EFFECTIVE CONDITIONAL BOUNDS ON SINGULAR $S$-UNITS

FRANCESCO CAMPAGNA

ABSTRACT. We provide a proof that, for every prime $\ell \geq 5$, if $S_0$ is the set of all primes congruent to 1 modulo 3 and $S_\ell = S_0 \cup \{\ell\}$, then under certain assumptions on the $L$-functions attached to imaginary quadratic fields, the set of singular $S_\ell$-units is finite and its cardinality can be effectively bounded.

1. INTRODUCTION

The present manuscript is devoted to the study of some diophantine properties of $j$-invariants of elliptic curves with complex multiplication defined over $\mathbb{C}$. These numbers, which are classically known with the name of singular moduli, have been studied since the time of Kronecker and Weber, who were interested in explicit generation of class fields relative to imaginary quadratic fields [12]. In this respect, singular moduli prove to be a useful tool, since they are indeed algebraic integers which can be used to generate ring class fields of imaginary quadratic fields [8, Theorem 11.1].

During the last decade, there has been an increasing interest in understanding more diophantine properties of these invariants. One of the questions that, for instance, has been addressed is the following: given a set $S$ of rational primes, is the set of singular moduli that are $S$-unit (singular $S$-units) finite? In case of affirmative answer, is it possible to give an effective bound on the cardinality of this set? This question, which has been originally motivated by the proof of some effective results of André-Oort type (see [3] and [23]), does not have at present a complete answer. Several partial results have nonetheless been achieved.

In [2] it is proved, building on the previous ineffective result of Habegger [19], that no singular modulus can be a unit in the ring of algebraic integers. This settles the case $S = \emptyset$ of the question. With different techniques, Li generalizes this theorem and proves in [26] that for every pair $j_1, j_2 \in \overline{\mathbb{Q}}$ of singular moduli, the algebraic integer $\Phi_N(j_1, j_2)$ can never be a unit. Here $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ denotes the classical modular polynomial of level $N$, so we recover the main result of [2] by setting $j_2 = 0$ and $N = 1$. In a different direction, the fact that no singular modulus is a unit has been used by the author of this manuscript to prove that, if $S_0$ is the infinite set of primes congruent to 1 mod 3, the set of singular moduli that are $S_0$-units is empty [5]. Moreover, very recently Herrero, Menares and Rivera-Letelier gave an ineffective proof of the fact that, for every finite set of primes $S$, the set of singular $S$-units is finite, see [20] [21] and [22].

The main goal of this paper is to explore the possibility of giving effective bounds on the cardinality of the set of singular $S$-units for some specific sets of primes $S$. More precisely, we will try to understand what happens if, to the set $S_0$ of primes 1 mod 3, we add a single prime $\ell \notin S_0$. In general, if $S_\ell := S_0 \cup \{\ell\}$, the set of singular $S_\ell$-units may be non-empty. For instance, for $\ell = 2$, the singular modulus $j = -32768 = -2^7$ is an $S_\ell$-unit ($j$ is the invariant of every elliptic curve with complex multiplication by the order of discriminant $\Delta = -11$). We have not been able to find more examples of $S_\ell$-units, and we conjecture that for every $\ell \neq 2$ there is...
none. In this article we prove a first conditional step towards this claim. To state precisely our results, we introduce some notation.

Recall that non-principal real primitive Dirichlet characters are precisely the Kronecker symbols attached to quadratic field extensions of \( \mathbb{Q} \). We say that such a Dirichlet character has discriminant \( D \in \mathbb{Z} \) if it is the Kronecker symbol attached to a quadratic field of discriminant \( D \).

**Definition 1.1.** Let \( k \in \mathbb{R} \) be a non-negative real number. A non-principal real primitive Dirichlet character \( \chi \) of discriminant \( D \) is said to satisfy property \( P(k) \) if

\[
\frac{L'(\chi, 1)}{L(\chi, 1)} \geq -0.2485 \log |D| - k
\]

where the left-hand side of the inequality is the logarithmic derivative of the Dirichlet \( L \)-function \( L(\chi, s) \) associated to \( \chi \).

