

Singular Moduli That Are Algebraic Units

P. Habegger

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2015-24
August 2015

www.math.unibas.ch

SINGULAR MODULI THAT ARE ALGEBRAIC UNITS

P. HABEGGER

ABSTRACT. 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 $j : \mathbf{H} \rightarrow \mathbf{C}$ at imaginary quadratic arguments; here \mathbf{H} denotes the upper half-plane in \mathbf{C} . For example, $j(\sqrt{-1}) = 1728$. Singular moduli are algebraic integers and their entirety is stable under ring automorphisms of \mathbf{C} . We refer to Lang's book [12] for such classical facts.

At the AIM workshop on unlikely intersections in algebraic groups and Shimura varieties in Pisa, 2011 David Masser, motivated by [2], 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 [9], its generalization due to Clozel-Ullmo [5], and Colmez's lower bound for the Faltings height of an elliptic curve with complex multiplication [6] supplemented by work of Nakkajima-Taguchi [14].

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 singular moduli j such that $j+1$ is a unit. Now there are examples, as $j((\sqrt{-3}+1)/2) = 0$ is a singular modulus.

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 \mathcal{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 any $f \in F[X \setminus C]$ there exists $\lambda \in F \setminus \{0\}$ such that $\lambda f(M) \subset \mathcal{O}_F$. By clearing denominators one sees that quasi-integral sets remain so after adding finitely many F -rational points. Siegel's Theorem, cf. Chapter 7 [16], states that a quasi-integral sets is finite if $C \neq \emptyset$ and the genus of X is positive, or if the cardinality $\#C$ of C is at least 3.

2010 *Mathematics Subject Classification.* 11G18 (primary), and 11G50, 11J86, 14G35, 14G40 (secondary).

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 \overline{F} be an algebraic closure of F and $\mathcal{O}_{\overline{F}}$ the ring of algebraic integers in \overline{F} . We again work with a finite set $C \subset X(\overline{F})$. A subset $M \subset X(\overline{F}) \setminus C$ is called quasi-algebraic-integral with respect to C if for all $f \in \overline{F}[X \setminus C]$ there is $\lambda \in \overline{F} \setminus \{0\}$ such that $\lambda f(M) \subset \mathcal{O}_{\overline{F}}$.

Let us recall some classical facts about modular curves. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$, i.e. Γ contains the kernel of the reduction homomorphism $\mathrm{SL}_2(\mathbf{Z}) \rightarrow \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ for an $N \geq 1$. Then Γ acts on \mathbf{H} , as does any subgroup of $\mathrm{SL}_2(\mathbf{R})$, by fractional linear transformations. The quotient \mathbf{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 $Y(1) = Y_{\mathrm{SL}_2(\mathbf{Z})}$ is the affine line, that the compactification is \mathbf{P}^1 , and that there is a single cusp ∞ . The natural map $\phi : Y_\Gamma \rightarrow Y(1)$ is algebraic. A point of $Y_\Gamma(\overline{F})$ is called special if it maps to a singular modulus under ϕ .

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

We require C to contain a non-cusp for good reason. Indeed, as singular moduli are algebraic integers, their totality is a quasi-algebraic-integral subset of $Y(1)(\overline{\mathbf{Q}})$ with respect to $C = \{\infty\}$. We recover Theorem 1 from Theorem 2 on taking $\Gamma = \mathrm{SL}_2(\mathbf{Z})$ 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 [7]. 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 reminiscent to M. Baker, Ih, and Rumely's result [1] on roots of unity that are S -integral relative to a divisor of \mathbf{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 [10] 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 [8] extension.

The author 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 ν of K is a non-Archimedean absolute value that restricts to the p -adic absolute value on \mathbf{Q} for some prime p . With this normalization we have $|p|_\nu = 1/p$. The completion of K with respect to ν is a field extension of degree d_ν of the completion of \mathbf{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

$$h(J) = \frac{1}{[K : \mathbf{Q}]} \left(\sum_{\sigma} \log \max\{1, |\sigma(J)|\} + \sum_{\nu} d_{\nu} \log \max\{1, |J|_{\nu}\} \right)$$

where σ runs over all field embeddings $\sigma : K \rightarrow \mathbf{C}$ and ν runs over all finite places of K . It is well-known that $h(J)$ does not change when replacing 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's book [4].

We state a height lower bound for singular moduli that follows easily from a result of Colmez and of Nakkajima-Taguchi. See Poonen's Lemma 3 [15] for a similar argument.

