [6], a necessary and sufficient condition for two solutions $u_1 + v_1\sqrt{D}$, $u_2 + v_2\sqrt{D}$ to the equation $x^2 - Dy^2 = k$ to be associated is that the two numbers

$$\frac{u_1u_2 - v_1v_2D}{k} \quad \text{and} \quad \frac{v_1u_2 - v_2u_1}{k}$$

be integers.

Among all solutions $x + y\sqrt{D}$ to (3.1) belonging to a given class, say $C$, we choose a solution $x^* + y^*\sqrt{D}$ in the following way: Let $y^*$ be the least positive value of $y$ which occurs in $C$ and let $x^*$ be positive, satisfying $(x^*)^2 - D(y^*)^2 = k$. Then, by the way $y^*$ was chosen, at least one of $x^* + y^*\sqrt{D}$ and $-x^* + y^*\sqrt{D}$ belongs to $C$. If both belong, then we define $x^* + y^*\sqrt{D}$ as the fundamental solution of the class $C$. Otherwise, we define the fundamental solution $\alpha^*$ as the sole solution among $x^* + y^*\sqrt{D}$ and $-x^* + y^*\sqrt{D}$ which belongs to $C$.

We will be interested in the case that $k$ is negative. In this case, Theorem 108a in [6] gives information on the size of the fundamental solution of a class. In particular, with $T$ and $U$ as defined above, Nagell proves the following.

Lemma 3.1. *With all the notation as above, we have*

$$0 < y^* < \frac{U}{\sqrt{2(T-1)}}\sqrt{|k|}, \qquad 0 < |x|^* < \sqrt{(1/2)(T-1)|k|}.$$

Along with bounds for the size of the fundamental solution of a class, we will need to refer to upper bounds for the number of classes of solutions to an equation of the form (3.1). Note that the above lemma shows that the number of classes is finite.

Notation. For a nonsquare positive integer $D$, and a nonzero integer $k$ for which (3.1) is solvable, denote by $n(D, k)$ the number of classes of solutions to equation (3.1).

It is important to note that if $x^* + y^*\sqrt{D}$ is a fundamental solution to (3.1) with $(x^*, y^*) = 1$, then all solutions $x + y\sqrt{D}$ in that class satisfy $(x, y) = 1$. Conversely, if $x + y\sqrt{D}$ is any solution to (3.1) with $(x, y) = 1$, then the fundamental solution of that class also has this property.

Lemma 3.2. *Let $D$ and $k$ be as above. The number of classes of solutions in coprime integers to* (3.1) *is at most* $2^{\omega(k)}$, *where $\omega(k)$ represents the number of distinct prime factors of $k$.*

*Proof.* For simplicity of exposition, we will restrict our attention to the case where $k$ is squarefree, as the proof extends to the general case in an identical manner. Let $t = \omega(k)$, and assume that $k$ has the factorization into primes given by $k = p_1 \cdots p_t$. Assuming that $x^2 - Dy^2 = k$ is solvable in coprime positive integers $x, y$, it follows that $D$ is a square modulo each of the $p_i$, and so for $1 \le i \le t$, we define $\Delta_i$ to be a fixed square root of $D$ modulo $p_i$. Assume that there are $l > 2^t$ solutions $\alpha_1 = u_1 + v_1\sqrt{D}, \ldots, \alpha_l = u_l + v_l\sqrt{D}$ to $x^2 - Dy^2 = k$. We will show that there is at least one pair of associated solutions among them. For each $1 \le i \le t$ and $1 \le j \le l$, we see that $u_j^2 \equiv Dv_j^2 \pmod{p_i}$, and so for each pair $i, j$ in these ranges, we define $\epsilon_{i,j} \in \{1, -1\}$ by

$$u_j \equiv \epsilon_{i,j} \Delta_i v_j \pmod{p_i}.$$

Since $l > 2^t$, there are values $j_1, j_2$ for which $\epsilon_{i,j_1} = \epsilon_{i,j_2}$ for all $1 \le i \le t$. It is readily deduced from this that both

$$\frac{u_{j_1}u_{j_2} - v_{j_1}v_{j_2}D}{k} \quad \text{and} \quad \frac{v_{j_1}u_{j_2} - v_{j_2}u_{j_1}}{k}$$

are integers, and hence $\alpha_{j_1}$ and $\alpha_{j_2}$ are associated solutions.

