ACTA ARITHMETICA
161.1 (2013)

An effective result of André–Oort type II

by

Lars Kühne (Pisa)

1. Introduction. In [13] the following result of André–Oort type is proven. Here, for an algebraic curve $\mathcal{C}$ defined over a number field we denote by $h(\mathcal{C})$ the naive logarithmic height of $\mathcal{C}$, so that $h(\mathcal{C})$ is just the projective logarithmic Weil height of a minimal defining polynomial of $\mathcal{C}$. Furthermore, a point of $\mathbb{A}^2(\mathbb{C})$ is called a *CM-point of discriminant* (Δ_1, Δ_2) if its first (resp. second) coordinate is the singular modulus associated with a complex elliptic curve whose endomorphism ring is of discriminant Δ_1 (resp. Δ_2).

Theorem 1. *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 $X_i|_{\mathcal{C}} : \mathcal{C} \to \mathbb{C}$ by δ_i and assume $\delta_i > 0$. Then for every $\varepsilon > 0$ there exists an effectively computable constant $C_1 = C_1(\varepsilon, \max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}]) > 0$ such that*

$$\max\{|\Delta_1|, |\Delta_2|\} < C_1 \max\{1, h(\mathcal{C})\}^{8+\varepsilon} \tag{1.1}$$

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

For brevity, we call geometrically irreducible algebraic curves $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ that are neither modular curves nor horizontal or vertical lines *non-special.* An immediate consequence of Theorem 1 is that a non-special curve $\mathcal{C}$ in $\mathbb{A}^2(\mathbb{C})$ contains only finitely many CM-points. In addition, their number and height can be bounded effectively by an expression in $h(\mathcal{C})$, $\max\{\delta_1, \delta_2\}$ and $[\mathbb{K} : \mathbb{Q}]$. In our particular instance of the André–Oort conjecture for a product of two modular curves, such a statement was obtained by Breuer [4] under GRH. Furthermore, his non-effective height bound depends only on $\max\{\delta_1, \delta_2\}$ and $[\mathbb{K} : \mathbb{Q}]$ but not on the height $h(\mathcal{C})$. Height bounds of this sort, depending only on $\max\{\delta_1, \delta_2\}$ and $[\mathbb{K} : \mathbb{Q}]$, are called *uniform* in what follows. Pila's more recent approach to the André–Oort conjecture in [15]

2010 *Mathematics Subject Classification*: Primary 14G35; Secondary 11G18, 14G05.
Key words and phrases: André–Oort conjecture, modular curve, effective, uniformity.

DOI: 10.4064/aa161-1-1

also exhibits uniform bounds, which are unconditional but not effectively computable. In Theorem 2 below we reprove the existence of such bounds as a negligible interlude to our main results, Theorems 3 and 4.

Before we state Theorems 2 and 3, we dwell on the difficulties to be overcome if one aims at inferring a uniform result from Theorem 1. For this, we now examine a naive approach, which makes only use of a trivial height bound for singular moduli. If $\mathbb{Z}+\tau\mathbb{Z}\subseteq\mathbb{C}$ is the lattice of a complex elliptic curve having an endomorphism ring of discriminant $\varDelta_\tau$, then $h(j(\tau))\leq c_1|\varDelta_\tau|^{1/2}$ with an absolute constant $c_1>0$. Indeed, $j(\tau)$ is an algebraic integer and all its complex conjugates have absolute value less than $c_2\exp(|\varDelta_\tau|^{1/2})$ for some $c_2>0$. Let $\underline{x}\in\mathbb{A}^2(\mathbb{C})$ be a CM-point on a non-special curve $\mathcal{C}$ and not contained in any modular curve $\mathcal{V}(\varPhi_m)$, $1\leq m\leq 4\max\{\delta_1,\delta_2\}^5$. Then, by Theorem 1, its affine logarithmic height $h(\underline{x})$ is bounded by

(1.2)
$$h(\underline{x})\leq\max\{h(x_1),h(x_2)\}<C_2(\varepsilon,\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])\max\{1,h(\mathcal{C})\}^{4+\varepsilon},$$

where

$$C_2(\varepsilon,\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])=c_1C_1(2\varepsilon,\max\{\delta_1,\delta_2\},[\mathbb{K}:\mathbb{Q}])^{1/2}>0$$

is an effectively computable constant. Additionally, for those CM-points that are intersection points of $\mathcal{C}$ with a modular curve $\mathcal{V}(\varPhi_m)$, $1\leq m\leq 4\max\{\delta_1,\delta_2\}^5$, a similar height bound can be deduced from an arithmetic version of Bézout's theorem (e.g. [14, Théorème 3]). More precisely, the exponent $4+\varepsilon$ can be even replaced by 1 in this case.

Unfortunately, the height bound in (1.2) is not uniform. Nevertheless, an absolute version of Siegel's lemma [18] is used in Lemma 2 below to show the following: For each pair $(\delta_1,\delta_2)\in\mathbb{N}^2$ there exists a linear polynomial $l_{(\delta_1,\delta_2)}(X)\in\mathbb{R}[X]$ with positive leading coefficient such that the number of points $\underline{x}$ on an affine curve $\mathcal{C}$ of bidegree (δ_1,δ_2) satisfying

$$h(\underline{x})<l_{(\delta_1,\delta_2)}(h(\mathcal{C}))\tag{1.3}$$

is bounded uniformly, i.e. bounded solely in terms of δ_1 and δ_2. Lemma 2 parallels a result of Zhang ([24, Theorem 6.2]) stated for algebraic subvarieties of tori. We cannot apply it directly to obtain a uniform bound on the number of CM-points on a non-special curve because the exponent of $h(\mathcal{C})$ in (1.2) above is considerably larger than the one in (1.3). Hence, a major task is to render Lemma 2 applicable by lowering this exponent. For this purpose, it is necessary to use more sophisticated height bounds for singular moduli. A standard estimate, given as Lemma 3 below, indicates that for any $\varepsilon>0$ there exists an effectively computable constant $c_3(\varepsilon)>0$ such that

$$h(j(\tau))\leq c_3(\varepsilon)|\varDelta_\tau|^{1/2}h_{\varDelta_\tau}^{-1+\varepsilon},$$

where h_{Δ_τ} is the class number of the unique imaginary quadratic order having discriminant Δ_τ. A classical theorem of Siegel [21] states that there exists some constant $c_4'(\varepsilon)$, depending only on ε, such that

$$|\Delta|^{1/2-\varepsilon} \leq c_4'(\varepsilon)h_\Delta \tag{1.4}$$

for any negative discriminant Δ. Using it, we deduce the following theorem and its corollary in Section 5.

Theorem 2. *For any non-special planar algebraic curve $\mathcal{C}$ of bidegree (δ_1, δ_2) defined over a number field $\mathbb{K}$ the number of CM-points on $\mathcal{C}$ is bounded uniformly from above by some constant $C_3'(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$.*

Corollary 1. *Let $\mathcal{C}$ be a non-special planar algebraic curve over a number field $[\mathbb{K} : \mathbb{Q}]$ of bidegree (δ_1, δ_2). Then there exists a constant $C_4' = C_4'(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$ such that*

$$\max\{|\Delta_1|, |\Delta_2|\} < C_4'$$

for every CM-point of discriminant (Δ_1, Δ_2) contained in $\mathcal{C}$. In addition, the height of CM-points on $\mathcal{C}$ is uniformly bounded by a certain constant $C_5'(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$.

Qualitatively, Corollary 1 supersedes the results of Breuer obtained in [4] under assumption of GRH for imaginary quadratic fields. In fact, Corollary 1 is a non-effective version of [4, Theorem 1.1] and can be made effective by assuming GRH. Interestingly, the final sentence of [4, Section 4] vaguely asserts that "André's method", namely his proof in [1], is intrinsically non-uniform. The above results suggest otherwise.

