ACTA ARITHMETICA
107.3 (2003)

Bounds for the smallest integer point of a rational curve

by

Dimitrios Poulakis (Thessaloniki)

1. Introduction. Let $F(X,Y)$ be an absolutely irreducible polynomial with integer coefficients of degree ≥ 2 such that the curve C defined by the equation $F(X,Y)=0$ is rational. Let $\overline{\mathbb{Q}}$ be an algebraic closure of the field $\mathbb{Q}$ of rational numbers and $\overline{\mathbb{Q}}(C)$ the function field of C over $\overline{\mathbb{Q}}$. Consider the valuation ring V_∞ of $\overline{\mathbb{Q}}(X)$ consisting of all elements $f(X)/g(X)$ such that $\deg f \leq \deg g$. We denote by C_∞ the set of discrete valuation rings of $\overline{\mathbb{Q}}(C)$ lying above V_∞. We call an element V of C_∞ *defined over a subfield* k of $\overline{\mathbb{Q}}$ if $\tau(V)=V$ for every $\tau \in \mathrm{Gal}(\overline{k}/k)$. Furthermore, we say that two elements V and W of C_∞ are *conjugate* over a quadratic field k if V and W are defined over k and there is $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which is not the identity on k such that $\sigma(V)=W$. Finally, we denote by $C(\mathbb{Z})$ the set of integer solutions to the equation $F(X,Y)=0$.

In the case where $|C_\infty| \geq 3$, E. Maillet [8], [9] proved that $C(\mathbb{Z})$ is finite (see also [6, Theorem 6.1, p. 146] and [7, Chapter 8, Section 5]). The first explicit upper bound for the elements of $C(\mathbb{Z})$ was obtained in [13] by using Baker's method. For a more recent result see [17]. Furthermore, a practical method for the explicit determination of all elements of $C(\mathbb{Z})$ is obtained in [18]. Let us consider the case where $|C_\infty| \leq 2$. In [19], a practical method for the explicit determination of all elements of $C(\mathbb{Z})$ is given. Note that in this case $C(\mathbb{Z})$ may have infinitely many elements. A necessary and sufficient condition for C to have infinitely many integer points is obtained in [19]. More precisely the following result has been proved:

Theorem A. *The set $C(\mathbb{Z})$ is infinite if and only if one of the following two conditions is satisfied*:

(a) *C_∞ consists of one element and $C(\mathbb{Z})$ has at least one simple point.*

(b) *C_∞ consists of two elements which are conjugate over a real quadratic field and $C(\mathbb{Z})$ has at least one simple point.*

2000 *Mathematics Subject Classification*: Primary 11D41; Secondary 11G30, 14H25.

Thus it is natural to ask for an estimate for the size of the smallest simple integer point on a rational curve $F(X,Y)=0$ satisfying (a) or (b). The purpose of this paper is to provide such an estimate. Moreover, in the case where C_∞ has only two elements which are defined over $\mathbb{Q}$ or are conjugate over a complex quadratic field, we calculate a bound for the size of all integer points on the rational curve $F(X,Y)=0$.

Let d be the g.c.d. of the coefficients of $F(X,Y)$. We define the *height* $H(F)$ of $F(X,Y)$ to be the maximum of $|f|/d$ over all the coefficients f of $F(X,Y)$. Finally, we set $N=\max\{\deg_X F, \deg_Y F\}$. We prove the following results:

THEOREM 1.1. *Suppose that $|C_\infty|=1$ and $C(\mathbb{Z})$ has at least one simple point. Then there is a simple point (x,y) of $C(\mathbb{Z})$ satisfying*

$$\max\{|x|,|y|\} < (5N^6e^N H(F)^2)^{72N^9}.$$

THEOREM 1.2. *Suppose that $|C_\infty|=2$. We have the following three cases*:

(i) *If the two elements of C_∞ are defined over $\mathbb{Q}$, then the points $(x,y)\in C(\mathbb{Z})$ satisfy*

$$\max\{|x|,|y|\} < (5N^6e^N H(F)^2)^{1360N^{11}}.$$

(ii) *If the two elements of C_∞ are conjugate over a complex quadratic field, then the points $(x,y)\in C(\mathbb{Z})$ satisfy*

$$\max\{|x|,|y|\} < (5N^6e^N H(F)^2)^{682N^{11}}.$$

(iii) *If the two elements of C_∞ are conjugate over a real quadratic field and $C(\mathbb{Z})$ has at least one simple point, then there is a simple point (x,y) of $C(\mathbb{Z})$ satisfying*

$$\max\{|x|,|y|\} < \exp\{(5N^6e^N H(F)^2)^{24000N^{13}}\}.$$

In case (i) of Theorem 1.2, when the homogeneous part of higher degree of $F(X,Y)$ has the form $a_0(a_1X+a_2Y)^\mu(a_3X+a_4Y)^\nu$, [2] and [24, Theorem 1] imply a sharper estimate. Similarly, in case (ii), when the homogeneous part of higher degree of $F(X,Y)$ has the form $a_0(a_1X^2+a_2YX+a_3Y^2)^\nu$ with $a_2^2-4a_1a_3<0$, we obtain from [15, Theorem 3] a sharper bound. Let $F_h(X,Y,Z)$ be the homogenization of $F(X,Y)$. We recall that the points $(x:y:0)$ of the projective plane with $F_h(x,y,0)=0$ are called points of C at infinity. If the points of C at infinity, in cases (i) and (ii) of Theorem 1.2, are simple then the homogeneous part of highest degree of $F(X,Y)$ has the above form, respectively.

The aforementioned theorems generalise the results of [4] and [20] on the smallest integer points of conics. Note that Theorem 2 of [4] shows that

the existence of the exponential function in the bound of Theorem 1.2(iii) is inavoitable.

The present paper is organised as follows. In Section 2, we obtain an effective basis for the Riemann–Roch space of the divisor defined by the sum of elements of C_∞. In Section 3, we give some lemmas which will be used for the proof of our results. Finally, Sections 4 and 5 are devoted to the proofs of Theorems 1.1 and 1.2, respectively.

2. Construction of a Riemann–Roch basis. Let k be an algebraic number field of degree d. We consider the set of standard absolute values on $\mathbb{Q}$ containing the ordinary absolute value $|\cdot|$ and for every prime p the p-adic absolute value $|\cdot|_p$. If $x = p^r a/b$, where a, b are integers not divisible by p, then by definition $|x|_p = p^{-r}$. We denote by $M(k)$ the set of symbols v such that with every $v \in M(k)$ there is associated precisely one absolute value $|\cdot|_v$ on k which extends one of the above absolute values of $\mathbb{Q}$. For every $v \in M(k)$ we denote by d_v the local degree of the absolute value $|\cdot|_v$. Thus for every $a \in k \setminus \{0\}$ we have the product formula

$$\prod_{v \in M(k)} |a|_v^{d_v} = 1.$$

Furthermore, we denote by $M_0(k)$ and $M_\infty(k)$ the subsets of $M(k)$ consisting of the symbols v such that $|\cdot|_v$ is a nonarchimedean and archimedean absolute value, respectively.

