Annals of Mathematics **176** (2012), 651–671
http://dx.doi.org/10.4007/annals.2012.176.1.13

An effective result of André-Oort type

By Lars Kühne

Abstract

Using transcendence theory we prove the André-Oort conjecture in case of the Shimura variety $\mathbb{A}^2_{\mathbb{C}}$. It is well known that this result implies the André-Oort conjecture for a product of two arbitrary modular curves. In contrast to all previous proofs we obtain a result that is at once effective and unconditional.

1. Introduction

This article is devoted to a new proof of the André-Oort conjecture for a product of two modular curves. For the specialist, we state the André-Oort conjecture in the most general case without explaining the terminology involved, which is of no further use in this article.

Conjecture. *Let $(G, \mathcal{X})$ be a Shimura datum, K a compact open subgroup of $G(\mathbb{A}_f)$, and $S \subseteq \mathrm{Sh}_K(G, \mathcal{X})(\mathbb{C})$ a set of points of Hodge type. Then every irreducible component of the Zariski closure $\overline{S}^{\mathrm{zar}}$ of S in $\mathrm{Sh}_K(G, \mathcal{X})_{\mathbb{C}}$ is a subvariety of Hodge type.*

Under the Generalized Riemann Hypothesis this conjecture was proved by Edixhoven and Yafaev for certain simple Shimura varieties $\mathrm{Sh}_K(G, \mathcal{X})$ [8], [9], [10], [28] and eventually by Klingler, Ullmo, and Yafaev [18], [26] in general. Edixhoven and Yafaev also proved the above conjecture unconditionally if all points of S are contained in one Hecke orbit [11]. In the case of a product of two modular curves, conditional height bounds for special points on nonspecial subvarieties were explicitly given by Breuer [4]. *Unconditional* proofs of the André-Oort conjecture in special cases were obtained by André[1] [1] using transcendence theory and more recently by Pila [21], [22]. For this, Pila used an improvement of a technique due to Bombieri and himself [3] for bounding

This article was written while holding a grant from the German National Academic Foundation.

[1]For a detailed exposition of André's proof in [1], which also fills in a gap, we refer to a recent book [30] of Zannier.

the number of rational points on the transcendental part of analytic varieties. This improvement, developed jointly by Pila and Wilkie [23], makes essential use of techniques from mathematical logic; in particular, o-minimal structures. It should be mentioned that the proof of the Manin-Mumford conjecture given by Pila and Zannier [24] and a result of Masser and Zannier [20], which both used [23], foreshadowed the proof pinned down in [22]. In all but a few cases, it is not known whether the obtained bounds can be made effective.

In this article we establish the first[2] *unconditional and effective* proof of the André-Oort conjecture for products of two modular curves. Before giving our main results let us mention the problems hindering both André and Pila from obtaining *unconditional* effective results: The proof of André relies on a noneffective theorem of Chowla [5] on the growth of the genus class number of imaginary quadratic fields. Similarly, in order to give suitable lower bounds for the cardinality of Galois orbits of special points, Pila relies on the noneffective theorem of Siegel-Brauer on the growth of the class number of imaginary quadratic fields. For the class number of imaginary quadratic fields, effective lower bounds are known by work of Goldfeld [14], Gross and Zagier [15]. Nevertheless, they are too weak for the model-theoretic approach given by Pila. For the genus class number, which is the number of ideal classes in the principal genus, no effective lower bound is known.

It is well known (cf. Proposition 2.1 of [10]) that the André-Oort conjecture for products of two modular curves is equivalent to the more elementary statement below. We call a point of $\mathbb{A}^2(\mathbb{C})$ a CM-point of discriminant (Δ_1, Δ_2) if both its coordinates are singular moduli associated with complex elliptic curves whose endomorphism rings are of discriminants Δ_1 and Δ_2, respectively. Given a positive integer m, we denote by $\Phi_m(X,Y)$ the m-th modular transformation polynomial and by $\mathcal{V}(\Phi_m)$ its zero set, the m-th modular curve.

THEOREM 1. *Let $\mathcal{C}$ be a geometrically irreducible algebraic curve in the two-dimensional complex affine space $\mathbb{A}^2(\mathbb{C})$. Then, there exist infinitely many* CM*-points on $\mathcal{C}$ if and only if either*

(1) *$\mathcal{C}$ is a horizontal line $\mathbb{A}^1(\mathbb{C}) \times \{j_0\}$, where j_0 is a singular modulus, or*
(2) *$\mathcal{C}$ is a vertical line $\{j_0\} \times \mathbb{A}^1(\mathbb{C})$, where j_0 is a singular modulus, or*
(3) *$\mathcal{C}$ is a modular curve $\mathcal{V}(\Phi_m)$.*

[2]While still writing this article (March 2011), the author got knowledge of the fact that Yuri Bilu, David Masser, and Umberto Zannier obtained simultaneously a similar result. They also proved that no two singular moduli $j(\tau_1)$, $j(\tau_2)$ satisfy $j(\tau_1) + j(\tau_2) = 1$ or $j(\tau_1)j(\tau_2) = 1$. The former result, stated below as Theorem 5, will be contained in another publication of the author, while the latter one will be the subject of a joint publication of Bilu, Masser, and Zannier.

Our main result is an effective version of Theorem 1, which we obtain by using transcendence theory as a major tool. We give it as Theorem 2 and refer to Section 6 for a deduction of Theorem 1 from it. Here, for an algebraic curve $\mathcal{C}$, whose ideal is generated by a polynomial $P \in \bar{\mathbb{Q}}[X_1, X_2]$, we understand by $h(\mathcal{C})$ the projective height of P. It is easy to see that $h(\mathcal{C})$ is well defined this way. See Section 2.2 for details on heights.

THEOREM 2. *For all* $\varepsilon > 0$ *and positive integers* δ *and* D, *there exists an effectively computable constant* $C_1(\varepsilon, \delta, D) > 0$ *with the following property*: *Let* $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ *be a geometrically irreducible algebraic curve defined over a number field* $\mathbb{K}$. *For* $i = 1, 2$, *denote the degree of* $X_i|_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathbb{C}$ *by* δ_i *and assume* $\delta_i > 0$. *Then*,

$$\max\{|\Delta_1|, |\Delta_2|\} < C_1(\varepsilon, \max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}]) \max\{1, h(\mathcal{C})\}^{8+\varepsilon}$$

for every CM-*point of discriminant* (Δ_1, Δ_2) *that is on* $\mathcal{C}$ *but not on any modular curve* $\mathcal{V}(\Phi_m)$, $1 \leq m \leq 4 \max\{\delta_1, \delta_2\}^5$.

We give a short summary of our proof of Theorem 2, which is given in Sections 4 and 5. Consider the toroidal compactification $\mathbb{P}^1(\mathbb{C}) \times \mathbb{P}^1(\mathbb{C})$ of $\mathbb{A}^2(\mathbb{C})$, and denote its cuspidal stratification $\mathbb{A}^1(\mathbb{C}) \times \{\infty\} \cup \{\infty\} \times \mathbb{A}^1(\mathbb{C}) \cup \{\infty\} \times \{\infty\}$ by Y_{cusp}. For all but finitely many CM-points $\underline{x}$, there exists a Galois automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\underline{x}^\sigma$ is contained in a sufficiently small neighborhood of Y_{cusp}. Let $\underline{x}$ be such a CM-point of discriminant (Δ_1, Δ_2) on $\mathcal{C}$. It suffices now to show Theorem 2 for $\underline{x}^\sigma$ on $\mathcal{C}^\sigma$. We have to distinguish two cases. Either $\underline{x}^\sigma$ is close to some point of $\overline{\mathcal{C}}^{\text{zar}}(\bar{\mathbb{Q}}) \cap (\mathbb{A}^1(\mathbb{C}) \times \{\infty\} \cup \{\infty\} \times \mathbb{A}^1(\mathbb{C}))$ or it is close to (∞, ∞). In the first case we construct a linear form Λ in elliptic logarithms, following André [1]. The so-constructed linear form Λ takes a small nonzero absolute value. Then we apply an elliptic transcendence measure originally due to Masser [19] and deduce an upper bound on $|\Delta_1|$ and $|\Delta_2|$ of the sort stated in Theorem 2. Instead of the original result in [19] we use here a more explicit transcendence measure given by David and Hirata-Kohno [7]. If $\underline{x}^\sigma$ is close to $(\infty, \infty) \in Y_{\text{cusp}}$, then we construct a linear form Λ in logarithms of algebraic numbers with algebraic coefficients from the fact that near ∞ the j-function can be well approximated by the first two terms of its q-expansion $e^{-2\pi i\tau} + 744 + e^{2\pi i\tau} P(e^{2\pi i\tau})$, $P \in \mathbb{Z}[[X]]$. In case of $\Lambda = 0$ we deduce by Baker's Theorem a $\mathbb{Q}$-linear dependence relation between the coefficients of Λ, which implies that $\sqrt{\Delta_1/\Delta_2}$ is rational. As can be shown, a CM-point of discriminant (Δ_1, Δ_2) is on a modular curve if and only if $\sqrt{\Delta_1/\Delta_2}$ is rational. This idea makes the use of class field theory as in [1] redundant. It only remains to bound the degree of the modular curve $\mathcal{V}(\Phi_m)$ containing $\underline{x}^\sigma$. Finally, from $\Lambda \neq 0$ we infer again by Baker's Theorem a bound for $|\Delta_1|$ and $|\Delta_2|$. For an overview on different versions of Baker's Theorem, including the state of the art, we refer to Section 2.8 of [2].

A lack of sufficiently good bounds for linear forms in elliptic logarithms leads to the exponent $(8+\varepsilon)$ in Theorem 2. An elliptic analogue of the Lang-Waldschmidt conjecture (Conjecture 1.7 of [7]) would give $(2+\varepsilon)$ instead. In addition, it is noteworthy that we invoke Baker's Theorem for linear forms with (essentially) purely imaginary coefficients. This is in stark contrast to its usual application in solving diophantine equations, where only rational coefficients appear.

Finally, we state three theorems, which are consequences of the results in this article and whose proofs are left to future publication. We note that Theorem 3 reproves a result of Pila in [21], while Theorems 4 and 5 are new to the literature.

THEOREM 3. *With the notations and assumptions of Theorem* 2 *there exists a constant* $C_1'(\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])$ *such that if there exists a* CM-*point of discriminant* (Δ_1,Δ_2) *on* $\mathcal{C}$, *then either*

$$\max\{|\Delta_1|,|\Delta_2|\} < C_1'(\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])$$

or $\mathcal{C}$ *is one of the curves mentioned in Theorem* 1.