With the bias of our previous work [13], however, we are more interested in obtaining results that are both effective and uniform. It is clear from the above that an effective version of Theorem 2 and its Corollary 1 needs an effective lower bound for the class number of imaginary quadratic fields. The best result in this direction is due to Goldfeld [8] and Gross–Zagier [9]. For every $0 < \varepsilon < 1$, [9, Theorem (8.1)] states the existence of an effective constant $c_5(\varepsilon) > 0$ such that

$$(\log|\Delta|)^{1-\varepsilon} \leq c_5(\varepsilon)h_\Delta. \tag{1.5}$$

This bound is not enough for our purpose here but it is nevertheless essential for Theorem 4 below. In contrast, the Siegel–Tatuzawa theorem [22] states that there exists an effectively computable constant $c_6(\varepsilon) > 0$ such that

$$|d|^{1/2-\varepsilon} < c_6(\varepsilon)h_d$$

for all fundamental discriminants d with at most one exception d_*. We recall that *fundamental discriminants* are the discriminants of maximal orders in imaginary quadratic fields. In spite of the exception d_*, it is possible to deduce by Lemma 2 a version of Theorem 1 that, partially, gives uniform effective bounds. Throughout this article, we often write a general discriminant Δ as a product f^2d, where we tacitly assume that f is a positive integer and $d < 0$ is a fundamental discriminant. This decomposition of Δ is obviously unique. Using the Siegel–Tatuzawa theorem instead of Siegel's above-mentioned result we obtain in Section 6 the following results.

Theorem 3. *Let $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ be a non-special curve of bidegree (δ_1, δ_2) that is defined over a number field $\mathbb{K}$. Then the number of CM-points on $\mathcal{C}$ of discriminant $(\Delta_1, \Delta_2) = (d_1 f_1^2, d_2 f_2^2)$, $(d_1, d_2) \neq (d_*, d_*)$, is bounded uniformly by $C_3(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$.*

Corollary 2. *There is an effective constant $C_4 = C_4(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$ such that*

$$\max\{|\Delta_1|, |\Delta_2|\} < C_4$$

for every CM-point on $\mathcal{C}$ of discriminant $(\Delta_1, \Delta_2) = (d_1 f_1^2, d_2 f_2^2)$, $(d_1, d_2) \neq (d_*, d_*)$. Consequently, this bound is true for all CM-points on $\mathcal{C}$ that are not contained in any modular curve. Hence, the height of these points is uniformly bounded by an effective constant $C_5(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$.

Our proof of Theorem 3 makes use of the following lemma. We remind the reader that a CM-point of discriminant $(d_1 f_1^2, d_2 f_2^2)$ is contained in a modular curve if and only if $d_1 = d_2$.

Lemma 1. *The number of CM-points on $\mathcal{C}$ that are not intersection points of $\mathcal{C}$ with a modular curve is bounded by an effective constant*

$$C_6(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}]) > 0.$$

For its proof, we follow closely the argument in [1, Section 2], which uses class field theory and has no counterpart in the first part of this article [13]. Indeed, a slight variation of the argument gives a completely effective version of [1]. This comes quite unanticipated, since André's proof has been generally considered ineffective (cf. [23]), which provided also a strong motivation for [13]. However, Lemma 1 confutes these claims.

To deduce Corollary 2 from Theorem 3 we use the effective lower bounds on class numbers due to Goldfeld [8] and Gross–Zagier [9]. It is not clear whether Theorem 3 and its Corollary 2 can be also deduced by means of Pila's techniques from [15] in combination with the Siegel–Tatuzawa theorem (the use of this theorem was actually suggested by a referee of Pila's article [16, Aside 11.3]). However, effective results depend on the effectivity of the underlying Pila–Wilkie counting technique [17] for some o-minimal structure, which is denoted by $\mathbb{R}_j$ in [16]. This is a widely open question, for comments on which we refer the reader again to [16, Aside 11.3].

Using Lemma 1 we can also give a uniform version of André–Oort for some curves.

Theorem 4. *For all positive integers δ and D there exists an effectively computable constant $C_7(\delta, D) > 0$ such that the following assertion is true: Let $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ be a non-special curve of bidegree (δ_1, δ_2), defined over a number field $\mathbb{K}$ and with Zariski closure $\mathcal{C} \cup \{(\infty, \infty)\}$ in $(\mathbb{P}^1 \times \mathbb{P}^1)(\mathbb{C})$. Then there exist at most $C_7(\max\{\delta_1, \delta_2\}, [\mathbb{K} : \mathbb{Q}])$ CM-points on $\mathcal{C}$.*

We remark that Theorem 4 can be used, in theory, to compute all pairs of singular moduli that satisfy any non-trivial $\mathbb{Q}$-linear relation. In practice, $C_7(\delta, D)$ can be computable with a reasonable amount of computation. However, in order to compute the corresponding list of CM-points one needs the weak lower bounds on class numbers of Gross–Zagier (1.5), which makes computations impractical. In contrast, Theorem 1 is more apt for computing CM-points on any given non-special curve. Therefore, Theorems 1 and 4 are complementary in some sense. Finally, as a demonstration of the techniques used in [13, proof of Theorem 1] we conclude this article with an explicit result, which seems to be new in the literature.

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

This theorem was also proven by David Masser and Umberto Zannier in an unpublished preprint [2] sent to the author. In fact, they proved the same for $j(\tau_1)j(\tau_2) = 1$ and also obtained a result similar to our Theorem 1 with help from Yuri Bilu [1]. We refer to [13, footnote on p. 652] for a more precise description of their achievements. We also know of a related (unpublished) result obtained by Philipp Habegger: Only finitely many units in rings of algebraic integers appear as singular moduli.

Notation. Throughout this article, we adopt the following conventions on constants: By $c_1, c_2, \ldots$ we denote effectively computable constants that might depend on some $\varepsilon > 0$, if indicated so, but are completely independent of any other data. In addition, $C_1(\ldots), C_2(\ldots), \ldots$ are constants that depend also effectively on some data of a given curve $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$. In fact, they always depend on its bidegree and the degree of its field of definition. Non-effective constants carry an additional upper prime to distinguish them from effective constants. When non-effective and effective statements parallel each other, as do Theorems 2 and 3, we use the same indices for a non-effective constant c_i' (resp. C_i') and its effective counterpart c_i (resp. C_i). Elsewise, for each index i we use either c_i or c_i' (resp. C_i or C_i'). *In general, all constants are positive and do not depend on any $\varepsilon > 0$ unless explicitly mentioned otherwise.*

[1] These results have meanwhile appeared as [3].

2. Preliminaries. In this section, we give certain definitions and results additional to those in [13, Section 2].

2.1. Heights. Let $\mathbb{K}$ denote an arbitrary number field. For any $\mathbb{K}$-linear subspace $V \subset \mathbb{K}^l$ of dimension r, its rth exterior product $\bigwedge_r V$ canonically defines a line in $\bigwedge_r \mathbb{K}^l$. We may identify $\bigwedge_r \mathbb{K}^l$ with $\mathbb{K}^m$, $m = l!/(l-r)!$, by use of standard bases. With respect to this identification, the exterior product $\bigwedge_r V$ defines a point $[\bigwedge_r V] \in \mathbb{P}^m(\mathbb{K})$ whose projective logarithmic height is called the *Schmidt height* $h(V)$ of V (cf. [19]). In Lemma 2 below, we use a variation $h_2(\cdot)$ of the height $h(\cdot)$ from [13] given by

$$\begin{aligned} h_2(p) = {} & \sum_{\nu \nmid \infty} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log \max\{|p_0|_\nu, |p_1|_\nu, \dots, |p_n|_\nu\} \\ & + \frac{1}{2} \sum_{\nu \mid \infty} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log(|p_0|_\nu^2 + |p_1|_\nu^2 + \dots + |p_n|_\nu^2) \end{aligned}$$

for a point $p = (p_0 : p_1 : \dots : p_n)$ in $\mathbb{P}^n(\mathbb{K})$. This expression depends neither on the choice of $\mathbb{K}$ nor on the representative $(p_0, p_1, \dots, p_n)$ of p. The height $h_2(\cdot)$ is a modification of $h(\cdot)$ that arises from replacing the ∞-norm with the 2-norm at archimedean places. It is easy to see that

$$h(p) \le h_2(p) \le h(p) + \tfrac{1}{2}\log(n+1). \tag{2.1}$$

This implies moreover that $h_2(p) = 0$ if and only if $p = (p_0 : p_1 : \dots : p_n)$ has a single non-zero entry. We also define a height $h_2(\cdot)$ of affine points, polynomials and vector spaces, substituting $h_2(\cdot)$ for $h(\cdot)$ at all its occurrences in [13, Section 2] and in the above. We use $h_2(\cdot)$ because it comports well with Hadamard's inequality (see [18, Lemma 4.7]).