In the case where $D$ and $k$ are squarefree, solutions to (3.1) are necessarily coprime, and so we record the following for later use.

Corollary 3.1. *Let $D > 0$ and $k$ be squarefree integers. Then*

$$n(D, k) \le 2^{\omega(k)}.$$

**4. The reduction to Thue equations.** Throughout this section, $D$ denotes a positive squarefree integer and $k$ denotes a negative squarefree integer. Let $(X, Y)$ be a solution to equation (1.1) with $X, Y$ positive. Then $X + Y^2\sqrt{D}$ is a solution to (3.1) belonging to a certain class $C$ of solutions. Denote by $x^* + y^*\sqrt{D}$ the fundamental solution of $C$. Then

$$X + Y^2\sqrt{D} = (x^* + y^*\sqrt{D})\epsilon_D^i \quad (i \in \mathbb{Z}),$$

where $\epsilon_D$ is defined in Section 3. Let $s + t\sqrt{D} = x^* + y^*\sqrt{D}$ if $i$ is even and $s + t\sqrt{D} = (x^* + y^*\sqrt{D})\epsilon_D$ if $i$ is odd. It is easy to see that $t > 0$ and, since $k$ is squarefree, that $\gcd(t, k) = 1$.

The above preliminaries imply that there is an integer $j$ for which

$$X + Y^2\sqrt{D} = (s + t\sqrt{D})(T + U\sqrt{D})^{2j}.$$

Let $m + n\sqrt{D} = (T + U\sqrt{D})^j$. Then $m^2 - Dn^2 = 1$ and

$$X + Y^2\sqrt{D} = (s + t\sqrt{D})(m + n\sqrt{D})^2 = (s + t\sqrt{D})(m^2 + Dn^2 + 2mn\sqrt{D}),$$

from which it follows that

$$Y^2 = tm^2 + 2smn + tDn^2.$$

Multiplying the above through by $t$, completing the square, and using the fact that $s^2 - Dt^2 = k$, gives

$$-(tm + sn)^2 + kn^2 + tY^2 = 0. \tag{4.1}$$

We now use Lemma 2.1 with $(-1,k,t)$ in place of $(a,b,c)$. We remark that these coefficients are pairwise coprime. We obtain

$$P(tm+sn)=Q(R_1u^2-2S_1uv+T_1v^2),\qquad Pn=Q(R_2u^2-2S_2uv+T_2v^2),$$

where, since $\gcd(m,n)=1$, it follows that $\gcd(u,v)=1$.

Solving the above equations for $m$ and $n$, and using $m^2-Dn^2=1$, it follows that

$$\begin{aligned}(4.2)\qquad [(R_1-sR_2)u^2-2(S_1-sS_2)uv+(T_1-sT_2)v^2]^2&\\ -D(R_2tu^2-2S_2tuv+T_2tv^2)^2=(Pt/Q)^2.&\end{aligned}$$

**5. The hypotheses of Theorem 1.1.** The purpose of this section is to show that the Thue equation in (4.2) satisfies all of the hypotheses of Theorem A stated in Section 1. In the situation at hand

$$(5.1)\qquad F(u,v)=a_0u^4+a_1u^3v+a_2u^2v^2+a_3uv^3+a_4v^4,$$

where, by the identity $s^2-Dt^2=k$, the coefficients are given explicitly by

$$\begin{aligned}a_0&=R_1^2-2sR_1R_2+kR_2^2,\\ a_1&=-4(R_1S_1-sR_1S_2-sR_2S_1+kR_2S_2),\\ a_2&=6(R_1T_1-sR_2T_1-sR_1T_2+kR_2T_2),\\ a_3&=-4(S_1T_1-sS_1T_2-sS_2T_1+kS_2T_2),\\ a_4&=T_1^2-2sT_1T_2+kT_2^2.\end{aligned}$$

