ISRAEL JOURNAL OF MATHEMATICS 90 (1995), 235–252

EFFECTIVE ANALYSIS OF INTEGRAL POINTS ON ALGEBRAIC CURVES

BY

YURI BILU

Department of Mathematics and Computer Science
Ben-Gurion University, Beer Sheva 84105, Israel
and
Université Bordeaux 2
Mathématiques Stochastiques
F-33076 Bordeaux Cedex, France

ABSTRACT

Let $\mathbf{K}$ be an algebraic number field, $S \supseteq S_\infty$ a finite set of valuations and C a non-singular algebraic curve over $\mathbf{K}$. Let $x \in \mathbf{K}(C)$ be non-constant. A point $P \in C(\mathbf{K})$ is *S-integral* if it is not a pole of x and $|x(P)|_v > 1$ implies $v \in S$. It is proved that all S-integral points can be effectively determined if the pair (C, x) satisfies certain conditions. In particular, this is the case if

(i) $x: C \to \mathbf{P}^1$ is a Galois covering and $\mathbf{g}(C) \geq 1$;

(ii) the integral closure of $\bar{\mathbf{Q}}[x]$ in $\bar{\mathbf{Q}}(C)$ has at least two units multiplicatively independent mod$\bar{\mathbf{Q}}^*$.

This generalizes famous results of A. Baker and other authors on the effective solution of Diophantine equations.

Introduction

Let C be a non-singular algebraic curve of genus $\mathbf{g} = \mathbf{g}(C)$ defined over the field of all algebraic numbers $\bar{\mathbf{Q}}$, $x \in \bar{\mathbf{Q}}(C)$ non-constant and $\Sigma = \Sigma(x)$ the set of poles of x. Let $\mathbf{K}$ be an algebraic number field such that both C and x are defined over

Received July 8, 1992 and in revised form March 6, 1994

$\mathbf{K}$, and S a finite set of valuations of $\mathbf{K}$, containing the set S_∞ of Archimedean valuations. Such $\mathbf{K}$ and S will be called **suitable**.

We study in this paper **the set of S-integral points**

$$C(x,\mathbf{K},S) = \{P \in C(\mathbf{K}) : |x(P)|_v \le 1 \text{ for } v \notin S\}. \tag{I.1}$$

The classical theorem of Siegel [S] (see [L1, Ch. 8] for a modern proof) states that *$C(x,\mathbf{K},S)$ is finite provided $|\Sigma| \ge 3$ or $\mathbf{g}(C) \ge 1$.* In the case $\mathbf{g}(C) \ge 2$ it is covered by Mordell's conjecture, proved by Faltings [F], which asserts that *$C(\mathbf{K})$ is finite provided $\mathbf{g}(C) \ge 2$.* Unfortunately, existing proofs of Siegel's theorem and Mordell's conjecture are non-effective, i.e. they do not provide with any explicit bound for the heights of the points from $C(x,\mathbf{K},S)$ (or $C(\mathbf{K})$).

In 1966 A. Baker [B1] obtained effective lower bounds for linear forms in the logarithms of algebraic number. This enabled him to solve effectively certain types of binary Diophantine equations (realizing an earlier idea of A.O. Gelfond [G]), i.e. to effectivize Siegel's theorem in some particular cases. See [Ba2] – [Ba4].

The investigations of A. Baker were supplemented and generalized by other authors. We refer to [Sp] and [ShT] for historical surveys and extensive bibliography. However, mainly studied were Diophantine equations of two classical types. The first one is the **Thue equation**

$$f(x,y) = A, \tag{I.2}$$

f being a form having three distinct linear factors, and $A \ne 0$. The second is the **superelliptic equation**

$$y^m = f(x), \tag{I.3}$$

where

$$f(x) = a\prod_{i=1}^{\nu}(x-\alpha_i)^{r_i},$$

$\alpha_i \ne \alpha_j$ for $i \ne j$ and the ν-tuple $\left(\frac{m}{(m_1,r_1)},\dots,\frac{m}{(m_1,r_\nu)}\right)$ is not of the type $(\mu,1,\dots,1)$ or $(2,2,1,\dots,1)$ (in particular, $\nu \ge 2$).

As was noticed already by Siegel, the case $\mathbf{g}(C) = 0$, $|\Sigma| \ge 3$ can be reduced to (I.2). The case $\mathbf{g}(C) = 1$ was considered by A. Baker and J. Coates [BaC] by reduction to (I.3). Thus, for curves of genus 0 and 1 Siegel's theorem is effective.

The case $\mathbf{g}(C) \geq 2$ still remains open (except for the particular cases discussed here).

V. G. Sprindžuk posed the problem of extending the method of Gelgond–Baker to classes of Diophantine equations more general than (2) and (3). An attempt at such an extension was made by H. Kleiman [K], who considered the general equation $f(x, y) = 0$, but made some strong assumptions about the polynomial $f(x, y)$. In the appendix to this paper we formulate Kleiman's results and show that they can be deduced from our Theorem A, formulated below.

It will be convenient to introduce the following concept. We say that (C, x) is a **universally effective pair** (UEP) if for any suitable $\mathbf{K}$ and S

$$\max_{P \in C(x, \mathbf{K}, S)} h_x(P) \leq c\ (C,\ x,\ \mathbf{K},\ S)\,, \tag{I.4}$$

c being effective. Here

$$h_x(P) = \begin{cases} h(1\colon x(P)), & x(P) \neq \infty, \\ 0, & x(P) = \infty, \end{cases}$$

where $h(\alpha_0\colon \alpha_1)$ is the **absolute logarithmic height** on the projective line $\mathbf{P}^1$.