2.2. Complex elliptic curves and class field theory. In order to describe the arithmetic properties of singular moduli we have to recall first some facts from elementary algebraic number theory. For every imaginary quadratic field $\mathbb{K}$ there exists a unique square-free integer $n < 0$ such that $\mathbb{K} = \mathbb{Q}(\sqrt{n})$. The discriminant d of the maximal order $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$ is n if $n \equiv 1 \pmod 4$ and $4n$ if $n \equiv 2, 3 \pmod 4$. The numbers arising as discriminants of imaginary quadratic fields are called *fundamental discriminants*. For every order $\mathcal{O}$ of $\mathbb{K}$ we define its *conductor* by

$$\mathfrak{f} = \{n \in \mathbb{Z} \mid n\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}\}.$$

Then, $\mathfrak{f} = (f)$ is an ideal in $\mathbb{Z}$ such that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_{\mathbb{K}}$ and the discriminant of $\mathcal{O}$ equals $f^2 d$. This implies that there exists only one imaginary quadratic order of a given discriminant.

For a CM-elliptic curve $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ with endomorphism ring $\mathcal{O}$, the field $\mathbb{Q}(\sqrt{d})(j(\tau))$ coincides with the ring class field $\mathrm{RCF}(\mathcal{O})$ of $\mathcal{O}$ by Weber's theorem (see [6, Chapter 11]). The extension $\mathrm{RCF}(\mathcal{O}_{\mathbb{K}})/\mathbb{K}$ has degree h_d, where h_d is the class number of $\mathbb{K}$ and is the largest unramified abelian extension of $\mathbb{K}$. The field $\mathrm{RCF}(\mathcal{O}_{\mathbb{K}})$ is called the *Hilbert class field* of $\mathbb{K}$. In general, the extension $\mathrm{RCF}(\mathcal{O})/\mathbb{K}$ is of degree ([6, Theorem 7.24])

$$h_{f^2d} = \frac{h_d f}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|f} \left(1 - \left(\frac{d}{p}\right) p^{-1}\right). \tag{2.2}$$

An important intermediate field of the extension $\mathrm{RCF}(\mathcal{O})/\mathbb{K}$ is the *genus field* $\mathrm{GF}(\mathcal{O})$. It is defined as the largest subfield of $\mathrm{RCF}(\mathcal{O})$ that is abelian over $\mathbb{Q}$. Via class field theory, $\mathrm{GF}(\mathcal{O})$ corresponds to the principal genus in the class group of $\mathcal{O}$. Therefore, the degree $[\mathrm{RCF}(\mathcal{O}) : \mathrm{GF}(\mathcal{O})]$ equals the index g_{f^2d} of the principal genus in the class group of $\mathcal{O}$. By analogy with the ordinary class number h_{f^2d} the index g_{f^2d} is commonly called the genus class number of $\mathcal{O}$. The structure of the field $\mathrm{GF}(\mathcal{O})$ is well-known in the classical case $f = 1$ (see [6, Theorem 6.1]) and for general f a similar description is given by Halter-Koch in [10]. We briefly recall [10, Theorem 2]. Write

$$d = 2^s p_1 \dots p_k q_1 \dots q_l \quad \text{and} \quad f = 2^t p_1^{a_1} \dots p_k^{a_k} r_1^{b_1} \dots r_m^{b_m},$$

where p_i ($i \in \{1, \dots, k\}$), q_i ($i \in \{1, \dots, l\}$), r_i ($i \in \{1, \dots, m\}$) denote $k+l+m$ distinct primes $\neq 2$, s, t non-negative integers, and a_i ($i \in \{1, \dots, k\}$), b_i ($i \in \{1, \dots, m\}$) positive integers. For any prime $p > 2$ we set $p^* = (-1)^{(p-1)/2} p$ and define

$$\mathbb{L} = \mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_k^*}, \sqrt{q_1^*}, \dots, \sqrt{q_l^*}, \sqrt{r_1^*}, \dots, \sqrt{r_m^*}).$$

With this notation we have

$$\mathrm{GF}(\mathcal{O}) = \begin{cases} \mathbb{L} & \text{if } s = 0 \text{ and } t \leq 1, \\ \mathbb{L}(\sqrt{-1}) & \text{if } (s = 0 \text{ and } t = 2) \text{ or } (s = 2 \text{ and } t \leq 1), \\ \mathbb{L}(\sqrt{2}) & \text{if } s = 3,\ t = 0 \text{ and } d/2^3 \equiv 1 \pmod 4, \\ \mathbb{L}(\sqrt{-2}) & \text{if } s = 3,\ t = 0 \text{ and } d/2^3 \equiv 3 \pmod 4, \\ \mathbb{L}(\sqrt{2}, \sqrt{-1}) & \text{otherwise.} \end{cases}$$

A simple consequence, well-known in the classical case $f = 1$, is the bound

$$[\mathrm{GF}(\mathcal{O}) : \mathbb{K}] \leq 2^{\omega(f^2d)+1}, \tag{2.3}$$

where $\omega(f^2d)$ is the number of distinct prime divisors of f^2d.

Finally, we need a version of the estimate [13, (2.4)], which is valid for all τ in the standard fundamental domain and not only for those satisfying $\mathrm{Im}(\tau) \geq 1$. If $\mathrm{Im}(\tau) \geq \sqrt{3}/2$, then we infer from [13, (2.4)] and

$$j(i\sqrt{3}/2) = (1417905000 - 818626500\sqrt{3}) < 2310$$

that $|j(\tau)|$ is bounded by

$$\max\{j(i\sqrt{3}/2), 1193 + \exp(2\pi \operatorname{Im}(\tau))\} < 2310 + \exp(2\pi \operatorname{Im}(\tau)). \tag{2.4}$$

3. Points of small height on affine curves. The lemma in this section specifies the fact that for any $\varepsilon > 0$ and any algebraic curve $\mathcal{C}$ there exist only few points satisfying (1.3). It does so by providing a uniform effective bound on their number.

LEMMA 2. *Let $\mathcal{C}$ be a geometrically irreducible algebraic curve in $\mathbb{A}^2(\mathbb{C})$ of bidegree (δ_1, δ_2) and set $\delta_* = 2\delta_1\delta_2 + 1$. Then there exist at most δ_*^2 points $\underline{x}$ on $\mathcal{C}$ such that*

$$h_2(\underline{x}) < \frac{1}{(\delta_1 + \delta_2)(\delta_* - 1)} h_2(\mathcal{C}). \tag{3.1}$$

In what follows, especially in the proof below, the points on $\mathcal{C}$ satisfying (3.1) are called *points of small height*. We frequently leave out the reference to a curve $\mathcal{C}$ (and hence to the degrees δ_1 and δ_2) since no confusion is possible here.

