COMPOSITIO MATHEMATICA

WOLFGANG M. SCHMIDT

Integer points on curves of genus 1

Compositio Mathematica, tome 81, n° 1 (1992), p. 33-59
<http://www.numdam.org/item?id=CM_1992__81_1_33_0>

Compositio Mathematica **81**: 33–59, 1992.

Integer points on curves of genus 1

WOLFGANG M. SCHMIDT[1]
Department of Mathematics, University of Colorado, Boulder, CO 80309, U.S.A.

Received 12 June 1990; accepted 11 March 1991

1. Introduction

We are interested in the number and the size of integer points on plane curves of genus 1. Although our main focus will be on general curves of genus 1 defined by polynomial equations $F(x, y) = 0$, it will be convenient to begin with Weierstrass curves

$$y^2 = x^3 + bx^2 + cx + d \qquad (\mathcal{W})$$

where the right-hand side is a cubic polynomial f with nonzero discriminant. Recently Evertse and Silverman [9] gave a bound for the number of integer solutions which depends on the class number of the splitting field of f. An easy consequence is as follows.

THEOREM 1. *Suppose* $f(X) = X^3 + bX^2 + cX + d$ *has discriminant* $\Delta(f) \neq 0$ *and has integer coefficients in an algebraic number field* k *of degree* δ *and discriminant* D_k. *Then given* $\varepsilon > 0$, *the number* Z *of solutions of* $(\mathcal{W})$ *in integers* x, y *of* k *has*

$$Z < c_1(\delta, \varepsilon)|D_k|^{3/2+\varepsilon}|\mathcal{N}_k(\Delta(f))|^{1/2+\varepsilon}, \qquad (1.1)$$

where $\mathcal{N}_k$ *is the norm from* k *to* $\mathbb{Q}$.

The constant $c_1(\delta, \varepsilon)$, like all the constants of this paper, is effectively computable.

We define the field height $H_k(\boldsymbol{\alpha})$ of a nonzero vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in k^n$ as in [5] or [15], and the absolute height to be $H(\boldsymbol{\alpha}) = H_k(\boldsymbol{\alpha})^{1/\delta}$. Thus

$$H_k(\boldsymbol{\alpha}) = \prod_{v \in M(k)} |\boldsymbol{\alpha}|_v^{d_v} \qquad (1.2)$$

where $M(k)$ is an indexing set for suitably normalized absolute values $|\cdot|$ of k, the d_v are the local degrees, and $|\boldsymbol{\alpha}|_v = \max(|\alpha_v, \ldots, |\alpha_n|_v)$. Given a polynomial f with coefficients in k, we define quantities $|f|_v$ and heights $H_k(f)$, $H(f)$ in terms of its

[1]Supported in part by NSF grant DMS-8603093.

coefficient vector. For a cubic polynomial f, we have $|\Delta(f)|_v \leqslant c(v)|f|_v^4$, where

$$c(v) = \begin{cases} c_2 & \text{when } v \text{ is archimedean,} \\ 1 & \text{when } v \text{ is non-archimedean,} \end{cases}$$

with an absolute constant c_2. The sum of the local degrees over the set $M_\infty(k)$ of the archimedean absolute values is δ, so that

$$|\mathcal{N}_k(\Delta(f))| = \prod_{v \in M_\infty(k)} |\Delta(f)|_v^{d_v} \leqslant c_2^\delta \prod_{v \in M_\infty(k)} |f|_v^{4d_v}.$$

When f has leading coefficient 1, then $|f|_v \geqslant 1$ for each v, and

$$|\mathcal{N}_k(\Delta(f))| \leqslant c_2^\delta H_k(f)^4. \tag{1.3}$$

Therefore (1.1) implies that

$$Z < c_3(\delta, \varepsilon)|D_k|^{3/2+\varepsilon} H_k(f)^{2+\varepsilon}. \tag{1.4}$$

In particular, in the case $K = \mathbb{Q}$ we obtain

$$Z < c_4(\varepsilon) H(f)^{2+\varepsilon}.$$

I conjecture that in fact for given $\varepsilon > 0$,

$$Z < c_5(\varepsilon) H(f)^{\varepsilon}.$$

More generally, I conjecture that the number Z of solutions $x, y \in \mathbb{Z}$ of an irreducible equation $F(x, y) = 0$ defining a curve of positive genus, with F having coefficients in $\mathbb{Z}$ and total degree N, has

$$Z < c_6(N, \varepsilon) H(F)^{\varepsilon}.$$

Beginning with the pioneering work of Baker [1], [2], a number of authors have estimated the size of integer solutions of the Equation ($\mathscr{W}$), or more generally of hyperelliptic equations $y^2 = f(x)$ where f is a polynomial of degree $\geqslant 3$ with nonzero discriminant. Given $\alpha \in k$, define $h_k(\alpha) = H_k((1, \alpha))$. A natural concept of size of an integer solution (x, y) would be $\max(h_k(x), h_k(y))$. Baker in [1] dealt with the case when $K = \mathbb{Q}$ and $\deg f = 3$, and obtained a bound which was exponential in $H(f)$, whereas in [2] he dealt with the general case and obtained a bound which was triply exponential in $H_k(f)$. Siegel [18] derived new estimates for fundamental units in number fields and remarked that these

estimates could be used to reduce Baker's bounds. In fact they reduce the bounds to just exponential in terms of $H_k(f)$ in the general case. Details were provided by Sprindžuk [21], but only in the case $k = \mathbb{Q}$. Although all the ingredients are available in the literature, we will for completeness provide a proof of

THEOREM 2. *Suppose* $f(X) = X^3 + bX^2 + cX + d$ *has nonzero discriminant, and has integer coefficients in an algebraic number field* k *of degree* δ *and discriminant* D_k. *Then solutions* x, y *of* $(\mathscr{W})$ *in the ring* $\mathcal{O}_k$ *of integers of* k *have*

$$\max(h_k(x), h_k(y)) < \exp(c_7(\delta)V(\log^* V)^{48\delta})$$

where

$$V = D_k^{48} H_k(f)^{128}, \tag{1.5}$$

and where the notation $\log^* z$ *stands for* $\max(1, \log z)$.

In particular, in the rational case $k = \mathbb{Q}$ we have

$$\max(|x|, |y|) < \exp(c_8 H(f)^{128}(\log^* H(f))^{48}).$$

It would have been easy to give a suitable generalization to hyperelliptic or even to superelliptic equations.

We now turn to more general equations

$$F(x, y) = 0 \tag{$\mathscr{C}$}$$

defining an irreducible curve of genus 1. We will suppose that F has coefficients in a number field k of degree δ, and we will denote the total degree of F by N. We will study solutions $(x, y) \in \mathcal{O}_k^2$.

THEOREM 3. *Let* F *be as above. The number of solutions* $(x, y) \in \mathcal{O}_k^2$ *of* $(\mathscr{C})$ *is*

$$< c_9(\delta, N)|D_k|^{8N}(H_k(F))^{(3N)^{13}}.$$

THEOREM 4. *Let* F *be as above. Solutions* $(x, y) \in \mathcal{O}_k^2$ *of* $(\mathscr{C})$ *have*

$$\max(h_k(x), h_k(y)) < \exp(c_{10}(\delta, N)W) \tag{1.6}$$

where

$$W = D_k^{433N} H_k(F)^{(4N)^{13}}. \tag{1.7}$$

In particular, when $k = \mathbb{Q}$,

$$\max(|x|, |y|) < \exp(c_{11}(N)H(F)^{(4N)^{13}}). \tag{1.8}$$

Baker and Coates [4] had given the bound

$$\max(|x|, |y|) < \exp\exp\exp((2H(F))^{10^{N^{10}}}). \tag{1.9}$$

As was pointed out above, the improvement from triple exponentiation to single exponentiation comes from Siegel's work on units. The improvement from $10^{N^{10}}$ to $(4N)^{13}$ will be discussed below. Theorems 3 and 4 will be proved by reduction to Theorems 1 and 2 via a suitable birational transformation from a general curve ($\mathscr{C}$) of genus 1 to a Weierstrass curve ($\mathscr{W}$). Such a transformation is described in

PROPOSITION 1. *There is a birational transformation* $x_1 = x_1(x, y)$, $y_1 = y_1(x, y)$ *from the curve* ($\mathscr{C}$) *to a Weierstrass curve*

$$y_1^2 = x_1^3 + bx_1^2 + cx_1 + d \tag{$\mathscr{W}$}$$

with the following properties.

The transformation is defined over a field $K \supset k$ *with* $[K:k] \leqslant n$, *where n is the degree of F with respect to y. The coefficients b, c, d are integers in K. We have*

$$|D_K| < c_{12}(\delta, N)|D_k|^n H_k(F)^{48N^{11}}, \tag{1.10}$$

and the polynomial $f = X^3 + bX^2 + cX + d$ *has*

$$H_K(f) < c_{13}(\delta, N)|D_k|^{3n} H_K(F)^{2\cdot 10^5 N^{12}}. \tag{1.11}$$

If $(X, \mathscr{Y})$ *is a generic point of* ($\mathscr{C}$) (*so that X is transcendental and* $F(X, \mathscr{Y}) = 0$), *and if* $(X, \mathscr{Y}) \in (\mathscr{C})$ *corresponds to* $(X_1, \mathscr{Y}_1) \in (\mathscr{W})$, *then* $X_1 \in K(X, \mathscr{Y})$ *is integral over* $\mathbb{Z}[X]$.

A proposition of this type had implicitly been derived by Baker and Coates [4], but with $k = \mathbb{Q}$ and $\deg K \leqslant 8^{N^6}$, and with $8^{N^{48}}$ instead of the exponent $2\cdot 10^5 N^{12}$ in (1.11). The improvement from $10^{N^{10}}$ in (1.9) to $(4N)^{13}$ in (1.8) comes from the improved estimates in Proposition 1. This proposition in turn rests on recent work on Eisenstein's theorem [15] and on the construction of bases in function fields [16].