We also say that, for a given negative integer \( \Delta = 0 \) or \( 1 \mod 4 \), the singular modulus \( j \) has discriminant \( \Delta \) if it is the \( j \)-invariant of an elliptic curve with complex multiplication by the order of discriminant \( \Delta \). We can now state our main theorem.

**Theorem 1.2.** Let \( S_0 \) be the set of rational primes congruent to \( 1 \) modulo \( 3 \), let \( \ell \geq 5 \) be an arbitrary prime and set \( S_\ell := S_0 \cup \{\ell\} \). Assume that all the Kronecker symbols \( \chi_D \) attached to an imaginary quadratic field of discriminant \( D \) satisfy property \( P(k) \) for some fixed \( k \in \mathbb{R}_{\geq 0} \). Then there exists an effectively computable bound \( B = B(\ell) \in \mathbb{R}_{\geq 0} \) such that the discriminant \( \Delta_j \) of every singular \( S_\ell \)-unit \( j \in \overline{\mathbb{Q}} \) satisfies \( |\Delta_j| \leq B \). In particular, the set of singular moduli that are \( S_\ell \)-units is finite and its cardinality can be effectively bounded.

The bound \( B \) can be made explicit from the details of the proof. We do not know how to evade the use of property \( P(k) \) in proving Theorem 1.2. It can be unconditionally deduced from [1, Theorem 1] that every non-principal real Dirichlet character of negative discriminant \( D \) satisfies

\[
\frac{L'(\chi, 1)}{L(\chi, 1)} \geq \frac{1}{2} \left( 1 - \frac{\sqrt{5}}{5} \right) \log |D| - \gamma \approx -0.2763 \log |D| - 0.5572
\]

where \( \gamma \in \mathbb{R} \) denotes the Euler-Mascheroni constant. This inequality is unfortunately too weak for our purposes. On the other hand, we note that if the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta function of imaginary quadratic fields, then property \( P(0) \) also holds for the associated Kronecker symbols with sufficiently big discriminant, and Theorem 1.2 follows. We remark, however, that satisfying property \( P(k) \) for some \( k \in \mathbb{R}_{\geq 0} \) is a weaker condition than satisfying GRH, since the latter implies an estimate of the form

\[
\frac{L'(\chi, 1)}{L(\chi, 1)} = O(\log \log |D|),
\]

see for instance [17, Lemma 4.3]. We also observe that in [27] the authors prove that the above logarithmic derivative is actually positive for infinitely many negative fundamental discriminants.

If we content ourselves with looking at singular \( S_\ell \)-units whose discriminant is divided by \( \ell \), the same techniques lead to the following unconditional, but weaker, result.

**Theorem 1.3.** Let \( \ell \geq 5 \) be a prime and let \( \mathcal{J}_\ell \) be the set of singular \( S_\ell \)-units whose discriminant is divided by \( \ell \). There exists an effectively computable bound \( B' = B'(\ell) \in \mathbb{R}_{\geq 0} \) such that the discriminant \( \Delta_j \) of every \( j \in \mathcal{J}_\ell \) satisfies \( |\Delta_j| \leq B' \). In particular, the set \( \mathcal{J}_\ell \) is finite and its cardinality can be effectively bounded.
The proof of Theorem 1.3, being essentially identical to the proof of Theorem 1.2, will be only sketched in Section 7. Note that the mere finiteness of the sets considered in these theorems, without providing effective bounds on their cardinality, could already be unconditionally achieved by combining the results in [5] and [22] (see [22, Section 1.1] and the beginning of Section 6 of the present manuscript for details).