Let y be another non-constant element of $\bar{\mathbf{Q}}(C)$. Then a simple argument shows that

(∗) *if $\Sigma(y) \subseteq \Sigma(x)$, then for any $\mathbf{K}$, S suitable for the pair (C, x) there exist $\mathbf{L}$, T, suitable for (C, y) and such that*

$$C(x, \mathbf{K}, S) \subseteq C(y, \mathbf{L}, T).$$

Moreover, for given C, x, y, $\mathbf{K}$ and S these $\mathbf{L}$ and T can be effectively constructed. Indeed, x and y satisfy an irreducible polynomial equation of the form

$$y^n + \sum_{i=0}^{m} \sum_{j=0}^{n-1} a_{ij} x^i y^j = 0.$$

Now let $\mathbf{L}$ be the extension of $\mathbf{K}$, generated by the coefficients a_{ij} $(0 \leq i \leq m$, $0 \leq j \leq n-1)$, and T the set of valuations of $\mathbf{L}$ which either extend the valuations from S, or satisfy

$$\max_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n-1}} |a_{ij}|_v > 1.$$

As follows from (∗),

$$(\Sigma(y) \subseteq \Sigma(x)) \Longrightarrow ((C, y) \text{ is a UEP} \Rightarrow (C, x) \text{ is a UEP})\,.$$

In particular,

$$(\Sigma(y) = \Sigma(x)) \Longrightarrow ((C, y) \text{ is a UEP} \Leftrightarrow (C, x) \text{ is a UEP}).$$

This gives rise to the following definition. Let Σ be a non-empty finite subset of $C(\bar{\mathbf{Q}})$. We say that (C, Σ) *is a* UEP if (C, x) is a UEP for all x with $\Sigma(x) = \Sigma$, or, equivalently, for at least one x with $\Sigma(x) = \Sigma$.

The classical results mentioned above can be easily formulated in terms of UEP. For example, (C, Σ) is a UEP if $\mathbf{g}(C) = 0$ and $|\Sigma| \geq 3$, or $\mathbf{g}(C) = 1$. Further, let C be a non-singular model of the superelliptic curve (I.3), and x the coordinate function. Then (C, x) is a UEP. Finally, let C be a non-singular model of the Thue curve (I.2), and $\Sigma = \Sigma(x) \cup \Sigma(y)$. Then (C, Σ) is a UEP.

Each non-constant $x \in \bar{\mathbf{Q}}(C)$ is considered also as a (ramified) covering

$$x: C \to \mathbf{P}^1.$$

For $\alpha \in \bar{\mathbf{Q}} \cup \{\infty\}$ denote

$$e_\alpha = \text{g.c.d.}\,(e_1, \ldots, e_r), \tag{I.5}$$

where $(e_1, \ldots, e_r)$ are the ramification indices of the points of C lying above α. (With a standard abuse of notations, we identify $\alpha \in \bar{\mathbf{Q}}$ with the point $(1{:}\, \alpha) \in \mathbf{P}^1(\bar{\mathbf{Q}})$, and ∞ with the point $(1{:}\, 0)$.)

The following theorem was originally proved in [Bi1], [Bi2], where it is stated in different terms.

THEOREM A: *Assume that*

$$\sum_{\alpha \in \bar{\mathbf{Q}}} \left(1 - e_\alpha^{-1}\right) > 1. \tag{I.6}$$

Then (C, x) *is a* UEP.

We do not repeat here the proof from [Bi1], [Bi2], but deduce Theorem A from our general Theorem E, formulated below.

The following result, first proved in [Bi2], is a simple consequence of Theorem A.

THEOREM B (effective Siegel's theorem for Galois coverings): *Assume that* $\mathbf{g}(C) \geq 1$ *and* $x: C \to \mathbf{P}^1$ *is a Galois covering. Then* (C, x) *is a* UEP.

Clearly, Theorems A and B cover the case of superelliptic equations. Theorem A also implies the above mentioned results of Kleiman (see Appendix). However, it does not cover Thue equations.

To formulate the main results of this paper we need some additional notations. Consider the group of Σ-units, i.e. functions $z \in \bar{\mathbf{Q}}(C)$ such that $\operatorname{supp} z \subseteq \Sigma$. This group is isomorphic to $\bar{\mathbf{Q}}^* \oplus \mathbf{Z}^\rho$, where $\rho = \rho(\Sigma)$ satisfies $0 \le \rho(\Sigma) \le |\Sigma| - 1$.

THEOREM C: *Assume that* $\rho(\Sigma) \ge 2$. *Then* (C, Σ) *is a* UEP.

As an easy corollary we obtain

THEOREM D: *Assume that* $\mathbf{g}(C) \ge 1$. *Then there exists* $\Sigma \subset C(\bar{\mathbf{Q}})$ *such that*

$$|\Sigma| \le \min\left(2\mathbf{g} - 1,\ 3\left[\frac{\mathbf{g}+1}{2}\right]\right)$$

and (C, Σ) *is a* UEP.

Effective theorems for the Thue equation and curves of genus 0 are particular cases of Theorem C. A natural question arises: is it possible to deduce all known theorems, formulated in terms of UEP, from a single general principle?

An answer to this question is given by the following generalization of Theorem C.

THEOREM E: *Let* $\varphi\colon \tilde{C} \to C$ *be a finite covering of algebraic curves, unramified over* $C \setminus \Sigma$. *Assume that* $\rho\left(\tilde{\Sigma}\right) \ge 2$, *where* $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$. *Then for any* $x \in \bar{\mathbf{Q}}(C)$ *with* $\Sigma(x) = \Sigma$ *and any suitable* $\mathbf{K}$ *and* S *we have*

$$\max_{P \in C(x, \mathbf{K}, S)} h_x(P) \le c\,(C,\, x,\, \mathbf{K},\, S,\, \varphi),$$

c being effective.

As we shall see in Sections 3–6, this theorem yields the classically known facts of universal effectiveness, discussed above, as well as some new results. For example, let X_Γ be the modular curve, corresponding to a finite index subgroup $\Gamma \le \mathrm{SL}_2(\mathbf{Z})$, and $j \in \bar{\mathbf{Q}}(X_\Gamma)$ the j-invariant. We shall see that $(X_\Gamma,\, j)$ is a UEP when Γ satisfies rather general conditions. Another application is to curves of genus 2. Using an idea of Y. Ihara [Ih], we construct an infinite subset $M \subseteq C(\bar{\mathbf{Q}})$ with the following property: *if* $|\Sigma \cap M| \ge 2$, *then* (C, Σ) *is a* UEP.

The plan of the paper is as follows. In Section 1 we prove Theorem C, and in Section 2 we prove Theorems D and E. In Section 3 we show that Theorem E implies the classical cases of UEP. In Section 4 we prove Theorems A and B. In Section 5 we consider modular curves, and in Section 6, curves of genus 2.