2. Proof of Theorem 1

Let $S \subset M(k)$ consist of the archimedean absolute values, as well as the non-archimedean absolute values v for which $|\Delta(f)|_v \neq 1$. Then $\Delta(f)$ lies in the group of S-units of K. Let s be the cardinality of S. Let L be the splitting field of f over k, and $h_2(L)$ the order of the subgroup of the ideal class group of L consisting of ideal classes $[\mathscr{A}]$ with $[\mathscr{A}]^2 = [1]$. Then if Z is defined as in Theorem 1, it follows from Theorem 1(b) of Evertse and Silverman [9] that

$$Z \leqslant 7^{[L:k](4\delta+9s)} h_2(L)^2 + 3. \tag{2.1}$$

In [9] only solutions with $y \neq 0$ were considered; our summand 3 takes care of possible solutions with $y = 0$.

As was kindly pointed out to me by Dr. Evertse, the factor $h_2(L)^2$ in (2.1) may be replaced by $h_2(E)$ when $L \neq k$ and $E = k(\alpha)$ with a root α of f which does not lie in k. This may be seen as follows. Let S' be the set of places of E lying above S, and let s' be the cardinality of S'. Let $\alpha = \alpha_1, \alpha_2, \alpha_3$ be the roots of f. Now when x, y is a solution of $(\mathscr{W})$, then $x - \alpha_1$ lies in E, and since $\Delta(f)$ is an S'-unit in E, we have $|x-\alpha_1|_v \equiv 0 \pmod 2$ when $v \notin S'$. By Lemma 1 of [9], there is a finite set of elements $q_1, \ldots, q_t$ in E with $t \leqslant 2^{s'+\kappa_2(E)}$, such that $x - \alpha_1 = q_j \xi^2$ with $1 \leqslant j \leqslant t$ and $\xi \in E$. Now suppose that $[E:k] = 3$ and let σ_2, σ_3 be the isomorphisms $E = k(\alpha_1) \to k(\alpha_2)$, $E = k(\alpha_1) \to k(\alpha_3)$ with $\sigma_2(\alpha_1) = \alpha_2$, $\sigma_3(\alpha_1) = \alpha_3$. Then $x - \alpha_2 = \sigma_2(q_j)\sigma_2(\xi)^2$, $x - \alpha_3 = \sigma_3(q_j)\sigma_3(\xi)^2$. Setting

$$z_1 = \frac{x-\alpha_1}{x-\alpha_3}, \qquad z_2 = \frac{x-\alpha_2}{x-\alpha_3}$$

we have $z_1 = w_j \zeta_1^2$, $z_2 = w_j' \zeta_2^2$ with $w_j = q_j/\sigma_3(q_j)$, $w_j' = \sigma_2(q_j)/\sigma_3(q_j)$, $\zeta_1 = \xi/\sigma_3(\xi)$, $\zeta_2 = \sigma_2(\xi)/\sigma_3(\xi)$. Therefore in the proof of Proposition 2 of [9], the set V_2 is contained in at most $2^{s'+\kappa_2(E)} = 2^{s'} h_2(E)$ sets of the type $V_2(w, w')$. This replaces the factor $4^s h_2(K)^2$ (which in our context should be written $4^{s'} h_2(L)^2$) of [9].

When $[E:k] = 2$, suppose that $\alpha = \alpha_1, \alpha_2$ are conjugate over k, and $\alpha_3 \in k$. Now $z_1 \in E = k(\alpha_1)$. Dealing directly with fractional ideals one sees that $z_1 = w_j \zeta_1^2$ where w_j is from a finite set $\{w_1, \ldots, w_t\}$. If σ is the isomorphism $k(\alpha_1) \to k(\alpha_2)$ with $\sigma(\alpha_1) = \alpha_2$, then $z_2 = \sigma(z_1) = w_j' \zeta_2^2$ where $w_j' = \sigma(w_j)$. Again the set V_2 of [9] is contained in at most $2^{s'} h_2(E)$ sets of the type $V_2(w, w')$.

All we have to do now is to estimate the right-hand side of (2.1). The number of archimedean absolute values in S is $\leqslant \delta$. The number of non-archimedean absolute values in S is equal to the number of prime ideals of the ring of integers of k dividing $\Delta(f)$, and this number is at most δ times the number of rational

primes p dividing $\mathcal{N}_k(\Delta(f))$. The latter number, as is well-known is

$$\ll \log|\mathcal{N}_k(\Delta(f))|/\log\log|\mathcal{N}_k(\Delta(f))|$$

when $|\mathcal{N}_k(\Delta(f))|$ is large. Therefore

$$s < \delta + O(\delta \log|\cdots|/\log\log|\cdots|).$$

Since $[L:k] \leqslant 6$, we obtain for every $\varepsilon > 0$,

$$7^{[L:k](4\delta+9s)} < c_1(\delta, \varepsilon)|\mathcal{N}_k(\Delta(f))|^{\varepsilon}. \tag{2.2}$$

(The numbering of constants $c_1, c_2, \ldots$ is started anew in each section.)

Next, I can do no better than $h_2(L) \leqslant h(L)$ where $h(L)$ is the class number. It is well known (see e.g. [18]) that

$$h(L) < c_2(l, \varepsilon)|D_L|^{(1/2)+\varepsilon}$$

where $l = \deg L \leqslant 6\delta$, where D_L is the discriminant of L, and ε (as throughout this section) is an arbitrary positive number. When $L = k$, we obtain

$$h^2(L)^2 \leqslant c_3(\delta, \varepsilon)|D_k|^{1+\varepsilon}. \tag{2.3}$$

When $L \neq k$, we will see below that a field E as above has

$$|D_E| \leqslant |D_k|^g|\mathcal{N}_k(\Delta(f))| \tag{2.4}$$

where $g = [E:k] \leqslant 3$. Then

$$h(E) \leqslant c_4(\delta, \varepsilon)|D_k|^{3/2+\varepsilon}|\mathcal{N}_k(\Delta(f))|^{1/2+\varepsilon}. \tag{2.5}$$

Theorem 1 follows by substituting (2.2) and (2.3) into (2.1) when $L = k$, and by substituting (2.2) and (2.5) into the modified version of (2.1) when $L \neq k$.

We still have to prove (2.4). If $\mathcal{D}_{E/\mathbb{Q}}$ is the different of E with respect to $\mathbb{Q}$, and similarly for $\mathcal{D}_{E/k}$ and $\mathcal{D}_{k/\mathbb{Q}}$, then ([11, Satz 111])

$$\mathcal{D}_{E/\mathbb{Q}} = \mathcal{D}_{E/k}\mathcal{D}_{k/\mathbb{Q}}.$$

Taking the norm $\mathcal{N}_{E/\mathbb{Q}}$ from E to $\mathbb{Q}$, we obtain

$$|D_E| = \mathcal{N}_{E/\mathbb{Q}}(\mathcal{D}_{k/\mathbb{Q}})\mathcal{N}_{E/\mathbb{Q}}(\mathcal{D}_{E/k}) = |D_k|^{[E:k]}\mathcal{N}_{k/\mathbb{Q}}(D_{E/k}) \tag{2.6}$$

where $D_{E/k} = \mathcal{N}_{E/k}(\mathcal{D}_{E/k})$ is the "discriminant ideal" of E in k. Given integers $\gamma_1, \ldots, \gamma_g$ in E which are a field basis of E over k, then ([12, III, Proposition 13])

$$D_{E/k} \geq (\delta(\gamma_1, \ldots, \gamma_g))^2,$$

where $\delta(\gamma_1, \ldots, \gamma_g) = \det(\gamma_j^{(i)})_{1 \leq i,j \leq g}$ and where $\alpha \mapsto \alpha^{(i)}$ $(i = 1, \ldots, g)$ denote the embeddings of E/k into a Galois extension of k containing E.

In the special case when $E = k(\alpha)$ and α is a root of a monic irreducible polynomial with integer coefficients in k, we may take $\gamma_1 = 1$, $\gamma_2 = \alpha, \ldots,$ $\gamma_g = \alpha^{g-1}$. Then $\delta(\gamma_1, \ldots, \gamma_g)^2 = \Delta(f)$ and $|\mathcal{N}_{k/\mathbb{Q}}(D_{E/k})| \leq |\mathcal{N}_{k/\mathbb{Q}}(\delta(\gamma_1, \ldots, \gamma_g))^2| = |\mathcal{N}_{k/\mathbb{Q}}(\Delta(f))|$. In conjunction with (2.6) this gives (2.4).

3. An effective estimate for unit equations

Our goal is

PROPOSITION 2. *Let M be an algebraic number field of degree m and with regulator $R = R_M$. Let m_1, m_2, m_3 be nonzero elements of M, and set $H_0 = H(m_1, m_2, m_3)$ and $T = R \log^* H_0$. Consider the equation*

$$m_1\varepsilon_1 + m_2\varepsilon_2 + m_3\varepsilon_3 = 0, \tag{3.1}$$

to be solved in units ε_1, ε_2, ε_3 of M. Every solution has

$$H(\varepsilon_1, \varepsilon_2, \varepsilon_3) < \exp(c_1(m) T \log^* T). \tag{3.2}$$

We will need the following

LEMMA 1. *Let*

$$\Gamma = \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1,$$

where $\alpha_1, \ldots, \alpha_n$ are nonzero algebraic numbers of degree $\leq m$ and with heights $h(\alpha_i) \leq A_i$ $(i = 1, \ldots, n)$ and where $b_1, \ldots, b_n$ are rational integers with $|b_i| \leq B$ $(i = 1, \ldots, n)$. Then if $\Gamma \neq 0$, we have

$$|\Gamma| > \exp\left(-c_2(m, n)\left(\prod_{i=1}^{n} \log^* A_i\right) \log^* B\right) \tag{3.3}$$

Proof. This is Theorem 1.2 in [14] and also follows from Theorem 1.6 in [22]. A slightly weaker result is contained in [3].