Here is an outline of the proof of Theorem 1.2. First of all, one can easily reduce to show that, under the given hypotheses, the set of singular $\ell$-units is finite and its cardinality can be effectively bounded. To attack this latter statement, we follow the same idea used in [2]: given a singular $\ell$-unit $j \in \mathbb{Q}$, we compute its (logarithmic) Weil height $h(j)$. This is defined, for every $x \in \mathbb{Q}$, as

$$h(x) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} [K_v : \mathbb{Q}_v] \log^+ |x|_v$$

where $K := \mathbb{Q}(x)$ is the field generated by $x$ over the rationals, $\mathcal{M}_K$ is the set of all places of $K$ and $\log^+ |x|_v := \log \max\{1, |x|_v\}$. Here, for every non-archimedean place $v$ corresponding to the prime ideal $p_v$ lying above the rational prime $p_v$, the absolute value $| \cdot |_v$ is normalized in such a way that

$$|x|_v = p_v^{-v_p(x)/e_v}$$

$e_v$ being the ramification index of $p_v$ over $p_v$. Hence the logarithmic Weil height naturally decomposes into an "archimedean" and "non-archimedean" part.

Since $j$ is an algebraic integer, the non-archimedean part of its Weil height vanishes. In order to exploit the fact that $j$ is an $\ell$-unit, we rather compute the height of $j^{-1}$. Using standard properties of the Weil height, we obtain

$$h(j) = h(j^{-1}) = (\text{archimedean part}) + (\text{non-archimedean part})$$

with

$$(\text{non-archimedean part}) = \frac{\log \ell}{[\mathbb{Q}(j) : \mathbb{Q}]} \sum_{p | \ell} f_p \cdot v_p(j).$$

Our goal is to effectively bound this height from above and from below in such a way that the two bounds contradict each other when the absolute value of the discriminant of the singular modulus $j$ becomes large. This will give the desired effective bound.

As far as the upper bound is concerned, the archimedean part has been already studied in [2]. In order to bound the non-Archimedean part, we have to understand the valuation of $j$ at primes above $\ell$. This requires the use of some deformation-theoretic arguments involving quaternion algebras. We detail this discussion in Section 3 and Section 4, which culminate with the proof of Theorem 4.1. For this proof, we have heavily used the works of Gross-Zagier [16] and Lauter-Viray [25].

Concerning the lower bound for the Weil height, we compare the Weil height of the singular modulus $j$ with the stable Faltings height of the elliptic curve with complex multiplication having $j$ as singular invariant. Using work of Colmez [6] and Nakkajima-Taguchi [28] it is possible to relate this Faltings height to the logarithmic derivative of the $L$-function corresponding to the CM field evaluated in 1. In this passage, we need to resort on the use of Property $P(k)$.

It will become apparent from the details of the proof (and we will comment on this in Section 7) that the only reason why Theorem 1.2 is conditional, is that the elliptic curve $E : y^2 = x^3 + 1$ with $j(E) = 0$ has "too many" automorphisms when reduced modulo $\ell$. Hence, it is very plausible that the same arguments could lead to unconditional effective bounds when considering analogous integrality problems for differences $j - \alpha$, with $\alpha$ a non-zero singular modulus. This will be object of future research.
We structure this manuscript as follows. In Section 2 we recall known facts from the theory of complex multiplication and quaternion algebras, and we fix the terminology which will be used in the paper. Section 3 describes the arithmetic of the elliptic curve \( E : y^2 = x^3 + 1 \) in characteristic \( \ell \geq 5 \). The results contained in this section are well-known, but we still provide complete proofs both for completeness and because in some cases we were not able to find adequate references. In Section 4 we prove Theorem 4.1, which allows to bound the \( p \)-adic absolute value of a singular modulus. Section 5 is concerned with the proof of a lower bound on the Weil height of a singular modulus under the assumption that property \( P(k) \) (for some non-negative \( k \)) holds for the Dirichlet character attached to the corresponding imaginary quadratic field. Finally in Section 6 we prove Theorem 1.2. We comment on this argument in Section 7, where we also prove Theorem 1.3.