Proof of Lemma 2. Choose a defining polynomial $P \in \overline{\mathbb{Q}}[X_1, X_2]$ of $\mathcal{C}$ such that $h_2(P) = h_2(\mathcal{C})$ and P has bidegree (δ_1, δ_2). In order to derive a contradiction, we may assume given a set $\mathcal{S} = \{\underline{x}_1, \ldots, \underline{x}_{\delta_*^2+1}\}$ of δ_*^2+1 points of small height on $\mathcal{C}$. The $\overline{\mathbb{Q}}$-span of all monomials $X_1^i X_2^j$, $0 \le i \le \delta_1$, $0 \le j \le \delta_2$, is isomorphic to $\overline{\mathbb{Q}}^{\delta_*}$ as a vector space. For what follows, we choose the isomorphism that associates $X_1^i X_2^j$ with the kth column vector $\underline{e}_k$, $k = i(\delta_2+1)+j+1$, of the standard basis in $\overline{\mathbb{Q}}^{\delta_*}$. This isomorphism is compatible with the polynomial height $h_2(\cdot)$ and the projective height $h_2(\cdot)$ on $\overline{\mathbb{Q}}^{\delta_*}$. The subspace V of $\overline{\mathbb{Q}}^{\delta_*}$ corresponding to polynomials vanishing at $\mathcal{S}$ has $\overline{\mathbb{Q}}$-dimension 1 by Bézout's theorem for $\mathbb{P}^1 \times \mathbb{P}^1$ (cf. [20, Example IV.2.1.2]). It is the kernel of multiplication by a matrix $A \in \overline{\mathbb{Q}}^{(\delta_*^2+1)\cdot\delta_*}$ such that the entry of A in the kth column and lth row is the evaluation of $X_1^i X_2^j$, where $k = i(\delta_2 + 1) + j + 1$, $0 \le i \le \delta_1$, and $0 \le j \le \delta_2$, at $\underline{x}_l$. By elementary linear algebra, there exists a $(\delta_* - 1) \times \delta_*$-minor A' of A such that V is the kernel of multiplication by A' and A' has maximal rank $\delta_* - 1$. Relabeling if necessary, we assume that the lth row $\underline{a}_l$ of A' is associated with $\underline{x}_l$, i.e. its entries are the evaluations of monomials $X_1^i X_2^j$, $0 \le i \le \delta_1$, $0 \le j \le \delta_2$, at $\underline{x}_l$. Now, the transposed rows $\underline{a}_l^t$, $1 \le l \le \delta_* - 1$, of A' form a basis of the orthogonal complement $V^\perp \subseteq \overline{\mathbb{Q}}^{\delta_*}$ of V with respect to the standard scalar product on $\overline{\mathbb{Q}}^{\delta_*}$. A rough estimation shows that $h_2(\underline{a}_l^t) \le (\delta_1 + \delta_2) h_2(\underline{x}_l)$. Thus, by [18, Lemma 4.7] we have

$$h_2(V^\perp) \le h_2(\underline{a}_1^t) + \cdots + h_2(\underline{a}_{\delta_*-1}^t) \le (\delta_1+\delta_2)(\delta_*-1) \max_{1 \le i \le \delta_*-1} h_2(\underline{x}_i) < h_2(\mathcal{C}).$$

Now, formula (4) of [19, p. 433] states that $h_2(V) = h_2(V^\perp)$. Since V is one-dimensional there exists a non-zero polynomial $Q \in V$ of height $h_2(V^\perp)$ by the very definition of the Schmidt height. Finally, P and Q are $\overline{\mathbb{Q}}$-collinear and hence

$$h_2(\mathcal{C}) = h_2(P) = h_2(Q) < h_2(\mathcal{C}).$$

This contradiction implies the lemma. ∎

4. Bounding the height of singular moduli. In the following sections, we need to bound the height of a singular modulus in terms of its discriminant and class number. Lemma 3 in combination with Lemma 5 suffices for this purpose. All claims in this section are well-known and we give proofs just because appropriate references seem rare to us.

Lemma 3. *For every $\varepsilon > 0$ there exists an absolute constant $c_3(\varepsilon) > 0$ having the following property: Let $j(\tau)$ be a singular modulus associated with a CM-elliptic curve whose endomorphism ring is an imaginary quadratic order of discriminant $\Delta_\tau = f_\tau^2 d_\tau$ and class number h_{Δ_τ}. Then the height $h(j(\tau))$ is bounded from above by*

$$c_3(\varepsilon)|\Delta_\tau|^{1/2} h_{\Delta_\tau}^{-1+\varepsilon}.$$

Proof. For readability, we write Δ, f, d instead of Δ_τ, f_τ, d_τ. We denote by $\mathcal{T}_\Delta$ the set of all triples (a,b,c) of integers such that $\gcd(a,b,c) = 1$, $\Delta = b^2 - 4ac$ and either $-a < b \leq a < c$ or $0 \leq b \leq a = c$. Recall that $j(\tau)$ is an algebraic integer and that its $h_\Delta = [\mathbb{Q}(j(\tau)) : \mathbb{Q}]$ Galois conjugates are

$$j\left(\frac{-b + i\sqrt{4ac - b^2}}{2a}\right), \qquad (a,b,c) \in \mathcal{T}_\Delta.$$

In particular, note that $|\mathcal{T}_\Delta| = h_\Delta$. This implies

$$h(j(\tau)) = \frac{1}{h_\Delta} \sum_{(a,b,c)\in\mathcal{T}_\Delta} \log\max\left\{1, \left| j\left(\frac{-b + i\sqrt{|\Delta|}}{2a}\right)\right|\right\}.$$

From (2.4) we deduce

$$h(j(\tau)) \leq \frac{c_7|\Delta|^{1/2}}{h_\Delta} \sum_{(a,b,c)\in\mathcal{T}_\Delta} a^{-1}$$

for some constant $c_7 > 0$. Denote by $\mathcal{T}_\Delta(a)$ the set of triples in $\mathcal{T}_\Delta$ having a as first component. In addition, for positive integers m, n we define

$$\mathcal{T}_m^*(n) = \{b \pmod{n} \mid m \equiv -b^2 \pmod{n}\} \subseteq \mathbb{Z}/n\mathbb{Z}.$$

Since $|b| \leq a$ the map sending $(a,b,c) \in \mathcal{T}_\Delta(a)$ to $b \pmod{4a} \in \mathcal{T}_{|\Delta|}^*(4a)$ is injective. From Lemma 4 below it follows that there exist at most

$$c_8(\varepsilon)\gcd(4a, f)(4a)^{\varepsilon/4}$$

elements in $\mathcal{T}^*_{|\Delta|}(4a)$. Thus,

$$h(j(\tau)) \le c_9(\varepsilon) h_\Delta^{-1} |\Delta|^{1/2} \sum_a \min\{\gcd(a,f) a^{\varepsilon/4}, |\mathcal{T}_\Delta(a)|\} a^{-1}$$

for some $c_9(\varepsilon) > 0$. Setting $t = \gcd(a,f)$, $a = ta_0$ and rearranging terms we obtain

$$\begin{aligned} h(j(\tau)) &\le c_9(\varepsilon) h_\Delta^{-1} |\Delta|^{1/2} \sum_{t|f} \sum_{\substack{a_0 \\ (a_0,f)=1}} \min\{t^{\varepsilon/4} a_0^{\varepsilon/4}, |\mathcal{T}_\Delta(ta_0)|\} a_0^{-1} \\ &\le c_9(\varepsilon) h_\Delta^{-1} |\Delta|^{1/2} \sum_{t|f} t^{\varepsilon/4} \Big(\sum_{\substack{a_0 \\ |\mathcal{T}_\Delta(ta_0)| \ne 0}} a_0^{-1+\varepsilon/4} \Big). \end{aligned}$$

The inner sum is bounded by $\sum_{a_0=1}^{h_\Delta} a_0^{-1+\varepsilon/4} \le \int_1^{h_\Delta} x^{-1+\varepsilon/4}\,dx + 1$. Together with [11, Theorem 315] this yields a constant $c_{10}(\varepsilon) > 0$ such that

$$h(j(\tau)) \le c_{10}(\varepsilon) |\Delta|^{1/2} f^{\varepsilon/2} h_\Delta^{-1+\varepsilon/4}.$$

From (2.2) we deduce $f^{2/3} \le f^{2/3} h_d \le c_{11} h_\Delta$ for an absolute constant $c_{11} > 0$. Hence, $f^{\varepsilon/2} \le c_{11}^{3\varepsilon/4} h_\Delta^{3\varepsilon/4}$ and

$$h(j(\tau)) \le c_3(\varepsilon) |\Delta|^{1/2} h_\Delta^{-1+\varepsilon}. \ \blacksquare$$

Lemma 4. *The set $\mathcal{T}^*_{|\Delta|}(n)$, where $\Delta = f^2 d$ is a negative discriminant, contains at most $c_8(\varepsilon)\gcd(n,f) n^\varepsilon$ elements.*