Before proceeding further we have to make some remarks on fundamental units of M. Let r be the rank of the group of units. Let $\alpha \mapsto \alpha^{(i)}$ $(i=1,\dots,m)$ be the embeddings of M into $\mathbb{C}$, arranged such that the first r embeddings contain no pair of complex conjugate embeddings. Set $e_i=1$ or $e_i=2$, depending on whether the embedding $\alpha \mapsto \alpha^{(i)}$ is real or complex. Now if $\eta_1,\dots,\eta_r$ is a set of fundamental units, the matrix

$$(e_i \log |\eta_j^{(i)}|)_{1 \leqslant i,j \leqslant r} \tag{3.4}$$

is nonsingular, and its absolute value is the regulator $R=R_M$. Given any algebraic number η, let $\overline{|\eta|}$ be the maximum absolute value of its conjugates, i.e. the maximum value of $|\sigma(\eta)|$ as σ runs through the embeddings of $\mathbb{Q}(\eta)$ into $\mathbb{C}$. As was pointed out by Siegel [18], there is a set of fundamental units $\eta_1,\dots,\eta_r$ such that

$$\prod_{i=1}^{r} \log \overline{|\eta_i|} < c_3(m)R. \tag{3.5}$$

These units will be fixed from now on. It was also pointed out by Siegel that every unit η which is not a root of 1 has $\overline{|\eta|} > 1 + c_4(m)$ where $c_4(m) > 0$, and therefore $\log \overline{|\eta|} > c_5(m) > 0$. (In fact this holds for every algebraic integer η of degree $\leqslant m$ which is not zero or a root of 1. See e.g. [8].) A consequence is that $R > c_6(m) > 0$. Therefore every subproduct of the product in (3.5) is $< c_7(m)R$, so that every minor of the matrix (3.4) has absolute value $< c_8(m)R$. This shows in particular that the inverse of the matrix in (3.4) has entries of modulus $< c_9(m)$. Another consequence is that (3.5) remains true if log is replaced by log* and $c_3(m)$ by some new constant $c_{10}(m)$. Now since η_i is a unit,

$$h_M(\eta_i) = \prod_{j=1}^{m} \max(1, |\eta_i^{(j)}|) \leqslant \overline{|\eta_i|}^m,$$

so that $h(\eta_i) \leqslant \overline{|\eta_i|}$ $(i=1,\dots,r)$ and

$$\prod_{i=1}^{r} \log^* h(\eta_i) < c_{10}(m)R. \tag{3.6}$$

Proof of Proposition 2. (3.1) yields

$$\frac{m_1\varepsilon_1}{m_3\varepsilon_3} = -\frac{m_2\varepsilon_2}{m_3\varepsilon_3} - 1.$$

We may write the unit $\varepsilon_2/\varepsilon_3$ as

$$\varepsilon_2/\varepsilon_3 = \zeta\eta_1^{b_1}\cdots\eta_r^{b_r} \tag{3.7}$$

where ζ is a root of 1 and $b_1,\ldots,b_r$ lie in $\mathbb{Z}$. Setting $\alpha_0 = -(m_2/m_3)\zeta$ and $b_0 = 1$, we have

$$|m_1\varepsilon_1/m_3\varepsilon_3| = |\alpha_0^{b_0}\eta_1^{b_1}\cdots\eta_r^{b_r} - 1|.$$

We now apply Lemma 1 with $n = r+1$. By (3.6) and since $h(\alpha_0) = h(m_2/m_3) \leqslant H(m_1, m_2, m_3) = H_0$, we obtain

$$|m_1\varepsilon_1/m_3\varepsilon_3| > \exp(-c_{11}(m)R(\log^* H_0)(\log^* B)) = \exp(-c_{11}(m)T\log^* B)$$

where $B = \max(1, |b_1|,\ldots,|b_r|)$. Since $|m_1/m_3| \leqslant H(m_1, m_2, m_3) = H_0$, and since $T = R\log^* H_0 > c_6(m)\log^* H_0$, we get

$$|\varepsilon_1/\varepsilon_3| > \exp(-c_{12}(m)T\log^* B). \tag{3.8}$$

Now from (3.7),

$$b_1\log|\eta_1^{(i)}| + \cdots + b_r\log|\eta_r^{(i)}| = \log|(\varepsilon_2/\varepsilon_3)^{(i)}| \quad (i = 1,\ldots,r)$$

(actually for $i = 1,\ldots,m$). The matrix of this system of linear equations in $b_1,\ldots,b_r$ is essentially the matrix (3.4), so that its inverse has entries of modulus $\leqslant c_{13}(m)$. Therefore $B = 1$ or

$$B < rc_{13}(m)\max_{1\leqslant i\leqslant r}\log|(\varepsilon_2/\varepsilon_3)^{(i)}| \leqslant rc_{13}(m)\log\overline{|\varepsilon_2/\varepsilon_2|}.$$

If we substitute this into (3.8) and take reciprocals, we get

$$|\varepsilon_3/\varepsilon_1| < \exp(c_{14}(m)T\log^*\log^*\overline{|\varepsilon_2/\varepsilon_3|}).$$

The same estimate holds for each conjugate $(\varepsilon_3/\varepsilon_1)^{(i)}$, so that

$$\overline{|\varepsilon_3/\varepsilon_1|} < \exp(c_{14}(m)T\log^*\log^*\overline{|\varepsilon_2/\varepsilon_3|}).$$

This last estimate remains true if we permute $\varepsilon_1, \varepsilon_2, \varepsilon_3$. Therefore if $\mu = \max\overline{|\varepsilon_u/\varepsilon_v|}$ over $1 \leqslant u, v \leqslant 3$, then

$$\mu < \exp(c_{14}(m)T\log^*\log^*\mu).$$

A standard argument yields

$$\mu < \exp(c_{15}(m)T \log^* T).$$

Finally,

$$H_M(\varepsilon_1, \varepsilon_2, \varepsilon_3) = H_M(1, \varepsilon_2/\varepsilon_1, \varepsilon_3/\varepsilon_1) = \prod_{i=1}^{m} \max(1, |(\varepsilon_2/\varepsilon_1)^{(i)}|, |(\varepsilon_3/\varepsilon_1)^{(i)}|) \leqslant \mu^m,$$

so that $H(\varepsilon_1, \varepsilon_2, \varepsilon_3) \leqslant \mu$. The proposition follows.

REMARKS. By using Theorem 2.2 of [14], one can prove a variation on Proposition 2, namely the bound

$$H(\varepsilon_1, \varepsilon_2, \varepsilon_3) < \exp(c_{16}(m)R(\log^* R)(R + \log^* H_0)). \tag{3.9}$$

This bound is better when H_0 is large. Since, as is well known,

$$R < c_{17}(m)|D_M|^{1/2}(\log^* |D_M|)^{m-1},$$

(3.2) and (3.9) lead to bounds for $H(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ in terms of $|D_M|$ and H_0. Estimates of this type which were a little weaker than ours, but explicit in terms of m, had been given by Györy [10].

4. Proof of Theorem 2

We follow Siegel's argument [17] which is by now classical. We begin by recalling a well known fact. Suppose M is a number field of degree m and with regulator R_M. Then if $a \in M$ is an integer, we may write a as

$$a = b\varepsilon$$

where ε is a unit and b is an integer of M with

$$\overline{|b|} \leqslant \mathcal{N}_M(a)|^{1/m} e^{c_1(m)R_M}.$$

Now consider the equation

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = f(x), \tag{4.1}$$

say, where $\alpha_1, \alpha_2, \alpha_3$ are integers in a field L of degree l. Let x, y be a solution,

where x, y are integers of L and where $y \neq 0$. We may write the principal ideal $(x-\alpha_i)$ as

$$(x - \alpha_i) = \mathscr{A}_i \mathscr{B}_i^2 \ (i = 1, 2, 3)$$

where $\mathscr{A}_i$, $\mathscr{B}_i$ are integral ideals of L and where $\mathscr{A}_i$ is square free. In view of (4.1), $\mathscr{A}_1\mathscr{A}_2\mathscr{A}_3$ is a square, so that if some prime ideal $\mathscr{P} \mid \mathscr{A}_i$ (i.e. $\mathscr{P}$ divides $\mathscr{A}_i$), then $\mathscr{P} \mid \mathscr{A}_j$ for some $j \neq i$. But then $\mathscr{P} \mid (x-\alpha_i)$, $\mathscr{P} \mid (x-\alpha_j)$, therefore $\mathscr{P} \mid (\alpha_i - \alpha_j)$. Therefore each prime divisor of $\mathscr{A}_i$, and therefore $\mathscr{A}_i$ itself, divides $(\alpha_i-\alpha_j)(\alpha_i-\alpha_h)$ where i, j, h is a cyclic permutation of 1, 2, 3. We may conclude that

$$\mathscr{A}_1\mathscr{A}_2\mathscr{A}_3 \mid (\Delta(f)). \tag{4.2}$$

There is an integral ideal $\mathscr{B}_i'$ in the ideal class of $\mathscr{B}_i$ with $\mathscr{N}_L(\mathscr{B}_i') \leqslant |D_L|^{1/2}$ ([11, Satz 96]). Let ξ_i be in L with $(\xi_i) = \mathscr{B}_i\mathscr{B}_i'^{-1}$ $(i = 1, 2, 3)$. Then

$$x - \alpha_i = a_i \xi_i^2 \ (i = 1, 2, 3) \tag{4.3}$$

where $a_i \in L$ with $(a_i) = \mathscr{A}_i \mathscr{B}_i'^2$. Then a_1, a_2, a_3 are integers of L with

$$|\mathscr{N}_L(a_1a_2a_3)| \leqslant |\mathscr{N}_L(\Delta(f))|\,|D_L|^3. \tag{4.4}$$