2. Prelude: CM elliptic curves, quaternion algebras and optimal embeddings

We recall in this section some of the main definitions and results that will be used in the rest of the paper. We fix once for all an algebraic closure \( \overline{\mathbb{Q}} \supseteq \mathbb{Q} \) of the rationals.

A singular modulus is the \( j \)-invariant of an elliptic curve defined over \( \overline{\mathbb{Q}} \) with complex multiplication. For every imaginary quadratic order \( \mathcal{O} \) of discriminant \( \Delta \in \mathbb{Z} \) there are exactly \( h_\Delta \) isomorphism classes of elliptic curves over \( \overline{\mathbb{Q}} \) with complex multiplication by \( \mathcal{O} \), where \( h_\Delta \in \mathbb{N} \) denotes the class number of the order \( \mathcal{O} \). Hence, there are \( h_\Delta \) corresponding singular moduli, which are all algebraic integers and form a full Galois orbit over \( \mathbb{Q} \) (see [8, Theorem 11.1] and [8, Proposition 13.2]). We call them singular moduli of discriminant \( \Delta \) or singular moduli relative to the order \( \mathcal{O} \).

Given a set \( S \subseteq \mathbb{N} \) of rational primes, we are interested in the study of the set of singular \( S \)-units, that is, of the set of singular moduli that are \( S \)-units. Recall that, given a number field \( K \subseteq \overline{\mathbb{Q}} \) and a set \( S \subseteq \mathbb{N} \) of rational primes, an element \( x \in K \) is called an \( S \)-unit if for every prime \( p \in S \), we have \( x \in \mathcal{O}_K^\times \), where \( \mathcal{O}_K^\times \subseteq \mathcal{O}_p \) denotes the ring of integers in the completion \( K_p \) of the number field \( K \) at the prime \( p \). Our study of singular \( S \)-units relies in a crucial way on the analysis of specific embeddings in certain suborders of the endomorphism ring of a supersingular elliptic curve.

Let \( k \) be a field of characteristic \( \text{char}(k) = \ell > 0 \) with algebraic closure \( \overline{k} \supseteq k \) and let \( E/k \) be an elliptic curve. We say that \( E \) is supersingular if \( E[\ell](\overline{k}) = \{0\} \) i.e. if the unique \( \ell \)-torsion point of \( E \) defined over \( \overline{k} \) is the identity \( O \in E(\overline{k}) \). If this is the case, then the endomorphism ring \( \text{End}_\overline{k}(E) \) is isomorphic to a maximal order in the unique (up to isomorphism) quaternion algebra over \( \mathbb{Q} \) ramified only at \( \ell \) and \( \infty \) (see [10] or [34, Theorem 42.1.9] for a modern exposition). The supersingular elliptic curves that will appear in our discussion mainly arise as the reduction of CM elliptic curves defined over number fields. Namely, let \( F \) be a number field and let \( E/F \) be an elliptic curve with CM by an order in an imaginary quadratic field \( K \). Fix a prime ideal \( p \subseteq \mathcal{O}_F \) lying above a rational prime \( p \in \mathbb{Z} \) that do not split in \( K \). Since CM elliptic curves have potential good reduction everywhere [32, VII, Proposition 5.5] we can assume, possibly after enlarging the field of definition \( F \), that \( E \) has good reduction at \( p \). Then the reduced elliptic curve \( \overline{E} := E \mod p \) is supersingular by [24, Theorem 13.12]. Moreover, the reduction map induces an injective ring homomorphism
\[
\varphi : \text{End}_F(E) \hookrightarrow \text{End}_{\overline{\mathbb{Q}}_\ell}(\overline{E})
\]
by [31, II, Proposition 4.4]. As we will see, in many cases (depending on the prime \( \ell \) and on the CM order of \( \overline{E} \)) the above embedding will be optimal, in the following sense.