Proof. We first bound the cardinality of $\mathcal{T}^*_m(n)$ for a general non-zero integer m coprime to n, which means $m \pmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Write n as a product $2^{a_0} p_1^{a_1} \ldots p_r^{a_r}$ of prime factors. We assume $a_i > 0$ for all $1 \le i \le r$. By the Chinese remainder theorem

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/2^{a_0}\mathbb{Z})^\times \times \prod_{i=1}^r (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times.$$

Hence, every solution $b \pmod n$ of $m \equiv -b^2 \pmod n$ corresponds uniquely to a tuple

$$(b_0 \pmod{2^{a_0}}, b_1 \pmod{p_1^{a_1}}, \ldots, b_r \pmod{p_r^{a_r}})$$

solving the following tuple of equations:

$$(m \equiv -b_0^2 \pmod{2^{a_0}}, m \equiv -b_1^2 \pmod{p_1^{a_1}}, \ldots, m \equiv -b_r^2 \pmod{p_r^{a_r}}).$$

Now, [5, Proposition 2.1.24] states that $(\mathbb{Z}/2\mathbb{Z})^\times = 1$ and $(\mathbb{Z}/2^n\mathbb{Z})^\times = (\mathbb{Z}/2^{n-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ for $n \ge 2$. The latter group is a product of two cyclic groups of even order. Thus, the number of solutions $b_0 \pmod{2^{a_0}}$ of $m \equiv -b_0^2 \pmod{2^{a_0}}$ is at most 4. Similarly, from $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times = \mathbb{Z}/p_i^{a_i-1}(p_i-1)\mathbb{Z}$ it follows that the equation $m \equiv -b_i^2 \pmod{p_i^{a_i}}$ has exactly $\big(1 + \big(\frac{-m}{p_i}\big)\big)$ solutions $b_i \pmod{p_i^{a_i}}$, where $\big(\frac{-m}{p_i}\big)$ is the Legendre symbol. In conclusion, the cardinality of $\mathcal{T}^*_m(n)$ is bounded from above by

$$4\prod_{\substack{p\mid n\\ p\neq 2}}\left(1+\left(\frac{-m}{p}\right)\right)\le c_{12}(\varepsilon)n^{\varepsilon}.$$

Assume now $\gcd(n,|\Delta|)=2^{c_0}p_1^{c_1}\dots p_s^{c_s}$, where $c_i>0$ for all $1\le i\le s$. Write $|\Delta|=2^{c_0}p_1^{c_1}\dots p_s^{c_s}m$ and $n=2^{c_0}p_1^{c_1}\dots p_s^{c_s}n_0$. We define a map

$$\varphi:\mathcal{T}^*_{|\Delta|}(n)\to\mathcal{T}^*_{\tilde m}(n_0),$$

where $\tilde m$ is some integer such that $(\tilde m,n_0)=1$. Let $b \pmod n$ be a solution of $\Delta\equiv -b^2 \pmod n$. Then $b\in 2^{\lceil c_0/2\rceil}p_1^{\lceil c_1/2\rceil}\dots p_s^{\lceil c_s/2\rceil}\mathbb{Z}/n\mathbb{Z}$, which means that b can be written as $b=2^{\lceil c_0/2\rceil}p_1^{\lceil c_1/2\rceil}\dots p_s^{\lceil c_s/2\rceil}b_0 \pmod n$ for some b_0 $\pmod n$. Furthermore, $|\Delta|\equiv -b^2 \pmod n$ is equivalent to

$$2^{c_0}p_1^{c_1}\dots p_s^{c_s}m\equiv -2^{2\lceil c_0/2\rceil}p_1^{2\lceil c_1/2\rceil}\dots p_s^{2\lceil c_s/2\rceil}b_0^2 \pmod{2^{c_0}p_1^{c_1}\dots p_s^{c_s}n_0}.$$

Cancelling $2^{c_0}p_1^{c_1}\dots p_s^{c_s}$, we infer from this

$$m\equiv -2^{c_0^*}p_1^{c_1^*}\dots p_s^{c_s^*}b_0^2 \pmod{n_0},$$

where c_i^* is 0 or 1 if c_i is even or odd, respectively. If $2^{c_0^*}p_1^{c_1^*}\dots p_s^{c_s^*}$ is not a unit in $\mathbb{Z}/n_0\mathbb{Z}$ then this equation is unsolvable because $(n_0,m)=1$. In this case, $\mathcal{T}^*_{|\Delta|}(n)$ must be empty and there is nothing left to define or to prove. Thus, we may assume that there exists some $k\in\mathbb{Z}$ such that $k\cdot 2^{c_0^*}p_1^{c_1^*}\dots p_s^{c_s^*}\equiv 1$ $\pmod{n_0}$. Setting $\tilde m=km$, we obtain

$$\tilde m\equiv -b_0^2 \pmod{n_0}.$$

Therefore, $b_0 \pmod{n_0}$ is an element of $\mathcal{T}^*_{\tilde m}(n_0)$. We set $\varphi(b)=b_0 \pmod{n_0}$. It is easy to see that φ is well-defined and maps at most $2^{\lfloor c_0/2\rfloor}p_1^{\lfloor c_1/2\rfloor}\dots$ $\dots p_s^{\lfloor c_s/2\rfloor}$ elements of $\mathcal{T}^*_{|\Delta|}(n)$ to each $b_0 \pmod{n_0}\in\mathcal{T}^*_{\tilde m}(n_0)$. In conclusion,

$$|\mathcal{T}^*_{|\Delta|}(n)|\le 2^{\lfloor c_0/2\rfloor}p_1^{\lfloor c_1/2\rfloor}\dots p_s^{\lfloor c_s/2\rfloor}|\mathcal{T}^*_{\tilde m}(n_0)|.$$

Since $\Delta=f^2d$ and d is square-free except for a possible square factor of 4,

$$2^{\lfloor c_0/2\rfloor}p_1^{\lfloor c_1/2\rfloor}\dots p_s^{\lfloor c_s/2\rfloor}\le 2\gcd(n,f).$$

By using $(\tilde m,n_0)=1$ we infer from our result above that

$$|\mathcal{T}^*_{|\Delta|}(n)|\le c_8(\varepsilon)\gcd(n,f)n^{\varepsilon}. \ \blacksquare$$

The following lemma gives us a good lower bound on the class number in most cases.

LEMMA 5. *There exists an effective constant $c_4(\varepsilon)>0$ and at most one fundamental discriminant $d_*<0$ such that $h_\Delta\ge c_4(\varepsilon)|\Delta|^{1/2-\varepsilon}$ for every discriminant $\Delta=df^2$ with $d\neq d_*$.*

Proof. According to [22, Theorem 3] (see also [12, Theorem 22.8]), there is an effectively computable constant $c_{13}(\varepsilon) > 0$ such that

$$c_{13}(\varepsilon)|d|^{1/2-\varepsilon} < h_d$$

for all but one fundamental discriminant $d_* < 0$. Furthermore, we deduce from (2.2) that

$$c_{14}(\varepsilon)f^{1-2\varepsilon}h_d \leq h_\Delta$$

for some constant $c_{14}(\varepsilon) > 0$. These two estimates readily imply the lemma. ■

For the non-effective Theorem 2, we use Siegel's theorem as given above in (1.4). Note that the bound (1.4) is a simple consequence of Lemma 5 since presuming knowledge about d_* (and hence about h_{d_*}) the constant $c_4(\varepsilon)$ can be easily altered into some (non-effective) constant $c'_4(\varepsilon)$ such that the bound (1.4) is valid in general.