If $\mathbf{x} = (x_0 : \ldots : x_r)$ is a point of the projective space $\mathbb{P}^r(k)$ over k, then we define the *field height* $H_k(\mathbf{x})$ of $\mathbf{x}$ by

$$H_k(\mathbf{x}) = \prod_{v \in M(k)} \max\{|x_0|_v, \ldots, |x_r|_v\}^{d_v}$$

and the *absolute height* $H(\mathbf{x})$ by $H(\mathbf{x}) = H_k(\mathbf{x})^{1/d}$. Further, for $x \in k$ we define $H_k(x) = H_k((1 : x))$ and $H(x) = H((1 : x))$. For $G \in k[X_1, \ldots, X_m]$, we define the field height $H_k(G)$ and the absolute height $H(G)$ of G as the field height and the absolute height of the point whose coordinates are the coefficients of G (in any order). If $|\cdot|_v$ is an absolute value of k, then we let $|G|_v$ be the maximum of $|g|_v$ over all the coefficients g of G. For $\mathbf{x} \in \mathbb{P}^r(\mathbb{Q})$, there are relatively prime integers $z_0, \ldots, z_r$ such that $\mathbf{x} = (z_0 : \ldots : z_r)$ and it follows that $H(\mathbf{x}) = \max\{|z_0|, \ldots, |z_r|\}$. Thus the definition of the height of $F(X, Y)$ given in the Introduction is consistent with the above definition. For an account of the properties of heights see [23, Chapter VIII] or [7, Chapter 3].

A *k-system* is a system $\{A_v\}_{v \in M(k)}$ of real numbers such that $A_v \geq 1$, $A_v = 1$ for all but finitely many v and A_v lies in the value group of $|\cdot|_v$ when $|\cdot|_v$ is nonarchimedean. The *field norm* of such a system is defined to

be

$$N_k\{A_v\} = \prod_{v\in M(k)} A_v^{d_v}.$$

LEMMA 2.1. *Let $F(X,Y)$ be a polynomial in $\mathbb{Z}[X,Y]$, without multiple factors, of degree $n \geq 2$ in Y and of degree $m \geq 1$ in X. Let $y(X) = c_0 + c_1X + \ldots$ be a power series satisfying $F(X, y(X)) = 0$. Then the coefficients $c_0, c_1, \ldots$ generate a number field K of degree $\delta \leq n$ and there are K-systems $\{A_v\}_{v\in M(K)}$ and $\{B_v\}_{v\in M(K)}$ with*

$$N_K\{A_v\} \leq (3e^{6n^2} n^n((m+1)^2(n+1)H(F)^2)^{2n-1})^\delta$$

and

$$N_K\{B_v\} \leq (3H(F)^2)^\delta$$

such that for every $v \in M(K)$,

$$|c_j|_v \leq A_v^{j+m} \quad (j = 0, 1, \ldots).$$

Proof. We may suppose, without loss of generality, that the coefficients of $F(X,Y)$ are relatively prime. A well-known theorem of Eisenstein asserts that there exist positive integers a_0 and a such that $a_0a^jc_j$ is an algebraic integer for all j. By [1], we have

$$a < ((m+1)H(F))^{2n-1}e^{6n^2}$$

and $a_0 = \lambda a^r$, where λ is a positive integer with $\lambda \leq |\alpha_r|$. Let K be the field generated by the coefficients $c_0, c_1, \ldots$ Since for every element $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have a series $y^\sigma(X) = \sigma(c_0)+\sigma(c_1)X+\ldots$ which is still a root of $F(X,Y)$, it follows that the degree of K is at most n.

For every $v \in M_0(K)$, we put $A_v = 1/|a|_v$ and $B_v = 1/|\lambda|_v$. Then

$$|c_j|_v \leq B_vA_v^{j+m} \quad (j = 0, 1, \ldots).$$

For all but finitely many $v \in M_0(K)$, we have $A_v = B_v = 1$ and A_v, B_v lie in the value group of $|\cdot|_v$. Furthermore, the product formula gives

$$\prod_{v\in M_0(K)} A_v^{d_v} = \prod_{v\in M_\infty(K)} |a|_v^{d_v} \leq (((m+1)H(F))^{2n-1}e^{6n^2})^\delta$$

and

$$\prod_{v\in M_0(K)} B_v^{d_v} = \prod_{v\in M_\infty(K)} |\lambda|_v^{d_v} \leq |a_r|^\delta.$$

Following the method of [21] and using [10, Corollary 2], we obtain

$$|c_j| < 2^{m+j}3H(F)(1 + ((m+1)(n+1)\sqrt{n}\,H(F))^{2n-1})^{m+j} \quad (j = 0, 1, \ldots).$$

Thus, given $v \in M_\infty(K)$, we have

$$|c_j|_v \leq B_vA_v^{j+m} \quad (j = 0, 1, \ldots),$$

where

$$A_v = 2 + 2((m+1)(n+1)\sqrt{n}\,H(F))^{2n-1} \quad \text{and} \quad B_v = 3H(F).$$

Finally, we conclude that the norms of the K-systems $\{A_v\}_{v\in M(K)}$ and $\{B_v\}_{v\in M(K)}$ satisfy the inequalities

$$N_K\{A_v\} \le (3e^{6n^2}n^n((m+1)^2(n+1)H(F)^2)^{2n-1})^\delta$$

and

$$N_K\{B_v\} \le (3H(F)^2)^\delta.$$

Let $F(X,Y)$ be an absolutely irreducible polynomial with integer coefficients. We assume that $F(X,Y)$ is of degree $m \ge 1$ in X and of degree $n \ge 2$ in Y. We denote by C the curve defined by the equation $F(X,Y) = 0$. Let $\Sigma(C)$ be the set of discrete valuation rings W of the function field $\overline{\mathbb{Q}}(C)$ of C such that $\overline{\mathbb{Q}} \subset W$. A divisor D on C is a formal sum

$$D = a_1W_1 + \ldots + a_sW_s,$$

where $a_1, \ldots, a_s \in \mathbb{Z}$ and $W_1, \ldots, W_s$ are pairwise distinct elements of $\Sigma(C)$. Given $f \in \overline{\mathbb{Q}}(C)$ and $W \in \Sigma(C)$, we denote by $\mathrm{ord}_W(f)$ the order of the function f at W. Let $L(D)$ be the set of functions $f \in \overline{\mathbb{Q}}(C)$ having $\mathrm{ord}_{W_i}(f) \ge -a_i$ and $\mathrm{ord}_W(f) \ge 0$ for every $W \in \Sigma(C)$, with $W \ne W_i$ $(i = 1, \ldots, s)$. Then $L(D)$ is a finite-dimensional vector space over $\overline{\mathbb{Q}}$ (see [5]).

Proposition 2.1. *Suppose C has genus zero and $C_\infty = \{V_1, \ldots, V_r\}$. Put $N = \max\{m,n\}$ and $E = V_1 + \ldots + V_r$. Then there are polynomials $g_i(X,Y)$ $(i = 1, \ldots, r+1)$ and $q(X)$ with integer coefficients satisfying*

$$\deg q < N^2, \quad \deg_X g_i < 4N^2, \quad \deg_Y g_i < N \quad (i = 1, \ldots, r+1)$$

and

$$H(q) < (6N^3H(F))^{2N^3}, \quad H(g_i) < H(F)^{67N^6}(5N^6e^N)^{34N^6} \quad (i = 1, \ldots, r+1)$$

such that the fractions $g_1(X,Y)/q(X), \ldots, g_{r+1}(X,Y)/q(X)$ represent a basis of the space $L(E)$.

Proof. By the Riemann–Roch theorem, $\dim L(E) = r+1$. Theorem A2 of [22] implies that there are polynomials $g_1(X,Y), \ldots, g_{r+1}(X,Y)$ and $q(X)$ satisfying

$$\deg q \le N(N-1), \quad \deg_X g_i < 4N^2, \quad \deg_Y g_i < N \quad (i = 1, \ldots, r+1)$$

such that the fractions $g_1(X,Y)/q(X), \ldots, g_{r+1}(X,Y)/q(X)$ represent a basis of the space $L(E)$. Furthermore, since the divisor E is defined over $\mathbb{Q}$, Theorem B2 of [22] shows that we may take the polynomials $g_1(X,Y), \ldots, g_{r+1}(X,Y)$ and $q(X)$ to have integer coefficients. Replacing Lemma 21 of [22] by the above Lemma 2.1 and making all the necessary changes in the

next lemmas, we deduce that the vectors $\delta_1, \dots, \delta_n$ of Lemma 26 of [22] satisfy

$$H(\delta_i) < (5N^6 e^N H(F)^2)^{33N^6} \quad (i = 1, \dots, n).$$

The equalities (A.5.6), (B.3.1) of [22] and the bound for $H(\delta_i)$ give the bound for $H(g_i)$.