Let \( \mathbb{B} \) be a quaternion algebra over \( \mathbb{Q} \) and let \( R \subseteq \mathbb{B} \) be an order. Let \( \overline{\mathbb{Q}} \subseteq K \) be a quadratic field extension and let \( \mathcal{O} \subseteq K \) also be an order. We say that an injective ring homomorphism
\( \iota : O \hookrightarrow R \) is an optimal embedding if
\[
\iota(O \otimes \mathbb{Q}) \cap R = \iota(O)
\]
where the above intersection takes place in \( \mathbb{B} \). There is a simple criterion which allows to determine whether a given imaginary quadratic order optically embeds into a quaternionic order. In order to state it, let us denote by \( \text{trd}, \text{nrd} : \mathbb{B} \to \mathbb{Q} \) respectively the reduced trace and the reduced norm in the quaternion algebra \( \mathbb{B} \).

**Lemma 2.1.** Let \( R \) be an order in a quaternion algebra \( \mathbb{B} \) and \( O \) an order of discriminant \( \Delta \) in an imaginary quadratic field \( K \). Let \( V \subseteq \mathbb{B} \) be the subspace of pure quaternions
\[
V := \{ x \in \mathbb{B} : \text{trd}(x) = 0 \}.
\]
Then \( O \) embeds optimally in \( R \) if and only if \( |\Delta| \) is primitively represented by the ternary quadratic lattice
\[
R_0 := V \cap (\mathbb{Z} + 2R)
\]
endowed with the natural scalar product induced by the reduced norm on \( \mathbb{B} \).

**Remark 2.2.** This lemma has been proved for non-optimal embeddings and for maximal orders \( R \) in \([14, \text{Proposition 12.9}]\). Probably for this reason, the lattice \( R_0 \) is sometimes called the *Gross lattice* associated to \( R \). The argument in loc. cit. easily generalizes to our situation. We provide a full proof for completeness.

**Proof.** We first prove that \( O \) embeds in \( R \) if and only if it is represented by \( R_0 \), and we discuss conditions on the optimality of this embedding at a second stage.

Write \( O = \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right] \) and suppose first that \( f : O \hookrightarrow R \) is an embedding. Let \( b := f(\sqrt{\Delta}) \) so that \( \text{trd}(b) = 0 \) and \( \text{nrd}(b) = |\Delta| \). Since
\[
f\left(\frac{\Delta + \sqrt{\Delta}}{2}\right) = \frac{\Delta + b}{2} \in R
\]
we see that \( b \in R_0 \) so that \( |\Delta| \) is represented by this lattice. Suppose conversely that there exists \( b \in R_0 \) such that \( \text{nrd}(b) = |\Delta| \). Since \( \text{trd}(b) = 0 \), we see that \( b^2 = \Delta \). By writing \( b = a + 2r \) with \( a \in \mathbb{Z} \) and \( r \in R \), one has
\[
b^2 = (a + 2r)^2 = a^2 + 4r^2 + 4ar = \Delta
\]
and this immediately implies that \( a \equiv \Delta \mod 2 \), so that \( \Delta + b \in 2R \). Hence we have \( (\Delta + b)/2 \in R \) and we obtain an embedding \( f : O \hookrightarrow R \) by setting
\[
f\left(\frac{\Delta + \sqrt{\Delta}}{2}\right) = \frac{\Delta + b}{2}.
\]

We now discuss optimality. Let \( \{\alpha_1, \alpha_2, \alpha_3\} \) be a basis of \( R_0 \) as a \( \mathbb{Z} \)-module and let \( Q(X, Y, Z) \) be the ternary quadratic form induced by the reduced norm with respect to this basis.