THEOREM 4. *There exists an effective constant* $C_2(\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])$ *such that*

$$\max\{|\Delta_1|,|\Delta_2|\} < C_2(\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])$$

for every CM-*point of discriminant* (Δ_1,Δ_2) *on* $\mathcal{C}$ *that is not contained in any modular curve.*

We emphasize that the constant C_2 in Theorem 4 is effectively computable, whereas C_1' in Theorem 3 is not.

THEOREM 5. *There exist no singular moduli* $j(\tau_1)$, $j(\tau_2)$ *such that* $j(\tau_1)+j(\tau_2)=1$.

Acknowledgement. This article owes its genesis to Ph.D. studies of the author under supervision of Gisbert Wüstholz. It is therefore a pleasant obligation for the author to thank him for all discussions and support during the last two years, whose impact on this work cannot be underestimated. He also thanks Philipp Habegger for the same reasons and especially for his many well justified comments on previous versions of this article. Finally, he thanks Umberto Zannier and the anonymous referee for their comments, which helped improving the exposition.

2. Preliminaries

2.1. *Notations.* Throughout this article $\log : \mathbb{C}\backslash(-\infty,0] \longrightarrow \mathbb{C}$ denotes the principal branch of the logarithm with base e. For a nonnegative real number r, we define $\log^+ r = \log\max\{1,r\}$ and $\log\log^+ r = \log^+(\log^+(r))$.

The total degree of a polynomial P in several variables is written $\deg(P)$, while the partial degree of P with respect to a certain indeterminate X is written $\deg_X(P)$.

2.2. *Heights.* For the convenience of the reader, we first recall some well-known facts about heights. We refer to [29] for more details. In this section, $\mathbb{K}$ denotes an arbitrary number field. For a point $p = (p_0 : p_1 : \cdots : p_n)$ of $\mathbb{P}^n(\mathbb{K})$, we define its (absolute logarithmic) Weil height by

$$h(p) = h(p_0 : \cdots : p_n) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\nu} [\mathbb{K}_\nu : \mathbb{Q}_\nu] \log \max\{|p_0|_\nu, |p_1|_\nu, \ldots, |p_n|_\nu\},$$

where ν runs through all archimedean and nonarchimedean places of $\mathbb{K}$. Here, for an archimedean place ν represented by $\sigma : \mathbb{K} \longrightarrow \mathbb{C}$ we set $|\alpha|_\nu = |\sigma(\alpha)|$, and for a nonarchimedean place $\mathfrak{q}$ the value $|\cdot|_\mathfrak{q}$ is normalized such that $|q|_\mathfrak{q} = q^{-1}$ for $(q) = \mathfrak{q} \cap \mathbb{Q}$, $q > 0$. This definition is independent of the chosen number field $\mathbb{K}$ and the chosen representative of p. The (affine absolute logarithmic) Weil height of a point $p = (p_1, \cdots, p_n)$ of $\mathbb{A}^n(\mathbb{K})$ is $h(p) = h(1 : p_1 : \cdots : p_n)$. In particular, for an algebraic number $\alpha \in \bar{\mathbb{Q}}$, we define its Weil height by $h(\alpha) = h(1 : \alpha)$. Now $h(\alpha\beta) \leq h(\alpha) + h(\beta)$ for all $\alpha, \beta \in \bar{\mathbb{Q}}$, and

$$h(\gamma_1 + \cdots + \gamma_n) \leq h(\gamma_1) + \cdots + h(\gamma_n) + \log n$$

for all positive integers n and all $\gamma_1, \ldots, \gamma_n \in \bar{\mathbb{Q}}$. Furthermore, $h(\alpha^\lambda) = |\lambda| h(\alpha)$ for all $\lambda \in \mathbb{Q}$, $\alpha \neq 0$. The height is Galois-invariant, which means that $h(\alpha^\sigma) = h(\alpha)$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. In addition, the inequality of Liouville ([29, Prop. 3.4]) states that for all $\alpha \in \bar{\mathbb{Q}}^\times$ and every place ν of $\mathbb{K}$,

$$-[\mathbb{Q}(\alpha) : \mathbb{Q}] h(\alpha) \leq \log |\alpha|_\nu \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] h(\alpha). \tag{2.1}$$

We define the Weil height $h(P)$ of a nonzero polynomial $P \in \mathbb{K}[X_1, \ldots, X_n]$ as the Weil height of a point in projective space whose homogeneous coordinates are the nonzero coefficients $p_{\underline{i}}$ of P with an arbitrary ordering. Note that $h(P)$ is well defined and $h(P) = h(\alpha P)$ for all $\alpha \in \bar{\mathbb{Q}}^\times$. In particular, this implies for any nonzero coefficient $p_{\underline{k}}$ of P that

$$h(P) = h(p_{\underline{k}}^{-1} P) = \sum_{\nu} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log \max_{\underline{i}} \{|p_{\underline{i}}/p_{\underline{k}}|_\nu\} \geq h(1 : p_{\underline{i}}/p_{\underline{k}}) = h(p_{\underline{i}}/p_{\underline{k}}).$$

Now applying (2.1) to $p_{\underline{i}}/p_{\underline{k}}$, we deduce a variant of Liouville's inequality for polynomials: There exists an algebraic number $\alpha \in \mathbb{K}^\times$, for example $p_{\underline{k}}^{-1}$ as above, such that for every nonzero coefficient $p_{\underline{i}}$ of P and all places ν of $\mathbb{K}$,

$$-[\mathbb{K} : \mathbb{Q}] h(P) \leq \log |p_{\underline{i}}|_\nu + \log |\alpha|_\nu \leq [\mathbb{K} : \mathbb{Q}] h(P). \tag{2.2}$$

Finally, let α be a root of a polynomial $P(X) \in \mathbb{K}[X]$. Then, the height of α is bounded by ([29, Exercise 3.6])

$$h(\alpha) \leq h(P) + \log \deg P. \tag{2.3}$$

2.3. *Complex elliptic curves and singular moduli.* For every point τ in the complex upper halfplane $\mathcal{H}$, we define a complex elliptic curve $\mathcal{E}_\tau$ as the quotient of the complex Lie group $(\mathbb{C},+)$ by its discrete subgroup $(\mathbb{Z}+\mathbb{Z}\tau)$. In addition, $\mathcal{E}_\tau$ is isomorphic to the complex points of a projective algebraic group. For instance, an isomorphism is induced by

$$\exp_{\mathcal{E}_\tau} : \mathbb{C} \longrightarrow \mathbb{P}^2(\mathbb{C}),\ z \longmapsto (1 : \wp_\tau(z) : \wp_\tau'(z)),$$

where $\wp_\tau$ is the Weierstrass $\wp$-function having poles at $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. The complex-analytic morphisms $\mathbb{C}/\Lambda_1 = \mathcal{E}_{\tau_1} \longrightarrow \mathcal{E}_{\tau_2} = \mathbb{C}/\Lambda_2$, $\Lambda_i = \mathbb{Z}+\tau_i\mathbb{Z}$, correspond one-to-one to the complex numbers α satisfying $\alpha\Lambda_1 \subseteq \Lambda_2$. This is why we identify in the sequel the endomorphism ring $\mathrm{End}(\mathcal{E}_\tau)$ with the multiplication ring $\{\alpha \in \mathbb{C} | \alpha\Lambda \subseteq \Lambda\}$ of the lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. Trivially, the integers are elements of the endomorphism ring of any elliptic curve. Furthermore, the following three statements are equivalent ([6], Theorem 10.14):

(1) $\mathrm{End}(\mathcal{E}_\tau) \neq \mathbb{Z}$.
(2) τ generates an imaginary quadratic extension of $\mathbb{Q}$ in $\mathbb{C}$.
(3) $\mathrm{End}(\mathcal{E}_\tau)$ is an order $\mathcal{O}$ in the imaginary quadratic extension $\mathbb{Q}(\tau)$ of $\mathbb{Q}$ in $\mathbb{C}$ and $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ is a proper $\mathcal{O}$-lattice, i.e., $\mathcal{O} = \{\alpha \in \mathbb{C} | \alpha\Lambda \subseteq \Lambda\}$.

If these statements are satisfied, then $\mathcal{E}_\tau$ is said to have complex multiplication by $\mathbb{Q}(\tau)$ or called a CM-elliptic curve for short. In addition, τ is then called a CM-period, $j(\tau)$ a singular modulus, and the discriminant of $\mathrm{End}(\mathcal{E}_\tau)$ is denoted by $\Delta_\tau < 0$. Consider the action of $\Gamma = \mathbf{SL}_2(\mathbb{Z})$ on the complex upper halfplane $\mathcal{H}$ which sends (γ,τ) to $\gamma\tau = \frac{a\tau+b}{c\tau+d}$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$. For every CM-period τ, there exists $\gamma \in \Gamma$ and integers a, b, c such that $\gamma\tau = (-b + i\sqrt{4ac-b^2})/(2a)$, $\gcd(a,b,c) = 1$ and either $-a < b \leq a < c$ or $0 \leq b \leq a = c$. Here, the integers a, b, c are unique and $\Delta_\tau = b^2 - 4ac$. Klein's j-invariant induces a bijection between $\Gamma\backslash\mathcal{H}$ and $\mathbb{C}$. Furthermore, its q-expansion is $j(\tau) = q^{-1} + 744 + 196884q + \cdots$, $q = e^{2\pi i\tau}$. This means that there exists a meromorphic function $J(z)$ on the unit disc $\{z \in \mathbb{C} \mid |z| < 1\}$ such that $j(\tau) = J(e^{2\pi i\tau})$ and $J(z)$ is holomorphic except for a simple pole at $z = 0$. More precisely, it follows from Lemme 1(ii) of [12] that

$$|j(\tau) - \exp(-2\pi i\tau) - 744| < j(i\,\mathrm{Im}(\tau)) - \exp(-2\pi\,\mathrm{Im}(\tau)) - 744 < 449 \tag{2.4}$$

if $\mathrm{Im}(\tau) \geq 1$. A simple consequence is

$$|j(\tau)\exp(2\pi i\tau) - 1| < 1193\exp(-2\pi\,\mathrm{Im}(\tau)) \tag{2.5}$$

for all $\tau \in \mathcal{H}$ such that $\mathrm{Im}(\tau) \geq 1$.

