

Algebra & Number Theory

Volume 9

2015

No. 7

Singular moduli that are algebraic units

Philipp Habegger



Singular moduli that are algebraic units

Philipp Habegger

We prove that only finitely many j -invariants of elliptic curves with complex multiplication are algebraic units. A rephrased and generalized version of this result resembles Siegel's theorem on integral points of algebraic curves.

1. Introduction

A singular modulus is the j -invariant of an elliptic curve with complex multiplication; we treat them as complex numbers in this note. They are precisely the values of Klein's modular function $j : \mathbb{H} \rightarrow \mathbb{C}$ at imaginary quadratic arguments; here \mathbb{H} denotes the upper half-plane in \mathbb{C} . For example, $j(\sqrt{-1}) = 1728$. Singular moduli are algebraic integers and the set of all singular moduli is stable under ring automorphisms of \mathbb{C} . We refer to [Lang 1987] for such classical facts.

At the AIM workshop on unlikely intersections in algebraic groups and Shimura varieties in Pisa, 2011 David Masser, motivated by [Bilu et al. 2013], asked if there are only finitely many singular moduli that are algebraic units. Here we provide a positive answer to this question.

Theorem 1. *At most finitely many singular moduli are algebraic units.*

Our theorem relies on several tools: Liouville's inequality from diophantine approximation, Duke's equidistribution theorem [1988], its generalization due to Clozel–Ullmo [2004], and Colmez's lower bound [1998] for the Faltings height of an elliptic curve with complex multiplication supplemented by [Nakkajima and Taguchi 1991].

A numerical computation involving sage reveals that no singular modulus of degree at most 100 over the rationals is an algebraic unit. There may be no such units at all. Currently, there is no way to be sure as Duke's theorem is not known to be effective.

Below, we formulate and prove a general finiteness theorem reminiscent of Siegel's theorem on integral points on curves. We will see in particular that there are only finitely many singular moduli j such that $j + 1$ is a unit. Such j do exist, since for instance $j((\sqrt{-3} + 1)/2) = 0$ is a singular modulus.

MSC2010: primary 11G18; secondary 11G50, 11J86, 14G35, 14G40.

Keywords: elliptic curves, complex multiplication, heights.

Suppose that X is a geometrically irreducible, smooth, projective curve defined over a number field F . We write $F[X \setminus C]$ for the rational functions on X that are regular outside of a finite subset C of $X(F)$. Let \mathbb{O}_F be the ring of algebraic integers of F . A subset $M \subset X(F) \setminus C$ is called quasi-integral with respect to C if for all $f \in F[X \setminus C]$, there exists $\lambda \in F \setminus \{0\}$ such that $\lambda f(M) \subset \mathbb{O}_F$. By clearing denominators one sees that quasi-integral sets remain so after adding finitely many F -rational points. Siegel's theorem, see [Serre 1997, Chapter 7], states that a quasi-integral set is finite if $C \neq \emptyset$ and the genus of X is positive, or if the cardinality $\#C$ of C is at least 3.

Our extension of [Theorem 1](#) deals with the question of finiteness for quasi-integral sets of special points on modular curves. Special points generalize singular moduli, we provide a definition for them below. Only finitely many singular moduli are rational over a fixed number field. Thus we adapt the notion of quasi-integrality in the following way. Let \bar{F} be an algebraic closure of F and $\mathbb{O}_{\bar{F}}$ the ring of algebraic integers in \bar{F} . We again work with a finite set $C \subset X(\bar{F})$. A subset $M \subset X(\bar{F}) \setminus C$ is called quasi-algebraic-integral with respect to C if for all $f \in \bar{F}[X \setminus C]$ there is a $\lambda \in \bar{F} \setminus \{0\}$ such that $\lambda f(M) \subset \mathbb{O}_{\bar{F}}$.

Let us recall some classical facts about modular curves. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e., Γ contains the kernel of the reduction homomorphism $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for an $N \geq 1$. Then Γ acts on \mathbb{H} , as does any subgroup of $\mathrm{SL}_2(\mathbb{R})$, by fractional linear transformations. The quotient \mathbb{H}/Γ can be equipped with the structure of an algebraic curve Y_Γ defined over a number field F . This algebraic curve has a natural compactification X_Γ , which is a geometrically irreducible, projective, smooth curve over F . The points of $X_\Gamma \setminus Y_\Gamma$ are called the cusps of Y_Γ . We remark that $Y(1) = Y_{\mathrm{SL}_2(\mathbb{Z})}$ is the affine line, that the compactification is \mathbb{P}^1 , and that there is a single cusp ∞ . The natural map $\phi : Y_\Gamma \rightarrow Y(1)$ is algebraic. A point of $Y_\Gamma(\bar{F})$ is called special if it maps to a singular modulus under ϕ .