Assume that \( f : O \hookrightarrow R \) is an optimal embedding and, with abuse of notation, denote by \( f \) also the extension
\[
f : K = O \otimes \mathbb{Q} \hookrightarrow R \otimes \mathbb{Q} = \mathbb{B}
\]
of this embedding to the imaginary quadratic field \( K \). Let \( b := f(\sqrt{\Delta}) \in R_0 \), and assume by contradiction that \( b = a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 \) with \( a_1, a_2, a_3 \in \mathbb{Z} \) not coprime, so that \( c := \gcd(a_1, a_2, a_3) > 1 \). Then \( \bar{b} := b/c \in R_0 \) satisfies
\[
\bar{b}^2 = \frac{\Delta}{c^2} \quad \text{and} \quad \frac{1}{2}\left(\bar{b} + \frac{\Delta}{c^2}\right) \in R.
\]
in the same way as above. Thus \( \frac{1}{2} \left( \frac{\sqrt{A}}{c} + \frac{b}{c^2} \right) \in K \) is an algebraic integer and the order \( \mathcal{O} := \mathbb{Z} \left[ \frac{1}{2} \left( \frac{\sqrt{A}}{c} + \frac{b}{c^2} \right) \right] \), which strictly contains \( \mathcal{O} \), also embeds in \( R \) through \( f \). This contradicts the optimality of \( f : O \hookrightarrow R \).

Suppose now that \( |\Delta| \) is primitively represented by \( R_0 \) i.e. that there exist \( a_1, a_2, a_3 \in \mathbb{Z} \) coprime such that \( nrd(a_1a_2 + a_2a_3 + a_3a) = |\Delta| \). We want to show that the embedding \( f \) defined by (1) is optimal. We will equivalently prove that, if \( c \in \mathbb{N} \) is such that \( \mathcal{O} := \mathbb{Z} \left[ \frac{1}{2} \left( \frac{\sqrt{A}}{c} + \frac{b}{c^2} \right) \right] \) is an order, then

\[
(2) \quad f(K) \cap R = f(\mathcal{O})
\]

implies \( \mathcal{O} = O \). Setting \( b := f(\sqrt{A}) \), equality (2) entails

\[
\frac{1}{2} \left( \frac{a_1}{c} \frac{b}{c^2} + \frac{a_2}{c} \frac{a_2}{c} + \frac{a_3}{c} \frac{a_3}{c} \right) \in R \text{ so that } b/c \in R_0. \text{ But now } \]

and all the coefficients \( a_i/c \) must be integral since \( R_0 \) is a lattice. By assumption, the \( a_i \)'s are coprime, so we must have \( c = 1 \). Hence \( \mathcal{O} = O \) and this concludes the proof. \( \Box \)

3. Arithmetic of the elliptic curve with \( j = 0 \) in positive characteristic

Roughly speaking, saying that a singular modulus \( j \) has a certain \( \mu \)-adic valuation \( n = v_\mu(j) \) for some prime ideal \( \mu \subseteq \mathbb{Q}(j) \), is equivalent to saying that the CM elliptic curve \( E_j \) with \( j(E_j) = j \) is isomorphic to the elliptic curve \( E_0 \) with \( j(E_0) = 0 \) when reduced modulo \( \mu^n \). Therefore, in order to understand the exponents appearing in the prime ideal factorization of a singular modulus, it is crucial to determine when such isomorphisms can occur. With this goal in mind, we study in this section the endomorphism ring of the reduction of \( E_0 \) modulo prime powers \( \ell^n \), for \( \ell \geq 5 \) a prime of supersingular reduction (this will be made precise soon). The content of the section is certainly well-known to the expert, and all the stated results already appear, although in a different and usually more general formulation, in the literature (see for instance [7], [15], [16], [25]). However, the author has not been able to find complete proofs of all the statements. For this reason, we decided to include here a self-contained exposition of the needed results in a very special case. We hope that this will be helpful to the reader.