If τ is a CM-period, then $j(\tau)$ is an algebraic integer. We define the so-called class equation as $H_{\mathcal{O}}(X) = \prod_\tau (X - j(\tau))$, where τ runs through a set of Γ-representatives of those $\tau \in \mathcal{H}$ satisfying $\mathrm{End}(\mathcal{E}_\tau) = \mathcal{O}$. It is a $\mathbb{Q}$-irreducible polynomial in $\mathbb{Z}[X,Y]$; cf. Section 13 of [6]. Consequently, $\mathcal{E}_{\tau_1}$ and $\mathcal{E}_{\tau_2}$ have the same endomorphism ring if and only if $j(\tau_1)$ and $j(\tau_2)$ are Galois conjugate.

2.4. *Transcendence measures for logarithms.* For the convenience of the reader, we quote two transcendence measures that we use in Section 5 below. We start with a transcendence measure for $G = \mathbb{G}_a \times \mathcal{E}_\tau$. It is a special case of a result due to David and Hirata-Kohno. Let $\mathcal{E}_\tau$ be an elliptic curve with Weierstrass model $Y^2 = 4X^3 - g_2X - g_3$, where both g_2 and g_3 are contained in a fixed number field $\mathbb{K}$. Note that the map $\exp_{\mathcal{E}_\tau}$ from last subsection has kernel $\mathbb{Z} + \tau\mathbb{Z}$. Let $\underline{u} = (u_0, u_1)$ be a point of $\mathbb{C}^2$ and

$$\underline{\gamma} = \exp_{\mathbb{G}_a \times \mathcal{E}_\tau}(\underline{u}) = (u_0, \exp_{\mathcal{E}_\tau}(u_1)) = (\gamma_0, \gamma_1) \in (\mathbb{G}_a \times \mathcal{E}_\tau)(\mathbb{K}).$$

Denote the canonical Néron-Tate height (cf. Section VIII of [25]) of $\gamma_1 \in \mathcal{E}_\tau(\mathbb{K}) \subset \mathbb{P}^2(\mathbb{K})$ by $\hat{h}(\gamma_1)$. Furthermore, consider a linear form $\mathcal{L} : \mathbb{C}^2 \longrightarrow \mathbb{C}$, $(z_0, z_1) \mapsto \beta_0 z_0 + \beta_1 z_1$, where $\beta_0, \beta_1 \in \mathbb{K}$. Finally, let B and V be positive real numbers satisfying

$$\log B \geq \max\{1, h(\beta_0), h(\beta_1)\}$$

and

$$\log V \geq \max\left\{\hat{h}(\gamma_1), \frac{|u_1|^2}{[\mathbb{K} : \mathbb{Q}]\,\mathrm{Im}(\tau)}\right\}.$$

For readability, we introduce the following stipulation. Given an algebraic subgroup H of $\mathbb{G}_a \times \mathcal{E}_\tau$, the connected component of $\exp^{-1}_{\mathbb{G}_a \times \mathcal{E}_\tau}(H(\mathbb{C}))$ that contains the origin in $\mathbb{C}^2$ is denoted by $\mathfrak{h}(\mathbb{C})$. It is easy to see that $\mathfrak{h}(\mathbb{C})$ is a linear subspace of $\mathbb{C}^2$, which can be interpreted as the tangent space of $H(\mathbb{C})$ at its identity element.

Proposition 1 (Theorem 1.6 of [7] for $k = 1$ and $E = e$). *There exists an effective absolute constant $c_1 > 0$ with the following property: Assume that $\underline{u} \notin \mathfrak{h}(\mathbb{C})$ for any connected algebraic subgroup H of $\mathbb{G}_a \times \mathcal{E}_\tau$ such that $\mathfrak{h}(\mathbb{C}) \subseteq \ker(\mathcal{L})(\mathbb{C})$. Then,*

$$\begin{aligned}\log|\mathcal{L}(\underline{u})| \geq -c_1 &\left(\log B + \max\{1, h(1 : g_2^3 : g_3^2)\} + \log\log^+(V) + \log[\mathbb{K} : \mathbb{Q}] + 1\right) \\ &\times \left(\log\log^+(V) + \max\{1, h(j(\tau))\} + \log[\mathbb{K} : \mathbb{Q}] + 1\right)^2 \\ &\times \left(\frac{[\mathbb{K} : \mathbb{Q}]^2}{\max\{1, h(j(\tau))\}} + [\mathbb{K} : \mathbb{Q}]^4 \log V\right).\end{aligned}$$

Now we recall a transcendence measure of the same sort for $G = \mathbb{G}_m^n$, which is classically known as the Theorem of Baker. We state a variant that was given by Gaudron as a corollary of his quantitative proof of Wüstholz's analytic subgroup theorem [27]. Again, we need to give some notations in advance. By $\exp : \mathbb{C} \longrightarrow \mathbb{G}_m(\mathbb{C}) = \mathbb{C}^\times$ we denote the classical complex exponential map. Let $\underline{u} = (u_1, \dots, u_n)$ be a point of $\mathbb{C}^n$ such that

$$\underline{\gamma} = \exp_{\mathbb{G}_m^n}(\underline{u}) = (\exp(u_1), \dots, \exp(u_n)) \in (\mathbb{G}_m^n)(\mathbb{K}).$$

Additionally, consider a linear form $\mathcal{L} : \mathbb{C}^n \longrightarrow \mathbb{C}$ given by

$$\mathcal{L}(\underline{z}) = \beta_1 z_1 + \cdots + \beta_n z_n,\ \underline{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{K}^n.$$

Finally, set

$$\mathfrak{a} = 1 + [\mathbb{K} : \mathbb{Q}] \log \left(1 + [\mathbb{K} : \mathbb{Q}] + \sum\nolimits_{i=1}^{n} (h(\gamma_i) + e|u_i|)\right),$$

$$V' = (\mathfrak{a} + 1) \times ([\mathbb{K} : \mathbb{Q}] h(1 : \beta_1 : \ldots : \beta_n) + \mathfrak{a}) \\ \times \prod\nolimits_{i=1}^{n} (1 + [\mathbb{K} : \mathbb{Q}] h(\gamma_i) + e|u_i|),$$

and let $\xi_1, \ldots, \xi_{[\mathbb{K}:\mathbb{Q}]}$ be an arbitrary $\mathbb{Q}$-basis of $\mathbb{K}$. For a subgroup H of $\mathbb{G}_m^n$ we define $\mathfrak{h}(\mathbb{C})$ as above, simply replacing $\exp_{\mathbb{G}_a \times \mathcal{E}_\tau}$ by $\exp_{\mathbb{G}_m^n}$.

Proposition 2 (Corollaire 1 of [13] for $E = e$). *For every positive integer n, there exists an effectively computable absolute constant $c_2(n) > 0$ such that the following assertion is true. Assume that $\underline{u} \notin \mathfrak{h}(\mathbb{C})$ for any connected algebraic subgroup H of $\mathbb{G}_m^n$ with $\mathfrak{h}(\mathbb{C}) \subseteq \ker(\mathcal{L})(\mathbb{C})$. Then,*

$$\log |\mathcal{L}(\underline{u})| \geq -c_2(n) \max \left\{V', [\mathbb{K} : \mathbb{Q}] \left(h(\xi_1 : \ldots : \xi_{[\mathbb{K}:\mathbb{Q}]}) + \log[\mathbb{K} : \mathbb{Q}]\right)\right\}.$$

For the later application of Proposition 2, it is useful to know which linear subspaces of $\mathbb{C}^n$ appear as $\mathfrak{h}(\mathbb{C})$ for algebraic subgroups H of $\mathbb{G}_m^n$. We observe that $\mathfrak{h}(\mathbb{C})$ runs through the linear subspaces of $\mathbb{C}^n$ defined by linear equations with rational coefficients when H runs through the algebraic subgroups of $\mathbb{G}_m^n$.

3. An elementary corollary of Puiseux's theorem

A fundamental idea of our proof of Theorem 1 below comes from Puiseux's theorem, which describes an algebraic curve at each of its points as a union of different analytic branches. However, by using rather elementary estimates we do not need to work explicitly with Puiseux series. The next lemma subsumes the facts from the context of Puiseux's theorem needed in our proof of Proposition 3 below. We do not try to obtain optimal bounds here. We assume that the number field $\mathbb{K}$ is embedded in the complex numbers, which allows us to consider the restriction $|\cdot|$ of the complex value to $\mathbb{K}$.

Lemma 1. *Let $P = \sum_{\underline{i}} p_{\underline{i}} \underline{X}^{\underline{i}} \in \mathbb{K}[X_1, X_2]$ be a nonconstant polynomial of bidegree (δ_1, δ_2). Set $\delta = \max\{\delta_1, \delta_2\}$, $D = [\mathbb{K} : \mathbb{Q}]$, $H = \exp(h(P))$ and $U = (\delta + 1)^2 H^{2D}$. Then, there exists a set $\mathcal{S}$ consisting of less than $(\delta + 1)^5$ triples*

$$(\alpha, k_1, k_2) \in \bar{\mathbb{Q}}^\times \times \mathbb{Z} \times \mathbb{Z},\ k_1 k_2 < 0,\ |k_1|, |k_2|, [\mathbb{K}(\alpha) : \mathbb{K}] \leq \delta,\ h(\alpha) \leq \delta \log(\delta H)$$

such that the following assertion is true. For every point $\underline{x} = (x_1, x_2) \in \mathbb{C}$ with $P(x_1, x_2) = 0$ and

$$0 < |x_1|, |x_2| < (\delta + 1)^{-6\delta^2} H^{-6D\delta^2} = U^{-3\delta^2}, \tag{3.1}$$

there exists some $(\alpha, k_1, k_2) \in \mathcal{S}$ *satisfying*

$$|x_1^{k_1} x_2^{k_2} - \alpha| < 2^\delta \delta U^3 \max\{|x_1|, |x_2|\}^{\delta^{-2}}.$$

Note that we do not assume that P has a zero at $(0,0)$.