Let $M = L(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$. Since $a_1a_2a_3$ is a square in L by (4.1), (4.3), the field M is obtained from L by adjoining any two of $\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3}$, and it has degree $m \leqslant 4l$. We may suppose that $|\mathscr{N}_L(a_1)| \leqslant |\mathscr{N}_L(a_2)| \leqslant |\mathscr{N}_L(a_3)|$, so that

$$|\mathscr{N}_L(a_1)\mathscr{N}_L(a_2)| \leqslant |\mathscr{N}_L(\Delta(f))|^{2/3}|D_L|^2$$

by (4.4). By an argument as in the proof of (2.4) above, and since $M = L(\sqrt{a_1}, \sqrt{a_2})$,

$$\begin{aligned} |D_M| &\leqslant c_2(l) D_L^4 \mathscr{N}_L(a_1)^2 \mathscr{N}_L(a_2)^2 \\ &\leqslant c_2(l) D_L^8 |\mathscr{N}_L(\Delta(f))|^{4/3}. \end{aligned} \tag{4.5}$$

(I used to have $\mathscr{N}_L(a_1)^4\mathscr{N}_L(a_2)^4$, etc., and I am grateful to Dr. Dimitrios Poulakis for pointing out that the present bounds are valid.)

Put $\sigma_i = \sqrt{a_i}\,\xi_i$ $(i = 1, 2, 3)$; then σ_i lies in M and is an integer by (4.3). We have $\alpha_i - \alpha_j = \sigma_j^2 - \sigma_i^2$, hence

$$\alpha_i - \alpha_j = (\sigma_j + \sigma_i)(\sigma_j - \sigma_i) \ (i \neq j).$$

Therefore

$$|\mathcal{N}_M(\sigma_j + \sigma_i)| \leqslant |\mathcal{N}_M(\alpha_i - \alpha_j)| \leqslant |\mathcal{N}_M(\Delta(f))|^{1/2}.$$

By the remark at the beginning, for given $i \neq j$ we have $\sigma_j + \sigma_i = b\varepsilon$ where ε is a unit and

$$\overline{|b|} < \mathcal{N}_M(\Delta(f))|^{1/(2m)} e^{c_3(l)R_M}.$$

In fact if (i, j, h) is a cyclic permutation of (1, 2, 3), we may write

$$\sigma_j + \sigma_i = b_h \varepsilon_h$$

and

$$\sigma_j - \sigma_i = g_h \delta_h,$$

where ε_h, δ_h $(h = 1, 2, 3)$ are units of M and b_h, g_h are integers of M with

$$\overline{|b_h|}, \overline{|g_h|} < |\mathcal{N}_L(\Delta(f))|^{1/(2l)} e^{c_3(l)R_M}. \tag{4.6}$$

We have

$$b_1\varepsilon_1 - b_2\varepsilon_2 - g_3\delta_3 = \sigma_2 + \sigma_3 - (\sigma_3 + \sigma_1) - (\sigma_2 - \sigma_1) = 0.$$

This is a unit equation in M with coefficient vector $\mathbf{m} = (b_1, -b_2, -g_3)$ and

$$H(\mathbf{m}) < |\mathcal{N}_L(\Delta(f))|^{1/(2l)} e^{c_3(l)R_M},$$

so that

$$\log^* H(\mathbf{m}) < c_4(l) R_M \log^* |\mathcal{N}_L(\Delta(f))|.$$

We now apply Proposition 2 and find that

$$H(\varepsilon_1, \varepsilon_2, \delta_3) < \exp(c_5(l) T_1 \log^* T_1)$$

where

$$T_1 = R_M^2 \log^* |\mathcal{N}_L(\Delta(f))|. \tag{4.7}$$

The same estimate holds for $H(\varepsilon_2, \varepsilon_3, \delta_1)$ and $H(\varepsilon_3, \varepsilon_1, \delta_2)$. It is a general fact that

$$H(\alpha, \beta_2, \ldots, \beta_p, \gamma_2, \ldots, \gamma_q) \leqslant H(\alpha, \beta_2, \ldots, \beta_p)H(\alpha, \gamma_2, \ldots, \gamma_q)$$

when $\alpha \neq 0$. (Hint: reduce to the case $\alpha = 1$.) Therefore

$$H(\varepsilon_1, \varepsilon_2, \varepsilon_3, \delta_1, \delta_2, \delta_3) < \exp(c_6(l)T_1 \log^* T_1).$$

In particular this bound holds for $H(\varepsilon_1, \delta_1)$. In view of (4.6), the same bound, but with $c_6(l)$ replaced by $c_7(l)$, holds for $H_M(b_1\varepsilon_1, g_1\delta_1)$. Therefore if $\alpha \mapsto \alpha^{(t)}$ $(t = 1, \ldots, m)$ are the embeddings of M into $\mathbb{C}$, then

$$|(b_1\varepsilon_1)^{(t)}|/|(g_1\delta_1)^{(t)}| < \exp(c_7(l)T_1 \log^* T_1) = C,$$

say. But $b_1\varepsilon_1 g_1\delta_1 = (\sigma_3 + \sigma_2)(\sigma_3 - \sigma_2) = \alpha_2 - \alpha_3$, so that

$$|(b_1\varepsilon_1)^{(t)}|^2 < C|\alpha_2^{(t)} - \alpha_3^{(t)}|.$$

The same estimate holds for $(g_1\delta_1)^{(t)}$. Since $2\sigma_3 = g_1\delta_1 + b_1\varepsilon_1$, and since $x - \alpha_3 = \sigma_3^2$, we obtain

$$|(x - \alpha_3)^{(t)}| < C|\alpha_2^{(t)} - \alpha_3^{(t)}|. \tag{4.8}$$

Now $R_M < c_8(m)|D_M|^{1/2}(\log^* |D_M|)^{m-1}$, so that by (4.5)

$$R_M^2 < c_9(l)T_2(\log^* T_2)^{2m-2}$$

with $T_2 = D_L^8|\mathcal{N}_L(\Delta(f))|^{4/3}$. Then T_1 as defined by (4.7) has

$$T_1 < c_{10}(l)T_2(\log^* T_2)^{2m-1} \quad \text{and} \quad T_1 \log^* T_1 < c_{11}(l)T_2(\log^* T_2)^{2m}.$$

Substitution into the definition of C, together with (4.8), gives

$$|(x - \alpha_3)^{(t)}| < |\alpha_2^{(t)} - \alpha_3^{(t)}| \exp(c_{12}(l)T_2(\log^* T_2)^{8l}).$$

Finally, as in (1.3), $|\mathcal{N}_L(\Delta(f))| \leqslant c_{13}(l)H_L(f)^4$, and of course we have $|\alpha_2^{(t)}|$, $|\alpha_3^{(t)}| < c_{14}(l)H_L(f)$. Therefore we obtain

$$\overline{|x|}, \overline{|y|} < \exp(c_{15}(l)T_3(\log^* T_3)^{8l}) \tag{4.9}$$

with $T_3 = D_L^8 H_L(f)^{16/3}$. Clearly this estimate is also true for solutions (x, y) with $y = 0$.

If f has coefficients in k and L is the splitting field of f, then in the worst case $[L:k]=6$, so that $H_L(f) \leqslant H_k(f)^6$ and

$$|D_L| \leqslant D_k^6 |\mathcal{N}(\Delta(f))|^3 < c_{16}(\delta) D_k^6 H_k(f)^{12}$$

in analogy to (2.4), by taking $\gamma_1 = 1, \gamma_2 = \alpha_1, \gamma_3 = \alpha_1^2, \gamma_4 = \alpha_2, \gamma_5 = \alpha_1\alpha_2, \gamma_6 = \alpha_1^2\alpha_2$ in the argument at the end of Section 3. Therefore

$$h_k(x),\ h_k(y) < \exp(c_{17}(\delta) V (\log^* V)^{48\delta})$$

with V given by (1.5). Theorem 2 is established.

5. Eisenstein's theorem

Let k be a number field of degree δ. A k-system is a system of numbers $\{A_v\}_{v \in M(k)}$, such that $A_v \geqslant 1$ for each v, and A_v lies in the value group of $|\cdot|_v$ for each non-archimedean v, and moreover $A_v = 1$ for all but finitely many v. (In particular, such a system is a "multiplicative M_k-divisor" as defined by Lang [13, Ch. 2, §5].) We define the norm

$$\mathcal{N}_k\{A_v\} = \prod_{v \in M(k)} A_v^{d_v},$$

where the d_v's are the local degrees.

LEMMA 2. *Let $F(X, Y)$ be a nonzero polynomial with coefficients in k, of degree n in Y, and of total degree N. Suppose that F has no multiple factors of positive degree in Y. Now let X be a variable and*

$$\mathcal{Y} = \alpha_0 + \alpha_1 X + \cdots$$

a series such that we have identically $F(X, \mathcal{Y}) = 0$. Then

(i) *The field $K = k(\alpha_0, \alpha_1, \ldots)$ generated over k by the coefficients of $\mathcal{Y}$ is a number field with degree $[K:k] \leqslant n$.*

(ii) *K is generated over k by $\alpha_0, \alpha_1, \ldots, \alpha_{2n^2}$.*

(iii) *There is a k-system $\{A_v\}$ such that*

$$|\alpha_s|_v \leqslant A_v^{N+s} \quad (s = 0, 1, \ldots) \tag{5.1}$$

for every $v \in M(k)$ and every extension of $|\cdot|_v$ to K. Moreover,

$$\mathcal{N}_k\{A_v\} < c_1(\delta, N) H_k(F)^{8n^2N}. \tag{5.2}$$

(iv) *The discriminant* D_K *of* K *has*

$$|D_K| < c_2(\delta, N)|D_k|^n H_k(F)^{48n^5N^2}. \tag{5.3}$$

Proof. Part (i) is easy and well known; see e.g. [6]. Part (ii) is contained in [6, Lemma 3]. Part (iii) is a quantitative version of Eisenstein's theorem given in [15, Theorem 2]*. It remains for us to prove (iv).