The quantity $J_F$ stated in Theorem A is given by

$$-72a_0a_2a_4-9a_1a_2a_3+2a_2^3+27a_0a_3^2+27a_4a_1^2,$$

and the result of substituting the expressions for the $a_i$ into $J_F$ is a polynomial of degree 6 in $R_1,R_2,S_1,S_2,T_1,T_2$. We forego displaying this rather lengthy polynomial here, but make the important remark that this polynomial can be written as another polynomial with integer coefficients in terms of $R_1,R_2,T_1,T_2,S_1^2,S_2^2,2S_1S_2$. Remarkably, upon using the identities (2.2) and (2.3), replacing the quantities $S_1^2,S_2^2,2S_1S_2$ by their respective values, it is readily found that $J_F=0$. We performed this check using the symbolic algebra package Maple.

Theorem A requires that $F(u,v)$ be reduced. This condition can be described in terms of the *Hessian*

$$H(u,v)=\frac{\partial^2F}{\partial u^2}\,\frac{\partial^2F}{\partial v^2}-\left(\frac{\partial^2F}{\partial u\partial v}\right)^2.$$

As noted in Section 7 of [1], since $J_F=0$,

$$(-1/9)H(u,v)=M^2(u,v),$$

where $M(u,v) = au^2 + buv + cv^2 \in \mathbb{Z}[u,v]$ is a positive definite quadratic form. $M(u,v)$ is said to be *reduced* if $|b| \le a \le c$, and $F(u,v)$ is defined as being reduced if $M(u,v)$ is reduced.

In the case at hand, it will be shown that $b = 0$, from which it immediately follows that $F(u,v)$ is reduced.

With $F(u,v)$ as in (5.1), then

$$H(u,v) = A_0u^4 + A_1u^3v + A_2u^2v^2 + A_3uv^3 + A_4v^4,$$

where the coefficients are given explicitly in terms of $F(u,v)$ by

$$\begin{aligned} A_0 &= 3(8a_0a_2 - 3a_1^2), & A_3 &= 12(6a_1a_4 - a_2a_3),\\ A_1 &= 12(6a_0a_3 - a_1a_2), & A_4 &= 3(8a_2a_4 - 3a_3^2).\\ A_2 &= 6(3a_1a_3 + 24a_0a_4 - 2a_2^2), \end{aligned}$$

Substituting the above expressions for $a_0, a_1, a_2, a_3, a_4$ into $A_1$ and $A_3$, and using (2.2),(2.3) to simplify the result, we find that

$$\begin{aligned} A_1 &= 288(s^2 - k)(R_1T_2 - R_2T_1)(S_2R_1 - S_1R_2),\\ A_3 &= -288(s^2 - k)(R_1T_2 - R_2T_1)(S_2T_1 - S_1T_2), \end{aligned}$$

which both vanish by the assertion in Lemma 2.1 that $R_1T_2 - R_2T_1 = 0$. Therefore, the coefficients of $M(u,v)$ satisfy $ab = bc = 0$, from which it follows that $b = 0$, since $M(u,v)$ is positive definite.

To complete the analysis of the hypotheses of Theorem A, we study the roots of the two quadratic polynomials

$$\begin{aligned} &[R_1 - R_2(s + \nu t\sqrt{D})]Z^2 - 2[S_1 - S_2(s + \nu t\sqrt{D})]Z\\ &\qquad\qquad + [T_1 - T_2(s + \nu t\sqrt{D})] \quad (\nu = \pm 1), \end{aligned}$$

the product of which is the dehomogenization of the homogeneous quartic in (4.2).

Using the quadratic formula, we find that the discriminants of these quadratic factors are given by

$$\begin{aligned} &4(S_1 - S_2(s \pm t\sqrt{D}))^2 - 4(R_1 - R_2(s \pm t\sqrt{D}))(T_1 - T_2(s \pm t\sqrt{D}))\\ &\quad = 4[S_1^2 - 2S_1S_2(s \pm t\sqrt{D}) + S_2^2(s \pm t\sqrt{D})^2]\\ &\qquad - 4[R_1T_1 - (R_1T_2 + R_2T_1)(s \pm t\sqrt{D}) + R_2T_2(s \pm t\sqrt{D})^2]. \end{aligned}$$