Lemma 1. *Let J be a singular modulus attached to an elliptic curve whose endomorphism ring is an order with discriminant $\Delta < 0$. Then*

$$(1) \quad h(J) \geq c_2 \log |\Delta| - c_3.$$

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 [6], Colmez 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 [14] 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 $p^n \mid f$ but $p^{n+1} \nmid f$ and $\chi(p)$ is Kronecker's symbol $(\frac{\Delta_0}{p})$. Now $\sum_{p|f} e_f(p) \log p \leq c_1 \log \log \max\{3, f\}$ by the arguments in the proof of Lemma 4.2 [11]. Therefore, the stable Faltings height of E is bounded from below logarithmically in terms of $|\Delta_0 f^2| = |\Delta|$.

Silverman's Proposition 2.1 [17] allows us to replace the stable Faltings height by $h(J)$ at the cost of adjusting the constants. \square

Our strategy to prove Theorem 1 is as follows. Let J and Δ be as in Lemma 1. 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

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

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

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

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

of the action of $\operatorname{SL}_2(\mathbf{Z})$ on \mathbf{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

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

We estimate their number using equidistribution in the next lemma.

Lemma 2. *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.

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

for a measurable subset $\Sigma \subset \mathcal{F}$. Duke [9] 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 a result of Clozel and Ullmo [5]. So $|\#\Gamma_\epsilon/D - \mu(\Sigma_\epsilon)| \rightarrow 0$ as $\Delta \rightarrow -\infty$. To prove the lemma we will bound $\mu(\Sigma_\epsilon)$ in terms of ϵ .

Let ζ be the unique root of unity in \mathbf{H} of order 6; it is a zero of j . By Theorem 2, Chapter 3 [12] Klein's modular function 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 \mathbf{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

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

for all $\tau \in \overline{\mathcal{F}}$ with $|j(\tau)| \leq 1$ where $\max\{|\tau - \zeta|, |\tau - \zeta^2|\} \geq |\zeta - \zeta^2|/2 = 1/2$ 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

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

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 first require a bound for the height of τ_σ .

Lemma 3. *Each τ_σ is imaginary quadratic and $h(\tau_\sigma) \leq \log \sqrt{|\Delta|}$.*

Proof. We abbreviate $\tau = \tau_\sigma$ and decompose $\Delta = \Delta_0 f^2$ as in the proof of Lemma 1. The endomorphism ring mentioned in the said lemma can be identified with $\mathbf{Z} + \omega f \mathbf{Z} \subset \mathbf{C}$ where $\omega = (\sqrt{\Delta_0} + \Delta_0)/2$. This ring acts on the lattice $\mathbf{Z} + \tau \mathbf{Z}$. So there exist $a, b, c, d \in \mathbf{Z}$ 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

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

Of course, τ is imaginary quadratic. We observe that ωf is a root of $T^2 - (a+d)T + ad - bc$. The discriminant of this quadratic 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 $|\operatorname{Re}(\tau)| \leq 1/2$. The second inequality implies $|a-d| \leq |b|$ and hence $|\tau|^2 \leq (b^2 + |\Delta|)/(2b)^2$. By Proposition 1.6.6 [4] 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 4. *We have $\log |\sigma(J)| \geq -c_8 \log |\Delta|$ for any $\sigma : \mathbf{Q}(J) \rightarrow \mathbf{C}$.*

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

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

We also remark $\tau_\sigma \neq \zeta$ since $\sigma(J) \neq 0 = j(\zeta)$. Liouville's inequality, Theorem 1.5.21 [4], tells us

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

But τ_σ and ζ are imaginary quadratic, so $[\mathbf{Q}(\tau_\sigma, \zeta) : \mathbf{Q}] \leq 4$. Moreover, $h(\zeta) = 0$ as ζ is a root of unity. The bound for $h(\tau_\sigma)$ from Lemma 3 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 Heilbronn and Hecke there are only finitely many singular moduli whose degree over \mathbf{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 2.

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 1. With this choice we conclude that $|\Delta|$ is bounded from above by an absolute constant. By Lemma 3 and Northcott's Theorem 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 \mathbf{C} . We fix a Weierstrass equation for E with coefficients in the said number field and a Weierstrass- \wp function that induces a uniformization $\mathbf{C} \rightarrow E(\mathbf{C})$. This is a group homomorphism whose kernel $\omega_1 \mathbf{Z} + \omega_2 \mathbf{Z}$ is a discrete subgroup of \mathbf{C} . We start numbering constants anew.