Lemma 6. *Let $\varepsilon > 0$. Denote by g_Δ the genus class number of the imaginary quadratic order $\mathcal{O}$ of discriminant Δ. Then there exists an effective constant $c_{15}(\varepsilon) > 0$ such that for all discriminants $\Delta = df^2$, where $d \neq d_*$, the bound $g_\Delta \geq c_{15}(\varepsilon)|\Delta|^{1/2-\varepsilon}$ holds.*

Proof. Recall that $[\mathrm{GF}(\mathcal{O}) : \mathbb{Q}(\sqrt{d})] \leq 2^{\omega(\Delta)+1}$ by (2.3). By [11, Theorem 315] there exists a constant $c_{16}(\varepsilon) > 0$ such that $2^{\omega(\Delta)+1} \leq c_{16}(\varepsilon)|\Delta|^\varepsilon$. We deduce

$$g_\Delta = \frac{[\mathrm{RCF}(\mathcal{O}) : \mathbb{Q}(\sqrt{d})]}{[\mathrm{GF}(\mathcal{O}) : \mathbb{Q}(\sqrt{d})]} \geq \frac{h_\Delta}{2^{\omega(\Delta)+1}} \geq c_{16}(\varepsilon/2)^{-1}h_\Delta|\Delta|^{-\varepsilon/2}.$$

From Lemma 5 above we infer

$$g_\Delta \geq c_4(\varepsilon/2)c_{16}(\varepsilon/2)^{-1}|\Delta|^{1/2-\varepsilon}. \; ■$$

5. Proof of Theorem 2 and Corollary 1. We set $\delta = \max\{\delta_1, \delta_2\}$, $D = [\mathbb{K} : \mathbb{Q}]$ and (again) $\delta_* = 2\delta_1\delta_2 + 1$ for readability. Choose some real number ε satisfying $0 < \varepsilon < 1/10$. Bézout's theorem implies that the number of CM-points which are intersections with modular curves $\mathcal{V}(\Phi_m)$, $1 \leq m \leq 4\delta^5$, is bounded from above by some constant $C_8(\delta)$. Hence, it remains to bound the number of CM-points on $\mathcal{C}$ for which the bound (1.1) of Theorem 1 is satisfied. Let $\underline{x} = (x_1, x_2)$ be such a CM-point of discriminant (Δ_1, Δ_2). Lemma 3 together with Siegel's theorem (1.4) implies that $\max\{h(x_1), h(x_2)\}$ is bounded from above by

$$c_3(\varepsilon/2)|\Delta_i|^{1/2}h_{\Delta_i}^{-1+\varepsilon/2} \leq c_3(\varepsilon/2)c'_4(\varepsilon/2)|\Delta_i|^{\varepsilon/2}h_{\Delta_i}^{\varepsilon/2} \leq c_3(\varepsilon/2)c'_4(\varepsilon/2)|\Delta_i|^\varepsilon.$$

Combining this with (1.1) we obtain

$$h(\underline{x}) \leq \max\{h(x_1), h(x_2)\} \leq C'_9(\varepsilon, \delta, D)\max\{1, h(\mathcal{C})\}^{9\varepsilon},$$

where $C_9'(\varepsilon,\delta,D) = c_3(\varepsilon/2)c_4'(\varepsilon/2)C_1(\varepsilon,\delta,D)^{\varepsilon}$ is a positive constant. In order to apply Lemma 2 we change from $h(\cdot)$ to $h_2(\cdot)$ using (2.1). This yields

$$h_2(\underline{x}) \le C_{10}'(\varepsilon,\delta,D)\max\{1,h_2(\mathcal{C})\}^{9\varepsilon},$$

where $C_{10}'(\varepsilon,\delta,D) = C_9'(\varepsilon,\delta,D) + \frac{1}{2}\log 3$.

We now distinguish two cases: If

$$(5.1)\quad C_{11}'(\varepsilon,\delta,D) = \max\{1,(\delta_1+\delta_2)(\delta_*-1)C_{10}'(\varepsilon,\delta,D)\}^{1/(1-9\varepsilon)} < h_2(\mathcal{C}),$$

then $\underline{x}$ is a point of small height on $\mathcal{C}$, i.e. it satisfies (3.1). By Lemma 2 the number of points of small height on $\mathcal{C}$ is bounded by δ_*^2. This proves Theorem 2 in case (5.1) holds. If it does not, i.e. $C_{11}'(\varepsilon,\delta,D) \ge h_2(\mathcal{C})$, then a direct application of Theorem 1 yields

$$\max\{|\Delta_1|,|\Delta_2|\} < C_1(\varepsilon,\delta,D)\max\{1,C_9'(\varepsilon,\delta,D)\}^{8+\varepsilon} = C_{12}'(\varepsilon,\delta,D).$$

Now, the observation that there exist only finitely many CM-points of bounded discriminant completes the proof of Theorem 2. Its Corollary 3 follows from the fact that the Galois orbit of a CM-point of discriminant (Δ_1,Δ_2) intersects $\mathcal{C}$ in at least $[\mathbb{K}:\mathbb{Q}]^{-1}\max\{h_{\Delta_1},h_{\Delta_2}\}$ CM-points of the same discriminant, and from Siegel's theorem (1.4).

6. Proof of Theorem 3 and Corollary 2. Choose again a real number ε with $0 < \varepsilon < 1/10$. The proof imitates Section 5: By Bézout's theorem we know that the number of CM-points on the intersections of $\mathcal{C}$ with the modular curves $\mathcal{V}(\Phi_m)$, $1 \le m \le 4\delta^5$, is bounded from above by $C_8(\delta) > 0$. For any CM-point $\underline{x}$ on $\mathcal{C}$ of discriminant $(d_1f_1^2, d_2f_2^2)$ such that $d_1 \ne d_*$ and $d_2 \ne d_*$, Lemma 3 together with Lemma 5 implies the upper bound $c_3(\varepsilon/2)c_4(\varepsilon/2)|\Delta_1|^{\varepsilon}$ on $\max\{h(x_1),h(x_2)\}$. As in Section 5 we see that the number of such CM-points is bounded from above. Furthermore, since $c_4(\varepsilon)$ is effectively computable, their number can be also effectively bounded. To finish the proof, we have to bound effectively the number of CM-points on $\mathcal{C}$ of discriminant $(d_*f_1^2, df_2^2)$ or $(df_1^2, d_*f_2^2)$ for some fundamental discriminant $d \ne d_*$. For this, we use Lemma 1, whose proof we give now.

Proof of Lemma 1. Let $\underline{x}$ be a CM-point of discriminant

$$(\Delta_1,\Delta_2) = (d_1f_1^2, d_2f_2^2),\qquad d_1 \ne d_2,$$

on $\mathcal{C}$. Furthermore, assume that $d_2 \ne d_*$. The argument in the second section ("Première réduction, via la théorie du corps de classes") of [1] shows that $\max\{g_{\Delta_1},g_{\Delta_2}\} \le \delta D$ ([2]). Furthermore, this implies $c_{13}(\varepsilon)|\Delta_2|^{1/2-\varepsilon} \le \delta D$ by Lemma 6 and hence $|\Delta_2| < C_{13}(\varepsilon,\delta,D)$ for some constant $C_{13}(\varepsilon,\delta,D) > 0$. For every discriminant $\Delta_2 < 0$ there exist at most $\delta_1 h_{\Delta_2}$ CM-points on $\mathcal{C}$

[2] Proofs of the same conclusion, slightly more accessible than that in [1], can be found in [7, Proposition 3.1] and [23, Section IV.3].

whose discriminant is of the form $(d_* f_1^2, \Delta_2)$. Hence, the number of CM-points on $\mathcal{C}$ having discriminant $(d_1 f_1^2, d_2 f_2^2)$, $d_1 \neq d_2$, $d_2 \neq d_*$, is bounded from above by the sum $\delta_1 \sum_\Delta h_\Delta$, where Δ ranges through all discriminants of imaginary quadratic orders of absolute value up to $C_{13}(\varepsilon, \delta, D)$. In the same way, we bound the number of CM-points on $\mathcal{C}$ having discriminant $(d_1 f_1^2, d_2 f_2^2)$, where $d_1 \neq d_2$ and $d_1 \neq d_*$. ■

This completes the proof of Theorem 3. Its Corollary 2 can be inferred like Corollary 1 by using the effective lower bound on h_Δ from Gross–Zagier's (1.5) instead of Siegel's theorem (1.4).