Remark 1: P. Vojta [V] applies a similar approach to the study of integral points on varieties of arbitrary dimension. He proves that under some conditions, similar to our condition $\rho(\Sigma) \geq 2$, the set of integral points is not dense in the Zariski topology. However, Vojta reduces the problem to the non-effective Roth–Schmidt theorem and therefore his results are also non-effective. See also a recent paper of F. Beukers [Be].

Remark 2: We do not obtain here any quantitative results. Quantitative versions of the results of this paper can be found in the author's thesis [Bi3].

ACKNOWLEDGEMENT: The late V. G. Sprindžuk was the initiator of this research. D. Berend read the first version of the paper and made a lot of useful comments. I had valuable discussions with D. Bertrand, Q. Liu, R. Livne and M. Matignon. Correspondence with Y. Ihara led to the result of Section 6. I would like to thank all of them.

1. Linear forms in logarithms and proof of Theorem C

All known results on the universal effectiveness are based on Baker's theory of linear forms in logarithms, and Theorem C is not an exception.

The main result of the theory of linear forms in logarithms, having applications in Diophantine equations, is the following:

Let $\alpha_1, \ldots, \alpha_n \in \bar{\mathbf{Q}}$, v be a valuation of the field $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ and $\varepsilon > 0$. If for some $b_1, \ldots, b_n \in \mathbf{Z}$

$$0 < \left|\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} - 1\right|_v < \exp(-\varepsilon B), \tag{1.1}$$

where $B = \max(|b_1|, \ldots, |b_n|)$, then $B \leq c(\alpha_1, \ldots, \alpha_n,\ v,\ \varepsilon)$, c being effective.

Following the first results of Baker [Ba1] (for Archimedean v), considerable advance was made in estimating c. The best results known to the author may be found in [BaW] for Archimedean v and in [Yu] for non-Archimedean v. However, as we do not obtain in this paper any quantitative results, it will be sufficient for our purposes to know only that, if (1.1) is true, then B is effectively bounded.

Now begin the proof of Theorem C. For any $P \in \Sigma$

$$\rho(\Sigma \setminus \{P\}) \geq 1. \tag{1.2}$$

Let $J = J(C)$ be the Jacobian of C. Consider the canonical embedding $C \to J$. We may assume that the origin of the addition law on J belongs to $\Sigma \setminus \{P\}$. In view of (1.2), the points of $\Sigma \setminus \{P\}$ satisfy at least one non-trivial linear relation on J. Then [M, Theorem A] shows that there exists such a relation with effectively bounded coefficients, or equivalently, there exists a non-trivial $(\Sigma \setminus \{P\})$-unit such that the orders of its poles and zeros are effectively bounded. (This implies, by the way, that the assumption $\rho(\Sigma) \geq 2$ can be effectively verified.) This enables constructing such a unit effectively, using for this purpose the constructive versions of Riemann-Roch theorem from [C] or [Sc1]. Denote this unit by z_P. As $z_P(P) \neq 0$, we may assume $z_P(P) = 1$.

Let $x \in \bar{\mathbf{Q}}(C)$ satisfy $\Sigma(x^{-1}) = \Sigma$. To prove the theorem it is sufficient to show that (C, x^{-1}) is a UEP. Choose $y \in \bar{\mathbf{Q}}(C)$ such that $\bar{\mathbf{Q}}(C) = \bar{\mathbf{Q}}(x, y)$. Then for any $P \in \Sigma$ we have Puiseux expansion for y of the form $\sum_{i=m_P}^{\infty} y_{iP} x^{i/e_P}$, where $e_P = \mathrm{ord}_P(x)$, $m_P = \mathrm{ord}_P(y)$, and all the coefficients y_{iP} $(i \geq m_P, P \in \Sigma)$ belong to an effectively constructible algebraic number field.

Fix now $\mathbf{K}$ and S. Replacing $\mathbf{K}$ by its effectively constructible finite extension, we may assume that y and all z_P belong to $\mathbf{K}(C)$. Adding to S finitely many valuations, we may assume that all z_P and z_P^{-1} are integral over the ring $\mathcal{R}_S[x^{-1}]$, where $\mathcal{R}_S$ is the ring of S-integers of the field $\mathbf{K}$. Then for any $P \in \Sigma$ and $Q \in C(x^{-1}, \mathbf{K}, S)$, the number $z_P(Q)$ is an S-unit of the field $\mathbf{K}$.

By $c_1, c_2, \ldots$ we denote effectively computable values. Take an arbitrary $Q \in C(x^{-1}, \mathbf{K}, S)$. Then either $Q \in \Sigma(x) \cup \Sigma(y)$, in which case $h_x(Q) \leq c_1$, or for some valuation $v \in S$

$$|x(Q)|_v \leq \exp\left(-\frac{1}{s} h_x(Q)\right),$$

where $s = \mathrm{card}\, S$. For this v either $|x(Q)|_v \geq c_2$ (and thus $h_x(Q) \leq c_3$), or for all $P \in \Sigma$ the series $\sum_{i=m_P}^{\infty} y_{iP}(x(Q))^{i/e_P}$ converge in v-metric (we fix a prolongation of v on $\bar{\mathbf{Q}}$). In the last case for some P and for some choice of the value of $(x(Q))^{1/e_P}$ the corresponding sum will be equal to $y(Q)$. Fix this v, this P and this choice of $(x(Q))^{1/e_P}$ up to the end of the argument.

We have $z_P = R(x, y)$, where $R \in \mathbf{K}(x, y)$ is rational in x and polynomial in y. Substituting $y = \sum_{i=m_P}^{\infty} y_{iP} x^{i/e_P}$, we obtain the Puiseux expansion of $z = z_P$ at P. By the definition of z_P, the expansion is of the form $\sum_{i=0}^{\infty} z_i x^{i/e_P}$, where $z_0 = z_P(P) = 1$. Again, $h_x(Q) \leq c_4$ or the series $\sum_{i=0}^{\infty} z_i (x(Q))^{i/e_P}$ converges in v-metric. In the last case, for the fixed choice of the value of $(x(Q))^{1/e_P}$, the sum is $z(Q)$. This implies that

$$|z(Q)-1|_v \le c_5|x(Q)|_v^{1/e_P} \le \exp\left(-c_6 h_x(Q)\right).$$

As we have seen above, $z(Q)$ is an S-unit and thus

$$z(Q) = \omega\alpha_1^{b_1}\cdot\ldots\cdot\alpha_t^{b_t},$$

where $t = s-1$, ω is a root of unity, $b_i \in \mathbf{Z}$ and $\alpha_1,\ldots,\alpha_t$ is a basis of the group of S-units of $\mathbf{K}$.