Lemma 5. *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 $\alpha, \beta \in \mathbf{C}$ are algebraic over \mathbf{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*

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

Proof. This follows from Theorem 1.6 [7]. \square

In our application, $\log B$ from (8) will be approximately $\log |\Delta|$ and will compete directly with the logarithmic lower bound in Lemma 1. 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 6. *Suppose $\eta \in \mathbf{H}$ 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 $\tau \in \mathbf{H}$ is imaginary quadratic with $\max\{1, h(\tau)\} \leq \log B$ for some real number $B > 0$ and if $\tau \neq \eta$, 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 5. We may assume that the periods $\omega_{1,2}$ satisfy $\eta = \omega_2/\omega_1$. As $\tau \neq \eta$ the lemma above 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 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 $P_0 \in C$ 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 non-constant, 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 7. *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 \mathbf{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 . Let us write $R = r_0 + (U - J_0)r_1 + \cdots + (U - J_0)^e r_e$ where $e = \deg_U R$ 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 Theorem 10.4 [13]. 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 $M \subset X(\overline{F})$ 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 $J_0 \notin \phi(M)$. Say $\lambda \in F \setminus \{0\}$ with $\lambda\psi(M) \subset \mathcal{O}_{\overline{F}}$. 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 $K \subset \overline{F}$ be a number field containing F and the values $\psi(P), \phi(P)$. Then

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

as usual, the sums run over field embeddings $\sigma : K \rightarrow \mathbf{C}$. Say $J = \phi(P) \in K$, then $R(J, \psi(P)^{-1}) = 0$. We apply Lemma 7 to $u = J$ and $v = \psi(P)$ to obtain

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

We already saw that R is not divisible by a linear polynomial in the variable V . So Proposition 5 [3] 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

$$h(J) \leq c_7 \left(1 + \frac{1}{[K : \mathbf{Q}]} \sum_{|\sigma(J - J_0)| < 1} -\log |\sigma(J - J_0)| \right)$$

and so

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

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 $\sigma : K \rightarrow \mathbf{C}$ we fix $\tau_\sigma \in \mathcal{F}$ with $j(\tau_\sigma) = \sigma(J)$. We now proceed as near (4) and apply Theorem 2, Chapter 3 [12]. If ϵ is sufficiently small and if $|\sigma(J - J_0)| < \epsilon$, then

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

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 6 and the height bound for τ_σ in Lemma 3 yield $\log |\sigma(J - J_0)| \geq -c_9 \log |\Delta|$. We use this inequality and (10) to bound

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

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

The rest of the proof resembles the proof of Theorem 1. Indeed, we may assume that $[\mathbf{Q}(J) : \mathbf{Q}]$ is sufficiently large and as in Lemma 2 we use equidistribution to prove that $[K : \mathbf{Q}]^{-1} \#\{\sigma : K \rightarrow \mathbf{C}; |\sigma(J - J_0)| < \epsilon\}$ is bounded from above linearly by a fixed power, derived from (11), of ϵ . Finally, we again use the height lower bound in Lemma 1 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

1. M. Baker, S. Ih, and R. Rumely, *A finiteness property of torsion points*, Algebra Number Theory **2** (2008), no. 2, 217–248.
2. 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), no. 1, 145–152.
3. Y. F. Bilu and D. W. Masser, *A quick proof of Sprindzhuk’s decomposition theorem*, Bolyai Soc. Math. Stud. **15** (2006).
4. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
5. L. Clozel and E. Ullmo, *Équidistribution des points de Hecke*, Contributions to automorphic forms, geometry, and number theory, Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 193–254.
6. P. Colmez, *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe*, Compositio Math. **111** (1998), no. 3, 359–368.
7. S. David and N. Hirata-Kohno, *Linear forms in elliptic logarithms*, J. Reine Angew. Math. **628** (2009), 37–89.
8. D. R. Dorman, *Special values of the elliptic modular function and factorization formulae*, J. Reine Angew. Math. **383** (1988), 207–220.
9. W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), no. 1, 73–90.
10. B. H. Gross and D. B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.
11. P. Habegger, *Weakly bounded height on modular curves*, Acta Math. Vietnam. **35** (2010), no. 1, 43–69.
12. S. Lang, *Elliptic Functions*, Springer, 1987.
13. H. Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989.
14. Y. Nakajima and Y. Taguchi, *A generalization of the Chowla-Selberg formula*, J. Reine Angew. Math. **419** (1991), 119–124.
15. B. Poonen, *Spans of Hecke points on modular curves*, Math. Res. Lett. **8** (2001), no. 5-6, 767–770.
16. J.-P. Serre, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.
17. J. H. Silverman, *Heights and Elliptic Curves*, Arithmetic Geometry (Gary Cornell and Joseph H. Silverman, eds.), Springer, 1986, pp. 253–265.