7. Proof of Theorem 4. Using Lemma 1, we can restrict to find an effective bound on the number of CM-points having some discriminant $(\Delta_1, \Delta_2) = (f_1^2 d, f_2^2 d)$. Let $\underline{x} = (x_1, x_2) \in \mathcal{C}$ be such a CM-point. Under the assumption on $\mathcal{C}$, we can modify [13, Proposition 3] to obtain

Proposition 1. *There exist constants $C_{14}(\delta, D), C_{15}(\delta, D) > 0$ such that the following is true: If $\underline{x} \in \mathcal{C}$ is a CM-point of discriminant $(\Delta_1, \Delta_2) = (f_1^2 d, f_2^2 d)$ then*

$$\max\{|\Delta_1|, |\Delta_2|\} \leq C_{14}(\delta, D) \max\{1, h(\mathcal{C})\}^2, \tag{7.1}$$

or there exists some $1 \leq m \leq C_{15}(\delta, D)$ for which $\underline{x} \in \mathcal{V}(\Phi_m)$.

Proof. We concentrate on the parts of the proof of [13, Proposition 3] that have to be modified. In particular, we make free use of the results from there. From now on assume $|\Delta_1| = \max\{|\Delta_1|, |\Delta_2|\}$. We may and do also assume

$$x_1 = j\left(\frac{\Delta_1 + i f_1 \sqrt{|d|}}{2}\right) \quad \text{and} \quad x_2 = j\left(\frac{-b + i f_2 \sqrt{|d|}}{2a}\right)$$

with integers a, b, c such that $|\Delta_2| = 4ac - b^2$, $(a, b, c) = 1$ and either $-a < b \leq a < c$ or $0 \leq b \leq a = c$. Since (∞, ∞) is the only point of $\mathcal{C}$ at infinity, [13, Lemma 2] states now that $|x_1| > (\delta + 1)^4 H^{4D}$ implies $|x_2| > |x_1|^{(2\delta)^{-1}}$ for all $\underline{x} \in \mathcal{C}$. Indeed, by our assumption the polynomial of Q in the proof of that lemma is constant and hence the second case of the lemma cannot be realized for the given curve $\mathcal{C}$. Consequently, we only need to deal with CM-points near (∞, ∞), omitting [13, Lemmas 3 and 4] completely.

In summary, there exists a constant $C_{16}(\delta, D) > 0$ such that $|\Delta_1| \geq C_{16}(\delta, D) \max\{1, \log H\}^2$ implies $|x_2| > |x_1|^{(2\delta)^{-1}}$. By using both [13, (2.4)] and inequality (2.4) in the present article we infer that

$$\exp\left(\frac{k_2 f_2}{a} \sqrt{|d|}\, \pi\right) + 2310 \geq \exp((2\delta)^{-1} k_1 f_1 \sqrt{|d|}\, \pi) - 1193.$$

Hence, either $f_1^2 |d| = |\Delta_1|$ is absolutely bounded from above by some positive constant $C_{17}(\delta)$, or

$$\frac{k_2 f_2}{a}\sqrt{|d|}\,\pi \geq \frac{k_1 f_1}{4\delta}\sqrt{|d|}\,\pi,$$

which implies $1 \leq a \leq 4\delta(k_2/k_1)(f_2/f_1)$.

Now, the final part of the second section in [1] shows that there exists a constant $C_{18}(\delta, D) > 0$ bounding the numerator and denominator of $f = f_2/f_1$ from above [3]. Write $\operatorname{den}(f)$ for the denominator of f. Then,

$$\frac{-b + i f_2\sqrt{|d|}}{2a} = \begin{pmatrix} 2f\operatorname{den}(f) & -f_1 f_2\operatorname{den}(f)d - b\operatorname{den}(f) \\ 0 & 2a\operatorname{den}(f)\end{pmatrix}\frac{\Delta_1 + i f_1\sqrt{|d|}}{2}.$$

Hence, (x_1, x_2) is on a modular curve $\mathcal{V}(\Phi_m)$, where

$$1 \leq m \leq 4af\operatorname{den}(f)^2 \leq 16\delta k_2 C_{18}(\delta, D)^4 \leq C_{14}(\delta, D). \ \blacksquare$$

We return to the proof of Theorem 4. By Bézout's theorem, we may restrict ourselves to bounding the number of CM-points satisfying (7.1). For this, we use again our Lemma 2. Choose some $0 < \varepsilon < 1$. Lemma 3 together with Gross–Zagier's (1.5) implies for a CM-point $\underline{x} = (x_1, x_2)$ with discriminant (Δ_1, Δ_2) that

$$h(x_i) \leq c_3(\varepsilon)|\Delta_i|^{1/2} h_{\Delta_i}^{-1+\varepsilon} \leq c_3(\varepsilon)c_5(\varepsilon)^{-1+\varepsilon}|\Delta_i|^{1/2}(\log|\Delta_i|)^{-(1-\varepsilon)^2}$$

for $i \in \{1, 2\}$. Our argument in Section 5 shows that we may assume $h(\mathcal{C}) \geq 1$. Since $x^{1/2}(\log x)^{-(1-\varepsilon)^2}$ increases monotonically for $x \geq c_{16}(\varepsilon)$ we infer by using Proposition 1 that the height $h(\underline{x})$ is bounded from above by

$$c_{17}(\varepsilon)C_{14}(\delta, D)^{1/2} h(\mathcal{C})(\log C_{14}(\delta, D) + 2\log h(\mathcal{C}))^{-(1-\varepsilon)^2},$$

where $c_{17}(\varepsilon)$ is some positive constant. We deduce by use of (2.1) that

$$h_2(\underline{x}) \leq C_{18}(\delta, D)(\log C_{14}(\delta, D) + 2\log h_2(\mathcal{C}))^{-(1-\varepsilon)^2} h_2(\mathcal{C}) + (\log 3)/2$$

for some constant $C_{18}(\delta, D) > 0$. Thus, $\underline{x}$ is a point of small height (3.1) if

$$C_{18}(\delta, D)(\log C_{14}(\delta, D) + 2\log h_2(\mathcal{C}))^{-(1-\varepsilon)^2} + (\log 3)/(2h_2(\mathcal{C}))$$

is less than $(\delta_1 + \delta_2)^{-1}(\delta_* - 1)^{-1}$. It is easy to see that this condition amounts to demanding that $h_2(\mathcal{C}) > C_{19}(\delta, D)$ for some effectively computable con-

[3] There are two unimportant errors in the exposition of André [1]: First, he claims that the composite of the ring class fields associated with the orders of discriminants $f_1^2 d$ and $f_2^2 d$ is the ring class associated with the order of discriminant $\operatorname{lcm}(f_1, f_2)^2 d$. This is wrong for $d = -3$ and $d = -4$, while it is true for all other fundamental discriminants. However, it is well known that the latter field is an extension of the former of degree at most 3. This suffices to complete the proof. Second, one of the formulas contains a typing error: The product must be taken over all primes $p \mid f$, $p \nmid f_1$ instead of over all primes $p \mid f/f_1$.

stant $C_{19}(\delta, D) > 0$. For the same reason as in Section 5 we may do so. Finally, an application of Lemma 2 concludes the proof.

8. Proof of Theorem 5. Suppose there exist singular moduli $j(\tau_1)$ and $j(\tau_2)$ such that $j(\tau_1) + j(\tau_2) = 1$. Set $\Delta_i = \Delta_{\tau_i}$ for $i \in \{1, 2\}$ and assume $|\Delta_1| \geq |\Delta_2|$. We may also assume that $\Delta_1 \neq -3, -4, -7, -8$ since otherwise $\{j(\tau_1), j(\tau_2)\} \subseteq \{0, 1728, 3375, 8000\}$ (cf. [6, (12.20)]). Therefore, we have $|\Delta_1| \geq 11$ in the following. The discriminant of the imaginary quadratic order

$$\mathbb{Z} + \frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2}\mathbb{Z}$$

is Δ_1. By the irreducibility of the class equation this implies that there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ such that

$$j(\tau_1)^\sigma = j\left(\frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2}\right).$$

Furthermore, there exist integers a and b with $|b| \leq a \leq \sqrt{|\Delta_2|/3}$ such that

$$j(\tau_2)^\sigma = j\left(\frac{-b + i\sqrt{|\Delta_2|}}{2a}\right),$$

and therefore

$$j\left(\frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2}\right) + j\left(\frac{-b + i\sqrt{|\Delta_2|}}{2a}\right) - 1 = j(\tau_1)^\sigma + j(\tau_2)^\sigma - 1 = 0. \tag{8.1}$$