We will apply (2.6), with K in place of E. By part (ii), the components of $\gamma = (1, \alpha_0, \ldots, \alpha_{2n^2})$ generate K over k. Then according to Silverman [20, end of §3],

$$\mathcal{N}_{k/\mathbb{Q}}(D_{K/k}) \leqslant g^{g\delta}\hat{H}(\gamma)^{2g(g-1)} \tag{5.4}$$

where $g = [K:k]$ and

$$\hat{H}(\gamma) = H_K(\gamma)^{1/[K:k]} = H(\gamma)^{\delta}.$$

(Our k, K, g, $\hat{H}$ correspond to Silverman's F, K, d, H. His δ_F now becomes δ_k (since his field F is our field k), and is the number of archimedean absolute values of k counted with multiplicities, so that $\delta_k = \delta$. His definition of $H(P)$ on page 396 gives our $\hat{H}(\gamma)$.) Substitution of (5.4) into (2.5) gives

$$|D_K| \leqslant g^{g\delta}|D_k|^g H(\gamma)^{2\delta g(g-1)}. \tag{5.5}$$

By (5.1),

$$|\gamma|_v \leqslant A_v^{N+2n^2} \leqslant A_v^{3nN},$$

so that by (5.2),

$$\hat{H}_k(\gamma) \leqslant (\mathcal{N}_k\{A_v\})^{3nN} < (c_1(\delta, N)H_k(F)^{8n^2N})^{3nN} < c_3(\delta, N)H_k(F)^{24n^3N^2}.$$

If we substitute this into (5.5) and observe that $g \leqslant n$ by (i), we obtain (5.3).

6. Construction of a Weierstrass equation

Let $F(X, Y)$ be a polynomial with coefficients in k, of total degree N, and of degree n in Y. Suppose that F is absolutely irreducible and that $F=0$ defines a curve of genus 1. As always, X will be a variable, and $\mathcal{Y}$ will be the algebraic function with $F(X, \mathcal{Y})=0$. Let S be the Riemann surface of $\mathcal{Y}$, so that S has n

*Added in proof. B. Dwork and A. J. van der Poorten in a recent manuscript improve the exponent from $8n^2N$ to $2n-1$. As a consequence, some of our exponents, such as e.g. the number 13 in Theorems 3, 4, may be reduced.

sheets. Now let $\mathfrak{q} \in S$ with $\mathfrak{q} \mid \infty$, i.e. $\mathfrak{q}$ lies above the infinite point of the Riemann sphere. Then $\mathscr{Y}$ has a Puiseux expansion at $\mathfrak{q}$, say

$$\mathscr{Y} = \sum_{s=s_0}^{\infty} \alpha_s X_{\mathfrak{q}}^s,$$

where $X_{\mathfrak{q}} = X_{\infty}^{1/e}$ with $X_{\infty} = 1/X$ and $e = e(\mathfrak{q})$ the ramification index of $\mathfrak{q}$. Since $\mathscr{Y}$ has a pole of order $\leqslant Ne$ at $\mathfrak{q}$, we have $s_0 \geqslant -Ne$. By allowing zero coefficients we may suppose $s_0 = -Ne$. Writing

$$\hat{X} = X_{\mathfrak{q}}, \qquad \hat{\mathscr{Y}} = \hat{X}^{Ne}\mathscr{Y} = \hat{X}^{-s_0}\mathscr{Y} = \alpha_{s_0} + \alpha_{s_0+1}\hat{X} + \cdots$$

we have $F(\hat{X}^{-e}, \hat{X}^{-Ne}\hat{\mathscr{Y}}) = 0$, therefore $\hat{X}^{Nen}F(\hat{X}^{-e}, \hat{X}^{-Ne}\hat{\mathscr{Y}}) = 0$. The latter is a polynomial equation without multiple factors of positive degree in $\hat{\mathscr{Y}}$. It is of degree n in $\hat{\mathscr{Y}}$, and of total degree $\leqslant Nen \leqslant n^2N$. By Lemma 2, the coefficients α_i generate a field $K = k(\alpha_{s_0}, \alpha_{s_0+1}, \ldots)$ with degree $[K:k] \leqslant n$ and with discriminant D_K satisfying

$$|D_K| < c_1(\delta, N)|D_k|^n H_k(F)^{48n^9N^2}. \tag{6.1}$$

Let $\mathbf{D}_3$ be the divisor $\mathbf{D}_3 = 3\mathfrak{q}$. The quantity[3] $\delta = \delta(\mathbf{D}_3)$ introduced in [16] has $\delta \leqslant 3$, and the quantity $\max(3, \delta, n, \deg_X F)$ is $\leqslant N$. By the Riemann–Roch theorem, the space $\mathscr{L}(\mathbf{D}_3) = \mathscr{L}(3\mathfrak{q})$ of functions f on the curve $F = 0$ (so that f lies in the function field $\mathbb{C}(X, \mathscr{Y})$) having at most a pole of order 3 at $\mathfrak{q}$, and having no other poles, has dimension 3. We construct a basis of $\mathscr{L}(3\mathfrak{q})$ as in [16, Theorem A2]. In our present case, this basis will be of the type

$$g_1, g_1X, g_1X^2, \quad \text{or} \quad g_1, g_1X, g_2, \quad \text{or} \quad g_1, g_2, g_3. \tag{6.2}$$

Since $\mathbf{D}_3$ is "defined over K", the g_1, g_2, g_3 lie in $K(X, \mathscr{Y})$ (see [16, §B]). They have expansions at $\mathfrak{q}$:

$$g_i = \sum_{s=-3}^{\infty} \alpha_{is} X_{\mathfrak{q}}^s \tag{6.3}$$

with coefficients $\alpha_{is} \in K$. Furthermore there are K-systems $\{A_v(\mathfrak{q})\}$, $\{B_v(i)\}$ defined for $v \in M(K)$ such that

$$|\alpha_{is}|_v \leqslant A_v(\mathfrak{q})^{s+4N^3} B_v(i) \quad (s \geqslant -3) \tag{6.4}$$

[3] Not to be confused with the degree of k.

for every $v \in M(K)$. We have

$$\mathcal{N}_K\{A_v(\mathfrak{q})\} < (2^7 N^5 H(F))^{9N^5 \deg K}, \tag{6.5}$$

$$\mathcal{N}_K\{B_v(i)\} < (9N^4 H(F))^{365N^{11} \deg K} \tag{6.6}$$

by [16, Theorem C2] (applied to K rather than k).

We now introduce a new notation f_1, f_2, f_3 for the basis in (6.2), and we write

$$f_i = \sum_{s=-3}^{\infty} \beta_{is} X_{\mathfrak{q}}^s \ (i = 1, 2, 3).$$

For instance, if $f_3 = g_1 X^2 = g_1 X_{\mathfrak{q}}^{-2e}$, then $\beta_{3s} = \alpha_{3,s+2e}$. In general, the subscripts are shifted at most by $2e \leqslant 2n$ so that

$$|\beta_{is}|_v \leqslant A_v(\mathfrak{q})^{s+4N^3+2n} B_v \ (i = 1, 2, 3) \tag{6.7}$$

where B_v is the product of the $B_v(i)$. (We are dealing with $B_v(1)$, or $B_v(1)$, $B_v(2)$, or $B_v(1)$, $B_v(2)$, $B_v(3)$ in the three cases in (6.2).)

By the Riemann–Roch theorem, some $\beta_{i,-3} \neq 0$. Say $\beta_{3,-3} \neq 0$. Set $h_3 = f_3$, so that $\operatorname{ord}_{\mathfrak{q}} h_3 = -3$ (i.e., h_3 has a pole of order 3 at $\mathfrak{q}$). Set

$$\begin{aligned} h_1 &= \beta_{3,-3} f_1 - \beta_{1,-3} f_3, \\ h_2 &= \beta_{3,-3} f_2 - \beta_{2,-3} f_3. \end{aligned} \tag{6.8}$$

These lie in $\mathscr{L}(2\mathfrak{q})$, so that in particular they have a pole of order $\leqslant 2$ at $\mathfrak{q}$. By the Riemann–Roch theorem again, at least one of h_1, h_2 has in fact a pole of order 2. Say h_2 does, so that $\operatorname{ord}_{\mathfrak{q}} h_2 = -2$. Writing

$$h_i = \sum_{s=-3}^{\infty} \gamma_{is} X_{\mathfrak{q}}^s \ (i = 2, 3),$$

we have $\gamma_{3,-3} \neq 0$, $\gamma_{2,-3} = 0$, $\gamma_{2,-2} \neq 0$. It is easily seen that

$$|\gamma_{is}|_v \leqslant A_v(\mathfrak{q})^{s+8N^3+4n} B_v^2 * 2 \ (i = 2, 3), \tag{6.9}$$

where $*2$ denotes an extra factor 2 when v is archimedean, and is to be ignored otherwise. (This convention will be used throughout).