Proof of Lemma 1. After multiplication of P with a scalar we may assume by (2.2) that

$$H^{-D} = \exp(-[\mathbb{K}:\mathbb{Q}]h(P)) \le |p_{\underline{i}}| \le \exp([\mathbb{K}:\mathbb{Q}]h(P)) = H^D. \tag{3.2}$$

Occasionally, we use this estimate in the sequel without further mention. For all $\underline{m} \neq \underline{n}$ with $p_{\underline{m}} \neq 0$, define

$$\mathcal{M}_{\underline{m},\underline{n}} = \left\{ \underline{z} \in \mathbb{C}^2 \Big| \max_{\underline{i} \neq \underline{m},\underline{n}} |p_{\underline{i}} \underline{z}^{\underline{i}}| \le |p_{\underline{n}} \underline{z}^{\underline{n}}| \le |p_{\underline{m}} \underline{z}^{\underline{m}}| \right\}.$$

The union of all sets $\mathcal{M}_{\underline{m},\underline{n}}$ is $\mathbb{A}^2(\mathbb{C})$. Therefore, $\underline{x} = (x_1, x_2)$ is contained in some $\mathcal{M}_{\underline{m},\underline{n}} \cap \mathcal{V}(P)$, $p_{\underline{m}} \neq 0$, $\underline{m} \neq \underline{n}$, and hence

$$|p_{\underline{n}} \underline{x}^{\underline{n}}| \le |p_{\underline{m}} \underline{x}^{\underline{m}}| \le (\delta_1 + 1)(\delta_2 + 1)|p_{\underline{n}} \underline{x}^{\underline{n}}| \le (\delta+1)^2 |p_{\underline{n}} \underline{x}^{\underline{n}}|.$$

Write $\underline{k} = \underline{m} - \underline{n} \neq \underline{0}$ and note that $|k_i| \le \delta$. Since $|x_1|, |x_2| \neq 0$ also $p_{\underline{n}} \neq 0$ and

$$U^{-1} = (\delta+1)^{-2} H^{-2D} \le |\underline{x}^{\underline{k}}| \le (\delta+1)^2 H^{2D} = U. \tag{3.3}$$

If both k_1 and k_2 are nonnegative or nonpositive, (3.1) implies, respectively, $|\underline{x}^{\underline{k}}| < U^{-3\delta^2}$ or $|\underline{x}^{\underline{k}}| > U^{3\delta^2}$. Since this contradicts (3.3) we conclude that k_1 and k_2 must be of opposite sign, i.e., $k_1 k_2 < 0$. By symmetry in x_1 and x_2 we may and do assume $k_1 > 0$. Now choose complex numbers t, u satisfying $x_1 = t^{-k_2} u^{1/k_1}$ and $x_2 = t^{k_1}$. The geometric idea behind this choice of coordinates is that of blowing up a possible singularity of $\mathcal{V}(P)$ at the origin; cf. Section 1.4 of [17]. With respect to this context, u is associated with the slopes of lines through the origin. Indeed, our choice of u implies $\underline{x}^{\underline{k}} = u$. In addition, from (3.1) we infer

$$|t| = |x_2|^{1/k_1} < U^{-3\delta^2/k_1} \le U^{-3\delta} < 1. \tag{3.4}$$

Furthermore, $0 = P(x_1, x_2) = P(t^{-k_2} u^{1/k_1}, t^{k_1}) = \sum_{\underline{i}} p_{\underline{i}} t^{-i_1 k_2 + i_2 k_1} u^{i_1/k_1}$. Multiplying by $t^{-\rho} \neq 0$, $\rho = \min_{p_{\underline{i}} \neq 0}\{-i_1 k_2 + i_2 k_1\}$, and grouping monomials yields

$$A(u^{1/k_1}) + tB(u^{1/k_1}, t) = 0,$$

where $0 \neq A \in \mathbb{K}[S]$ and $B \in \mathbb{K}[S,T]$ are polynomials such that

$$\max\{\deg_S A, \deg_S B\} \le \delta \text{ and } \max\{h(A), h(B)\} \le h(P).$$

The absolute value of $B(u^{1/k_1}, t)$ is bounded above by

$$(\delta+1)^2 H^D \max\{1, |u|^{1/k_1}\}^{\deg_S B} \max\{1, |t|\}^{\deg_T B} \le U^{\delta+1} H^{-D} \tag{3.5}$$

since $|t| < 1$ and $|u| = |\underline{x}^{\underline{k}}| \leq U$ by (3.3). Combining with (3.4) gives

$$|A(u^{1/k_1})| = |tB(u^{1/k_1}, t)| \leq U^{-2\delta+1}H^{-D} < H^{-D}, \tag{3.6}$$

and hence A cannot be a constant polynomial by (3.2). Thus, there exists a nontrivial factorization

$$A(S) = \textstyle\sum_{i=0}^{\deg_S A} a_i S^i = a_{\deg_S A}(S - \alpha_1) \cdots (S - \alpha_{\deg_S A}),$$

where α_i, $1 \leq i \leq \deg_S A$, is a complex algebraic number such that $[\mathbb{K}(\alpha_i) : \mathbb{K}] \leq \delta$. Note that a_i, $i = 0, \dots, \deg_S A$, is an element of $\mathbb{K}$ satisfying $|a_i| \geq H^{-D}$. In addition, (2.3) implies that

$$h(\alpha_i) \leq h(A) + \log \deg_S A \leq \log(\delta H).$$

There exists some $i \in \{1, \dots, \deg_S A\}$ such that

$$|u^{1/k_1} - \alpha_i|^{\deg_S A} \leq |a_{\deg_S A}^{-1} A(u^{1/k_1})| < U^{-2\delta+1} < 1, \tag{3.7}$$

where $|a_{\deg_S A}| \geq H^{-D}$ and (3.6) imply the second inequality. Taking the δ-th root and using both $\deg_S A \leq \delta$ and the bound (3.5) for $|B(u^{1/k_1}, t)|$, one obtains

$$|u^{1/k_1} - \alpha_i| \leq |a_{\deg_S A}^{-1} tB(u^{1/k_1}, t)|^{\delta^{-1}} < U^{1+\delta^{-1}} |t|^{\delta^{-1}} \leq U^2 |t|^{\delta^{-1}}. \tag{3.8}$$

If α_i is zero, then $U^{-1} \leq |u|^{1/k_1} < U^2 |t|^{\delta^{-1}}$ by (3.3). Using (3.1), we infer from this the contradiction $U^{-3} < |t|^{\delta^{-1}} = |x_2|^{\delta^{-1}/k_1} < U^{-3}$. Therefore, α_i must not be zero. Note that $[\mathbb{K}(\alpha_i^{k_1}) : \mathbb{K}] \leq \delta$ and $h(\alpha_i^{k_1}) = k_1 h(\alpha_i) \leq \delta \log(\delta H)$. From $\underline{x}^{\underline{k}} = u$, we infer

$$|x_1^{k_1} x_2^{k_2} - \alpha_i^{k_1}| = |u^{(k_1-1)/k_1} + u^{(k_1-2)/k_1}\alpha_i + \cdots + \alpha_i^{k_1-1}||u^{1/k_1} - \alpha_i|.$$

The first factor on the right-hand side is bounded from above by

$$k_1 \max\{1, |u|^{1/k_1}, |\alpha_i|\}^{k_1-1} \leq k_1(|u|^{1/k_1} + 1)^{k_1} \leq 2^{k_1} k_1 \max\{1, |u|\} \leq 2^\delta \delta U,$$

where we used (3.7) in the first and (3.3) in the third inequality. The second factor $|u^{1/k_1} - \alpha_i|$ is bounded from above by (3.8). Using $|t| < 1$, $x_2 = t^{k_1}$ and $0 < k_1 \leq \delta$, we deduce $|u^{1/k_1} - \alpha_i| < U^2 |x_2|^{\delta^{-2}}$ from this. A combination of these bounds yields

$$|x_1^{k_1} x_2^{k_2} - \alpha_i^{k_1}| < 2^\delta \delta U^3 |x_2|^{\delta^{-2}}.$$

So the theorem is true if $(\alpha_i^{k_1}, k_1, k_2)$ belongs to $\mathcal{S}$. Finally, we need to bound the number of triples $(\alpha, k_1, k_2) \in \mathcal{S}$ that have to be contained in $\mathcal{S}$ for this purpose. This number can be bounded from above by the number of nonempty sets $\mathcal{M}_{\underline{m},\underline{n}}$ times the maximal degree of all $A \in \mathbb{K}[S]$ arising as above. Thus, $\mathcal{S}$ can be easily chosen to contain less than $(\delta + 1)^5$ triples. □

4. **Proof of Theorem 2**

Let $P = \sum_{\underline{i}} p_{\underline{i}} \underline{X}^{\underline{i}} \in \mathbb{K}[X_1, X_2]$ be a generating polynomial of the ideal of $\mathcal{C}$. Since the degree of $X_i|_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathbb{C}$ is $\delta_i > 0$ the polynomial P is of bidegree (δ_1, δ_2) with respect to X_1 and X_2. As in the proof of Lemma 1 we may assume by (2.2) that

$$\exp(-[\mathbb{K} : \mathbb{Q}]h(P)) \le |p_{\underline{i}}| \le \exp([\mathbb{K} : \mathbb{Q}]h(P)).$$

We use this fact without explicit mention in the following.

We establish some notational conventions on the constants in this article. By $c_1, c_2, \ldots$ we denote absolute constants that depend neither on the curve $\mathcal{C}$ nor on the polynomial P. Furthermore, we set $\delta = \max\{\delta_1, \delta_2\}$, $D = [\mathbb{K} : \mathbb{Q}]$, $H = \exp(h(P))$ and $U = (\delta + 1)^2 H^{2D}$. Then $C_1(\delta, D), C_2(\delta, D), \ldots$ denote constants that depend effectively on δ and D but are independent of H. For readability we usually write C_i instead of $C_i(\delta, D)$. *All constants are positive and do not depend on* ε *unless explicitly mentioned otherwise.*

We prove Theorem 2 by use of the following proposition. Since we want to complete the proof of Theorem 2 first its proof is postponed until the next section.

PROPOSITION 3. *There exists a constant* $C_3(\delta, D) > 0$ *such that the following is true. If* $\underline{x} \in \mathcal{C}$ *is a* CM*-point of discriminant* (Δ_1, Δ_2), *then*

$$\max\{|\Delta_1|(\log|\Delta_1|)^{-2}, |\Delta_2|(\log|\Delta_2|)^{-2}\} \le C_3(\delta, D) \max\{1, \log H\}^8 \tag{4.1}$$

or there exists some $1 \le m \le 4\delta^5$ *for which* $\underline{x} \in \mathcal{V}(\Phi_m)$.