Let $F_Y(X, Y)$ be the partial derivative of $F(X, Y)$ with respect to Y. We denote by $R(X)$ the resultant of $F(X, Y)$ and $F_Y(X, Y)$ with respect to Y. By [22, Lemma 4],

$$H(R) < (3N^3 H(F))^{2N-1}.$$

Let $D(X)$ be the discriminant of $F(X, Y)$ considered as a polynomial with coefficients in $\mathbb{Z}[X]$. By [22, Theorem A2], the roots of $q(X)$ are among the roots of $D(X)$. We may assume, without loss of generality, that

$$q(X) = (X - a_1) \dots (X - a_s),$$

where $s \le N(N-1)$. Since $D(X)$ divides $R(X)$, we have $R(a_i) = 0$ $(i = 1, \dots, r)$. Thus [14, Lemma 4] and [23, Theorem 5.9, p. 211] give

$$H(q) \le 2^{N(N-1)} H(a_1) \dots H(a_s) < (4H(R))^{N(N-1)}.$$

Finally, using the bound for $H(R)$, we obtain

$$H(q) < (6N^3 H(F))^{2N^3}.$$

3. Auxiliary results. In this section we give some results which will be used in the proofs of Theorems 1.1 and 1.2.

LEMMA 3.1 ([16, Lemma 3.2]). *Let $P(X, Y, V), Q(X, Y, W)$ be polynomials in $\mathbb{Z}[X, Y, V, W] \setminus \mathbb{Z}$. Denote by $R(X, V, W)$ the resultant of $P(X, Y, V)$ and $Q(X, Y, W)$, considered as polynomials with coefficients in $\mathbb{Z}[X, V, W]$. Put $\deg_X P = m_1$, $\deg_Y P = n_1$, $\deg_V P = r_1$ and $\deg_X Q = m_2$, $\deg_Y Q = n_2$, $\deg_W Q = r_2$. Assume that $R(X, V, W) \neq 0$. Then*

$$H(R) \le (n_1 + n_2)!((r_1 + 1)(m_1 + 1))^{n_2}((r_2 + 1)(m_2 + 1))^{n_1} H(P)^{n_2} H(Q)^{n_1}.$$

LEMMA 3.2 ([7, Proposition 2.4, p. 57]). *Let f and g be two polynomials in n variables with integer coefficients and $\deg f + \deg g < d$. Then*

$$4^{-d^n} H(fg) \le H(f)H(g) \le 4^{d^n} H(fg).$$

LEMMA 3.3 ([20]). *Let $G(X, Y) = aX^2 + bXY + cY^2 + dX + eY + f$ be a nondegenerate conic with integer coefficients. Set $\delta = b^2 - 4ac$. Suppose that (x, y) is an integer solution to $G(X, Y) = 0$. If $\delta < 0$, then*

$$\max\{|x|, |y|\} < 9H(G)^2$$

and if $\delta > 0$ is a perfect square, then

$$\max\{|x|, |y|\} < 20H(G)^4.$$

LEMMA 3.4 ([15, Lemma 7]). *Let $F(X,Y)$ be a polynomial in $\mathbb{Z}[X,Y]$ of degree $m>0$ in X and $n>0$ in Y. Let $x,y\in\mathbb{Q}$ with $F(x,y)=0$ and $\deg F(x,Y)=n$. Then*

$$H(y)<2(m+1)H(F)H(x)^m.$$

LEMMA 3.5 ([16, Lemma 5.1]). *Let $G(X,Y,Z)$ be a projective conic with integer coefficients. Suppose that the equation $G(X,Y,Z)=0$ has a solution over $\mathbb{Q}$. Then there are $x,y,z\in\mathbb{Q}$ with $G(x,y,z)=0$ such that*

$$H(x:y:z)<30H(G).$$

LEMMA 3.6. *Let $G(X,Y)$ be a conic with integer coefficients. Suppose that the equation $G(X,Y)=0$ has a solution $(x,y)\in\mathbb{Q}^2$. Then there are polynomials $f_1(T),f_2(T),f_3(T)\in\mathbb{Z}[T]$ of degree ≤ 2 such that the conic $G(X,Y)$ has the parametrization*

$$X=\frac{f_1(T)}{f_3(T)},\qquad Y=\frac{f_2(T)}{f_3(T)}$$

and the polynomials $f_1(T)-Sf_3(T)$, $f_2(T)-Sf_3(T)\in\mathbb{Z}[T,S]$ satisfy

$$H(f_i(T)-Sf_3(T))\le 3H(x,y,1)H(G)\quad (i=1,2).$$

Proof. Write

$$G(X,Y)=\alpha X^2+\beta XY+\gamma Y^2+\delta X+\varepsilon Y+\zeta=0.$$

Setting $Y=y+T(X-x)$ in the equation $G(X,Y)=0$, we obtain

$$X=\frac{f_1(T)}{f_3(T)}\quad\text{and}\quad Y=\frac{f_2(T)}{f_3(T)},$$

where

$$\begin{aligned}f_1(T)&=\alpha xT^2-(2\alpha y+\varepsilon)T-\beta x-\gamma y,\\ f_2(T)&=(-\alpha y+\varepsilon+\gamma x)T^2-2\beta xT+\beta y,\\ f_3(T)&=T^2+\gamma T+\beta.\end{aligned}$$

For every $v\in M(\mathbb{Q})$ we have

$$|f_i(T)-Sf_3(T)|_v\le|G|_v\max\{|x|_v,|y|_v,1\}3^{e(v)},$$

where $e(v)=1$ if $|\cdot|_v$ is archimedean and $e(v)=0$ otherwise. Thus the result follows.

LEMMA 3.7. *Let $R(X,Z,W)=R_0(Z,W)X^\mu+\ldots+R_\mu(Z,W)$ be a polynomial in $\mathbb{Z}[X,Z,W]$, $M=\max_{0\le i\le\mu}\{\deg R_i\}$ and $R_{i,h}(Z,W,U)$ the homogenization of $R_i(Z,W)$. Suppose that $f(T),g(T),h(T)\in\mathbb{Z}[T]$ with degrees ≤ 2. Set $R_i'(T)=R_{i,h}(f(T),g(T),h(T))h(T)^{M-\deg R_i}$ and $R'(X,T)=R_0'(T)X^\mu+\ldots+R_\mu'(T)$. Then*

$$H(R')<4^{3M^2+5M}3M^2H(R)H(\Theta)^M,$$

where Θ is a point in the projective space with coordinates the coefficients of $f(T)$, $g(T)$ and $h(T)$.

Proof. Let $|\cdot|_v$ be an absolute value of $\mathbb{Q}$. Using Propositions 2.1 and 2.3 of [7, Chapter 3], we obtain

$$|f^k g^l h^{M-k-l}|_v < |f^k|_v |g^l|_v |h^{M-k-l}|_v 4^{(3M^2+5M)e(v)},$$

where $e(v) = 1$ if $|\cdot|_v$ is archimedean and $e(v) = 0$ otherwise. Thus

$$|R_i'(T)|_v < |R|_v \max\{|f|_v, |g|_v, |h|_v\}^M (4^{3M^2+5M} 3M^2)^{e(v)},$$

which yields the required result.