Theorem 2. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $F \subset \mathbb{C}$ a number field over which Y_Γ is defined. Let $C \subset X_\Gamma(\bar{F})$ be a finite set containing a point that is not a cusp of Y_Γ . Any set of special points in $Y_\Gamma(\bar{F})$ that is quasi-algebraic-integral with respect to C is finite.*

We require C to contain a noncusp for good reason. Indeed, as singular moduli are algebraic integers, the set of all singular moduli is a quasi-algebraic-integral subset of $Y(1)(\bar{\mathbb{Q}})$ with respect to $C = \{\infty\}$. We recover [Theorem 1](#) from [Theorem 2](#) by taking $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $C = \{0, \infty\}$. The proof of [Theorem 2](#) relies on the same basic strategy as [Theorem 1](#). However, instead of the Liouville inequality we require David and Hirata-Kohno's sharp lower bound for linear forms in elliptic logarithms [2009]. Earlier, Masser and others obtained lower bounds in this setting after A. Baker's initial work on linear forms in classical logarithms.

Our theorems are similar to M. Baker, Ih, and Rumely's result [2008] on roots of unity that are S -integral relative to a divisor of \mathbb{G}_m . Indeed, both finiteness results are based on an equidistribution statement. However, the Weil height of a root of unity is zero, whereas the height of a singular modulus can be arbitrarily large. Indeed, the quality of Colmez's growth estimate for the Faltings height plays a crucial role in our argument. Moreover, finiteness need not hold in the multiplicative setting if the support of the divisor consists of roots of unity. This is in contrast to [Theorem 1](#) where the support of the corresponding divisor is the singular modulus 0. Finally, our work considers only the case where S consists only of the Archimedean places whereas M. Baker, Ih, and Rumely also allow finite places.

Gross and Zagier [1985] gave a formula for the norm of the j -invariant of certain elliptic curves with complex multiplication. However, the author was unable to deduce the finiteness statement in [Theorem 1](#) from their result or from Dorman's extension [1988].

Habegger would like to thank the organizers of the AIM workshop in Pisa, 2011, for providing a stimulation environment. He also thanks Su-ion Ih for helpful remarks concerning his paper with M. Baker and Rumely.

2. Unitary Singular Moduli

In this section, c_1, c_2, \dots denote positive and absolute constants.

Let K be a number field. A finite place v of K is a non-Archimedean absolute value that restricts to the p -adic absolute value on \mathbb{Q} for some prime p . With this normalization we have $|p|_v = 1/p$. The completion of K with respect to v is a field extension of degree d_v of the completion of \mathbb{Q} with respect to the p -adic absolute value. Let J be an algebraic number in a number field K . The absolute logarithmic Weil height of J , or just height for short, is

$$h(J) = \frac{1}{[K : \mathbb{Q}]} \left(\sum_{\sigma} \log \max\{1, |\sigma(J)|\} + \sum_v d_v \log \max\{1, |J|_v\} \right)$$

where σ runs over all field embeddings $\sigma : K \rightarrow \mathbb{C}$ and v runs over all finite places of K . It is well-known that $h(J)$ does not change when we replace K by another number field containing J . For this and other facts on heights we refer to Sections 1.5 and 1.6 of [\[Bombieri and Gubler 2006\]](#).

We state a height lower bound for singular moduli that follows easily from a result of Colmez and of Nakkajima–Taguchi. See [\[Poonen 2001, Lemma 3\]](#) for a similar argument.

Lemma 3. *Let J be a singular modulus attached to an elliptic curve whose endomorphism ring is an order with discriminant $\Delta < 0$. Then*

$$h(J) \geq c_2 \log |\Delta| - c_3. \tag{1}$$

Proof. We write $\Delta = \Delta_0 f^2$ where $\Delta_0 < 0$ is a fundamental discriminant and f is the conductor of the endomorphism ring of E , an elliptic curve attached to j . In Corollaire 7, Colmez [1998] proved (1) with $h(J)$ replaced by the stable Faltings height of E when Δ is a fundamental discriminant, i.e., if $f = 1$. For $f > 1$ Nakkajima and Taguchi [1991] found that one must add

$$\frac{1}{2} \log f - \frac{1}{2} \sum_{p|f} e_f(p) \log p$$

to the stable Faltings height; here the sum runs over prime divisors p of f and

$$e_f(p) = \frac{1 - \chi(p)}{p - \chi(p)} \frac{1 - p^{-n}}{1 - p^{-1}}$$

if $p^n | f$ but $p^{n+1} \nmid f$ and $\chi(p)$ is Kronecker’s symbol $(\frac{\Delta_0}{p})$. The arguments in the proof of [Habegger 2010, Lemma 4.2] give $\sum_{p|f} e_f(p) \log p \leq c_1 \log \log \max\{3, f\}$. Therefore, the stable Faltings height of E is logarithmically bounded from below in terms of $|\Delta_0 f^2| = |\Delta|$.