By (2.2), the middle terms vanish, which after some rearranging, and applying Lemma 2.1 again, results in

$$4(S_1^2 - R_1T_1) + 4(s \pm t\sqrt{D})^2(S_2^2 - R_2T_2) = 4(-ktz_1^2) + 4(s \pm t\sqrt{D})^2(tz_1^2).$$

Some further simplifications result in that the discriminants of the two quadratic polynomials above are given by

$$8t^2z_1^2\sqrt{D}(\pm s + t\sqrt{D}). \tag{5.2}$$

Recall that $s^2 - Dt^2 = k < 0$, and so $\pm s + t\sqrt{D}$ is positive for both choices of sign. It follows that all of the roots of the two quadratic polynomials above are real, and since these are precisely the roots of $F(u,1)$, we see that $F(u,v)$ splits over $\mathbb{R}$.

The final condition remaining is to verify that $F(u,v)$ is irreducible over $\mathbb{Q}$. This is actually a consequence of the explicit description of the discriminants of the two quadratic factors of $F(u,1)$ given in (5.2). In particular, from the fact that $D$ is squarefree, it is a simple exercise to verify that none of the expressions in (5.2) are squares of elements in $\mathbb{Q}(\sqrt{D})$.

**6. Bounds.** The purpose of this section is to prove an upper bound for $|Y|$ for the nonexceptional solutions, and a bound for the number of exceptional (large) solutions, where

$$X^2 - DY^4 = k, \tag{6.1}$$

with $k < 0$, and both $k$ and $D$ are squarefree.

Let $(X,Y)$ be a positive integer solution to (6.1). The element $X+Y^2\sqrt{D}$ lies in a class of solutions to

$$X^2 - DY^2 = k. \tag{6.2}$$

Our conclusions concerning $X + Y^2\sqrt{D}$ are stated in Section 4.

The upper bound for $|Y|$ will be given in terms of $k, D, \epsilon_D$. It is preferrable to present the upper bound for $|Y|$ in this way, as it shows the dependence on $\epsilon_D$, and also shows that the bound can be small at times (when $\epsilon_D$ is small).

Note that by Lemma 3.1, we have the following upper bounds for $x^*, y^*$:

$$|x^*| \le \sqrt{\frac{|k|(T-1)}{2}}, \qquad y^* \le U\sqrt{\frac{|k|}{2(T-1)}}. \tag{6.3}$$

Using (6.3), it follows that

$$|s| \le (1/2)\epsilon_D^{3/2}\sqrt{|k|}, \qquad t \le \epsilon_D^{3/2}\sqrt{|k|/2D}.$$

We apply Lemma 2.1 to equation (4.1) with specific values $a = -1$, $b = k$, $c = t$. Because of the fact that $k$ is squarefree, some of the particular values arising in the proof of Lemma 2.1 are as follows: $a_0 = -1$, $A = 1$, $b_0 = k$, $B = 1$, $c_0C^2 = t$, $d = e = f = 1$, and moreover, $a_1 = -1, b_1 = k$, and $c_1 = c_0$.

We now apply Lemma 2.2 to the quadratic equation (4.1). By Lemma 2.2, and using the fact that $c_0 \le t$, we may assert that there is a positive integer solution $(x_1, y_1, z_1)$ to (4.1) with

$$x_1 \le \sqrt{|kt|}, \qquad y_1 \le \sqrt{t}, \qquad z_1 \le \sqrt{|k|}.$$

We can now bound the quantity $P$ appearing in the proof of Lemma 2.1. As shown in that proof,

$$|P| = |dABC| \leq |2a_1b_1c_1defABCz_1^3|,$$

but since many of the factors therein are ±1, we get

$$|P| \leq |2b_1c_1Cz_1^3| \leq 2t|k|(\sqrt{|k|})^3 \leq 2t|k|^{5/2}. \tag{6.5}$$

We now derive upper bounds for $|R_2|, |S_2|, |T_2|$ by using the quantities each of these terms represents in the proof of Lemma 2.1. In the case of $R_2$, we see that

$$|R_2| \leq |-a_1efACy_1| \leq |Cy_1| \leq t.$$

In fact, a similar argument shows that $|S_2| \leq t\sqrt{|k|}$ and that $|T_2| \leq t|k|$.