LEMMA 3.8. *Let δ be a positive integer which is not a perfect square and A any nonzero integer. Suppose that the equation $X^2 - \delta Y^2 = A$ has an integer solution (x_0, y_0). Let (a, b) be the fundamental solution of the equation $X^2 - \delta Y^2 = 1$. Then there exists a fundamental solution (α, β) of the equation $X^2 - \delta Y^2 = A$ such that for every positive integer M, there are integers m, n with $0 \le m < n \le M^2$ and solutions (z_i, w_i) of $X^2 - \delta Y^2 = A$ given by*

$$z_i + w_i\sqrt{\delta} = (a + b\sqrt{\delta})^{m+in}(\alpha + \beta\sqrt{\delta}) \quad (i = 0, 1, \ldots),$$

which satisfy

$$z_i \equiv x_0 \pmod{M} \quad \textit{and} \quad w_i \equiv y_0 \pmod{M}.$$

Proof. Let the solutions (a_i, b_i) $(i = 0, \pm 1, \pm 2, \ldots)$ of $X^2 - \delta Y^2 = 1$ be defined by $a_i + b_i\sqrt{\delta} = (a + b\sqrt{\delta})^i$. Considering $(a_1, b_1), \ldots, (a_{M^2+1}, b_{M^2+1})$, we see that there are at least two indices $1 \le j < s \le M^2 + 1$ such that $(a_j, b_j) \equiv (a_s, b_s) \pmod{M}$, and so $(a_n, b_n) \equiv (1, 0) \pmod{M}$, where $n = s - j$. It follows that for every integer i we have $a_{in} \equiv 1 \pmod{M}$ and $b_{in} \equiv 0 \pmod{M}$.

Let (α, β) be a fundamental solution of the equation $X^2 - \delta Y^2 = A$ and k a positive integer such that

$$x_0 + y_0\sqrt{\delta} = \pm(a + b\sqrt{\delta})^k(\alpha + \beta\sqrt{\delta}).$$

Write $k = nq + m$ with $0 \le m < n$. It follows that

$$x_0 + y_0\sqrt{\delta} = (c + d\sqrt{\delta})(a_{qn} + b_{qn}\sqrt{\delta}),$$

where

$$c + d\sqrt{\delta} = \pm(a_m + b_m\sqrt{\delta})(\alpha + \beta\sqrt{\delta}).$$

Since $a_{qn} \equiv 1 \pmod{M}$ and $b_{qn} \equiv 0 \pmod{M}$, we find that $x_0 \equiv c \pmod{M}$ and $y_0 \equiv d \pmod{M}$. On the other hand, we deduce that the solutions (z_i, w_i) of $X^2 - \delta Y^2 = A$ given by

$$z_i + w_i\sqrt{\delta} = (c + d\sqrt{\delta})(a_{in} + b_{in}\sqrt{\delta}) \quad (i = 0, 1, \ldots),$$

satisfy $z_i \equiv c \pmod M$ and $w_i \equiv d \pmod M$, and so we obtain the required result.

REMARK. For an account of the solutions of $X^2 - \delta Y^2 = A$ see [11] or [12].

LEMMA 3.9 ([17, Lemma 3.1]). *Let $f(T)$, $g(T)$ be two relatively prime polynomials in $\mathbb{Z}[T]$ with degrees $n \geq 1$ and $m \geq 1$ respectively. Let Ω be a point in a projective space having as coordinates 1 and the coefficients of $f(T)$ and $g(T)$ (in any order). Then there exist $\alpha \in \mathbb{Z}\backslash\{0\}$ and $A(T), B(T) \in \mathbb{Z}[T]$ with $\deg A(T) < m$, $\deg B(T) < n$, and*

$$H(\alpha), H(A), H(B) \leq (m+n-1)! H(\Omega)^{m+n-1}$$

satisfying

$$A(T)f(T) + B(T)g(T) = \alpha.$$

LEMMA 3.10 ([18, Lemma 2.1]). *Let $F(X,Y,Z)$ be a homogeneous, absolutely irreducible polynomial in $\mathbb{Q}[X,Y,Z]$ of degree $M \geq 3$ and C the projective curve defined by $F(X,Y,Z) = 0$. Let $u(S,T), v(S,T), w(S,T) \in \mathbb{Z}[S,T]$ be homogeneous polynomials of the same degree, with no common nonconstant factor, such that the correspondence*

$$(S,T) \mapsto (u(S,T), v(S,T), w(S,T))$$

defines a birational map ϕ over $\mathbb{Q}$ of $\mathbb{P}^1$ to C. Then ϕ is a birational morphism of $\mathbb{P}^1$ onto C and $\deg u(S,T) = \deg v(S,T) = \deg w(S,T) = M$. Furthermore, if $(x : y : 1)$ is a nonsingular point of C defined over $\mathbb{Q}$, then there exist $s, t \in \mathbb{Z}$ with $s \geq 0$ and $\gcd(s,t) = 1$ such that $x = u(s,t)/w(s,t)$ and $y = v(s,t)/w(s,t)$.

LEMMA 3.11. *Let δ be a positive nonsquare integer and (a,b) the fundamental solution of the equation $X^2 - \delta Y^2 = 1$. Then*

$$a + b\sqrt{\delta} < \exp\{\sqrt{\delta}\,(2 + \log 4\delta)\}.$$

Moreover, if (α, β) is a fundamental solution of equation $X^2 - \delta Y^2 = A$, where A is a nonzero integer, then

$$\max\{|\alpha|, |\beta|\} < \frac{1}{2}\sqrt{|A|}\exp\{\sqrt{\delta}\,(2 + \log 4\delta)\}.$$

Proof. The bound for $a + b\sqrt{\delta}$ is obtained in [4, p. 86] as a consequence of a result of Hua [3]. This bound and [11, Theorems 6.2.5 and 6.2.6] or [12, Theorems 108 and 108a] imply the estimate for $\max\{|\alpha|, |\beta|\}$.

LEMMA 3.12. *Let $f(X,Y)$ be an irreducible polynomial in $\mathbb{Z}[X,Y]$ such that the equation $f(X,Y) = 0$ has infinitely many integer solutions. Then the highest terms in X and Y occur separately, as aX^m, bY^n.*

Proof. This is a consequence of Runge's theorem about Diophantine equations (see [24]).

4. Proof of Theorem 1.1. Suppose that $\Sigma_\infty = \{V\}$. If $\deg F = 2$ then Lemma 3.3(i) implies the result. So, we may assume $\deg F \geq 3$. By Proposition 2.1, there are polynomials $g_i(X,Y)$ $(i = 1,2)$ and $q(X)$, with integer coefficients, satisfying

$$\deg q < N^2, \quad \deg_X g_i < 4N^2, \quad \deg_Y g_i < N \quad (i = 1,2)$$

and

$$H(q) < (6N^3 H(F))^{2N^3}, \quad H(g_i) < H(F)^{67N^6}(5N^6 e^N)^{34N^6} \quad (i = 1,2),$$

such that the functions f_1 and f_2 represented by the fractions $g_1(X,Y)/q(X)$ and $g_2(X,Y)/q(X)$ form a basis of the space $L(V)$. Since $1 \in L(V)$, we may suppose, without loss of generality, that $f_1 = 1$.

The function $t = f_2$ lies in $\mathbb{Q}(C)$ and has only a pole at V of order 1. Thus $\mathbb{Q}(C) = \mathbb{Q}(t)$. Let x and y be the coordinate functions on C. Since the only pole of x is at V, we see that $x = A(t)/a$, where a is a positive integer and $A(t)$ a polynomial in t with integer coefficients. In view of our hypothesis, we may suppose that the homogeneous part of highest degree of $F(X,Y)$ has the form $a_0(a_1X + a_2Y)^n$ with $a_2 \neq 0$. It follows that y is an integral element over the ring $\mathbb{Q}[x]$, whence y has only a pole at V. Thus, $y = B(t)/b$, where b is a positive integer and $B(t)$ a polynomial in t with integer coefficients.