Assume that $\underline{x} \in \mathcal{C}$ is a CM-point of discriminant (Δ_1, Δ_2) as given in the statement of Theorem 2, and use the proposition above. If there exists some $1 \le m \le 4\delta^5$ such that $\underline{x} \in \mathcal{V}(\Phi_m)$, there is nothing left to prove. Assume that the inequality (4.1) is true. Then, there exists some $C_1(\varepsilon, \delta, D) > 0$ such that

$$\max\{|\Delta_1|, |\Delta_2|\} < C_1(\varepsilon, \delta, D) \max\{1, \log H\}^{8+\varepsilon}.$$

5. **Proof of Proposition 3**

Let $\underline{x} = (x_1, x_2) \in \mathcal{C}$ be a CM-point of discriminant (Δ_1, Δ_2). Since the modular transformation polynomials $\Phi_m(X_1, X_2)$, $m > 1$, are symmetric in both variables and $\Phi_1(X_1, X_2) = X_1 - X_2$ we may assume without loss of generality that $|\Delta_1| = \max\{|\Delta_1|, |\Delta_2|\}$. The discriminant of the imaginary quadratic order $\mathcal{O}$ generated by 1 and $(\Delta_1 + i\sqrt{|\Delta_1|})/2$ is Δ_1. Thus, the elliptic curves with j-invariants x_1 and $j((\Delta_1 + i\sqrt{|\Delta_1|})/2)$ both have endomorphism ring $\mathcal{O}$. From the irreducibility of the class equation $H_{\mathcal{O}}(X)$ it follows that there exists some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that

$$x_1^\sigma = j\left(\frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2}\right).$$

Now $\underline{x}^\sigma = (x_1^\sigma, x_2^\sigma)$ is a CM-point of discriminant (Δ_1, Δ_2) on the curve $\mathcal{C}^\sigma$ given by $P^\sigma \in \mathbb{K}^\sigma[X_1, X_2]$. If Proposition 3 is true for $\underline{x}^\sigma$ and $\mathcal{C}^\sigma$, it is also true for $\underline{x}$ and $\mathcal{C}$ because all Φ_m have rational coefficients. Thus, by replacing $\underline{x}$ with $\underline{x}^\sigma$ and $\mathcal{C}$ with $\mathcal{C}^\sigma$ we may assume that $x_1 = j((\Delta_1 + i\sqrt{|\Delta_1|})/2)$ without any loss of generality. Additionally, there exist integers a, b, c such that $(a, b, c) = 1$ and either $-a < b \leq a < c$ or $0 \leq b \leq a = c$ and

$$x_2 = j\left(\frac{-b + i\sqrt{|\Delta_2|}}{2a}\right), \; |\Delta_2| = 4ac - b^2.$$

Finally, we may also assume that $|\Delta_1| \geq 7$ and, therefore, by (2.4) that

$$|x_1| \geq \exp(\pi\sqrt{|\Delta_1|}) - 1193 > \exp(\frac{\pi}{2}\sqrt{|\Delta_1|}) > 1. \tag{5.1}$$

We use the following lemma to distinguish quantitatively the case that $\underline{x}$ is close to $(\infty, \infty) \in Y_{\mathrm{cusp}}$ from the case that $\underline{x}$ is close to some point of $\overline{\mathcal{C}}^{\mathrm{zar}}(\bar{\mathbb{Q}}) \cap (Y_{\mathrm{cusp}} \setminus \{(\infty, \infty)\})$.

Lemma 2. *If $\underline{x} \in \mathcal{C}$ satisfies $|x_1| > U^2 = (\delta + 1)^4 H^{4D}$, then $|x_2| > |x_1|^{(2\delta)^{-1}}$ or there exists some $(\infty, \beta) \in \overline{\mathcal{C}}^{\mathrm{zar}}(\bar{\mathbb{Q}}) \cap (Y_{\mathrm{cusp}} \setminus \{(\infty, \infty)\})$ such that $|x_2 - \beta| \leq U^{\delta^{-1}} |x_1|^{-(2\delta)^{-1}}$, where β is an algebraic number such that $h(\beta) \leq \log(\delta H)$ and $[\mathbb{K}(\beta) : \mathbb{K}] \leq \delta$.*

Proof. Since $x_1 \neq 0$ we can write

$$0 = x_1^{-\deg_{X_1} P} P(x_1, x_2) = Q(x_2) + x_1^{-1} R(x_1^{-1}, x_2),$$

where $0 \neq Q \in \mathbb{K}[X_2]$ and $R \in \mathbb{K}[X_1, X_2]$ with $\deg_{X_i} Q, \deg_{X_i} R \leq \delta$, $i = 1, 2$, and $\max\{h(Q), h(R)\} \leq h(P)$. Note that $|R(x_1^{-1}, x_2)|$ is bounded from above by

$$(\delta + 1)^2 H^D \max\{1, |x_1^{-1}|\}^{\deg_{X_1} R} \max\{1, |x_2|\}^{\deg_{X_2} R} \leq U H^{-D} \max\{1, |x_2|^\delta\}.$$

Assume that $|x_2| \leq |x_1|^{(2\delta)^{-1}}$. This implies $|Q(x_2)| = |x_1^{-1} R(x_1^{-1}, x_2)| \leq U H^{-D} |x_1|^{-1/2} < H^{-D}$. We deduce that Q cannot be a constant polynomial. Therefore, there exists a decomposition $Q(X_2) = q_{\deg_{X_2} Q} \prod_{1 \leq i \leq \deg_{X_2} Q} (X_2 - \beta_i)$. Obviously, $[\mathbb{K}(\beta_i) : \mathbb{K}] \leq \delta$ and $h(\beta_i) \leq \log(\delta H)$ by (2.3). Additionally, there exists some $1 \leq i \leq \deg_{X_2} Q$ such that

$$|x_2 - \beta_i| \leq |q_{\deg_{X_2} Q}^{-1} Q(x_2)|^{(\deg_{X_2} Q)^{-1}} \leq (U|x_1|^{-1/2})^{\delta^{-1}} \leq U^{\delta^{-1}} |x_1|^{-(2\delta)^{-1}}. \quad \square$$

By choosing $C_3(\delta, D) > 0$ sufficiently large we may assume

$$|\Delta_1| > 16\pi^{-2} (\log U)^2 = 64\pi^{-2} (\log(\delta + 1) + D \log H)^2.$$

By (5.1) this implies

$$|x_1| > \exp\left(\frac{\pi}{2}\sqrt{|\Delta_1|}\right) \geq U^2$$

and Lemma 2 is applicable. We deduce that

$$|x_2| > |x_1|^{(2\delta)^{-1}} \tag{5.2}$$

or there exists some $\beta \in \bar{\mathbb{Q}}$ such that $h(\beta) \leq \log(\delta H)$, $[\mathbb{K}(\beta) : \mathbb{K}] \leq \delta$ and

$$|x_2 - \beta| \leq U^{\delta^{-1}} \exp\left(-\frac{\pi}{4\delta}\sqrt{|\Delta_1|}\right) = C_4(\delta) H^{2\delta^{-1}D} \exp(-C_5(\delta)\sqrt{|\Delta_1|}). \tag{5.3}$$

Lemmas 3 and 4 below deal with the case of (5.3).

LEMMA 3. *Let* $x_2 \in \{0, 1728, \beta\}$, *where* $h(\beta) \leq \log(\delta H)$ *and* $[\mathbb{K}(\beta) : \mathbb{K}] \leq \delta$. *Then*,

$$|\Delta_1| \leq C_6(\delta, D) \max\{1, \log H\}^2$$

if $C_6(\delta, D) > 0$ *is sufficiently large.*

Proof. This is an easy exercise in standard height estimations. □

LEMMA 4. *Assume* $x_2 \notin \{0, 1728, \beta\}$ *and* (5.3) *for some* $\beta \in \bar{\mathbb{Q}}$ *such that* $h(\beta) \leq \log(\delta H)$ *and* $[\mathbb{K}(\beta) : \mathbb{K}] \leq \delta$. *If* $C_6(\delta, D) > 0$ *is sufficiently large*, *then* $|\Delta_1| \leq C_6(\delta, D) \max\{1, \log H\}^2$ *or*

$$|\Delta_1|(\log|\Delta_1|)^{-2} \leq C_3(\delta, D) \max\{1, \log H\}^8. \tag{5.4}$$

Proof. Here and in the following, we write $\zeta_6 = \exp(\pi i/3)$. From

$$h((-b + i\sqrt{4ac - b^2})/(2a)) = \log(c)/2 < \log(|\Delta_2|)/2$$

and (2.1) we obtain

$$\min_{z \in \{i, \zeta_6, \zeta_6^2\}} \left\{ \frac{-b + i\sqrt{|\Delta_2|}}{2a} - z \right\} > \exp(-2\log|\Delta_2| - 4\log 2) \geq \frac{|\Delta_1|^{-2}}{16}.$$

Note that $(-b + i\sqrt{|\Delta_2|})/(2a)$ is located in the standard fundamental domain $\mathcal{F}$ consisting of all $\tau \in \mathcal{H}$ such that either $|\tau| > 1$ and $-1/2 \leq \operatorname{Re}\tau < 1/2$ or $|\tau| = 1$ and $-1/2 \leq \operatorname{Re}\tau \leq 0$. The derivative j' has simple zeros at γi, $\gamma \in \Gamma$, double zeros at $\gamma\zeta_6$, $\gamma \in \Gamma$, and is nonzero elsewhere. Therefore, there exists an absolute constant $c_3 > 0$ such that

$$\min_{j_0 \in \{0, 1728\}} \{|x_2 - j_0|\} > c_3|\Delta_1|^{-6}.$$

Set $\varphi : [0, 1] \longrightarrow \mathbb{A}^1(\mathbb{C})$, $\varphi(t) = (1 - t)x_2 + t\beta$. For all $t \in [0, 1]$ and $j_0 \in \{0, 1728\}$,

$$|\varphi(t) - j_0| \geq |x_2 - j_0| - |\varphi(t) - x_2| \geq |x_2 - j_0| - |x_2 - \beta|. \tag{5.5}$$

If $c_3|\Delta_1|^{-6} < 2C_4 H^{2\delta^{-1}D} \exp(-C_5\sqrt{|\Delta_1|})$, then

$$\log(c_3) - 6\log|\Delta_1| < \log(2C_4) + 2\delta^{-1}D\log H - C_5\sqrt{|\Delta_1|}.$$