By [Silverman 1986, Proposition 2.1], we can replace the stable Faltings height by $h(J)$ at the cost of adjusting the constants. □

Our strategy to prove Theorem 1 is as follows. Let J and Δ be as in Lemma 3. Assume in addition that J is an algebraic unit. We will find an upper bound for $h(J)$ that contradicts the previous lemma for sufficiently large $|\Delta|$. This will leave us with only finitely many Δ and hence finitely many J , as we will see.

The norm of J is ± 1 and the finite places do not contribute to the height of the algebraic integer J . Thus we can rewrite

$$h(J) = \frac{1}{D} \sum_{|\sigma(J)| > 1} \log |\sigma(J)| = -\frac{1}{D} \sum_{|\sigma(J)| < 1} \log |\sigma(J)| \tag{2}$$

where $D = [\mathbb{Q}(J) : \mathbb{Q}]$ and where the sums run over field embeddings $\sigma : \mathbb{Q}(J) \rightarrow \mathbb{C}$.

For each σ we have $\sigma(J) = j(\tau_\sigma)$ for some τ_σ in the classical fundamental domain

$$\mathcal{F} = \{ \tau \in \mathbb{H}; \operatorname{Re}(\tau) \in (-1/2, 1/2], |\tau| \geq 1 \text{ and } \operatorname{Re}(\tau) \geq 0 \text{ if } |\tau| = 1 \}$$

of the action of $\operatorname{SL}_2(\mathbb{Z})$ on \mathbb{H} .

To bound the right-hand side of (2) from above we must control those conjugates $\sigma(J)$ that are small in modulus. Let $\epsilon \in (0, 1]$ be a parameter that is to be determined; the c_i will not depend on ϵ . We define

$$\Sigma_\epsilon = \{ \tau \in \mathcal{F}; |j(\tau)| < \epsilon \}.$$

The field embeddings that contribute most to the height of J are in

$$\Gamma_\epsilon = \{\sigma : \mathbb{Q}(J) \rightarrow \mathbb{C}; \tau_\sigma \in \Sigma_\epsilon\}.$$

We estimate their number using equidistribution in the next lemma.

Lemma 4. *We have $\#\Gamma_\epsilon \leq c_6 \epsilon^{2/3} D$ if D is sufficiently large with respect to ϵ .*

Proof. Let μ denote the hyperbolic measure on \mathcal{F} with total mass 1, i.e.,

$$\mu(\Sigma) = \frac{3}{\pi} \int_{x+yi \in \Sigma} \frac{dx dy}{y^2} \quad (3)$$

for a measurable subset $\Sigma \subset \mathcal{F}$. Duke [1988] proved that the τ_σ are equidistributed with respect to μ as $\Delta \rightarrow -\infty$ runs over fundamental discriminants. For general discriminants, equidistribution follows from [Clozel and Ullmo 2004]. So, for $\Delta \rightarrow -\infty$, we get $|\#\Gamma_\epsilon/D - \mu(\Sigma_\epsilon)| \rightarrow 0$. To prove the lemma we will bound $\mu(\Sigma_\epsilon)$ in terms of ϵ .

Let ζ be the unique root of unity in \mathbb{H} of order 6; it is a zero of j . By [Lang 1987, Chapter 3, Theorem 2], Klein's modular function j has a triple zero at ζ and at ζ^2 and does not vanish anywhere else on $\overline{\mathcal{F}}$, the closure of \mathcal{F} in \mathbb{H} . So $\tau \mapsto j(\tau)(\tau - \zeta)^{-3}(\tau - \zeta^2)^{-3}$ does not vanish on $\overline{\mathcal{F}}$. Now j has a pole at infinity and so $|j(\tau)| > 1$ if the imaginary part of τ is sufficiently large. Therefore

$$|j(\tau)| \geq c_4 |\tau - \zeta|^3 |\tau - \zeta^2|^3 \geq \frac{c_4}{8} \min\{|\tau - \zeta|, |\tau - \zeta^2|\}^3 \quad (4)$$

for all $\tau \in \overline{\mathcal{F}}$ with $|j(\tau)| \leq 1$ where $\max\{|\tau - \zeta|, |\tau - \zeta^2|\} \geq |\zeta - \zeta^2|/2 = \frac{1}{2}$ was used in the second inequality. Because the imaginary part of an element in \mathcal{F} is at least $\sqrt{3}/2$ we can use (3) to estimate $\mu(\Sigma_\epsilon) \leq c_5 \epsilon^{2/3}$. \square