Put $\Phi(X,Y,T) = q(X)T - g_2(X,Y)$. We denote by $R_1(X,T)$ and $R_2(Y,T)$ the resultants of $\Phi(X,Y,T)$ and $F(X,Y)$, respectively, with respect to Y and X. Lemma 3.1 yields

$$H(R_i) < (5N^6 e^N)^{35N^7} H(F)^{68N^7} \quad (i = 1,2).$$

Further, $\deg_X R_1 < 4N^3 + N^2$, $\deg_Y R_2 < 4N^3 + N^2$ and $\deg_T R_i \leq N$ $(i = 1,2)$. Moreover, $R_1(x,t) = 0$ and $R_2(y,t) = 0$. It follows that $aX - A(T)$ and $bY - B(T)$ divide $R_1(X,T)$ and $R_2(Y,T)$, respectively. Using Lemma 3.2 we obtain

$$H(aX - A(T)), H(bY - B(T)) < (5N^6 e^N)^{36N^7} H(F)^{68N^7}.$$

Furthermore, $\deg A \leq N$ and $\deg B \leq N$.

Let (x_0, y_0) be a nonsingular integer point of C. Thus, Lemma 3.10 shows that there are integers s_0, t_0, with $\gcd(s_0, t_0) = 1$, and $t_0 \neq 0$ such that $x_0 = A_h(s_0,t_0)/at_0^\mu$ and $y_0 = B_h(s_0,t_0)/bt_0^\nu$, where $A_h(S,T)$, $B_h(S,T)$ are the homogenizations of $A(T)$, $B(T)$, respectively, and $\deg A = \mu$, $\deg B = \nu$. Hence at_0^μ divides $A_h(s_0,t_0)$ and bt_0^ν divides $B_h(s_0,t_0)$. If α and β are the leading coefficients of $A(T)$ and $B(T)$, respectively, then t_0 divides $\gcd(\alpha,\beta)$. Further, s_0 is a solution of the congruences

$$a' t_0^{M-\mu} A_h(S,t_0) \equiv 0 \pmod{L|t_0|^M}, \quad b' t_0^{M-\nu} B_h(S,t_0) \equiv 0 \pmod{L|t_0|^M},$$

where $L = \operatorname{lcm}(a,b)$, $a' = L/a$, $b' = L/b$ and $M = \max\{\mu,\nu\}$. On the other

hand, Bézout's theorem implies that C has at most $(N-1)^2$ singular points at finite distance. Thus there exists an integer s_1, with $|s_1| < N^2 L|t_0|^M/2$, satisfying the above congruences such that (x_1, y_1), with $x_1 = A_h(s_1, t_0)/at_0^\mu$ and $y_1 = B_h(s_1, t_0)/bt_0^\nu$, is a simple point on C. We have

$$|x_1| \le |A|(N+1)\max\{|s_1|, |t_0|\}^M \le N^{2N}|A|L^N|t_0|^{N^2} \le N^{2N}|A|^{1+N^2}(ab)^N.$$

Hence, we obtain

$$|x_1| < N^{2N}((5N^6e^N)^9 H(F)^{17})^{4(N+1)^2N^7}.$$

Similarly, we deduce that the same bound is valid for $|y_1|$.

5. Proof of Theorem 1.2. Suppose that $\Sigma_\infty = \{V_1, V_2\}$. If $\deg F = 2$, then Lemma 3.3 implies the required result. Thus, assume that $\deg F \ge 3$. By Proposition 2.1, there is a basis $\{f_1, f_2, f_3\}$ of the space $L(V_1 + V_2)$ and polynomials $g_i(X, Y)$ $(i = 1, 2, 3)$, $q(X)$, with integer coefficients, satisfying

$$\deg q < N^2, \quad \deg_X g_i < 4N^2, \quad \deg_Y g_i < N \quad (i = 1, 2, 3)$$

and

$$H(q) < (6N^3 H(F))^{2N^3}, \quad H(g_i) < (5N^6e^N)^{34N^6} H(F)^{67N^6} \quad (i = 1, 2, 3),$$

such that the fraction $g_i(X, Y)/q(X)$ represents the function f_i. Since $1 \in L(V_1 + V_2)$, we may suppose that $f_1 = 1$. Further, we may suppose that the coefficients of each of the polynomials $g_i(X, Y)$ $(i = 2, 3)$ and $q(X)$ are relatively prime. If for every $i \in \{2, 3\}$ we have $\mathrm{ord}_{V_j}(f_i) \ge 0$, where $j \in \{1, 2\}$, then $1, f_2, f_3 \in L(V_k)$ with $k \in \{1, 2\} - \{j\}$. Since $\dim L(V_k) = 2$, it follows that the functions $1, f_2, f_3$ are $\overline{\mathbb{Q}}$-linearly dependent, which is a contradiction. Hence, for every $j \in \{1, 2\}$ there is $i \in \{2, 3\}$ such that $\mathrm{ord}_{V_j}(f_i) = -1$. It follows that there are $a, b, c, d \in \{0, \pm 1\}$ such that the functions $f = af_2 + bf_3$ and $g = cf_2 + df_3$ satisfy

$$\mathrm{ord}_{V_k}(f) = \mathrm{ord}_{V_k}(g) = -1 \quad (k = 1, 2).$$

Suppose that $f \in \overline{\mathbb{Q}}(g)$. Then $f = G_1(g)/G_2(g)$, where $G_i(T) \in \overline{\mathbb{Q}}[T]$ $(i = 1, 2)$ with $\gcd(G_1(T), G_2(T)) = 1$. Since f has poles only at V_1 and V_2, we deduce that $G_2(g)$ is a constant. Thus $f = AG_1(g)$, where $A \in \overline{\mathbb{Q}}$. We have

$$-1 = \mathrm{ord}_{V_j}(f) = (\deg G_1)\,\mathrm{ord}_{V_j}(g) = -(\deg G_1).$$

Thus $f = a_0 + a_1 g$, with $a_0, a_1 \in \overline{\mathbb{Q}}$, which is a contradiction. Hence f does not lie in $\overline{\mathbb{Q}}(g)$. On the other hand, since the only poles of g are at V_1 and V_2 with order 1, we have $[\overline{\mathbb{Q}}(C) : \overline{\mathbb{Q}}(g)] = 2$. Therefore $\overline{\mathbb{Q}}(C) = \overline{\mathbb{Q}}(f, g)$.

The functions $1, f, g, fg, f^2, g^2$ lie in the space $L(2V_1 + 2V_2)$. By the Riemann–Roch theorem, the dimension of $L(2V_1 + 2V_2)$ is equal to 5. It

follows that there are $b_i \in \overline{\mathbb{Q}}$ $(i = 1, \ldots, 5)$ such that

$$f^2 + b_1 g^2 + b_2 fg + b_3 f + b_4 g + b_5 = 0.$$

Since f does not lie in $\overline{\mathbb{Q}}(g)$, it follows that the polynomial

$$G(X, Y) = Y^2 + b_1 X^2 + b_2 YX + b_3 Y + b_4 X + b_5$$

is irreducible over $\overline{\mathbb{Q}}$. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we put

$$G^\sigma(X, Y) = Y^2 + \sigma(b_1)X^2 + \sigma(b_2)YX + \sigma(b_3)Y + \sigma(b_4)X + \sigma(b_5).$$

The polynomial $G^\sigma(X, Y)$ is irreducible over $\overline{\mathbb{Q}}$ and, since $f, g \in \mathbb{Q}(C)$, we have $G^\sigma(f, g) = \sigma(G(f, g)) = 0$. Hence $G^\sigma(X, Y) = G(X, Y)$. It follows that $\sigma(b_i) = b_i$ $(i = 1, \ldots, 5)$ and so $b_i \in \mathbb{Q}$ $(i = 1, \ldots, 5)$.