A simple calculation shows that

$$B = \max|b_i| \le c_8 h_z(Q)$$

and on the other side $h_z(Q) \le c_9 B$. By the quazi-equivalence of heights we have

$$h_x(Q) \le c_{10}h_z(Q) + c_{11},$$
$$h_z(Q) \le c_{12}h_x(Q) + c_{13}.$$

Now either $z(Q) = 1$ and thus $h_x(Q) \le c_{14}$, or

$$0 < \left|\omega\alpha_1^{b_1}\cdot\ldots\cdot\alpha_t^{b_t} - 1\right|_v \le c_{15}\exp\left(-c_{16}B\right).$$

By the theory of linear forms in logarithms $B \le c_{17}$, whence $h_x(Q) \le c_{18}$, i.e. the heights of the points from $C(x^{-1}, \mathbf{K}, S)$ are bounded by an effectively computable value. This proves the theorem. ∎

2. Proof of Theorems D and E

We start from Theorem D. Let P be a Weierstrass point of the curve C. Then $\dim\mathcal{L}(g\,P) \ge 2$, i.e. there exists a non-constant $z \in \mathcal{L}(g\,P)$. Since $\mathbf{g}(C) > 0$, the covering $z\colon C \to \mathbf{P}^1$ is ramified over at least three points of $\mathbf{P}^1$. One of them is ∞, let $\alpha_1, \alpha_2 \in \bar{\mathbf{Q}}$ be two more. Put $z_i = (z-\alpha_i)^{-1}$. Then $|\Sigma(z_i)| \le \mathbf{g}-1$. Clearly, z_1 and z_2 are multiplicatively independent mod$\bar{\mathbf{Q}}^*$. For $\Sigma = \Sigma(z_1)\cup\Sigma(z_2)\cup\{P\}$ we have $|\Sigma| \le (2\mathbf{g}-1)$ and $\rho(\Sigma) \ge 2$.

Further, as proved in [KlL], there always exist an effective divisor D with

$$\deg D \le \left[\frac{\mathbf{g}+1}{2}\right] + 1 \quad \text{and} \quad \dim\mathcal{L}(D) \ge 2.$$

Let z be a non-constant element of $\mathcal{L}(D)$. Again, the covering $z\colon C \to \mathbf{P}^1$ is ramified over at least three distinct points α_1, α_2, $\alpha \in \bar{\mathbf{Q}} \cup \{\infty\}$. Put

$$z_i = \frac{z-\alpha}{z-\alpha_i} \quad \text{if } \alpha_1, \alpha_2, \alpha \in \bar{\mathbf{Q}} \quad \text{and} \quad z_i = \frac{1}{z-\alpha_i} \quad \text{if } \alpha = \infty.$$

In the both cases

$$|\Sigma(z_i)| \le \left[\frac{\mathbf{g}+1}{2}\right] \quad \text{and} \quad |\Sigma(z_1^{-1}) \cup \Sigma(z_2^{-1})| \le \left[\frac{\mathbf{g}+1}{2}\right].$$

For

$$\Sigma = \Sigma(z_1) \cup \Sigma(z_2) \cup \Sigma(z_1^{-1}) \cup \Sigma(z_2^{-1})$$

we have

$$|\Sigma| \le 3\left[\frac{\mathbf{g}+1}{2}\right] \quad \text{and} \quad \rho(\Sigma) \ge 2.$$

The proof of Theorem D is complete. ∎

Theorem E follows immediately from Theorem C and the following

Proposition 2.1: *Let $\varphi\colon \tilde{C} \to C$ be a finite covering of algebraic curves, unramified over $C \setminus \Sigma$. Then for any $x \in \bar{\mathbf{Q}}(C)$ and for any suitable $\mathbf{K}$ and S there exist an effectively constructible field $\tilde{\mathbf{K}}$ and a finite set $\tilde{S}$ of valuations of $\tilde{\mathbf{K}}$ such that*

$$\varphi^{-1}\left(C(x, \mathbf{K}, S)\right) \subseteq \tilde{C}\left(\tilde{x}, \tilde{\mathbf{K}}, \tilde{S}\right).$$

Here $\tilde{x} = x \circ \varphi$.

This proposition is the one-dimensional case of the well-known *Chevalley–Weil Theorem*. A very explicite version of Proposition 2.1 is proved in [Bi3, Ch.4]. The case of arbitrary dimension is treated in [V, Th.1.4.11]. ∎

3. Classical cases

In this section we shall see that Theorems C and E easily imply the classical cases of UEP, mentioned in the introduction. To distinguish between independent variables and the corresponding coordinate functions, we denote the former with the capital letters X, Y, Z,... and the latter with the corresponding small letters.

Example 3.1: Curves of genus 0. In this case $\rho(\Sigma) = |\Sigma| - 1$, therefore (C, Σ) is an UEP provided $|\Sigma| \geq 3$. On the other hand, it is well-known that, if $|\Sigma(x)| \leq 2$, then there always exist suitable $\mathbf{K}$ and S such that $C(x, \mathbf{K}, S)$ is infinite. Thus, we get the following statement, already mentioned in the introduction:

$$\text{if } \mathbf{g}(C) = 0, \text{ then } ((C, \Sigma) \text{ is a UEP}) \Longleftrightarrow (|\Sigma| \geq 3).$$

Explicit bounds for integral points on curves of genus 0 can be found in [Po] and [Bi3, Ch.5].