Using this lemma with (2) we can bound the height of J from above as

$$\begin{aligned} h(J) &= -\frac{1}{D} \left(\sum_{|\sigma(J)| < \epsilon} \log|\sigma(J)| + \sum_{\epsilon \leq |\sigma(J)| < 1} \log|\sigma(J)| \right) \\ &\leq c_6 \epsilon^{2/3} \max_{|\sigma(J)| < \epsilon} \log(|\sigma(J)|^{-1}) + |\log \epsilon|. \end{aligned} \quad (5)$$

Soon we will use Liouville's inequality from diophantine approximation to bound $|j(\tau_\sigma)|$ from below if $\sigma \in \Gamma_\epsilon$. To do this, we require a bound for the height of τ_σ .

Lemma 5. *Each τ_σ is imaginary quadratic and we have $h(\tau_\sigma) \leq \log \sqrt{|\Delta|}$.*

Proof. We abbreviate $\tau = \tau_\sigma$ and decompose $\Delta = \Delta_0 f^2$ as in the proof of Lemma 3. The endomorphism ring mentioned in Lemma 3 can be identified with $\mathbb{Z} + \omega f \mathbb{Z} \subset \mathbb{C}$ where $\omega = (\sqrt{\Delta_0} + \Delta_0)/2$. This ring acts on the lattice $\mathbb{Z} + \tau \mathbb{Z}$. So there exist

$a, b, c, d \in \mathbb{Z}$ with $\omega f = a + b\tau$, $\omega f \tau = c + d\tau$ and $b \neq 0$. We substitute the first equality into the second one and obtain

$$b\tau^2 + (a - d)\tau - c = 0. \tag{6}$$

Hence, τ is imaginary quadratic. We note that ωf is a root of $T^2 - (a+d)T + ad - bc$. The discriminant of this polynomial is $(a + d)^2 - 4(ad - bc) = (\omega - \bar{\omega})^2 f^2 = \Delta$. Hence $\tau = (-(a - d) \pm \sqrt{\Delta})/2b$ and therefore $|\tau|^2 = ((a - d)^2 + |\Delta|)/(2b)^2$.

As τ lies in \mathcal{F} , we have $|\operatorname{Re}(\tau)| \leq 1/2$. This inequality implies $|a - d| \leq |b|$ and hence $|\tau|^2 \leq (b^2 + |\Delta|)/(2b)^2$. By Proposition 1.6.6 of [Bombieri and Gubler 2006] the value $2h(\tau)$ is at most the logarithmic Mahler measure of $bT^2 + (a - d)T - c$. So $2h(\tau) \leq \log(|b||\tau|^2) \leq \log(|b|/4 + |\Delta|/(4|b|))$. The imaginary part of τ is at least $\sqrt{3}/2$ and so $|b| \leq \sqrt{|\Delta|/3}$. As $x \mapsto x + |\Delta|/x$ is decreasing on $[1, \sqrt{|\Delta|}]$, we conclude $2h(\tau) \leq \log((1 + |\Delta|)/4) \leq \log|\Delta|$. \square

Now we use Liouville’s inequality to bound the conjugates of J away from zero.

Lemma 6. *We have $\log|\sigma(J)| \geq -c_8 \log|\Delta|$ for any $\sigma : \mathbb{Q}(J) \rightarrow \mathbb{C}$.*

Proof. We retain the notation of the proof of Lemma 4 and assume $|\tau_\sigma - \zeta| \leq |\tau_\sigma - \zeta^2|$; the reverse case is similar. According to (4), we have

$$|\sigma(J)| = |j(\tau_\sigma)| \geq c_7 |\tau_\sigma - \zeta|^3. \tag{7}$$

We also remark that $\tau_\sigma \neq \zeta$ since $\sigma(J) \neq 0 = j(\zeta)$. Liouville’s inequality, see [Bombieri and Gubler 2006, Theorem 1.5.21], tells us

$$-\log|\tau_\sigma - \zeta| \leq [\mathbb{Q}(\tau_\sigma, \zeta) : \mathbb{Q}](h(\tau_\sigma) + h(\zeta) + \log 2).$$