The 7 functions

$$l_1 = 1, \ l_2 = h_2, \ l_3 = h_3, \ l_4 = h_2^2, \ l_5 = h_2 h_3, \ l_6 = h_2^3, \ l_7 = h_3^2$$

lie in $\mathscr{L}(6\mathfrak{q})$, say

$$l_i = \sum_{s=-6}^{\infty} \delta_{is} X_{\mathfrak{q}}^s \ (i = 1, \dots, 7).$$

Since $N \geqslant 3$ and therefore $8N^3 + 4n < 9N^3$, and using simple facts on products of Puiseux series (e.g. [16, Lemma 18]), we obtain

$$|\delta_{is}|_v \leqslant A_v(\mathfrak{q})^{s+27N^3} B_v^6 * 8(s+7)^2 \quad \begin{pmatrix} 1 \leqslant i \leqslant 7 \\ s \geqslant -6 \end{pmatrix}.$$

By the Riemann–Roch theorem, the 7 functions $l_1, \dots, l_7$ in $\mathscr{L}(6\mathfrak{q})$ are linearly dependent. In particular the matrix (δ_{is}) with $1 \leqslant i \leqslant 7$, $-6 \leqslant s \leqslant 0$ must be singular. The system of equations

$$\sum_{j=1}^{7} z_j \delta_{js} = 0 \quad (-6 \leqslant s \leqslant 0) \tag{6.10}$$

has a solution $\mathbf{z} = (z_1, \dots, z_7) \neq \mathbf{0}$ in K^7. A typical coefficient vector $\boldsymbol{\delta}_s = (\delta_{1s}, \dots, \delta_{7s}) \in K^7$ has

$$|\boldsymbol{\delta}_s|_v \leqslant A_v(\mathfrak{q})^{27N^3} B_v^6 * 400$$

since $8(s+7)^2 \leqslant 8 \cdot 7^2 < 400$ when $s \leqslant 0$. If the system (6.10) of equations has rank 6, then there is a solution $\mathbf{z}$ whose components are determinants of order 6 of the coefficient matrix (δ_{js}), so that

$$|\mathbf{z}|_v \leqslant A_v(\mathfrak{q})^{162N^3} B_v^{36} * 6!(400)^6. \tag{6.11}$$

In fact there is always a solution $\mathbf{z} \neq \mathbf{0}$ of (6.10) satisfying these inequalities. The function $z_1 l_1 + \cdots + z_7 l_7$, that is

$$z_1 + z_2 h_2 + z_3 h_3 + z_4 h_2^2 + z_5 h_2 h_3 + z_6 h_2^3 + z_7 h_3^2,$$

has no poles, and has a zero at $\mathfrak{q}$, hence vanishes identically. Since $l_1, \dots, l_6$ have poles of different orders at $\mathfrak{q}$, the coefficient $z_7 \neq 0$. Similarly $z_6 \neq 0$. One can get rid of the terms $z_2 h_2$ and $z_5 h_2 h_3$ by the method of 'completion of the squares'. Setting

$$X' = h_2, \qquad \mathscr{Y}' = 2z_7 h_3 + z_5 h_2 + z_3$$

one obtains

$$\mathscr{Y}'^2 = a_0X'^3 + b_0X'^2 + c_0X' + d_0 \tag{6.12}$$

where $a_0 = -4z_6z_7$, $b_0 = z_5^2 - 4z_4z_7$, $c_0 = 2z_3z_5 - 4z_2z_7$, $d_0 = z_3^2 - 4z_1z_7$. Therefore a_0, b_0, c_0, d_0 lie in K and have

$$|a_0|_v, |b_0|_v, |c_0|_v, |d_0|_v \leqslant A_v(\mathfrak{q})^{324N^3}B_v^{72} * C_0 \tag{6.13}$$

with some absolute constant C_0, for $v \in M(K)$. Our construction of $X', \mathscr{Y}'$ is well known and standard (see e.g. Deuring [7, §19] or Silverman [19, §III.3]); only the estimate (6.13) is new. It is well known that the function field $\mathscr{K} = K(X, \mathscr{Y}) = K(X', \mathscr{Y}')$, so that $X, \mathscr{Y} \mapsto X', \mathscr{Y}'$ defines a birational map from the curve $F = 0$ to the curve (6.12), and this map is defined over K.

The coefficient a_0 in (6.12) can easily be got rid of, as we will see below. A greater difficulty is as follows. Since $X' = h_2$ has no finite poles (i.e. poles above $\mathbb{C}$), X' is integral over $\mathbb{C}[X]$. Since $X' \in K(X, \mathscr{Y})$ is algebraic over $K(X)$, hence over $\mathbb{Q}(X)$, we see that X' is integral over $\mathbb{Q}[X]$. However, the quantity X_1 of Proposition 1 is supposed to be integral over $\mathbb{Z}[X]$. This is why we have to put in more work to obtain this proposition.

7. An equation satisfied by X' over $K[X]$

Since X' is integral over $K[X]$, it satisfies a polynomial equation with coefficients in $K[X]$, and with leading coefficient 1. We will exhibit such an equation. For every place $\mathfrak{p} \mid \infty$ we have an expansion

$$\mathscr{Y} = \sum_{s=s_0(\mathfrak{p})}^{\infty} \alpha_s(\mathfrak{p})X_{\mathfrak{p}}^s \tag{7.1}$$

where $X_{\mathfrak{p}} = X_{\infty}^{1/e(\mathfrak{p})}$. This gives isomorphic embeddings of the function field $\mathscr{K} = K(X, \mathscr{Y})$ into the field of Puiseux series in $X_{\infty} = 1/X$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ lie above ∞ (in symbols: $\mathfrak{p}_i \mid \infty$) this gives l embeddings, but not necessarily n embeddings where $n = [\mathscr{K} : K(X)]$. But in the case when $e(\mathfrak{p}) > 1$, the expansion (7.1) of $\mathscr{Y}$ is not unique: one may replace $X_{\mathfrak{p}}$ by $X_{\mathfrak{p}}\zeta$, and therefore $\alpha_s(\mathfrak{p})$ by $\alpha_s(\mathfrak{p})\zeta^s$, where ζ is an $e(\mathfrak{p})$th root of 1. Since $\Sigma_{\mathfrak{p}\mid\infty} e(\mathfrak{p}) = n$, we obtain in this way n embeddings of $\mathscr{K}$ into the field of Puiseux series in X_{∞}. Let these embeddings map X' into

$$\sum_{s=t_0(\mathfrak{p})}^{\infty} \gamma_s(\mathfrak{p})\zeta^s X_{\mathfrak{p}}^s = u_{\mathfrak{p}\zeta}, \tag{7.2}$$

say. Here $\mathfrak{p} \mid \infty$ and ζ lies in $U_{\mathfrak{p}}$, the group of $e(\mathfrak{p})$th roots of 1. Now if T is a new variable then

$$\prod_{\substack{\mathfrak{p}\mid\infty \\ \zeta\in U_{\mathfrak{p}}}} (T - u_{\mathfrak{p}\zeta}) = T^n + p_1 T^{n-1} + \cdots + p_n, \tag{7.3}$$

where, up to sign, p_i is the ith elementary symmetric polynomial in the n quantities $u_{\mathfrak{p}\zeta}$. Therefore, up to sign, each p_i is an elementary symmetric polynomial in X' and its conjugates over $K(X)$, and this shows that (7.3) is the field polynomial of X' in the field $\mathscr{K} = K(X, \mathscr{Y})$ over $K(X)$. Since X' is integral over $K[X]$, we infer that $p_i \in K[X]$ $(i = 1, \ldots, n)$. Since $X' = h_2$ has a pole of order 2 at $\mathfrak{q}$, and has no other pole, we may take $t_0(\mathfrak{q}) = -2$, and $t_0(\mathfrak{p}) = 0$ for $\mathfrak{p} \neq \mathfrak{q}$. Since there are $e(\mathfrak{q})$ series (7.2) with $\mathfrak{p} = \mathfrak{q}$ starting with $X_{\mathfrak{q}}^{-2} = X_\infty^{-2/e(\mathfrak{q})}$ and since the other series (7.2) have no negative powers of X_∞, we see that each p_i certainly contains only powers X_∞^{μ} with $\mu \geqslant -2$ in its Puiseux series. But since p_i is a polynomial in X, it is in fact a quadratic polynomial in X. Write

$$p_i = \sum_{s=0}^{2} \pi_{is} X^s = \sum_{s=0}^{2} \pi_{is} X_\infty^{-s} = \sum_{s=-2}^{0} \pi_{i,-s} X_\infty^{s}.$$

We have for $-2 \leqslant s \leqslant 0$ and $1 \leqslant i \leqslant n$ that

$$\pi_{i,-s} = (-1)^i \sum_{\substack{\mathfrak{p}_1,\zeta_1,s_1;\ldots;\mathfrak{p}_i,\zeta_i,s_i \\ s_1/e(\mathfrak{p}_1)+\cdots+s_i/e(\mathfrak{p}_i)=s}} \gamma_{s_1}(\mathfrak{p}_1)\zeta_1^{s_1} \cdots \gamma_{s_i}(\mathfrak{p}_i)\zeta_i^{s_i}. \tag{7.4}$$

In the sum here, each $\mathfrak{p}_j \mid \infty$ and $\zeta_j \in U_{\mathfrak{p}_j}$; moreover, the pairs $\mathfrak{p}_j$, ζ_j for $j = 1, \ldots, i$ are all distinct.