Example 3.2: Curves of genus 1. Let now C be an elliptic curve. Without loss of generality, the origin of the group law on C belongs to Σ. Following [L2, section 3.6], consider an isogeny φ: $\tilde{C} \to C$ of degree at least 3. For example, put $\tilde{C} = C$ and let φ be the multiplication by 2. Then $\mathrm{Ker}\varphi \subset C_{\mathrm{tor}}$, therefore $\rho(\mathrm{Ker}\varphi) = \deg\varphi - 1 \geq 2$, and, since $\tilde{\Sigma} = \varphi^{-1}(\Sigma) \supseteq \mathrm{Ker}\varphi$, we have $\rho\left(\tilde{\Sigma}\right) \geq 2$. From Theorem E we conclude that (C, Σ) *is a* UEP *for any non-empty* Σ.

Unfortunately, this approach does not work if $\mathbf{g} > 1$. Suppose in this case that C is embedded into its Jacobian $J(C)$. Consider an isogeny φ: $A \to J(C)$, where A is an abelian variety over $\bar{\mathbf{Q}}$. Then $\mathrm{Ker}\varphi \subset A_{\mathrm{tor}}$, but, in general, $\mathrm{Ker}\varphi \not\subset J(\tilde{C})_{\mathrm{tor}}$, where $\tilde{C} = \varphi^{-1}(C)$.

A very sharp explicit bound for integral points on curves of genus 1 was recently obtained by W. Schmidt [Sc2]. See also [KT] and [Bi3, Ch.5].

Example 3.3: Thue equation. We shall prove that Theorem C implies an effective bound for the S-integral solutions of a generalization of Thue equation.

Let

$$f(X, Y) = f_1(X, Y) \prod_{i=1}^{3} (\alpha_i X + \beta_i Y + \gamma_i) - A, \tag{3.1}$$

where $f_1(X, Y) \in \bar{\mathbf{Q}}(X, Y)$ is an arbitrary non-zero polynomial, and

$$A \cdot \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{vmatrix} \cdot \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_3 & \beta_3 \end{vmatrix} \cdot \begin{vmatrix} \alpha_2 & \beta_2 \\ \alpha_3 & \beta_3 \end{vmatrix} \neq 0. \tag{3.2}$$

Fix an algebraic number field $\mathbf{K}$ and a finite set of its valuations $S \supseteq S_\infty$, and prove that S-integral solutions of the equation $f(x, y) = 0$ are effectively bounded.

Let

$$f(X, Y) = g_1(X, Y) \cdots g_k(X, Y)$$

be the irreducible decomposition of $f(X,Y)$ over $\bar{\mathbf{Q}}$. We should prove that for any g_i the S-integral solutions of $g_i(X,Y)=0$ are effectively bounded. So, let $g(X,Y)$ be one of the polynomials $g_1,\dots,g_k$, and C a non-singular projective model of the plane curve $g(X,Y)=0$. Denote $\Sigma=\Sigma(x)\cup\Sigma(y)$. It is sufficient to prove that (C,Σ) is a UEP. Clearly, $z_i=\alpha_i x+\beta_i y+\gamma_i$ are Σ-units. We shall prove that z_1 and z_2 are multiplicatively independent mod $\bar{\mathbf{Q}}^*$ and hence $\rho(\Sigma)\geq 2$.

Indeed, we have $\alpha_3 x+\beta_3 y+\gamma_3=\alpha z_1+\beta z_2+\gamma$, where $\alpha\,\beta\neq 0$ by (3.2). Hence we have $\varphi(z_1,z_2)=0$, where

$$\varphi(Z_1,Z_2)=Z_1Z_2\,(\alpha Z_1+\beta Z_2+\gamma)\,\varphi_1(Z_1,Z_2)-A,$$

for some polynomial $\varphi_1(Z_1,Z_2)$.

Now suppose that z_1, z_2 are multiplicatively dependent. Then $\Phi\,(z_1,z_2)=0$, where $\Phi\,(Z_1,Z_2)$ is a polynomial of one of the types $Z_1^{p_1}Z_2^{p_2}-\mu$ or $Z_1^{p_1}-\mu Z_2^{p_2}$. Here $\mu\in\bar{\mathbf{Q}}^*$ and $(p_1,\,p_2)=1$.

Clearly, $\varphi\,(Z_1,Z_2)$ and $\Phi\,(Z_1,Z_2)$ have a common factor. But $\Phi\,(Z_1,Z_2)$ is irreducible, hence $\Phi|\varphi$. However, if $\Phi=Z_1^{p_1}-\mu Z_2^{p_2}$ and $p_1,\,p_2>0$, then $\Phi(0,0)=0$, and $\varphi(0,0)=-A\neq 0$. If $\Phi=Z_1^{p_1}Z_2^{p_2}-\mu$ and $p_1>0$, then, taking δ_1 satisfying the equation

$$(-1)^{p_2}\,(\alpha\,\delta_1+\gamma)^{p_2}\,\delta_1^{p_1}=\beta^{p_2}\mu,$$

and defining

$$\delta_2=-\beta^{-1}\,(\alpha\,\delta_1+\gamma)\,,$$

we have $\Phi\,(\delta_1,\delta_2)=0$, and $\varphi\,(\delta_1,\delta_2)=-A\neq 0$. In the both cases we get a contradiction. ∎

In particular, we have an effective bound for the S-integral solutions of the equation

$$N_{\mathbf{L}/\mathbf{K}}(X+\beta Y+\gamma)=A,$$

where $\mathbf{L}=\mathbf{K}(\beta)$, $[\mathbf{L}\colon\mathbf{K}]\geq 3$ and $A\in\mathbf{K}\smallsetminus 0$. In the case $S=S_\infty$, such a bound also follows from a theorem of Sprindžuk [Sp, §4.5].

4. Proof of Theorems A and B

We start from Theorem A. We have two possible cases. Either

(i) $e_\alpha \geq 3$, $e_\beta \geq 2$ for distinct $\alpha, \beta \in \bar{\mathbf{Q}}$, or

(ii) $e_{\alpha_1} = e_{\alpha_2} = e_{\alpha_3} = 2$ for pairwise distinct $\alpha_1, \alpha_2, \alpha_3 \in \bar{\mathbf{Q}}$.