Without loss of generality we assume that

$$\tau_1 = \frac{\Delta_1 + i\sqrt{|\Delta_1|}}{2} \quad \text{and} \quad \tau_2 = \frac{-b + i\sqrt{|\Delta_2|}}{2a}.$$

Then $\mathrm{Im}(\tau_1) = \sqrt{|\Delta_1|}/2 > 1$, so [13, (2.4)] in combination with the bound (2.4) of the present article gives

$$-1194 + \exp(2\pi\,\mathrm{Im}(\tau_1)) \leq |j(\tau_1)| - 1 \leq |j(\tau_2)| \leq 2310 + \exp(2\pi\,\mathrm{Im}(\tau_2)),$$

which implies $\mathrm{Im}(\tau_2) > \log(-3504 + \exp(\pi\sqrt{11}))/(2\pi) > 1$. Thus, we can apply [13, (2.4)] for $\tau = \tau_1$ and $\tau = \tau_2$. This way, we infer from equation (8.1) that

$$|\exp(-2\pi i\tau_1) + \exp(-2\pi i\tau_2) + 1487| < 898.$$

Multiplication by $|\exp(2\pi i\tau_1)|$ yields

$$|1 + \exp(-2\pi i\tau_2 + 2\pi i\tau_1)| < 2385|\exp(2\pi i\tau_1)|.$$

More concretely, this means

$$|1 + \exp(\pi i(\Delta_1 + b/a))\exp(-\pi(\sqrt{|\Delta_1|} - \sqrt{|\Delta_2|}/a))| < 2385\exp(-\pi\sqrt{|\Delta_1|}). \tag{8.2}$$

Now $2385\exp(-\pi\sqrt{|\Delta_1|}) > 1/2$ if and only if $|\Delta_1| < (\log 4770)^2/\pi^2 < 8$. So by assumption, the left-hand side of the inequality must be less than or equal to 1/2. Below, we denote the principal branch of the logarithm on $\mathbb{C} \setminus (-\infty, 0]$ by log. Note that $|\log(1+u)| < 2|u|$ for $|u| \leq 1/2$. Setting

$$u = -1 - \exp(\pi i(\Delta_1 + b/a))\exp(-\pi(\sqrt{|\Delta_1|} - \sqrt{|\Delta_2|}/a))$$

we deduce that

$$\big|\log\big(-\exp(\pi i(\Delta_1 + b/a))\exp(-\pi(\sqrt{|\Delta_1|} - \sqrt{|\Delta_2|}/a))\big)\big|$$

is bounded from above by $4470\exp(-\pi\sqrt{|\Delta_1|})$. In this inequality, denote the interior of the absolute value on the left-hand side by Λ.

We want to express Λ as a linear form in logarithms of algebraic numbers with algebraic coefficients. Note that $\log(rz) = \log r + \log z$ for all positive reals r, and therefore

$$\Lambda = \log\big(-\exp(\pi i(\Delta_1 + b/a))\big) - \pi(\sqrt{|\Delta_1|} - \sqrt{|\Delta_2|}/a).$$

Denote the $2a$th root of unity $-\exp(\pi i(\Delta_1 + b/a))$ by ρ in the following. Inequality (8.2) above shows that $\rho \neq -1$. Then

$$\Lambda = \log\rho + (i\sqrt{|\Delta_1|} - i\sqrt{|\Delta_2|}/a)(i\pi).$$

In the general case of Theorem 1 we would now apply Baker's theorem on Λ, using the fact that $\exp(i\pi) = -1$ is algebraic. However, in this particular case a simpler argument is possible. Indeed, if $\rho \neq 1$ then

$$\begin{aligned} 4770\exp(-\pi\sqrt{|\Delta_1|}) > |\mathrm{Im}(\Lambda)| &= |\mathrm{Im}(\log\rho)| \\ &\geq \sin\left(\frac{\pi}{2a}\right) \geq \sin\left(\frac{\pi}{2\sqrt{|\Delta_1|}}\right), \end{aligned}$$

which is impossible for $|\Delta_1| \geq 11$. Hence, $\rho = 1$ and $\Lambda = \pi(\sqrt{|\Delta_1|} - \sqrt{|\Delta_2|}/a)$. This implies that if $a \neq 1$ then $|\Lambda| \geq \pi\sqrt{|\Delta_1|}/2 > 1/2$, which is a contradiction. Thus $a = 1$ and $\Lambda = \pi(\sqrt{|\Delta_1|} - \sqrt{|\Delta_2|})$. If $\Delta_1 \neq \Delta_2$ then

$$\sqrt{|\Delta_1|} - \sqrt{|\Delta_1| - 1} < |\Lambda| < 2385\exp(-\pi\sqrt{|\Delta_1|}),$$

which implies $|\Delta_1| < 11$. We infer $\Delta_1 = \Delta_2$, which gives a contradiction to (8.1) itself.

Acknowledgments. The results of this article were obtained during PhD studies of the author under supervision of Gisbert Wüstholz at ETH Zürich. The author thanks him and Philipp Habegger for all support and discussions during that time. Furthermore, the author has to acknowledge considerable help from Umberto Zannier and Yuri Bilu in improving the exposition. He is also in debt to the referee for an indication on how to simplify the proof of Proposition 1.

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

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.

[2] Y. Bilu, D. Masser, and U. Zannier, *An effective "Theorem of André" for CM-points on a plane curve*, unpublished preprint, 2011.

[3] Y. Bilu, D. Masser, and U. Zannier, *An effective "Theorem of André" for CM-points on a plane curve*, Math. Proc. Cambridge Philos. Soc. 154 (2013), 145–152.

[4] F. Breuer, *Heights of CM points on complex affine curves*, Ramanujan J. 5 (2001), 311–317.

[5] H. Cohen, *Number Theory. Vol. I. Tools and Diophantine Equations*, Grad. Texts in Math. 239, Springer, New York, 2007.

[6] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, Wiley, New York, 1989,

[7] B. Edixhoven, *Special points on the product of two modular curves*, Compos. Math. 114 (1998), 315–328.

[8] D. M. Goldfeld, *The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields*, Astérisque 41-42 (1977), 219–227.

[9] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225–320.

[10] F. Halter-Koch, *Geschlechtertheorie der Ringklassenkörper*, J. Reine Angew. Math. 250 (1971), 107–108.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford Univ. Press, Oxford, 2008.

[12] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq., Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[13] L. Kühne, *An effective result of André–Oort type*, Ann. of Math. (2) 176 (2012), 651–671.

[14] P. Philippon, *Sur des hauteurs alternatives. III*, J. Math. Pures Appl. (9) 74 (1995), 345–365.

[15] J. Pila, *Rational points of definable sets and results of André–Oort–Manin–Mumford type*, Int. Math. Res. Notices 2009, 2476–2507.

[16] J. Pila, *O-minimality and the André–Oort conjecture for $\mathbb{C}^n$*, Ann. of Math. (2) 173 (2011), 1779–1840.

[17] J. Pila and A. Wilkie, *The rational points of a definable set*, Duke Math. J. 133 (2006), 591–616.

[18] D. Roy and J. L. Thunder, *An absolute Siegel's lemma*, J. Reine Angew. Math. 476 (1996), 1–26; Addendum and erratum, ibid. 508 (1999), 47–51.

[19] W. M. Schmidt, *On heights of algebraic subspaces and diophantine approximations*, Ann. of Math. (2) 85 (1967), 430–472.

[20] I. R. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space*, 2nd ed., Springer, Berlin, 1994.

[21] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86.

[22] T. Tatuzawa, *On a theorem of Siegel*, Japan. J. Math. 21 (1951), 163–178.

[23] U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Ann. of Math. Stud. 181, Princeton Univ. Press, Princeton, NJ, 2012.

[24] S. Zhang, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. 8 (1995), 187–221.

Lars Kühne
SNS Pisa
Piazza dei Cavalieri 7
56126 Pisa, Italy
E-mail: lars.kuhne@sns.it

Received on 4.6.2012
and in revised form on 10.6.2013 (7083)