An upper bound for $|Q|$ can be determined from the proof of Lemma 2.1. If $M$ represents $\gcd(x, y, z)$, then $Q \leq M \gcd(A, B, C) = M$. Recall that

$$-x^2 + ky^2 + z^2 = -(tm + sn)^2 + kn^2 + tY^2 = 0,$$

and so if $p$ is a prime dividing $M$, and $p^{w_1}$ properly divides $M$, then $p^{w_2}$ properly divides $\gcd(tm+sn, n)$ for some $w_2 \geq w_1$. Also, since $\gcd(m, n) = 1$, it follows that $p^{w_2}$ divides $t$. Therefore,

$$|Q| \leq M \leq t.$$

We now derive upper bounds for the quantities $|m|$ and $|n|$. By Theorem A, we may assume that both $|u|$ and $|v|$ are bounded by $((Pt)^2)^{3/4}$, but at the price of there being 24 exceptional solutions instead of 12. We will generously disregard the factor $(3I)^{1/8}$ appearing in Theorem A, since it has little effect on the final bounds obtained here.

Using the expression for $Pn$ in Section 4, and the above bounds, we deduce that

$$\begin{aligned}|Pn| &\leq |Q(R_2u^2 - 2S_2uv + T_2v^2)|\\ &\leq 4t\max(|R_2|, |S_2|, |T_2|)\max(|u^2|, |uv|, |v^2|) \leq 4t(t|k|)(Pt)^3,\end{aligned}$$

and therefore,

$$|n| \leq 4t^5|k|P^2 \leq 4t^5|k|(2t|k|^{5/2})^2 \leq 16t^7|k|^6.$$

We recall that $m^2 - Dn^2 = 1$, and so $|m - n\sqrt{D}|$ is very small. By the discreteness of the integers, along with the fact that we were at times somewhat conservative in estimating $|n|$, we get

$$|m| \leq |n|\sqrt{D} \leq 16\sqrt{D}\,t^7|k|^6.$$

We are now in a position to obtain a bound for $|Y|$. Recall from Section 4 that $Y^2 = tm^2+2smn+tDn^2$, so that by the above bounds for $|m|, |n|, |s|, t$,

$$Y^2 \leq 2^{10}Dt^{15}k^{12},$$

and so by using the bound

$$t \le \epsilon_D^{3/2}\sqrt{|k|/2D},$$

we deduce that

$$|Y| \le \frac{2^{5/4}|k|^{39/4}\epsilon_D^{45/4}}{D^{13/4}}.$$

We complete the proof by estimating the number of exceptional large solutions. Since $D$ and $k$ are squarefree, any solution in integers $x, y$ to $x^2 - Dy^2 = k$ has the property that $x$ and $y$ are coprime. By Lemma 3.2, the number of classes of solutions to $x^2 - Dy^2 = k$ is at most $2^{\omega(k)}$. For each class, the above analysis shows that one gets two cases depending on the parity of $i$, and two cases in order to assert that both $|u|$ and $|v|$ are bounded by $((Pt)^2)^{3/4} = (Pt)^{3/2}$. In total then, there are at most

$$12 \cdot 2^{\omega(k)+2}$$

exceptional solutions.

**Acknowledgements.** The author gratefully acknowledges discussions on this topic with Shabnam Akhtari and Michael Bennett, along with the extremely helpful comments by an anonymous referee. The author also gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

## References

[1] S. Akhtari, *The method of Thue–Siegel for binary quartic forms*, Acta Arith., to appear.

[2] J.-H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to* $Y^n = f(X)$, Math. Proc. Cambridge Philos. Soc. 100 (1986), 237–248.

[3] L. Holzer, *Minimal solutions of diophantine equations*, Canad. J. Math. 11 (1950), 238–244.

[4] H. W. Lenstra, Jr., *Solving the Pell equation*, Notices Amer. Math. Soc. 49 (2002), 182–192.

[5] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[6] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1964.

[7] N. Tzanakis, *On the diophantine equation* $x^2 - Dy^4 = k$, Acta Arith. 46 (1986), 257–269.

Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada, K1N 6N5
E-mail: gwalsh@uottawa.ca

*Received on 27.5.2008*
*and in revised form on 11.2.2009* (5719)