In the case (i), put $p = e_\alpha$, $q = e_\beta$ and denote by ε_p, ε_q primitive roots of unity of degrees p and q respectively. Put also

$$\gamma = (\alpha - \beta)^{1/q}, \quad t = (x - \beta)^{1/q},$$
$$u_i = \left(t - \varepsilon_q^i \gamma\right)^{1/p} \quad (0 \leq i \leq q-1).$$

The extension $\bar{\mathbf{Q}}(C)(t, u_0, u_1)/\bar{\mathbf{Q}}(C)$ corresponds to a covering $\varphi\colon \tilde{C} \to C$ unramified over $C \setminus \Sigma$, where $\Sigma = \Sigma(x)$. Functions u_0, u_1 satisfy the equation

$$u_0^p - u_1^p = (\varepsilon_q - 1)\,\gamma.$$

By the method of the previous section we can prove that $z_i = u_0 - \varepsilon_p^i u_i$ $(i = 0, 1)$ are $\tilde{\Sigma}$–units multiplicatively independent mod $\bar{\mathbf{Q}}^*$, where $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$.

In the case (ii) denote $t_i = \sqrt{x - \alpha_i}$ $(i = 1, 2, 3)$, and $z_i = t_i - t_3$ $(i = 1, 2)$. Again, the extension $\bar{\mathbf{Q}}(C)(t_1, t_2, t_3)/\bar{\mathbf{Q}}(C)$ corresponds to a covering $\varphi\colon \tilde{C} \to C$ unramified over $C \setminus \Sigma$, and z_1, z_2 are $\tilde{\Sigma}$–units. If they are multiplicatively dependent then $\Phi(z_1, z_2) = 0$, where $\Phi(Z_1, Z_2)$ is as in the previous section. The functions z_1, z_2 also satisfy $g(z_1, z_2) = 0$, where

$$g(Z_1, Z_2) = Z_1^2 Z_2 - Z_1 Z_2^2 + (\alpha_1 - \alpha_3) Z_2 - (\alpha_2 - \alpha_3) Z_1.$$

If we prove that g is irreducible, we shall obtain $\Phi = \lambda g$ $(\lambda \in \bar{\mathbf{Q}})$, which is a contradiction. Hence z_1, z_2 are multiplicatively independent mod $\bar{\mathbf{Q}}^*$.

To prove that $g(Z_1, Z_2)$ is irreducible consider its discriminant with respect to Z_1:

$$\Delta(Z_2) = Z_2^4 + Z_2^2(-4\alpha_1 + 2\alpha_2 + 2\alpha_3) + (\alpha_2 - \alpha_3)^2.$$

The discriminant of $\Delta(Z_2)$ is

$$4096\,(\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_3 - \alpha_1)^2 \neq 0.$$

Hence $\Delta(Z_2)$ is not a square, and therefore $g(Z_1, Z_2)$ is irreducible.

Thus, in the both cases we constructed a covering satisfying the conditions of Theorem E. The proof is complete. ∎

Theorem B follows easily from Theorem A. Indeed, in the case of Galois covering all ramification indices over a point α are equal to e_α. Hence we may write Hurwitz formula as

$$2\mathbf{g} - 2 + 2n = \sum_{\alpha \in \bar{\mathbf{Q}} \cup \{\infty\}} \frac{n}{e_\alpha} (e_\alpha - 1).$$

Then

$$\sum_{\alpha \in \bar{\mathbf{Q}}} \left(1 - e_\alpha^{-1}\right) = 1 + \frac{2\mathbf{g} - 2}{n} + e_\infty^{-1} > 1,$$

and we may apply Theorem A. ∎

Another proof of Theorem B was proposed by R. Dvornicich and U. Zannier (unpublished).

5. Modular curves

As noted in [KL, Ch.8], the method of Gelfond–Baker can be applied to effective analysis of integral points on modular curves.

Let $\mathbf{H}$ be the upper half-plane and $\bar{\mathbf{H}} = \mathbf{H} \cup \mathbf{Q} \cup \{\infty\}$. Given a finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$, denote by X_Γ a projective embedding of $\Gamma \setminus \bar{\mathbf{H}}$, defined over $\bar{\mathbf{Q}}$ (see [L3, Ch.3] and [L4, Ch.6]). We use the standard notation $\nu_\infty = \nu_\infty(\Gamma)$ for the number of cusps.

PROPOSITION 5.1: *Let Γ satisfy one of the following conditions:*

(a) *Γ is a congruence subgroup and $\nu_\infty(\Gamma) \geq 3$;*

(b) *Γ is torsion-free.*

Then (X_Γ, j) is a UEP, *where $j \in \bar{\mathbf{Q}}(X_\Gamma)$ is the j-invariant.*

Before proving the proposition note that its assumption is satisfied for $\Gamma = \Gamma(N)$ when $N \geq 2$, $\Gamma = \Gamma_1(N)$ $(N \geq 4)$, $\Gamma = \Gamma_0(N)$ (N is not prime). We refer to [Sh] and [O] for the definitions and necessary computations. For $\Gamma(N)$ $(N \geq 7)$ the proposition is proved in [KL, Th.8.1.2]. We can also give an alternative proof for $\Gamma = \Gamma(N)$. Indeed, if $2 \leq N \leq 5$, then $\mathbf{g}(X_\Gamma) = 0$, $\nu_\infty(\Gamma) \geq 3$, and this is the case of Example 3.1. If $N \geq 6$, then $\mathbf{g}(X_\Gamma) \geq 1$, and we can use Theorem B, because $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbf{Z})$.

Proof: (a) Let $\Sigma = \Sigma(j)$ be the set of cusps. Then by the Manin-Drinfeld theorem [L3]

$$\rho(\Sigma) = |\Sigma| - 1 = \nu_\infty(\Gamma) - 1 \geq 2,$$

and we may use Theorem C. ∎

(b) Denote $\Gamma' = \Gamma \cap \Gamma(2)$. Consider the natural correspondence

$$X_\Gamma \xleftarrow{\varphi} X_{\Gamma'} \xrightarrow{\psi} X_{\Gamma(2)}.$$

Denote by Σ' and Σ'' the sets of cusps of $X_{\Gamma'}$ and $X_{\Gamma(2)}$ respectively. Then $\Sigma' = \psi^{-1}(\Sigma'')$, and so $\rho(\Sigma') \geq \rho(\Sigma'') = 2$. But $\Sigma' = \varphi^{-1}(\Sigma)$, and φ is unramified everywhere outside cusps (because Γ is torsion-free), so we may use Theorem E. ∎

Another proof of (b): Since Γ is torsion-free, we have $e_\alpha = 3$ for $\alpha = 0$ and $e_\beta = 2$ for $\beta = 1728$. Therefore the covering $j: X_\Gamma \to \mathbf{P}^1$ satisfies the condition (I.6), and we may apply Theorem A. ∎

6. Curves of genus 2

A. Baker's classical result on effective solution of hyperelliptic equation [Ba4] can be formulated as follows:

Let C be a hyperelliptic curve and Σ an orbit of its canonical involution. Then (C, Σ) is a UEP.