But τ_σ and ζ are imaginary quadratic, so $[\mathbb{Q}(\tau_\sigma, \zeta) : \mathbb{Q}] \leq 4$. Moreover, $h(\zeta) = 0$ as ζ is a root of unity. The bound for $h(\tau_\sigma)$ from Lemma 5 yields

$$-\log|\tau_\sigma - \zeta| \leq 4 \log(2\sqrt{|\Delta|}).$$

The lemma now follows from $|\Delta| \geq 3$ and (7). \square

Proof of Theorem 1. We will see soon how to fix ϵ in terms of the c_i . By a classical result of Hecke and Heilbronn [Davenport 1980, Chapter 21], there are only finitely many singular moduli whose degree over \mathbb{Q} are bounded by a prescribed constant. So there is no loss of generality if we assume that D is large enough as in Lemma 4.

We use the previous lemma to bound the first term in (5) from above. Thus

$$h(J) \leq c_6 c_8 \epsilon^{2/3} \log|\Delta| + |\log \epsilon|.$$

We fix ϵ to satisfy $c_6 c_8 \epsilon^{2/3} < c_2/2$, where c_2 comes from the height lower bound in Lemma 3. With this choice we conclude that $|\Delta|$ is bounded from above by an absolute constant. By Lemma 5 and Northcott’s theorem [Bombieri and Gubler 2006, Theorem 1.6.8] there are only finitely many possible τ_σ and thus only finitely many possible J . \square

3. Proof of Theorem 2

We begin by stating a special case of David and Hirata–Kohno’s deep lower bound for linear forms in n elliptic logarithms if $n = 2$ and when the elliptic logarithms are periods. Let E be an elliptic curve defined over a number field in \mathbb{C} . We fix a Weierstrass equation for E with coefficients in the said number field and a Weierstrass- \wp function that induces a uniformization $\mathbb{C} \rightarrow E(\mathbb{C})$. This is a group homomorphism whose kernel $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ is a discrete subgroup of \mathbb{C} . We start numbering constants anew.

Lemma 7. *Let $d \geq 1$. There exists a constant $c_1 > 0$ depending on E , d , the choice of Weierstrass equation, and the choice $\omega_{1,2}$ with the following property. Suppose $\alpha, \beta \in \mathbb{C}$ are algebraic over \mathbb{Q} of degree at most d and $\max\{1, h(\alpha), h(\beta)\} \leq \log B$ for some real number $B > 0$. If $\alpha\omega_1 + \beta\omega_2 \neq 0$, then*

$$\log|\alpha\omega_1 + \beta\omega_2| \geq -c_1 \log B. \quad (8)$$

Proof. This follows from [David and Hirata-Kohno 2009, Theorem 1.6]. \square

In our application, the $\log B$ from (8) will be approximately $\log|\Delta|$ and will compete directly with the logarithmic lower bound of Lemma 3. It is thus essential that David and Hirata-Kohno’s inequality is logarithmic in B . A worse dependency, such as $-c_1(\log B)(\log \log B)$, would not suffice.

We further distill this result into a formulation adapted to our application.

Lemma 8. *Let $\eta \in \mathbb{H}$ be such that $j(\eta)$ is an algebraic number. There exists a constant $c_2 > 0$ which may depend on η with the following property. If $\tau \neq \eta \in \mathbb{H}$ is imaginary quadratic with $\max\{1, h(\tau)\} \leq \log B$ for some real number $B > 0$, then*

$$\log|\tau - \eta| \geq -c_2 \log B.$$

Proof. The algebraic number $j(\eta)$ is the j -invariant on an elliptic curve as introduced before Lemma 7. We may assume that the periods $\omega_{1,2}$ satisfy $\eta = \omega_2/\omega_1$. As $\tau \neq \eta$, Lemma 7 with $\alpha = \tau$ and $\beta = -1$ implies $\log|\tau\omega_1 - \omega_2| \geq -c_1 \log B$. We subtract $\log|\omega_1|$ and obtain $\log|\tau - \eta| \geq -c_1 \log B - \log|\omega_1|$. This lemma follows with an appropriate c_2 as $\log B \geq 1$. \square

Let us suppose that Γ , F , and C are as in Theorem 2. We recall that ϕ is the natural morphism $Y_\Gamma \rightarrow Y(1)$ and we may regard it as an element in the function field of X . We abbreviate $X = X_\Gamma$. In the following, we enlarge F to a number field for which $X(F)$ contains C and all poles of ϕ .