For $C_6(\delta, D) > 0$ sufficiently large, this implies $|\Delta_1| \leq C_6(\delta, D)\max\{1, \log H\}^2$. Therefore, we may assume $c_3|\Delta_1|^{-6} \geq 2C_4H^{2\delta^{-1}D}\exp(-C_5\sqrt{|\Delta_1|})$ in the sequel. Inserting (5.3) in (5.5), we obtain

$$|\varphi(t) - j_0| > c_3|\Delta_1|^{-6} - C_4H^{2\delta^{-1}D}\exp(-C_5\sqrt{|\Delta_1|}) \geq \frac{c_3}{2}|\Delta_1|^{-6} \tag{5.6}$$

for $j_0 \in \{0, 1728\}$ and all $t \in [0,1]$. Consider the ramified covering $j : \mathcal{H} \longrightarrow \mathbb{A}^1(\mathbb{C})$. The covering is ramified above $j(\zeta_6) = j(\zeta_6^2) = 0$ and $j(i) = 1728$. By (5.6), $\operatorname{im}(\varphi)$ contains neither 0 nor 1728. Thus, there exists a unique smooth lifting $\tilde{\varphi} : [0,1] \longrightarrow \mathcal{H}$ of φ satisfying $\tilde{\varphi}(0) = (-b + i\sqrt{|\Delta_2|})/(2a)$. Deriving $j \circ \tilde{\varphi} = \varphi$ we obtain $j'(\tilde{\varphi}(t))\tilde{\varphi}'(t) = \varphi'(t)$ for all $t \in [0,1]$. Since $\gamma i, \gamma\zeta_6 \notin \operatorname{im}(\tilde{\varphi})$ for all $\gamma \in \Gamma$, we conclude that

$$\max_{t\in[0,1]}\{|\tilde{\varphi}'(t)|\} \leq \max_{\tau\in\operatorname{im}(\tilde{\varphi})}\{|j'(\tau)|^{-1}\}\,|x_2 - \beta|\,.$$

If β is not real, the absolute value of its imaginary part is bounded from below by (2.1). In fact, $|\operatorname{Im}(\beta)| = \left|\frac{\beta-\bar{\beta}}{2}\right| \geq \exp(-2\delta^2D^2(\log(\delta H) + \log(2)))$. We may assume that

$$C_4(\delta)H^{2\delta^{-1}D}\exp(-C_5(\delta)\sqrt{|\Delta_1|}) < \exp(-2\delta^2D^2(\log(\delta H) + \log(2))).$$

Indeed, the converse inequality implies $|\Delta_1| \leq C_6(\delta, D)\max\{1, \log H\}^2$ for suitably large $C_6(\delta, D) > 0$. We infer

$$|x_2 - \beta| \leq C_4(\delta)H^{2\delta^{-1}D}\exp(-C_5(\delta)\sqrt{|\Delta_1|}) < |\operatorname{Im}(\beta)|,$$

and hence $\operatorname{im}(\varphi)$ does not contain real numbers. Since j is real-valued on the boundary $\partial\mathcal{F}$ of $\mathcal{F}$, $\operatorname{im}(\tilde{\varphi})$ must be contained in $\mathcal{F}$. Assume now that β is real. If additionally x_2 is real, then $\operatorname{im}(\varphi) \subseteq \mathbb{R}\backslash\{0, 1728\}$, and hence $\operatorname{im}(\tilde{\varphi})$ is in $\mathcal{F}$. Finally, if β is real and x_2 is not, $\operatorname{im}(\varphi|_{[0,1)})$ contains no real numbers. Hence, $\operatorname{im}(\tilde{\varphi})$ contains no points on $\partial\mathcal{F}$ except maybe $\tilde{\varphi}(1) = \tau_0$. Since $\tilde{\varphi}(0) \in \mathcal{F}$ this implies $\operatorname{im}(\tilde{\varphi}) \subseteq \mathcal{F} \cup \partial\mathcal{F}$. The only zeros of j' on $\mathcal{F} \cup \partial\mathcal{F}$ are located at i, ζ_6, and ζ_6^2. Furthermore, $|j'(\tau)| \to \infty$ for $\tau \to \infty$. This implies

$$\max_{\tau\in\operatorname{im}(\tilde{\varphi})}\{|j'(\tau)|^{-1}\} \leq c_4 \min_{t\in[0,1]}\left\{|\varphi(t)|^{-2/3}, |\varphi(t) - 1728|^{-1/2}\right\} < c_5|\Delta_1|^4$$

with absolute constants $c_4, c_5 > 0$. In conclusion,

$$\left|\frac{-b + i\sqrt{|\Delta_2|}}{2a} - \tau_0\right| \leq \max_{t\in[0,1]}|\tilde{\varphi}'(t)| < c_5C_4H^{2\delta^{-1}D}|\Delta_1|^4\exp(-C_5\sqrt{|\Delta_1|}). \tag{5.7}$$

Note that since $|\operatorname{Re}(\tau_0)| \leq 1/2$,

$$\max\{1, \operatorname{Im}(\tau_0)\} \geq \frac{2}{\sqrt{5}}|\tau_0|. \tag{5.8}$$

If $\mathrm{Im}(\tau_0) \geq 2$, then by (2.4),

$$|\beta| = |j(\tau_0)| \geq \exp(2\pi \,\mathrm{Im}(\tau_0)) - 1193 > \exp(\pi \max\{1, \mathrm{Im}(\tau_0)\}) > \exp(|\tau_0|).$$

Since $|\beta| \leq (\delta H)^{\delta D}$ by (2.1) this implies $|\tau_0| < \delta D \log(\delta H)$. In case of $\mathrm{Im}(\tau_0) < 2$, we obtain $|\tau_0| < \sqrt{5}$ from (5.8). Thus, in general,

$$|\tau_0| < \max\{\sqrt{5}, \delta D \log(\delta H)\}. \tag{5.9}$$

Consider the elliptic curve $\mathcal{E}_{\tau_0}$ having j-invariant $\beta \in \bar{\mathbb{Q}}$. Note that $\mathcal{E}_{\tau_0}$ is defined over $\mathbb{Q}(\beta)$ as a projective variety. By Lemma 3.1 of [16] there exists an absolute constant $c_6 > 0$ such that there exist algebraic numbers $g_2, g_3 \in \mathbb{Q}(\beta)$ satisfying $\max\{h(g_2), h(g_3)\} < c_6 \max\{1, h(\beta)\} \leq c_6 \max\{1, \log(\delta H)\}$ and giving a Weierstrass model $Y^2 = 4X^3 - g_2 X - g_3$ of $\mathcal{E}_{\tau_0}$. We now use Proposition 1 for $\mathbb{G}_a \times \mathcal{E}_{\tau_0}$. Define the linear form

$$\mathcal{L}(X_1, X_2) = \frac{-b + i\sqrt{|\Delta_2|}}{2a} X_1 - X_2 \in \mathbb{Q}(i\sqrt{|\Delta_2|})[X_1, X_2],$$

and set $\underline{u} = (1, \tau_0)$, $\underline{\gamma} = \exp_{\mathbb{G}_a \times \mathcal{E}_{\tau_0}}(\underline{u})$ and $\Lambda = \mathcal{L}(\underline{u})$. From the fact that τ_0 is a period of $\mathcal{E}_{\tau_0}$ we deduce $\underline{\gamma} = (1, 0_{\mathcal{E}_{\tau_0}}) \in (\mathbb{G}_a \times \mathcal{E}_{\tau_0})(\mathbb{Q}(\beta))$. In these terms (5.7) states that

$$|\Lambda| < c_5 C_4(\delta) H^{2\delta^{-1} D} |\Delta_1|^4 \exp(-C_5(\delta)\sqrt{|\Delta_1|}). \tag{5.10}$$

Furthermore, $\beta \neq x_2$ implies $\Lambda \neq 0$, and hence $\underline{u} \notin \ker(\mathcal{L})(\mathbb{C})$. Thus, $\underline{u} \notin \mathfrak{h}(\mathbb{C})$ for any connected algebraic subgroup H of $\mathbb{G}_a \times \mathcal{E}_{\tau_0}$ with $\mathfrak{h}(\mathbb{C}) \subseteq \ker(\mathcal{L})(\mathbb{C})$. Hence, the condition of Proposition 1 is satisfied. It remains to choose the constants B and V from Section 2.4. It is easy to see that $B = |\Delta_1|$ satisfies the restriction on B stated there. In order to choose V note that $\hat{h}(\gamma_1) = \hat{h}(0_{\mathcal{E}_{\tau_0}}) = 0$. Additionally, from (5.8) and (5.9) we infer that there exists a constant $c_7 > 0$ such that

$$\frac{|\tau_0|^2}{[\mathbb{Q}(\beta, \Delta_2) : \mathbb{Q}]\,\mathrm{Im}(\tau_0)} \leq \frac{|\tau_0|^2}{\mathrm{Im}(\tau_0)} < c_7 \delta D \log(\delta H).$$

Thus, we may choose $V = \exp(c_7 \delta D \log(\delta H))$. Now Proposition 1 yields a constant $C_7(\delta, D) > 0$ such that

$$\log|\Lambda| \geq -C_7(\delta, D) \max\{1, \log H\}^4 \log|\Delta_1|.$$

Combining this with (5.10), we obtain

$$|\Delta_1| \leq C_3(\delta, D) \max\{1, \log H\}^8 (\log|\Delta_1|)^2$$

for some sufficiently large $C_3(\delta, D) > 0$. □

By Lemmas 3 and 4 it remains to deal with the case (5.2). We may assume

$$\Delta_1 > (12\delta^3 \pi^{-1} \log U)^2 = 576 \delta^6 \pi^{-2} (\log(\delta + 1) + D \log H))^2.$$

Indeed, this is no loss of generality if $C_3(\delta, D) > 0$ is sufficiently large. Then, $|x_1| > \exp(\frac{\pi}{2}\sqrt{|\Delta_1|}) > U^{6\delta^3}$ by (5.1) and hence $|x_2| > |x_1|^{(2\delta)^{-1}} > U^{3\delta^2}$ by (5.2). Since $\max\{|x_1^{-1}|, |x_2^{-1}|\} < U^{-3\delta^2}$ we can apply Lemma 1 for the polynomial $X_1^{\deg_{X_1} P} X_2^{\deg_{X_2} P} P(X_1^{-1}, X_2^{-1})$ of height $h(P)$ and bidegree (δ_1, δ_2). It implies that

$$|x_1^{k_1} x_2^{k_2} - \alpha| < 2^\delta \delta U^3 \max\{|x_1^{-1}|, |x_2^{-1}|\}^{\delta^{-2}} < 2^\delta \delta U^3 |x_1|^{-\delta^{-3}/2} < 2^\delta \delta \tag{5.11}$$

for some triple $(\alpha, k_1, k_2) \in \bar{\mathbb{Q}}^\times \times \mathbb{Z} \times \mathbb{Z}$ satisfying $k_1 k_2 < 0, |k_1|, |k_2|, [\mathbb{K}(\alpha) : \mathbb{K}] \leq \delta$ and $h(\alpha) \leq \delta \log(\delta H)$.