In particular, *if C is hyperelliptic, then (C, Σ) is a* UEP *for infinitely many two-element sets Σ*. The last statement can be strengthened for curves of genus 2. In this case, following an idea of Y. Ihara [I], we construct an infinite set $M \subseteq C(\bar{\mathbf{Q}})$ with the following property: *(C, Σ) is a* UEP *for any two-element subset $\Sigma \subset M$.*

Let C be a curve of genus 2. Then there exists an unramified double covering $\varphi: \tilde{C} \to C$, where $\mathrm{g}(\tilde{C}) = 3$. Let $\varphi_*: \tilde{J} \to J$ be the induced map of Jacobians.

Let E_0 be the zero-component of $\operatorname{Ker} \varphi_*$. Then $\dim E_0 = 1$ and $\operatorname{Ker} \varphi_*/E_0$ is a finite group. Therefore for any component E of $\operatorname{Ker} \varphi_*$ we have $|E \cap \tilde{J}_{\mathrm{tor}}| = \infty$.

Let $\kappa: \tilde{C} \to \tilde{C}$ be the involution of $\tilde{C}$ associated with φ (that is, the unique non-constant map satisfying $\varphi \circ \kappa = \varphi$). Consider the map

$$\psi: \tilde{C} \to \tilde{J}$$
$$P \to \mathrm{Cl}\,(P - \kappa(P)).$$

It is non-constant; indeed, $\psi(P)$ belongs to 2-torsion if and only if P is a Weierstrass point. We have also $\psi(\tilde{C}) \subseteq \operatorname{Ker} \varphi_*$. Hence $\psi(\tilde{C})$ coinsides with a component of $\operatorname{Ker}\varphi_*$; denote it by E. Finally, let

$$\tilde{M} = \psi^{-1}\left(E \cap \tilde{J}_{\mathrm{tor}}\right) \subseteq \tilde{C}(\bar{\mathbf{Q}}),$$
$$M = \varphi(\tilde{M}) \subseteq C(\bar{\mathbf{Q}}).$$

PROPOSITION 6.1: *Let $\Sigma \subset C(\bar{\mathbf{Q}})$ satisfy $|\Sigma \cap M| \geq 2$. Then (C, Σ) is a* UEP.

Proof: Let $P \in M$ and $\varphi^{-1}(P) = \{P_1, P_2\}$. Then $P_1 - P_2 \in \tilde{J}_{\mathrm{tor}}$, hence

$$\rho\left(\varphi^{-1}(P)\right) = 1.$$

Therefore for any $\Sigma \subset C(\bar{\mathbf{Q}})$ we have $\rho\left(\tilde{\Sigma}\right) \geq |\Sigma \cap M|$, where $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$. This completes the proof in view of Theorem E. ∎

Appendix. The results of H. Kleiman

Let G be the monodromy group of the covering $x\colon C \to \mathbf{P}^1$, i.e.

$$G = \operatorname{Gal}\left(\mathcal{K}/\bar{\mathbf{Q}}(x)\right),$$

where $\mathcal{K}$ is the smallest extension of $\bar{\mathbf{Q}}(C)$, normal over $\bar{\mathbf{Q}}(x)$. We use here the standard representations of G by permutations of the set $\{1, \ldots, n\}$, where $n = \deg x$. A permutation σ is **stabilizing** if $\sigma(i) = i$ for some $i \in \{1, \ldots, n\}$.

Denote by $\mathcal{R}$ the integral closure of the ring $\bar{\mathbf{Q}}[x]$ in $\bar{\mathbf{Q}}(C)$. Let $\Delta(x)$ be the discriminant of $\mathcal{R}$ over $\bar{\mathbf{Q}}[x]$. Since $\Delta(x)$ is defined up to a constant multiple, we may assume that its leading coefficient is 1.

Although the following assertion is not stated explicitly in [K], it can be easily deduced from the argument on p. 129 of Kleiman's paper.

PROPOSITION K1: *If*

(i) *all stabilizing permutations of G are even and*

(ii) *$\Delta(x)$ has at least 3 distinct roots of odd order,*

then (C, x) is a UEP.

Kleiman proves also

PROPOSITION K2 ([K, Th.4]): *Let $\mathbf{K}_0$ be the smallest field containing the coefficients of $\Delta(x)$. Assume that G is imprimitive with two sets of* *imprimitivity, and all* $\mathbf{K}_0$*-irreducible factors of* $\Delta(x)$ *are of degree at least 3. Then* (C, x) *is a* UEP.

We shall prove that Propositions K1 and K2 follow from Theorem A.

Proof of Proposition K1: A permutation σ is **of the type** $(e_1, \dots, e_s)$ if it is a product of s commuting cycles $\xi_1, \dots \xi_s$ of lenghts $e_1, \dots, e_s$, respectively. Let now $\alpha \in \mathbf{P}^1$ and $e_1, \dots, e_s$ the ramification indices above α. Then there exists $\sigma = \sigma_\alpha \in G$ of the type $(e_1, \dots, e_s)$ [Che, §41].

The condition (i) implies now that, if σ_α is an odd permutation then all the numbers e_i are even and thus $e_\alpha \geq 2$. (If some e_i is odd, then $\sigma_\alpha^{e_i}$ is an odd permutation, stabilizing the elements of the cycle ξ_i.) The condition (ii) means that for at least three distinct $\alpha \in \bar{\mathbf{Q}}$, the permutation σ_α is odd. Thus

$$\sum_{\alpha \in \bar{\mathbf{Q}}} \left(1 - e_\alpha^{-1}\right) \geq \frac{3}{2},$$

i.e. (I.6) holds. ∎

Proof of Proposition K2: Let I_1 and I_2 be the imprivitivity sets and

$$H = \{\sigma \in G \colon \sigma I_1 = I_1\}.$$

Then $[G\colon H] = 2$, therefore $\left[\mathcal{K}^H \colon \bar{\mathbf{Q}}(x)\right] = 2$. Since H contains all stabilizing permutations from G, $\mathcal{K}^H$ is a subfield of $\bar{\mathbf{Q}}(C)$.