By hypothesis there is a $P_0 \in C$ that is not a cusp of Y_Γ . We write $J_0 \in F$ for the value of ϕ at P_0 . The Riemann–Roch theorem provides a nonconstant, rational function $\psi \in F[X \setminus \{P_0\}]$ that vanishes at the poles of ϕ . As ψ is regular outside of P_0 , it must have a pole at P_0 .

The functions ϕ and ψ^{-1} are algebraically dependent, i.e., there is an irreducible polynomial $R \in F[U, V]$ with $R(\phi, \psi^{-1}) = 0$. We observe $\deg_U R > 0$.

Lemma 9. *There exists a constant $c_5 \in (0, 1]$ which depends only on R with the following property. Let $K \supset F$ be a number field and $|\cdot|$ an absolute value on K that extends the Archimedean absolute value on \mathbb{Q} . If $u \in K$ and $v \in K \setminus \{0\}$ with $R(u, v) = 0$, $|v| < c_5$, and $u \neq J_0$, then $\log|u - J_0| < (\log|v|)/(2 \deg_U R)$.*

Proof. In this proof, $c_{3,4} > 0$ depend only on R . We put $e = \deg_U R$ and write $R = r_0 + (U - J_0)r_1 + \dots + (U - J_0)^e r_e$, with $r_i \in F[V]$ and $r_e \neq 0$.

By construction, the poles of ϕ are among the poles of ψ^{-1} . So ϕ , and thus $\phi - J_0$, are integral over the ring $F[\psi^{-1}]$, see for example [Matsumura 1989, Theorem 10.4]. Hence, r_e is constant and without loss of generality we may assume $r_e = 1$. Next we claim $r_i(0) = 0$ if $0 \leq i \leq e - 1$. If this were not the case, we could find $J'_0 \neq J_0$ with $R(J'_0, 0) = 0$. This is impossible by our choice of ψ . Therefore,

$$R = VQ + (U - J_0)^e$$

for some $Q \in F[U, V]$ with $\deg_U Q \leq e - 1$.

Now let u and v be as in the hypothesis; we will see how to fix $c_5 \in (0, 1]$ below. We have $|u - J_0|^e = |vQ(u, v)|$ and $|vQ(u, v)| \leq c_3 \max\{1, |u|\}^{e-1}$ as $|v| \leq 1$. If $|u| \geq \max\{1, 2|J_0|\}$, then $|u - J_0| \geq |u| - |J_0| \geq |u|/2$ and so $|u|^e \leq 2^e c_3 |u|^{e-1}$. We find $|u| \leq 2^e c_3$. In this case, $|u - J_0|^e = |vQ(u, v)| \leq c_4 |v|$ for some $c_4 \geq 1$. After adjusting, c_4 the same bound holds if $|u| < \max\{1, 2|J_0|\}$. We set $c_5 = c_4^{-2}$ and observe $c_4 |v| < |v|^{1/2}$ if $|v| < c_5$. Thus $|u - J_0|^e \leq |v|^{1/2} < 1$ and the lemma follows on taking the logarithm. \square

Let us now prove Theorem 2. For this we must verify that a set $M \subset X(\bar{F})$ of special points that is quasi-algebraic-integral with respect to C is finite. By definition, M cannot contain the pole of ψ and without loss of generality we may assume that M does not contain its zeros either. Finally, we may assume that $J_0 \notin \phi(M)$. Let $\lambda \in F \setminus \{0\}$ satisfy $\lambda\psi(M) \subset \mathbb{O}_{\bar{F}}$. To simplify notation we replace $\lambda\psi$ by ψ and adapt R accordingly.

We will use c_6, c_7, \dots to denote positive constants that may depend on Γ, F, C , and M . Suppose $P \in M$ and let $K \subset \bar{F}$ be a number field containing F and the values $\psi(P), \phi(P)$. Then, as usual,

$$\begin{aligned} h(\psi(P)) &= \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(\psi(P))| > 1} \log|\sigma(\psi(P))| \\ &= \frac{1}{[K : \mathbb{Q}]} \left(\sum_{1 < |\sigma(\psi(P))| \leq c_5^{-1}} \log|\sigma(\psi(P))| + \sum_{|\sigma(\psi(P))| > c_5^{-1}} \log|\sigma(\psi(P))| \right) \\ &\leq -\log c_5 + \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(\psi(P))| > c_5^{-1}} \log|\sigma(\psi(P))|, \end{aligned}$$

where the sums run over field embeddings $\sigma : K \rightarrow \mathbb{C}$. Say $J = \phi(P) \in K$, then $R(J, \psi(P)^{-1}) = 0$. We apply [Lemma 9](#) to $u = J$ and $v = \psi(P)$ to obtain

$$h(\psi(P)) \leq c_6 \left(1 + \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(J - J_0)| < 1} -\log|\sigma(J - J_0)| \right). \quad (9)$$