By [16, Theorem C2], the g_i of (6.2) have expansions analogous to (6.3) for every $\mathfrak{p} \mid \infty$, with coefficients $\alpha_{is}(\mathfrak{p})$ in a field $K(\mathfrak{p}) \supset K$, and with

$$|\alpha_{is}(\mathfrak{p})|_v \leqslant A_v(\mathfrak{p})^{s+4N^3} B_v(i), \tag{7.5}$$

in analogy to (6.4). Here $\{A_v(\mathfrak{p})\}$ is a K-system and $B_v(i)$ is a K-system independent of $\mathfrak{p}$, so that it is the system of (6.4). The system $\{A_v(\mathfrak{p})\}$ satisfies a relation like (6.5). Writing $f_i = \Sigma_s \beta_{is}(\mathfrak{p}) X_{\mathfrak{p}}^s$, we have the analogue of (6.7). By (6.8), the coefficients in the Puiseux expansions of $h_2 h_3$ involve both the coefficients $\beta_{is}(\mathfrak{p})$ and certain $\beta_{is}(\mathfrak{q})$. These coefficients therefore lie in $K(\mathfrak{p})$. Writing $h_i = \Sigma_s \gamma_{is}(\mathfrak{p}) X_{\mathfrak{p}}^s$, we obtain

$$|\gamma_{is}(\mathfrak{p})|_v \leqslant A_v(\mathfrak{p})^{s+4N^3+2n} A_v(\mathfrak{q})^{4N^3+2n} B_v^2 * 2 \ (i = 2, 3)$$

in place of (6.9). Since $X' = h_2$, the expansion (7.2) has in particular

$$|\gamma_s(\mathfrak{p})|_v \leqslant A_v(\mathfrak{p})^{s+5N^3} C_v,$$

where

$$C_v = A_v(\mathfrak{q})^{5N^3} B_v^2 * 2.$$

This holds for every $v \in M(K)$ and every extension of $|\cdot|$ to $K(\mathfrak{p})$. Therefore a typical summand on the right-hand side of (7.4) has absolute value

$$|\cdots|_v \leqslant A_v(\mathfrak{p}_1)^{s_1+5N^3} \cdots A_v(\mathfrak{p}_i)^{s_i+5N^3} C_v^i. \tag{7.6}$$

This holds for $v \in M(K)$ and every extension of $|\cdot|_v$ to a field big enough to contain the fields $K(\mathfrak{p})$ and the elements of $U_{\mathfrak{p}}$ for every $\mathfrak{p} \mid \infty$. In the sum (7.4) we have $s_j \geqslant -2$ when $\mathfrak{p}_j = \mathfrak{q}$, and $s_j \geqslant 0$ otherwise. Therefore each subsum of

$$\frac{s_1}{e(\mathfrak{p}_1)} + \cdots + \frac{s_i}{e(\mathfrak{p}_i)}$$

occurring in (7.4) is $\geqslant -2$, so that each subsum is $\leqslant s+2 \leqslant 2$. Therefore $s_j \leqslant 2e(\mathfrak{p}_j) \leqslant 2n$. Thus the exponents $s_j + 5N^3$ in (7.6) may be replaced by $5N^3 + 2n < 6N^3$, and (7.6) yields (Observe that the same $\mathfrak{p}_j$ may occur up to $e(\mathfrak{p}_j)$ times in (7.6))

$$|\cdots|_v \leqslant C_v^n D_v$$

where

$$D_v = \prod_{j=1}^{l} A_v(\mathfrak{p}_j)^{6N^3 e(\mathfrak{p}_j)}.$$

By what we have just said, $-2 \leqslant s_j \leqslant 2n$, so that the number of possibilities for each s_j is $\leqslant 5n$, and the number of summands in (7.4) is $\leqslant (5n^2)^i \leqslant (5n^2)^n$. Therefore the coefficients π_{is} of p_i have

$$|\pi_{is}|_v \leqslant C_v^n D_v * (5n^2)^n.$$

We now set

$$W_v = A_v(\mathfrak{q})^{5N^4+324N^3} B_v^{2N+72} \left(\prod_{j=1}^{l} A_v(\mathfrak{p}_j)^{6N^3 e(\mathfrak{p}_j)} \right) * (10n^2)^n C_0,$$

where C_0 is the constant in (6.13). We then have proved

LEMMA 3. (i) $|a_0|_v, |b_0|_v, |c_0|_v, |d_0|_v \leqslant W_v$ *for every* $v \in M(K)$.
(ii) X' *satisfies an equation*

$$X'^n + p_1(X)X'^{n-1} + \cdots + p_n(X) = 0$$

where each $p_i(X)$ *is a polynomial in* X *of degree* $\leqslant 2$ *with coefficients* π_{is} *in* K *having*

$$|\pi_{is}|_v \leqslant W_v$$

for $v \in M(K)$.

Finally, we remark that from the estimates (6.5), (6.6), and the analogous estimates for $\mathscr{N}_K\{A_v(\mathfrak{p})\}$, and since $\Sigma e(\mathfrak{p}_j) = n \leqslant N$, and $H_K(F) = H(F)^{\deg K}$, we get

$$\mathscr{N}_K\{W_v\} < c_1(\delta, N)H_K(F)^{9N^5(5N^4+324N^3+6N^4)+3\cdot 365N^{11}(2N+72)}.$$

Note that $c_1(\delta, N)$, as well as all the other constants, is effectively computable. Since $N \geqslant 3$, the exponent here is $< 3\cdot 10^4 N^{12}$, and we obtain

$$\mathscr{N}_K\{W_v\} < c_1(\delta, N)H_K(F)^{3\cdot 10^4 N^{12}}. \tag{7.7}$$

8. Proof of Proposition 1

Let $M_0(K)$, $M_\infty(K)$ denote the set of non-archimedean and of archimedean absolute values in $M(K)$, respectively. Given a K-system $\{W_v\}$, set

$$\mathscr{N}_{Kj}\{W_v\} = \prod_{v \in M_j(K)} W_v^{d_v} \quad (j = 0, \infty),$$

where d_v is the local degree of v. (Here $v \in M(K)$, whereas in the Introduction we had local degrees d_v for $v \in M(k)$. No confusion should occur.)

LEMMA 4. *Let* $\{W_v\}$ *be a* K*-system. There is an integer* $\alpha \neq 0$ *in* K *having*

$$|\alpha|_v \leqslant W_v^{-1} \quad \text{for } v \in M_0(K), \tag{8.1}$$

$$|\alpha|_v \leqslant (|D_K|^{1/2}\mathscr{N}_{K0}\{W_v\})^{1/\deg K} \quad \text{for } v \in M_\infty(K). \tag{8.2}$$

Proof. With non-archimedean v there is associated a prime ideal $\mathscr{P}_v$ of K, and this prime ideal divides a prime number p_v. We have $d_v = \varepsilon_v f_v$ where ε_v is the

ramification index and f_v is the degree of the residue class field of $\mathfrak{P}_v$. Given $\gamma \neq 0$ in K we have $|\gamma|_v = p_v^{-c_v/\varepsilon_v}$ where c_v is the exponent of $\mathfrak{P}_v$ in the factorization of the principal ideal (γ) as a product of prime ideals.

Suppose now that $W_v = p_v^{w_v/\varepsilon_v}$ for $v \in M_0(K)$, and let $\mathfrak{A}$ be the ideal

$$\mathfrak{A} = \prod_{v \in M_0(K)} \mathfrak{P}_v^{w_v}.$$

Then $\mathfrak{A}$ is an integral ideal of K of norm

$$\mathcal{N}_K(\mathfrak{A}) = \prod_{v \in M_0(K)} p_v^{w_v f_v} = \prod_{v \in M_0(K)} W_v^{\varepsilon_v f_v} = \mathcal{N}_{K0}\{W_v\}.$$

The condition (8.1) means precisely that $\alpha \in \mathfrak{A}$. By Minkowski's theorem (see, e.g. [11, middle of p. 120]) there is an $\alpha \neq 0$ in $\mathfrak{A}$ with

$$|\alpha|_v \leqslant |\Delta|^{1/\deg K} \quad \text{for } v \in M_\infty(K),$$

where $\Delta = \mathcal{N}_K(\mathfrak{A})\sqrt{|D_K|}$. The lemma follows.

The proof of Proposition 1 is completed as follows. Let $\{W_v\}$ be the system of Lemma 3, and construct α as in Lemma 4. With X', $\mathcal{Y}'$, a_0, b_0, c_0, d_0 as in (6.12), set

$$X_1 = \alpha^2 a_0 X', \qquad \mathcal{Y}_1 = \alpha^3 a_0 \mathcal{Y}'.$$

Then

$$\mathcal{Y}_1^2 = X_1^3 + bX_1^2 + cX_1 + d \tag{8.3}$$

with $b = \alpha^2 b_0$, $c = \alpha^4 a_0 c_0$, $d = \alpha^6 a_0^2 d_0$. Since $|\alpha|_v \leqslant W_v^{-1}$ for $v \in M_0(K)$, and in view of Lemma 3(i), the coefficients b, c, d are integers of K. The polynomial $f = X^3 + bX^2 + cX + d$ has

$$|f|_v \leqslant W_v^3(|D_K|^{1/2}\mathcal{N}_{K0}\{W_v\})^{6/\deg K}$$

for $v \in M_\infty(K)$. Since f has integer coefficients,

$$\begin{aligned} H_K(f) &\leqslant \prod_{v \in M_\infty(K)} (W_v^{3d_v}(|D_K|^{1/2}\mathcal{N}_{K0}\{W_v\})^{6d_v/\deg K}) \\ &\leqslant |D_K|^3(\mathcal{N}_K\{W_v\})^6, \end{aligned}$$

so that by (5.3) and (7.7),

$$H_K(f) < c_2(\delta, N)|D_k|^{3n}H_K(F)^{2\cdot 10^5 N^{12}}, \tag{8.4}$$

which is (1.11).

Let $P(T)$ be the polynomial of the last section, having $P(X')=0$. Then if $Q(T)=\alpha^n P(T/\alpha)$, we have $Q(\alpha X')=0$. Here Q again has leading coefficient 1, and its other coefficients are quadratic polynomials $q_i(X)$, where each $q_i(X)$ in turn has coefficients $\phi_{is}=\pi_{is}\alpha^i$, so that by Lemma 3(ii) and our construction of α, $|\phi_{is}|_v \leqslant 1$ for $v \in M_0(K)$. Therefore the coefficients of $Q(T)$ lie in $\mathcal{O}_K[X]$, where $\mathcal{O}_K$ is the ring of integers of K. We may conclude that $\alpha X'$, being a root of Q, is integral over $\mathcal{O}_K[X]$. Since αa_0 is an integer, also $X_1=\alpha^2 a_0 X'$ is integral over $\mathcal{O}_K[X]$, therefore over $\mathbb{Z}[X]$.