There exists at least one $\alpha \in \bar{\mathbf{Q}}$ ramified in $\mathcal{K}^H$. This implies that $2 \mid e_\alpha$. Let $\alpha = \alpha_1, \dots, \alpha_m$ be all conjugates of α over $\mathbf{K}_0$. Then $e_{\alpha_i} = e_\alpha \geq 2$ for $1 \leq i \leq m$. We get

$$\sum_{\alpha \in \bar{\mathbf{Q}}} \left(1 - e_\alpha^{-1}\right) \geq \frac{m}{2} \geq \frac{3}{2},$$

and (I.6) is again satisfied. ∎

References

[Ba1] A. Baker, *Linear forms in the logarithms of algebraic numbers I*, Mathematica **13** (1966), 204–216; II, ibid. **14** (1967), 102–107; III, ibid. **14** (1967); 220–224; IV, ibid. **15** (1968), 204–216.

[Ba2] A. Baker, *Contributions to the theory of Diophantine equations. I, II*, Philosophical Transactions of the Royal Society of London **263** (1967–68), 173–208.

[Ba3] A. Baker, *The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$*, Journal of the London Mathematical Society **43** (1968), 1–9.

[Ba4] A. Baker, *Bounds for the solutions of the hyperelliptic equations*, Proceedings of the Cambridge Philosophical Society **65** (1969), 439–444.

[BaC] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proceedings of the Cambridge Philosophical Society **67** (1970), 592–602.

[BaW] A. Baker and G. Wüstholz, *Logarithmic forms and Group Varieties*, Journal für die Reine und Angewandte Mathematik **442** (1993), 19–62.

[Be] F. Beukers, *Ternary form equations*, preprint No. 771, University of Utrecht, 1993.

[Bi1] Yu. Bilu (Belotserkovski), *Effective analysis of a class of Diophantine equations* (Russian), Vestsi Akademii Navuk BSSR, Ser. Fiz.-Math. Navuk **3** (1988), 111–115.

[Bi2] Yu. Bilu (Belotserkovski), *Effective analysis of a new class of Diophantine equations (Russian)*, Vestsi Akad. Navuk BSSR, Ser. Fiz.-Math. Navuk **6** (1988), 34–39, 125.

[Bi3] Yu. Bilu, *Effective analysis of integral points on algebraic curves*, Thesis, Beer Sheva, 1993.

[C] J. Coates, *Construction of rational functions on a curve*, Proceedings of the Cambridge Philosophical Society **68** (1970), 105–123.

[Ch] W. L. Chow, *The Jacobian variety of an algebraic curve*, American Journal of Mathematics **76** (1954), 453–476.

[Che] N. G. Chebotarev, *The Theory of of Algebraic Functions* (Russian), Moscow–Leningrad, 1948.

[F] G. Faltings, *Eindlichkeitssätze für abelche Varietäten über Zahlkörpern*, Inventiones Mathematicae **3** (1983), 349–366; Erratum: **75** (1984), p. 381.

[G] A. O. Gelfond, *Transcendent and Algebraic Numbers*, (Russian), Moscow 1952; English transl.: New York, Dover, 1960.

[I] Y. Ihara, a letter to the author from 28.09.92.

[K] H. Kleiman, *On the Diophantine equation $f(x, y) = 0$*, Journal für die Reine und Angewandte Mathematik **286/287** (1976), 124–131.

[KlL] S. L. Kleiman and D. Laksov, *Another proof of the existence of special divisors*, Acta Mathematica **132** (1974), 163–176.

[KL] D. Kubert and S. Lang, *Modular Units*, Springer, Berlin, 1981.

[KT] S. V. Kotov and L. A. Trellina, *S-ganze Punkte auf elliptischen Kurven*, Journal für die Reine und Angewandte Mathematik **306** (1979), 28–41.

[L1] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, Berlin, 1983.

[L2] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer, Berlin, 1978.

[L3] S. Lang, *Introduction to Modular Forms*, Springer, Berlin, 1977.

[L4] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.

[M] D. W. Masser, *Linear relations on algebraic groups*, in *New Advances in Transcendence Theory*, Cambridge Univ. Press, 1988, pp. 248–263.

[O] A. P. Ogg, *Modular Forms and Dirichlet Series*, Benjamin, 1969.

[Po] D. Poulakis, *Points entiers sur les courbes de genre 0*, Colloquium Mathematicum **66** (1983), 1–7.

[PW] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*, in *New Advances in Transcendence Theory*, Cambridge Univ. Press, 1988, pp. 280–312.

[S] C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss Akad. Wiss. Phys.-Math. Kl., 1929, Nr. 1.

[Sc1] W. M. Schmidt, *Construction and Estimation of Bases in Function Fields*, Journal of Number Theory **39** (1991), 181–224.

[Sc2] W. M. Schmidt, *Integer points on curves of genus 1*, Compositio Mathematica **81** (1992), 33–59.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Function*, Iwanami Shoten and Princeton Univ. Press, 1971.

[ShT] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge, 1986.

[Sp] V. G. Sprindžuk, *Classical Diophantine Equations in Two Unknowns* (Russian), Nauka, Moscow, 1982; English transl.: Lecture Notes in Math. **1559**, Springer, Berlin, 1994.

[V] P. Vojta, *Diophantine Approximation and Value Distribution Theory*, Lecture Notes in Math. **1239**, Springer, Berlin, 1987.

[Wü] G. Wüstholz, *A new approach to Baker's theorem on linear forms in logarithms III*, in *New Advances in Transcendence Theory*, Cambridge Univ. Press, 1988, pp. 399–410.

[Yu] Kunrui Yu, *Linear forms in p-adic logarithms II*, Compositio Mathematica **74** (1990), 15–113.