Set

$$(q_1, q_2) = \left(\exp\left(2\pi i \frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2}\right), \exp\left(2\pi i \frac{-b + i\sqrt{|\Delta_2|}}{2a}\right)\right).$$

We now want to estimate the value of $q_1^{-k_1} q_2^{-k_2} - x_1^{k_1} x_2^{k_2}$ from above. First, note that it equals

$$x_1^{k_1} x_2^{k_2} \left[x_1^{-k_1} q_1^{-k_1} (x_2^{-k_2} q_2^{-k_2} - 1) + (x_1^{-k_1} q_1^{-k_1} - 1) \right]. \tag{5.12}$$

Here, the first factor is bounded by

$$|x_1^{k_1} x_2^{k_2}| \leq |\alpha| + |x_1^{k_1} x_2^{k_2} - \alpha| \leq (\delta H)^{\delta^2 D} + 2^\delta \delta \leq 3(\delta H)^{\delta^2 D}.$$

For the second factor, recall that (2.5)[3] states

$$|x_i q_i - 1| < 1193 \exp(-\pi\sqrt{|\Delta_i|}) \leq 1193 \exp(-\pi\sqrt{|\Delta_1|}),$$

which implies $|x_i q_i| < 1194$. Since we assume $|\Delta_1| \geq 7$ another consequence is

$$|x_i q_i| > 1 - 1193 \exp(-\pi\sqrt{|\Delta_1|}) > \frac{1}{4}.$$

Furthermore, we obtain also

$$|x_i^{-1} q_i^{-1} - 1| = |x_i^{-1} q_i^{-1}||x_i q_i - 1| < 4772 \exp(-\pi\sqrt{|\Delta_1|}).$$

From this we infer that there exists a constant $c_8 > 0$ such that for all integers $k > 0$,

$$\begin{aligned} |x_i^{-k} q_i^{-k} - 1| &= |x_i^{-1} q_i^{-1} - 1||x_i^{-k+1} q_i^{-k+1} + \cdots + 1| \\ &< c_8^{|k|} \exp(-\pi\sqrt{|\Delta_1|}). \end{aligned}$$

[3]We remind the reader that (2.5) is valid only under the condition $\mathrm{Im}(\tau) \geq 1$, which for $i = 2$ (resp. $i = 1$) means that $\sqrt{|\Delta_2|}/(2a) \geq 1$ (resp. $\sqrt{|\Delta_1|}/2 \geq 1$). However, by choosing the constant $C_3(\delta, D)$ large enough, $|x_2| > |x_1|^{(2\delta)^{-1}}$ in combination with (2.4) shows that we may assume that the former inequality is true. (The latter one is trivially true by our assumption $\Delta_1 \geq 7$.)

Similarly, $|x_i^k q_i^k - 1| = |x_i q_i - 1||x_i^{k-1}q_i^{k-1} + \cdots + 1| < c_8^{|k|}\exp(-\pi\sqrt{|\Delta_1|})$ for all $k > 0$ after some augmentation of c_8. Using these estimates, the second factor in (5.12) can be bounded from above by

$$|x_1q_1|^{-k_1}|x_2^{-k_2}q_2^{-k_2} - 1| + |x_1^{-k_1}q_1^{-k_1} - 1| < c_9^\delta \exp(-\pi\sqrt{|\Delta_1|})$$

for some absolute constant $c_9 > 0$. Thus, there exists a constant $C_8(\delta, D) > 0$ such that

$$|q_1^{-k_1}q_2^{-k_2} - x_1^{k_1}x_2^{k_2}| < 3c_9^\delta(\delta H^2)^{\delta^2 D}\exp(-\pi\sqrt{|\Delta_1|}) = C_8 H^{2\delta^2 D}\exp(-\pi\sqrt{|\Delta_1|}).$$

Together with (5.1) and (5.11), this implies

$$\begin{aligned}|q_1^{-k_1}q_2^{-k_2} - \alpha| &< C_8 H^{2\delta^2 D}\exp(-\pi\sqrt{|\Delta_1|}) + 2^\delta \delta U^3 \exp(-\frac{\pi}{4\delta^3}\sqrt{|\Delta_1|}) \\ &\le C_9 H^{6\delta^2 D}\exp(-\frac{\pi}{4\delta^3}\sqrt{|\Delta_1|})\end{aligned}$$

for some constant $C_9(\delta, D) > 0$. There exists $a' \in \{-a+1, \ldots, a\}$ such that $k_1\Delta_1 - k_2\frac{b}{a} \equiv \frac{a'}{a} \pmod{2\mathbb{Z}}$. Furthermore, there exists $u_1 \in \mathbb{C}$ such that $\exp(u_1) = \alpha$, $|u_1| \le \log|\alpha| + \pi$ and $-\pi < \mathrm{Im}(u_1) \le \pi$. Now $|-\frac{a'}{a}\pi - \mathrm{Im}(u_1)| < 2\pi$ and there exists some $n \in \{-1, 0, 1\}$ such that $|-(\frac{a'}{a} + 2n)\pi - \mathrm{Im}(u_1)| \le \pi$. We apply Proposition 2 for $\mathbb{G}_m^2$. For this, set $\mathbb{K}' = \mathbb{Q}(i\sqrt{|\Delta_1|}, i\sqrt{|\Delta_2|}, \alpha)$ and choose a basis $\xi_1, \ldots, \xi_{[\mathbb{K}':\mathbb{Q}]}$ of $\mathbb{K}'$ such that $h(\xi_1 : \ldots : \xi_{[\mathbb{K}':\mathbb{Q}]}) \le C_{10} h(i\sqrt{|\Delta_1|} : i\sqrt{|\Delta_2|} : \alpha)$ for some constant $C_{10}(\delta, D) > 0$. Define the linear form

$$\mathcal{L}(X_1, X_2) = \left(\frac{a'}{a} + 2n + ik_1\sqrt{|\Delta_1|} + i\frac{k_2}{a}\sqrt{|\Delta_2|}\right)X_1 - X_2 \in \mathbb{K}'[X_1, X_2],$$

and set $\underline{u} = (-\pi i, u_1)$, $\underline{\gamma} = \exp_{\mathbb{G}_m^2}(\underline{u})$, and $\Lambda = \mathcal{L}(\underline{u})$. The choice of $\underline{u}$ implies both $\underline{\gamma} = (-1, \alpha) \in \mathbb{G}_m^2(\mathbb{K}')$ and

$$\Lambda = \left(\frac{a'}{a} + 2n + ik_1\sqrt{|\Delta_1|} + i\frac{k_2}{a}\sqrt{|\Delta_2|}\right)(-\pi i) - u_1.$$

Note that $|\mathrm{Im}(\Lambda)| = |-(\frac{a'}{a} + 2n)\pi - \mathrm{Im}(u_1)| \le \pi$. We deduce that

$$\alpha(\exp(\Lambda) - 1) = \exp\left(-\pi i\cdot\left(k_1\Delta_1 - k_2\frac{b}{a}\right) + \pi\cdot\left(k_1\sqrt{\Delta_1} + \frac{k_2}{a}\sqrt{\Delta_2}\right)\right) - \alpha.$$

Since $|\alpha|^{-1} \le (\delta H)^{\delta^2 D}$ by Liouville's inequality (2.1) this implies

$$|\exp(\Lambda) - 1| < C_{11} H^{7\delta^2 D}\exp\left(-\frac{\pi}{4\delta^3}\sqrt{|\Delta_1|}\right),$$

where $C_{11} = \delta^{\delta^2 D} C_9 > 0$. By choosing $C_3(\delta, D) > 0$ large enough we can enforce that the quantity on the right-hand side of the inequality is less than 1/2. Since $|\log z| \le 2|z-1|$ if $|z-1| \le 1/2$ we deduce

$$|\Lambda| \le 2C_{11} H^{7\delta^2 D}\exp\left(-\frac{\pi}{4\delta^3}\sqrt{|\Delta_1|}\right).$$

The following two lemmas deal separately with the cases $\Lambda = 0$ and $\Lambda \neq 0$ and complete our proof of Proposition 3. Note that Lemma 6 implies inequality (4.1) in fact with some exponent $2+\varepsilon'$, $\varepsilon' > 0$, of $\log H$.

LEMMA 5. *If $\Lambda = 0$, then $\underline{x} = (x_1, x_2)$ lies on a modular curve $\mathcal{V}(\Phi_m)$, $1 \leq m \leq 4\delta^5$.*

LEMMA 6. *For every $\varepsilon' > 0$, there exists a constant $C_{12}(\delta, D, \varepsilon') > 0$ such that if $\Lambda \neq 0$, then*

$$|\Delta_1|(\log|\Delta_1|)^{-2} \leq C_{12}(\delta, D, \varepsilon') \max\{1, \log H\}^{2+\varepsilon'}.$$

Proof of Lemma 5. If $\mathcal{L}(\underline{u}) = 0$, then Proposition 2 implies that there exists an algebraic subgroup H of $\mathbb{G}_m^2$ such that $\underline{u} \in \mathfrak{h}(\mathbb{C}) \subseteq \ker(\mathcal{L})(\mathbb{C})$. Since $\underline{u} \neq 0$ the coefficients of $\mathcal{L}(X_1, X_2)$ must be $\mathbb{Q}$-linearly dependent. This implies $\sqrt{\Delta_1/\Delta_2} = -k_2/(k_1 a)$ and hence also

$$1 \leq a = -\frac{k_2\sqrt{|\Delta_2|}}{k_1\sqrt{|\Delta_1|}} \leq -\frac{k_2}{k_1} \leq \delta.$$