9. Proof of Theorems 3 and 4

Let M be the birational map from the curve $(\mathscr{C})$ to the Weierstrass curve $(\mathscr{W})$ as described in Proposition 1. When $\mathbf{p}$ is a nonsingular point of $(\mathscr{C})$, then $M(\mathbf{p})$ is well defined ([19, Ch. II, Proposition 2.1]). Further since X_1 is integral over $\mathbb{Z}[X]$, and by (8.3), it follows that when $\mathbf{p}=(x, y)$ is a finite (i.e. not on the line at infinity) point on $(\mathscr{C})$, then $M(\mathbf{p})$ is a finite point on the Weierstrass curve $(\mathscr{W})$. Since the Weierstrass curve is nonsingular, the inverse map M^{-1} is defined on $M(\mathbf{p})$, and $M^{-1}M(\mathbf{p})=\mathbf{p}$. Therefore M provides an injection from finite nonsingular points of $(\mathscr{C})$ to finite points of $(\mathscr{W})$.

For nonsingular $(x, y)=\mathbf{p}$ on $(\mathscr{C})$, write $M(x, y)=(x_1, y_1)$. When $(x, y)\in K^2$, then also $(x_1, y_1)\in K^2$, since M is defined over K. Moreover, when $x\in\mathcal{O}_K$, then also $x_1\in\mathcal{O}_K$ since X_1 is integral over $\mathbb{Z}[X]$, therefore x_1 is integral over $\mathbb{Z}[x]$. Since (x_1, y_1) lies on the Weierstrass curve $(\mathscr{W})$, we also have $y_1\in\mathcal{O}_K$. Therefore the number of nonsingular points on $(\mathscr{C})$ with coordinates in $\mathcal{O}_K$ is bounded by the number of points on the curve $(\mathscr{W})$ with coordinates in $\mathcal{O}_K$. By (1.4), the latter number is

$$<c_1(\delta, N, \varepsilon)|D_K|^{3/2+\varepsilon}H_K(f)^{2+\varepsilon}$$

where $f=X^3+bX^2+cX+d$ and where we used the fact that $\deg K \leqslant \delta N$. If we insert our estimates (1.10) and (1.11) and observe that $\varepsilon>0$ was arbitrary, we obtain

$$<c_2(\delta, N)|D_k|^{(3/2)N+2\cdot 3N+(1/2)N}H_k(F)^{(3/2)\cdot 50N^{11}}H_K(F)^{5\cdot 10^5 N^{12}}$$

$$<c_2(\delta, N)|D_k|^{8N}H_k(F)^{6\cdot 10^5 N^{13}}.$$

Since the number of singular points on $(\mathscr{C})$ is $\leqslant\frac{1}{2}N(N-1)$, Theorem 3 follows.

We now turn to Theorem 4. Our algebraic function X' satisfied $P(X')=0$, i.e. $X'^n+p_1(X)X'^{n-1}+\cdots+p_n(X)=0$ with $p_i(X)=\pi_{i0}+\pi_{i1}X+\pi_{i2}X^2$. Consider the

polynomial

$$P(X, T) = T^n + p_1(X)T^{n-1} + \cdots + p_n(X)$$

in variables X, T, and note that $P(X, T)$ has no factor independent of X, since when considered as a polynomial in T it was the field polynomial of the non-constant algebraic function X' over $K(X)$. Further $X_1 = \alpha^2 a_0 X'$ satisfies $R(X, X_1) = 0$ where $R(X, T) = (\alpha^2 a_0)^n P(X, T/(\alpha^2 a_0))$. The coefficients of $R(X, T)$ are $\pi_{is}(\alpha^2 a_0)^i$. They are integers of K. For given x_1, the polynomial $R^*(X) = R(X, x_1)$ is a nonzero quadratic polynomial in X. We have

$$|R^*|_v \leqslant \left(\max_{i,s} |\pi_{is}|_v |\alpha^2 a_0|_v^i\right)(\max(1, |x_1|_v^n)) * (n + 1).$$

By Lemma 3, and by our construction of α (in particular see (8.2)) we have for $v \in M_\infty(K)$ that

$$|R^*|_v \leqslant W_v^{n+1}(|D_K|^{1/2}\mathcal{N}_{K0}\{W_v\})^{2n/\deg K} \max(1, |x_1|_v^n) * (n + 1).$$

Since R has integer coefficients, so does R^* when $x_1 \in \mathcal{O}_K$. We obtain

$$H_K(R^*) \leqslant (|D_K|^{1/2}\mathcal{N}_K\{W_v\})^{2n} h_K(x_1)^n \cdot (n + 1)^{\deg K},$$

and therefore by (1.10), (7.7),

$$H_K(R^*) < c_3(\delta, N)|D_k|^{N^2} H_k(F)^{48N^{12}} H_K(F)^{6 \cdot 10^4 N^{13}} h_K(x_1)^n,$$

so that

$$H_K(R^*) < c_3(\delta, N)|D_k|^{N^2} H_k(F)^{7 \cdot 10^4 N^{14}} h_K(x_1)^n.$$

Now if (x, y) is on $(\mathscr{C})$ and $M(x, y) = (x_1, y_1)$, then $R(x, x_1) = 0$, $R^*(x) = 0$. Since R^* is quadratic, we have $h(x) \leqslant 3H(R^*)$ ([15, Lemma 3]). Therefore when $(x, y) \in \mathcal{O}_k^2$, so that $(x_1, y_1) \in \mathcal{O}_K$, then

$$h_K(x) < c_4(\delta, N)|D_k|^{N^2} H_k(F)^{7 \cdot 10^4 N^{14}} h_K(x_1)^n. \tag{9.1}$$

On the other hand, by Theorem 2,

$$h_K(x_1) < \exp(c_5(\delta, N)V(\log^* V)^{48\delta N}) < \exp(c_6(\delta, N, \varepsilon)V^{1+\varepsilon})$$

where $V = D_K^{48} H_K(f)^{128}$. By (1.10), (1.11),

$$V < c_7(\delta, N) D_k^{48N+128\cdot 3^N} H_k(F)^{48\cdot 48^{N^{11}}} H_K(F)^{256\cdot 10^{5N^{12}}}$$
$$< c_7(\delta, N) D_k^{432^N} H_k(F)^{3\cdot 10^{7N^{13}}},$$

so that $V^{1+\varepsilon} < c_8(\delta, N)W$ when $\varepsilon > 0$ is sufficiently small, where W is given by (1.7). In conjunction with (9.1) this gives

$$h_k(x) \leqslant h_K(x) < \exp(c_9(\delta, N)W).$$

By symmetry, the same estimate holds for y.

All this was for nonsingular points (x, y). It is easily seen that a much better estimate holds for singular points on $(\mathscr{C})$. Theorem 4 is established.

References

[1] A. Baker: The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, *J. London Math. Soc.* 43 (1968), 1–9.

[2] A. Baker: Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* 65 (1969), 439–444.

[3] A. Baker: The theory of linear forms in logarithms. Transcendence theory: Advances and applications, *Proceedings of 1976 Cambridge Conference*, Academic Press (1977), pp. 1–27.

[4] A. Baker and J. Coates: Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* 67 (1970), 595–602.

[5] E. Bombieri and J. Vaaler: On Siegel's lemma, *Invent. Math.* 73 (1983), 11–32.

[6] J. Coates: Construction of rational functions on a curve, *Proc. Camb. Phil. Soc.* 68 (1970), 105–123.

[7] M. Deuring: Lectures on the theory of algebraic functions of one variable, *Springer Lecture Notes* 314 (1973).

[8] E. Dobrowolski: On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* 34 (1979), 391–401.

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

[10] K. Győry: On the solutions of linear diophantine equations in algebraic integers of bounded norm. Ann. Univ. Budapest, *Eötvös, Sect. Math.* 22–23 (1979/80), 225–233.

[11] E. Hecke: *Vorlesungen über die Theorie der Algebraischen Zahlen*, Akademische Verlagsges, Leipzig (1923).

[12] S. Lang: *Algebraic Numbers*, Addison-Wesley Publ. Co. (1964).

[13] S. Lang: *Fundamentals of Diophantine Geometry*, Springer-Verlag (1983).

[14] P. Philippon and M. Waldschmidt: *Lower Bounds for Linear Forms in Logarithms*, (New advances in transcendence theory, 1986 symposium, Durham), Cambridge University Press (1988).

[15] W.M. Schmidt: Eisenstein's theorem on power series expansions of algebraic functions, *Acta Arith.* 56 (1990), 161–179.

[16] W.M. Schmidt: Construction and estimation of bases in function fields, *J. Number Theory* (to appear).

[17] C.L. Siegel (under the pseudoname X): The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$, *J. London Math. Soc.* 1 (1926), 66–68.

[18] C.L. Siegel: Abschätzung von Einheiten, *Nachr. Akad. d. Wiss. Göttingen, Math.-Phys. Kl.* (1969), 71–86 (Collected Works, No. 88).
[19] J.H. Silverman: The arithmetic of elliptic curves, *Springer Graduate Texts* 106 (1986).
[20] J.H. Silverman: Lower bounds for height functions, *Duke Math. J.* 51 (1984), 395–403.
[21] V.G. Sprindžuk: Hyperelliptic diophantine equations and the number of ideal classes, *Acta. Arith.* 30 (1976), 95–108 (in Russian).
[22] G. Wüstholz: *A New Approach to Baker's Theorem on Linear Forms in Logarithms III*, (New advances in transcendence theory, 1986 symposium, Durham), Cambridge University Press.