Put $h_1(X, Y) = ag_2(X, Y) + bg_3(X, Y)$ and $h_2(X, Y) = cg_2(X, Y) + dg_3(X, Y)$. We consider the polynomials

$$\Phi_1(X, Y, Z) = h_1(X, Y) - Zq(X), \qquad \Phi_2(X, Y, T) = h_2(X, Y) - Tq(X)$$

and denote by $R_1(X, Z)$, $R_2(X, T)$ the resultants of $\Phi_1(X, Y, Z)$, $\Phi_2(X, Y, T)$, respectively, with $F(X, Y)$ considered as polynomials in Y. Since the functions f and g are not zero, we have $R_i \neq 0$ $(i = 1, 2)$. Using Lemma 3.1 and the bounds for the degrees and heights of $g_i(X, Y)$, we deduce that

$$H(R_i) < H(F)^{68N^7}(5N^6 e^N)^{35N^7} \qquad (i = 1, 2).$$

Furthermore, $\deg_X R_i < 4N^3 + N^2$ $(i = 1, 2)$, $\deg_Z R_1 \leq N$ and $\deg_T R_2 \leq N$. Let $S(Z, T)$ be the resultant of $R_1(X, Z)$ and $R_2(X, T)$ with respect to X. If $S(Z, T)$ is zero, then $R_1(X, Z)$, $R_2(X, T)$ have a common factor of the form $A(X) \in \mathbb{Q}[X] \setminus \mathbb{Q}$. Then $R_1(X, Z) = A(X)P(X, Z)$, where $P(X, Z) \in \mathbb{Q}[X, Z]$. It follows that for every $x, z \in \overline{\mathbb{Q}}$ with $A(x) = 0$, there is $y \in \overline{\mathbb{Q}}$ such that $\Phi_1(x, y, z) = 0$ and $F(x, y) = 0$. Thus we have finitely many values for x and y and finitely many for z, which is a contradiction. Hence the polynomial $S(Z, T)$ is not zero. Furthermore, $\deg S < 9N^4$. By Lemma 3.1, we obtain

$$S(Z, T) < (5N^6 e^N)^{316N^{10}} H(F)^{612N^{10}}.$$

Now, if we denote by x and y the coordinate functions on the curve C we have $F(x, y) = 0$, $\Phi_1(x, y, f) = 0$ and $\Phi_2(x, y, g) = 0$. It follows that $R_1(x, f) = 0$ and $R_2(x, g) = 0$ and so $S(f, g) = 0$. Thus we deduce that the polynomial $G(X, Y)$ divides $S(X, Y)$. So Lemma 3.2 yields

$$H(G) \leq 4^{(\deg S+1)^2} H(S) < (5N^6 e^N)^{320N^{10}} H(F)^{612N^{10}}.$$

Let $I_i(X, Y) = B_{i,0}(X)Y^{s_i} + \ldots + B_{i,s_i}(X)$ $(i = 1, 2)$ be two irreducible polynomials with relatively prime integer coefficients such that $I_1(x, f) = 0$ and $I_2(x, g) = 0$. Since the only poles of f and g are at V_1 and V_2, it follows that $B_{i,0}(X) = \beta_i \in \mathbb{Z}$ $(i = 1, 2)$. The polynomial $I_i(X, Y)$ divides $R_i(X, Y)$

and so, using Lemma 3.2, we obtain

$$|\beta_i| \le H(I_i) \le 4^{(\deg R_i+1)^2} H(R_i) < (5N^6e^N)^{38N^7} H(F)^{68N^7} \quad (i=1,2).$$

Put $f' = \beta_1 f$ and $g' = \beta_2 g$. The functions f' and g' are integral elements over the ring $\mathbb{Z}[x]$. So, if $(u,v) \in \mathbb{Z}^2$ with $F(u,v)=0$, then $f'(u,v), g'(u,v) \in \mathbb{Z}$. On the other hand, the functions f' and g' satisfy the equation

$$G'(X,Y) = \gamma_1 Y^2 + \gamma_2 X^2 + \gamma_3 YX + \gamma_4 Y + \gamma_5 X + \gamma_6 = 0,$$

where

$$\gamma_1 = \beta_1^2, \quad \gamma_2 = \beta_2^2 b_1, \quad \gamma_3 = \beta_1\beta_2 b_2,$$
$$\gamma_4 = \beta_1^2\beta_2 b_3, \quad \gamma_5 = \beta_1\beta_2^2 b_4, \quad \gamma_6 = \beta_1^2\beta_2^2 b_5.$$

Furthermore,

$$H(G') < (5N^6e^N)^{339N^{10}} H(F)^{646N^{10}}.$$

We denote by K the conic defined by the equation $G'(f',g')=0$. Since K is irreducible, it follows that K is smooth and so the discrete valuation rings of $\overline{\mathbb{Q}}(C)$ are the local rings O_P at the points P of K.

We have the following three cases:

Case 1: *V_1 and V_2 are defined over $\mathbb{Q}$.* Then V_1 and V_2 are the local rings at the points P_1 and P_2 of K which are at infinity. Hence, P_1 and P_2 are defined over $\mathbb{Q}$. It follows that $\gamma_2^2 - 4\gamma_1\gamma_3$ is a nonzero perfect square. Let $(u,v) \in \mathbb{Z}^2$ with $F(u,v)=0$. Then $f'(u,v), g'(u,v) \in \mathbb{Z}$ and hence Lemma 3.3 yields

$$\max\{|f'(u,v)|, |g'(u,v)|\} < 20H(G')^4.$$

On the other hand, $f'(u,v) = \beta_1 f(u,v)$ and $R_1(u, f(u,v)) = 0$. By Lemma 3.4, we obtain

$$|u| < 2(N+1)H(R_1)H(f(u,v))^N \le 2(N+1)H(R_1)\max\{|f'(u,v)|, |\beta_1|\}^N.$$

Using the bounds for the quantities $H(R_1)$, $|\beta_1|$, $|f'(u,v)|$ and $H(G')$, we obtain

$$|u| < (5N^6e^N)^{1360N^{11}} H(F)^{2589N^{11}}.$$

Similarly, we deduce the same bound for $|v|$.

Case 2: *V_1 and V_2 are conjugate over an imaginary quadratic field k.* Then we deduce, as in Case 1, that the points P_1 and P_2 of K at infinity are defined over k, whence $\gamma_2^2 - 4\gamma_1\gamma_3 < 0$. Thus, working as in the previous case, we obtain

$$\max\{|u|, |v|\} < (5N^6e^N)^{682N^{11}} H(F)^{1297N^{11}}.$$

Case 3: *V_1 and V_2 are conjugate over a real quadratic field k.* Since the equation $F(X,Y)=0$ has infinitely many integer solutions, Lemma 3.12 implies that the highest powers of X and Y occur as isolated terms cX^m and dY^n. It follows that the function y is an integral element over the ring

$\mathbb{Q}[x]$. Further, the homogeneous part of highest degree of $F(X,Y)$ has the form either $a_0(a_1X + a_2Y)^\nu$ or $a_0(a_1X^2 + a_2XY + a_3Y^2)^\nu$. In the second case, if $a_1 = 0$ or $a_3 = 0$, then V_1 and V_2 are defined over $\mathbb{Q}$, which is a contradiction. Hence $a_1 \neq 0$ and $a_3 \neq 0$. So interchanging the roles of X and Y if necessary, we may suppose that $N = n$. Thus $n = \deg F \geq 3$. We denote by e_i the ramification index of $1/x$ in V_i. Since V_1 and V_2 are conjugate, we have $e_1 = e_2 = n/2$. So n is even, whence $N = n \geq 4$.