Now, $\sqrt{\Delta_2/\Delta_1}$ is a rational number with numerator and denominator bounded by δ^2 and δ, respectively. Denote its denominator by d. Since

$$x_2 = \frac{-b + i\sqrt{|\Delta_2|}}{2a} = \begin{pmatrix} 2d\sqrt{\frac{\Delta_2}{\Delta_1}} & +d\sqrt{\Delta_1\Delta_2} - bd \\ 0 & 2ad \end{pmatrix} \frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2}$$

the point $\underline{x} = (x_1, x_2)$ lies on a modular curve $\mathcal{V}(\Phi_m)$, where

$$m \leq 4ad^2\sqrt{\frac{\Delta_2}{\Delta_1}} \leq 4\delta^5. \qquad \square$$

Proof of Lemma 6. If $\mathcal{L}(\underline{u}) \neq 0$, then Proposition 2 implies

$$\log|\mathcal{L}(\underline{u})| \geq -c_2(n) \max\left\{V', [\mathbb{K}' : \mathbb{Q}](h(\xi_1 : \ldots : \xi_{[\mathbb{K}':\mathbb{Q}]}) + \log[\mathbb{K}' : \mathbb{Q}])\right\}$$

with V' as defined in Section 2.4. Recall that

$$h(\xi_1 : \ldots : \xi_{[\mathbb{K}':\mathbb{Q}]}) \leq C_{10} h(i\sqrt{|\Delta_1|} : i\sqrt{|\Delta_2|} : \alpha),$$

and hence there exists a constant $C_{13}(\delta, D) > 0$ such that

$$h(\xi_1 : \ldots : \xi_{[\mathbb{K}':\mathbb{Q}]}) \leq C_{13}(\delta, D) \max\{1, \log H\} \log|\Delta_1|.$$

There exists a constant $C_{14}(\delta, D) > 0$ such that

$$\mathfrak{a} \leq C_{14}(\delta, D) \max\{1, \log\log^+ H\}.$$

Furthermore, there exists a constant $C_{15}(\delta, D, \varepsilon') > 0$ satisfying

$$V' \leq C_{15}(\delta, D, \varepsilon') \max\{1, \log H\}^{1+\varepsilon'/2} \log|\Delta_1|.$$

Therefore,

$$\sqrt{|\Delta_1|} \leq C_{16}(\delta, D, \varepsilon') \max\{1, \log H\}^{1+\varepsilon'/2} \log |\Delta_1|$$

for some constant $C_{16}(\delta, D, \varepsilon') > 0$, and the lemma follows. □

6. Proof of Theorem 1

It is easy to see that all curves of the types listed in Theorem 1 contain infinitely many CM-points. We show the converse by using Theorem 2. Assume that $\mathcal{C}$ is a geometrically irreducible algebraic curve of $\mathbb{A}^2(\mathbb{C})$ containing infinitely many CM-points. We may and do assume that $\mathcal{C}$ is neither a horizontal nor a vertical line, which means that $\mathcal{C}$ is of positive degree $\delta_i > 0$ in X_i for $i = 1, 2$. Now choose some $\varepsilon > 0$. For every CM-point $\underline{x} \in \mathcal{C}$ of discriminant (Δ_1, Δ_2), Theorem 2 implies that

$$\max\{|\Delta_1|, |\Delta_2|\} < C_1(\varepsilon, \max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}]) \max\{1, h(\mathcal{C})\}^{8+\varepsilon}$$

or $\underline{x} \in \mathcal{C}$ is on a modular curve $\mathcal{V}(\Phi_m)$, $1 \leq m \leq 4 \max\{\delta_1, \delta_2\}^5$. Since there exist only finitely many CM-points of bounded discriminant the latter case must occur infinitely often. Thus, there exists some $1 \leq f \leq 4 \max\{\delta_1, \delta_2\}^5$ such that $\mathcal{V}(\Phi_f)$ has infinitely many intersection points with $\mathcal{C}$. As $\mathcal{V}(\Phi_f)$ and $\mathcal{C}$ are geometrically irreducible this implies $\mathcal{V}(\Phi_f) = \mathcal{C}$.

References

[1] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203–208. MR 1662256. Zbl 0918.14010. http://dx.doi.org/10.1515/crll.1998.118.

[2] A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, *New Math. Monogr.* **9**, Cambridge Univ. Press, Cambridge, 2007. MR 2382891. Zbl 1145.11004. http://dx.doi.org/10.1017/CBO9780511542862.

[3] E. Bombieri and J. Pila, The number of integral points on arcs and ovals, *Duke Math. J.* **59** (1989), 337–357. MR 1016893. Zbl 0718.11048. http://dx.doi.org/10.1215/S0012-7094-89-05915-2.

[4] F. Breuer, Heights of CM points on complex affine curves, *Ramanujan J.* **5** (2001), 311–317. MR 1876703. Zbl 1021.11022. http://dx.doi.org/10.1023/A:1012982812988.

[5] S. Chowla, An extension of Heilbronn's class-number theorem, *Q. J. Math. Oxf. Ser.* **5** (1934), 304–307. Zbl 0010.33705. http://dx.doi.org/10.1093/qmath/os-5.1.304.

[6] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, *A Wiley-Interscience Publ.*, John Wiley & Sons, New York, 1989. MR 1028322. Zbl 0701.11001.

[7] S. David and N. Hirata-Kohno, Linear forms in elliptic logarithms, *J. Reine Angew. Math.* **628** (2009), 37–89. MR 2503235. Zbl 1169.11034. http://dx.doi.org/10.1515/CRELLE.2009.018.

[8] B. Edixhoven, Special points on the product of two modular curves, *Compositio Math.* **114** (1998), 315–328. MR 1665772. Zbl 0928.14019. http://dx.doi.org/10.1023/A:1000539721162.

[9] ———, On the André-Oort conjecture for Hilbert modular surfaces, in *Moduli of Abelian Varieties* (Texel Island, 1999), *Progr. Math.* **195**, Birkhäuser, Basel, 2001, pp. 133–155. MR 1827018. Zbl 1029.14007.

[10] ———, Special points on products of modular curves, *Duke Math. J.* **126** (2005), 325–348. MR 2115260. Zbl 1072.14027. http://dx.doi.org/10.1215/S0012-7094-04-12624-7.

[11] B. Edixhoven and A. Yafaev, Subvarieties of Shimura varieties, *Ann. of Math.* **157** (2003), 621–645. MR 1973057. Zbl 1053.14023. http://dx.doi.org/10.4007/annals.2003.157.621.

[12] A. Faisant and G. Philibert, Quelques résultats de transcendance liés à l'invariant modulaire j, *J. Number Theory* **25** (1987), 184–200. MR 0873876. Zbl 0633.10035. http://dx.doi.org/10.1016/0022-314X(87)90024-2.

[13] É. Gaudron, Mesures d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif, *Invent. Math.* **162** (2005), 137–188. MR 2198327. Zbl 1120.11031. http://dx.doi.org/10.1007/s00222-005-0440-5.

[14] D. M. Goldfeld, The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields, in *Journées Arithmétiques de Caen* (Univ. Caen, Caen, 1976), *Astérisque* **41**–**42**, Soc. Math. France, Paris, 1977, pp. 219–227. MR 0447176. Zbl 0355.12005.

[15] B. H. Gross and D. B. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320. MR 0833192. Zbl 0608.14019. http://dx.doi.org/10.1007/BF01388809.

[16] P. Habegger, Weakly bounded height on modular curves, *Acta Math. Vietnam.* **35** (2010), 43–69. MR 2642162. Zbl 05723514.

[17] R. Hartshorne, *Algebraic Geometry*, *Grad. Texts in Math.* **52**, Springer-Verlag, New York, 1977. MR 0463157. Zbl 0367.14001.

[18] B. Klingler and A. Yafaev, The André-Oort conjecture, submitted preprint (available from Klingler's homepage).

[19] D. Masser, *Elliptic Functions and Transcendence*, *Lecture Notes in Math.* **437**, Springer-Verlag, New York, 1975. MR 0379391. Zbl 0312.10023.

[20] D. Masser and U. Zannier, Torsion anomalous points and families of elliptic curves, *Amer. J. Math.* **132** (2010), 1677–1691. MR 2766181. Zbl 1225.11078. http://dx.doi.org/10.1016/j.crma.2008.03.024.

[21] J. Pila, Rational points of definable sets and results of André-Oort-Manin-Mumford type, *Int. Math. Res. Not.* **2009** (2009), 2476–2507. MR 2520786. Zbl 05586932. http://dx.doi.org/10.1093/imrn/rnp022.

[22] ———, O-minimality and the André-Oort conjecture for $\mathbb{C}^n$, *Ann. of Math.* **173** (2011), 1779–1840. MR 2800724. Zbl 05960693. http://dx.doi.org/10.4007/annals.2011.173.3.11.

[23] J. Pila and A. J. Wilkie, The rational points of a definable set, *Duke Math. J.* **133** (2006), 591–616. MR 2228464. Zbl 1217.11066. http://dx.doi.org/10.1215/S0012-7094-06-13336-7.

[24] J. Pila and U. Zannier, Rational points in periodic analytic sets and the Manin-Mumford conjecture, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei Mat. Appl.* **19** (2008), 149–162. MR 2411018. Zbl 1164.11029. http://dx.doi.org/10.4171/RLM/514.

[25] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second ed., *Grad. Texts in Math.* **106**, Springer-Verlag, New York, 2009. MR 2514094. Zbl 1194.11005. http://dx.doi.org/10.1007/978-0-387-09494-6.

[26] E. Ullmo and A. Yafaev, Galois orbits and equidistribution: towards the André-Oort conjecture, 2006. Available at http://www.math.u-psud.fr/~ullmo/.

[27] G. Wüstholz, Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen, *Ann. of Math.* **129** (1989), 501–517. MR 0997311. Zbl 0675.10025. http://dx.doi.org/10.2307/1971515.

[28] A. Yafaev, Special points on products of two Shimura curves, *Manuscripta Math.* **104** (2001), 163–171. MR 1821181. Zbl 0982.14016. http://dx.doi.org/10.1007/PL00005868.

[29] U. Zannier, *Lecture Notes on Diophantine Analysis*, with an appendix by Francesco Amoroso, *Appunti. Scuola Normale Superiore di Pisa* (*Nuova Serie*) [*Lecture Notes. Scuola Normale Superiore di Pisa* (*New Series*)] **8**, Edizioni della Normale, Pisa, 2009. MR 2517762. Zbl 1186.11001.

[30] ———, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, with appendixes by David Masser, *Ann. of Math. Studies* **181**, Princeton Univ. Press, Princeton, NJ, 2012. Zbl 06022187.

(Received: June 6, 2011)
(Revised: December 10, 2011)

ETH Zürich, Zürich, Switzerland
E-mail: kuehne@math.ethz.ch