We have already seen that R is not divisible by a linear polynomial in the variable V . So, [\[Bilu and Masser 2006, Proposition 5\]](#) and $R(J, \psi(P)^{-1}) = 0$ allow us to bound $h(J)$ from above linearly in terms of $h(\psi(P)^{-1}) = h(\psi(P))$. Together with [\(9\)](#) we get

$$\begin{aligned} h(J) &\leq c_7 \left(1 + \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(J - J_0)| < 1} -\log|\sigma(J - J_0)| \right) \\ &\leq c_7 \left(|\log \epsilon| + \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(J - J_0)| < \epsilon} -\log|\sigma(J - J_0)| \right) \end{aligned} \quad (10)$$

for any $\epsilon \in (0, 1/2]$.

The points in M are special, so J is a singular modulus. An elliptic curve attached to J has complex multiplication by an order with discriminant $\Delta < 0$. As in the previous section, we will find an upper bound for $|\Delta|$.

For any embedding $\sigma : K \rightarrow \mathbb{C}$ we fix $\tau_\sigma \in \mathcal{F}$ with $j(\tau_\sigma) = \sigma(J)$. We now proceed as near [\(4\)](#) and apply [\[Lang 1987, Chapter 3, Theorem 2\]](#). If ϵ is sufficiently small and if $|\sigma(J - J_0)| < \epsilon$, then

$$|\sigma(J - J_0)| \geq \begin{cases} c_8 |\tau_\sigma - \eta_\sigma|^3 & \text{if } J_0 = 0, \\ c_8 |\tau_\sigma - \eta_\sigma|^2 & \text{if } J_0 = 1728, \\ c_8 |\tau_\sigma - \eta_\sigma| & \text{else.} \end{cases} \quad (11)$$

for some $\eta_\sigma \in \overline{\mathcal{F}}$ with $j(\eta_\sigma) = \sigma(J_0)$. It is harmless that there are 2 choices for η_σ on the boundary of $\overline{\mathcal{F}}$. We note that η_σ depends only on the base point J_0 and that τ_σ is imaginary quadratic. Thus [Lemma 8](#) and the height bound for τ_σ in [Lemma 5](#) yield $\log|\sigma(J - J_0)| \geq -c_9 \log|\Delta|$. We use this inequality and [\(10\)](#) to bound

$$h(J) \leq c_{10} \left(\log|\epsilon| + \log|\Delta| \frac{\#\{\sigma : K \rightarrow \mathbb{C}; |\sigma(J - J_0)| < \epsilon\}}{[K : \mathbb{Q}]} \right)$$

for all $\epsilon \in (0, 1/2]$.

The rest of the proof resembles the proof of [Theorem 1](#). Indeed, we may assume that $[\mathbb{Q}(J) : \mathbb{Q}]$ is sufficiently large and as in [Lemma 4](#) we use equidistribution to prove that $[K : \mathbb{Q}]^{-1} \#\{\sigma : K \rightarrow \mathbb{C}; |\sigma(J - J_0)| < \epsilon\}$ is bounded from above linearly by a fixed power, derived from [\(11\)](#), of ϵ . Finally, we again use the height lower bound of [Lemma 3](#) to fix an appropriate ϵ which leads to a bound on $|\Delta|$. As before, this leaves us with only finitely many possibilities for $J = \phi(P)$. \square