The poles of the function x are at V_1 and V_2 which are the local rings of the points of K at infinity. Thus $x \in O_P$ for every P on K which is not at infinity, whence x is regular on K. On the other hand, $f, g \in \mathbb{Q}(C)$. It follows that the fixed field of $\overline{\mathbb{Q}}(C) = \overline{\mathbb{Q}}(f,g)$ under the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is $\mathbb{Q}(C) = \mathbb{Q}(f,g)$. Hence, x is a regular function of $\mathbb{Q}(f,g)$. Thus there are $A(X,Y) \in \mathbb{Z}[X,Y]$ and $a \in \mathbb{Z}$ such that $x = A(f,g)/a$. Further, y is an integral element over $\mathbb{Q}[x]$, whence the only poles of y are at V_1 and V_2. Thus, as previously, there are $B(X,Y) \in \mathbb{Z}[X,Y]$ and $b \in \mathbb{Z}$ such that $y = B(f,g)/b$.

From our hypothesis that the curve C has a simple integer point, we infer that C has infinitely many points defined over $\mathbb{Q}$ and therefore the conic $G(f,g) = 0$ has a point defined over $\mathbb{Q}$. By Lemma 3.5, there is a point P on the projective closure of $G(f,g) = 0$ with coordinates over $\mathbb{Q}$ satisfying

$$H(P) < 30H(G).$$

Further, the fact that V_1 and V_2 are conjugate over a real quadratic field k implies that the points at infinity of the projective closure of $G(f,g) = 0$ are not defined over $\mathbb{Q}$. Hence, P is not at infinity. Thus Lemma 3.6 shows that the conic $G(f,g) = 0$ has the parametrization

$$f = \frac{f_1(t)}{f_3(t)}, \qquad g = \frac{f_2(t)}{f_3(t)},$$

where $f_1(T), f_2(T), f_3(T) \in \mathbb{Z}[T]$ with degree ≤ 2, such that the polynomials $f_i(T) - Zf_3(T)$ $(i = 1, 2)$ satisfy

$$H(f_i(T) - Zf_3(T)) \leq 90H(G)^2.$$

Since the only poles of f and g are at V_1 and V_2 which are conjugate over k, it follows that $\deg f_3 = 2$ and the two roots of $f_3(T)$ are distinct and conjugate over k.

Now, replacing f and g in $x = A(f,g)/a$ and $y = B(f,g)/b$ by $f_1(t)/f_3(t)$ and $f_2(t)/f_3(t)$, respectively, we see that there are $A_1(T), B_1(T) \in \mathbb{Z}[T]$ such that

$$x = \frac{A_1(t)}{af_3(t)^p}, \qquad y = \frac{B_1(t)}{bf_3(t)^q},$$

where p and q are positive integers. We have

$$p = -\operatorname{ord}_{V_j}(x) = e_j = n/2 = N/2.$$

Furthermore, since $\operatorname{ord}_{V_1}(y) = \operatorname{ord}_{V_2}(y)$, we obtain

$$q = -\operatorname{ord}_{V_j}(y) = [\overline{\mathbb{Q}}(C) : \overline{\mathbb{Q}}(y)]/2 = m/2.$$

Since x and y have no other poles than V_1 and V_2, we deduce that $\deg A_1 \le N$ and $\deg B_1 \le m$. Moreover, we may suppose, without loss of generality, that the coefficients of each of the polynomials $A_1(T) - aXf_3(T)^p$ and $B_1(T) - bYf_3(T)^q$ are relatively prime.

We denote by $R_3(X,Z,T)$ and $R_4(Y,Z,T)$ the resultants of $\Phi_1(X,Y,Z)$ and $\Phi_2(X,Y,T)$, respectively, with respect to Y and X. Lemma 3.1 gives

$$H(R_3) < (5N^6e^N)^{68N^7}H(F)^{134N^7}, \quad H(R_4) < (5N^6e^N)^{272N^8}H(F)^{536N^8}.$$

Further, $\deg_X R_3 \le 8N^2(N-1)$, $\deg_Z R_3 \le N-1$, $\deg_T R_3 \le N-1$, $\deg_Y R_4 \le 8N^2(N-1)$, $\deg_Z R_4 < 4N^2$ and $\deg_T R_4 < 4N^2$. Moreover, $R_3(x,f,g) = 0$ and $R_4(y,f,g) = 0$. Let

$$R_3(X,Z,T) = R_{3,0}(Z,T)X^\mu + \ldots + R_{3,\mu}(Z,T)$$

and $M = \max_{0\le i\le\mu}\{\deg R_i\}$. We set

$$R'_{3,i}(T) = R_{3,i,h}(f_1(T), f_2(T), f_3(T))f_3(T)^{M-\deg R_i},$$

where $R_{3,i,h}(Z,T,U)$ is the homogenization of $R_{3,i}(Z,T)$. By Lemma 3.7, the height of the polynomial $R'_3(X,T) = R'_{3,0}(T)X^\mu + \ldots + R'_{3,\mu}(T)$ satisfies

$$H(R'_3) < 2^{24N^2}H(R_3)H(\Theta)^{2N-2},$$

where Θ is a point in the projective space with coordinates the coefficients of $f_1(T)$, $f_2(T)$ and $f_3(T)$. Since

$$H(\Theta) \le H(f_1(T) - Zf_3(T))H(f_2(T) - Zf_3(T)) \le 8100H(G)^4,$$

we get

$$H(R'_3) < 2^{37N^2}H(G)^{8(N-1)}H(R_3).$$

The degree of $R'_3(X,T)$ is $< 8N^3$. Furthermore, $R'_3(x,t) = 0$, whence the polynomial $af_3(T)^{N/2}X - A_1(T)$ divides $R'_3(X,T)$. Using Lemma 3.2, we obtain

$$H(af_3(T)^{N/2}X - A_1(T)) \le 4^{64N^6}H(R'_3).$$

Combining the bounds for $H(R'_3)$, $H(G)$ and $H(R_3)$, we deduce that

$$H(af_3(T)^{N/2}X - A_1(T)) < ((5N^6e^N)^{80}H(F)^{153})^{32N^{11}}.$$

Suppose that $f_3(T) = \alpha T^2 + \beta T + \gamma$. Setting $u = 2\alpha t + \beta$, we obtain

$$x = \frac{L_1(u)}{aL_3(u)} \quad \text{and} \quad y = \frac{L_2(u)}{bL_3(u)},$$

where $L_i(U)$ $(i = 1, 2, 3)$ are polynomials with integer coefficients and

$$L_3(U) = (4\alpha(U^2 - (\beta^2 - 4\alpha\gamma)))^{N/2}.$$

The two roots of $f_3(T)$ are distinct and conjugate over k. Hence the integer

$$\delta = \beta^2 - 4\alpha\gamma$$

is positive. Since $N \geq 4$, we have

$$\begin{aligned}\delta &\leq 5\max\{|\alpha|, |\beta|, |\gamma|\}^2 \leq 5H(af_3(T)^{N/2}X - A_1(T)) \\ &< 5((5N^6e^N)^{80}H(F)^{153})^{32N^{11}}.\end{aligned}$$

Furthermore,

$$\begin{aligned}H(aL_3(U)X - L_1(U)) &< 4^{N^2}H(af_3(T)^{N/2}X - A_1(T))^{2N+1} \\ &< ((5N^6e^N)^{81}H(F)^{153})^{72N^{12}}.\end{aligned}$$