DEPARTEMENT MATHÉMATIK UND INFORMATIK, UNIVERSITÄT BASEL, SPIEGELGASSE 1, 4051 BASEL, SWITZERLAND

E-mail address: philipp.habegger@unibas.ch

LATEST PREPRINTS

No.	Author: Title
2015-01	Ali Hyder <i>Existence of Entire Solutions to a Fractional Liouville Equation in R^n</i>
2015-02	H. Harbrecht, M. Peters <i>Solution of Free Boundary Problems in the Presence of Geometric Uncertainties</i>
2015-03	M. Dambrine, C. Dapogny, H. Harbrecht <i>Shape Optimization for Quadratic Functionals and States with Random Right-Hand Sides</i>
2015-04	A. Bohun, F. Bouchut, G. Crippa <i>Lagrangian Flows for Vector Fields with Anisotropic Regularity</i>
2015-05	A. Bohun, F. Bouchut, G. Crippa <i>Lagrangian Solution to the Vlasov-Poisson System with L^1 Density</i>
2015-06	S. Iula, A. Maalaoui, L. Martinazzi <i>A fractional Moser-Trudinger type inequality in one dimension and its critical points</i>
2015-07	A. Hyder <i>Structure of conformal metrics on R^n with constant Q-curvature</i>
2015-08	M. Colombo, G. Crippa, S. Spirito <i>Logarithmic Estimates for Continuity Equations</i>
2015-09	M. Colombo, G. Crippa, S. Spirito <i>Renormalized Solutions to the Continuity Equation with an Integrable Damping Term</i>
2015-10	G. Crippa, N. Gusev, S. Spirito, E. Wiedemann <i>Failure of the Chain Rule for the Divergence of Bounded Vector Fields</i>
2015-11	G. Crippa, N. Gusev, S. Spirito, E. Wiedemann <i>Non-Uniqueness and Prescribed Energy for the Continuity Equation</i>
2015-12	G. Crippa, S. Spirito <i>Renormalized Solutions of the 2D Euler Equations</i>
2015-13	G. Crippa, E. Semenova, S. Spirito <i>Strong Continuity for the 2D Euler Equations</i>

LATEST PREPRINTS

No.	Author: Title
2015-14	J. Diaz, M. J. Grote <i>Multi-Level Explicit Local Time-Stepping Methods for Second-Order Wave Equations</i>
2015-15	F. Da Lio, L. Martinazzi, T. Riviere <i>Blow-up analysis of a nonlocal Liouville-type equation</i>
2015-16	A. Maalaoui, L. Martinazzi, A. Schikorra <i>Blow-up behaviour of a fractional Adams-Moser-Trudinger type inequality in odd dimension</i>
2015-17	T. Boulenger, E. Lenzmann <i>Blowup for Biharmonic NLS</i>
2015-18	D. Masser, U. Zannier (with Appendix by V. Flynn) <i>Torsion point on families of simple abelian surfaces and Pell's equation over polynomial rings</i>
2015-19	M. Bugeanu, R. Di Remigio, K. Mozgawa, S. S. Reine, H. Harbrecht, L. Frediani <i>Wavelet Formulation of the Polarizable Continuum Model. II. Use of Piecewise Bilinear Boundary Elements</i>
2015-20	J. Dölz, H. Harbrecht, M. Peters <i>An interpolation-based fast multipole method for higher order boundary elements on parametric surfaces</i>
2015-21	A. Schikorra <i>Nonlinear Comutators for the fractional p-Laplacian and applications</i>
2015-22	L. Martinazzi <i>Fractional Adams-Moser-Trudinger type inequalities</i>
2015-23	P. Habegger, J. Pila <i>O-Minimality and certain atypical intersections</i>
2015-24	P. Habegger <i>Singular Moduli that are Algebraic Units</i>