References

- [Baker et al. 2008] M. Baker, S.-i. Ih, and R. Rumely, “A finiteness property of torsion points”, *Algebra Number Theory* **2:2** (2008), 217–248. [MR 2009g:11078](#) [Zbl 1182.11030](#)
- [Bilu and Masser 2006] Y. F. Bilu and D. Masser, “A quick proof of Sprindzhuk’s decomposition theorem”, pp. 25–32 in *More sets, graphs and numbers*, edited by E. Györi et al., Bolyai Soc. Math. Stud. **15**, Springer, Berlin, 2006. [MR 2007b:11031](#) [Zbl 1147.11018](#)
- [Bilu et al. 2013] Y. Bilu, D. Masser, and U. Zannier, “An effective “theorem of André” for CM -points on a plane curve”, *Math. Proc. Cambridge Philos. Soc.* **154:1** (2013), 145–152. [MR 3002589](#)
- [Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs **4**, Cambridge Univ. Press, 2006. [MR 2007a:11092](#) [Zbl 1115.11034](#)
- [Clozel and Ullmo 2004] L. Clozel and E. Ullmo, “Équidistribution des points de Hecke”, pp. 193–254 in *Contributions to automorphic forms, geometry, and number theory*, edited by H. Hida et al., Johns Hopkins Univ. Press, Baltimore, MD, 2004. [MR 2005f:11090](#) [Zbl 1068.11042](#)
- [Colmez 1998] P. Colmez, “Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe”, *Compositio Math.* **111:3** (1998), 359–368. [MR 99e:11074](#) [Zbl 0918.11025](#)
- [Davenport 1980] H. Davenport, *Multiplicative number theory*, 2nd ed., Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980. [MR 82m:10001](#) [Zbl 0453.10002](#)
- [David and Hirata-Kohno 2009] S. David and N. Hirata-Kohno, “Linear forms in elliptic logarithms”, *J. Reine Angew. Math.* **628** (2009), 37–89. [MR 2010c:11084](#) [Zbl 1169.11034](#)
- [Dorman 1988] D. R. Dorman, “Special values of the elliptic modular function and factorization formulae”, *J. Reine Angew. Math.* **383** (1988), 207–220. [MR 89k:11026](#) [Zbl 0626.10022](#)
- [Duke 1988] W. Duke, “Hyperbolic distribution problems and half-integral weight Maass forms”, *Invent. Math.* **92:1** (1988), 73–90. [MR 89d:11033](#) [Zbl 0628.10029](#)
- [Gross and Zagier 1985] B. H. Gross and D. B. Zagier, “On singular moduli”, *J. Reine Angew. Math.* **355** (1985), 191–220. [MR 86j:11041](#) [Zbl 0545.10015](#)
- [Habegger 2010] P. Habegger, “Weakly bounded height on modular curves”, *Acta Math. Vietnam.* **35:1** (2010), 43–69. [MR 2011g:11124](#) [Zbl 1253.11070](#)
- [Lang 1987] S. Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics **112**, Springer, New York, 1987. [MR 88c:11028](#) [Zbl 0615.14018](#)
- [Matsumura 1989] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, 1989. [MR 90i:13001](#) [Zbl 0666.13002](#)
- [Nakkajima and Taguchi 1991] Y. Nakkajima and Y. Taguchi, “A generalization of the Chowla-Selberg formula”, *J. Reine Angew. Math.* **419** (1991), 119–124. [MR 92g:11113](#) [Zbl 0721.11045](#)
- [Poonen 2001] B. Poonen, “Spans of Hecke points on modular curves”, *Math. Res. Lett.* **8:5-6** (2001), 767–770. [MR 2002k:11092](#) [Zbl 1081.11043](#)
- [Serre 1997] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, 3rd ed., Aspects of Mathematics **15**, Friedr. Vieweg & Sohn, Braunschweig, 1997. [MR 2000m:11049](#) [Zbl 0863.14013](#)
- [Silverman 1986] J. H. Silverman, “Heights and elliptic curves”, pp. 253–265 in *Arithmetic geometry* (Storrs, Conn., 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986. [MR 861979](#) [Zbl 0603.14020](#)

Communicated by Joseph Silverman

Received 2014-03-19

Revised 2015-05-30

Accepted 2015-07-15

philipp.habegger@unibas.ch

Departement Mathematik und Informatik, Universität Basel,
Spiegelgasse 1, CH-4051 Basel, Switzerland

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Roger Heath-Brown	Oxford University, UK	Michel van den Bergh	Hasselt University, Belgium
Craig Huneke	University of Virginia, USA	Marie-France Vignéras	Université Paris VII, France
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Kei-Ichi Watanabe	Nihon University, Japan
János Kollár	Princeton University, USA	Efim Zelmanov	University of California, San Diego, USA
Yuri Manin	Northwestern University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US \$255/year for the electronic version, and \$440/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2015 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 9 No. 7 2015

Singular moduli that are algebraic units	1515
PHILIPP HABEGGER	
Irreducibility of the Gorenstein loci of Hilbert schemes via ray families	1525
GIANFRANCO CASNATI, JOACHIM JELISIEJEW and ROBERTO NOTARI	
p-adic heights of Heegner points on Shimura curves	1571
DANIEL DISEGNI	
Calculabilité de la cohomologie étale modulo ℓ	1647
DAVID A. MADORE and FABRICE ORGOGOZO	