It is easily seen that at least one of the $L_i(U)$ $(i = 1, 2)$ is not a constant. So, we may suppose that $\deg L_1 > 0$. We put

$$L_i(U, V) = L_{i,h}(U, V)V^{\deg L_3 - \deg L_i},$$

where $L_{i,h}(U, V)$ is the homogenization of $L_i(U)$ $(i = 1, 2)$ and we denote by $L_3(U, V)$ the homogenization of $L_3(U)$. By Lemma 3.9, there exists a nonzero integer κ and polynomials $\Gamma(U)$, $\Delta(U)$ with integer coefficients satisfying

$$\Gamma(U)L_1(U) + \Delta(U)aL_3(U) = \kappa$$

such that $\deg \Gamma < N$, $\deg \Delta < N$ and

$$|\kappa|, H(\Gamma), H(\Delta) \leq (2N - 1)!H(\Omega)^{2N-1},$$

where Ω is a point in a projective space having as coordinates 1 and the coefficients of $L_1(U)$ and $aL_3(U)$ (in any order). Since the coefficients of $aL_3(U)X - L_1(U)$ are relatively prime integers, we have

$$H(\Omega) = H(aL_3(U)X - L_1(U)).$$

According to our assumptions, there is a simple integer point (x_0, y_0) on C. By Lemma 3.10, there are $u_0, v_0 \in \mathbb{Z}$ with $u_0 \geq 0$ and $\gcd(u_0, v_0) = 1$ such that

$$x_0 = \frac{L_1(u_0, v_0)}{aL_3(u_0, v_0)} \quad \text{and} \quad y_0 = \frac{L_2(u_0, v_0)}{aL_3(u_0, v_0)}.$$

Thus

$$\Gamma(u_0, v_0)L_1(u_0, v_0) + \Delta(u_0, v_0)aL_3(u_0, v_0) = \kappa v_0^{\zeta},$$

where ζ is a positive integer $< 2N$ and $\Gamma(U, V)$, $\Delta(U, V)$ are forms with integer coefficients of degrees $< N$. It follows that $L_3(u_0, v_0)$ divides κv_0^{ζ}. Since $\gcd(u_0, v_0) = 1$, we obtain $\gcd((u_0^2 - \delta v_0^2)^{N/2}, v_0^{\zeta}) = 1$ and hence

$(u_0^2 - \delta v_0^2)^{N/2}$ divides κ. Thus $u_0^2 - \delta v_0^2 = \lambda$, where λ is a nonzero integer with

$$|\lambda| \le N^4 H(\Omega)^4.$$

Let (c, d) be the fundamental solution of equation $X^2 - \delta Y^2 = 1$. By Lemma 3.8, there exists a fundamental solution (η, θ) of equation $X^2 - \delta Y^2 = \lambda$ such that there are integers r, s with $0 \le r < s \le a^2(4\alpha|\lambda|)^N$ and solutions (z_i, w_i) of $X^2 - \delta Y^2 = \lambda$ given by

$$z_i + w_i\sqrt{\delta} = (c + d\sqrt{\delta})^{r+is}(\eta + \theta\sqrt{\delta}) \quad (i = 0, 1, \ldots),$$

satisfying

$$z_i \equiv u_0 \pmod{a(4\alpha|\lambda|)^{N/2}} \quad \text{and} \quad w_i \equiv v_0 \pmod{a(4\alpha|\lambda|)^{N/2}}.$$

Thus the points $P_i = (x_i, y_i)$ $(i = 0, 1, \ldots)$ of C, with

$$x_i = \frac{L_1(z_i, w_i)}{aL_3(z_i, w_i)} \quad \text{and} \quad y_i = \frac{L_2(z_i, w_i)}{aL_3(z_i, w_i)},$$

are integral.

Let $F_X(X, Y)$ and $F_Y(X, Y)$ be the derivatives of $F(X, Y)$ with respect to X and Y, respectively. As is well known, a singular point on C which is not at infinity satisfies the equations $F_X(X, Y) = F_Y(X, Y) = 0$. Since the degree of $F(X, Y)$ is equal to N, Bézout's theorem implies that C has at most $(N - 1)^2$ singular points which are not at infinity. Thus at least one of the points P_i $(i = 0, 1, \ldots, (N - 1)^2)$ is simple. Lemma 3.11 and the estimates for δ, λ and $H(\Omega)$ imply that for $i = 0, 1, \ldots, (N - 1)^2$ we have

$$\max\{|z_i|, |w_i|\} < \exp\{((5N^6e^N)^{81}H(F)^{153})^{294N^{13}}\}.$$

It follows that

$$|x_i| < (N + 1)H(\Omega)\max\{|z_i|, |w_i|\}^N \quad (i = 0, 1, \ldots, (N - 1)^2).$$

Finally, Lemma 3.4 implies the result.

Acknowledgements. The author wish to thank the referee for helpful suggestions and comments.

References

[1] B. M. Dwork and J. van der Poorten, *The Eisenstein constant*, Duke Math. J. 65 (1992), 23–43 (see also ibid. 76 (1994), 669–672).

[2] A. Grytczuk and A. Schinzel, *On Runge's theorem about Diophantine equations*, in: Colloq. Math. Soc. J. Bolyai 60, North-Holland, 1991, 329–356.

[3] L. K. Hua, *On the least solution of Pell's equation*, Bull. Amer. Math. Soc. 48 (1942), 731–735.

[4] D. M. Kornhauser, *On the smallest solution to the general binary quadratic diophantine equation*, Acta Arith. 55 (1990), 83–94.

[5] S. Lang, *Introduction to Algebraic and Abelian Functions*, Springer, 1982.

[6] S. Lang, *Elliptic Curves. Diophantine Analysis*, Springer, 1978.
[7] —, *Fundamentals of Diophantine Geometry*, Springer, 1983.
[8] E. Maillet, *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*, C. R. Acad. Sci. Paris 168 (1918), 217–220.
[9] —, *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*, J. Ecole Polytech. (2) 20 (1919), 115–156.
[10] M. Mignotte, *An inequality on the greatest root of a polynomial*, Elem. Math. 46 (1991), 85–86.
[11] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, 1998.
[12] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981.
[13] D. Poulakis, *Points entiers sur les courbes de genre* 0, Colloq. Math. 66 (1993), 1–7.
[14] —, *Integer points on algebraic curves with exceptional units*, J. Austral. Math. Soc. Ser. A 63 (1997), 145–164.
[15] —, *Polynomial bounds for the solutions of a class of diophantine equations*, J. Number Theory 66 (1997), 271–281.
[16] —, *Bounds for the minimal solution of genus zero diophantine equations*, Acta Arith. 86 (1998), 51–90.
[17] —, *Bounds for the size of integral points on curves of genus zero*, Acta Math. Hungar. 93 (2001), 327–346.
[18] D. Poulakis and E. Voskos, *On the practical solution of genus zero diophantine equations*, J. Symbolic Comput. 30 (2000), 573–582.
[19] —, —, *Solving genus zero diophantine equations with at most two infinite valuations*, ibid. 33 (2002), 479–491.
[20] A. Schinzel, *Integer points on conics*, Comment. Math. 16 (1972), 133–135 (see also 17 (1973), 305).
[21] W. M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. 56 (1990), 161–179.
[22] —, *Construction and estimation of bases in function fields*, J. Number Theory 39 (1991), 181–224.
[23] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Berlin, 1986.
[24] P. G. Walsh, *A quantitative version of Runge's theorem on diophantine equations*, Acta Arith. 63 (1992), 157–172.

Department of Mathematics
Aristotle University of Thessaloniki
54124 Thessaloniki, Greece
E-mail: poulakis@ccf.auth.gr

Received on 27.11.2001
and in revised form on 15.4.2002 (4160)