Let \( \ell \geq 5 \) be a prime satisfying \( \ell \equiv 2 \mod 3 \) and let \( L := \mathbb{Q}_\ell^{nr} \) be the completion of the maximal unramified extension of \( \mathbb{Q}_\ell \). Consider \( W \subseteq L \) the ring of integers and set \( \pi \in W \) to be a uniformizer. Note that our assumptions on the prime \( \ell \) imply that \( W \) contains a primitive 3rd root of unity. Consider the elliptic scheme \( \mathcal{E}_0 \to \text{Spec } W \) defined by the equation \( y^2 = x^3 + 1 \):

- the generic fiber \( E = \mathcal{E}_0 \times_W \text{Spec } L \) is an elliptic curve with complex multiplication by the order of discriminant \( \Delta = -3 \) and with \( j(E) = 0 \). Since the CM order is contained in \( W \), all the endomorphisms of \( E \) are already defined over \( L \);
- the special fiber \( E_0 := \mathcal{E}_0 \times_W \text{Spec } W/\pi \) is a supersingular elliptic curve since, by assumption, \( \ell \) does not split in \( \mathbb{Q}(\sqrt{-3}) \) (see [24, Theorem 13.12]).

For all \( n \in \mathbb{N} \), set \( E_n := E_0 \times_W \text{Spec } W/\pi^{n+1} \). We are interested in understanding the endomorphisms rings \( A_{\ell,n} := \text{End}_{W/\pi^{n+1}}(E_n) \). We begin by explicitly determining the ring \( A_{\ell,0} \), i.e. the endomorphism ring of the elliptic curve \( E_0 : y^2 = x^3 + 1 \) over \( \mathbb{F}_\ell \).

It is well known that the ring \( A_{\ell,0} \) is isomorphic to a maximal order in the unique (up to isomorphism) definite quaternion algebra over the rationals which ramifies only at \( \ell \) and \( \infty \). If we call this quaternion algebra \( \mathbb{B}_{\ell,\infty} \), an easy computation with Hilbert symbols shows that

\[
\mathbb{B}_{\ell,\infty} \cong \left( \frac{-3,-\ell}{\mathbb{Q}} \right)
\]
where the right-hand side denotes the quaternion algebra with standard basis \(\{1, i, j, ij\}\) satisfying the relations \(i^2 = -3, j^2 = -\ell\) and \(ij = -ji\). We define
\[
\zeta_3 = \frac{-1 + i}{2}, \quad \pi = j
\]
whose minimal polynomials over the rationals are \(f_\zeta(x) = x^2 + x + 1\) and \(f_\pi(x) = x^2 + \ell\) respectively. Now, the ring \(\operatorname{End}_{\mathbb{F}_\ell}(E_0)\) contains the order \(\mathbb{Z}[\alpha_1, \alpha_2]\) generated by the two \(\mathbb{Z}\)-linearly independent endomorphisms
\[
\alpha_1 : (x, y) \mapsto (\zeta x, y), \quad \alpha_2 : (x, y) \mapsto (x^\ell, y^\ell)
\]
where \(\zeta \in \overline{\mathbb{F}_\ell}\) denotes a fixed primitive third root of unity. Since \(f_\zeta(\alpha_1) = 0 = f_\pi(\alpha_2)\), the association \(\alpha_1 \mapsto \zeta_3, \alpha_2 \mapsto \pi\) gives an isomorphism \(\mathbb{Z}[\alpha_1, \alpha_2] \cong \mathbb{Z}[^3\zeta, \pi]\) which extends to an isomorphism of quaternion algebras

\[(3) \quad \operatorname{End}_{\mathbb{F}_\ell}(E_0) \otimes \mathbb{Q} \cong B_{\ell,\infty}.
\]

The image of \(A_{\ell,0}\) under the isomorphism (3) strictly contains \(\mathbb{Z}[^3\zeta, \pi]\), since a discriminant computation readily shows that the latter has index 3 in a maximal order [34, Theorem 15.5.5]. However, one can recover the order \(A_{\ell,0}\) from the order \(\mathbb{Z}[^3\zeta, \pi]\) as in the proof of the following theorem, kindly suggested to the author by John Voight.

**Theorem 3.1.** Let \(\ell \geq 5\) be a prime with \(\ell \equiv 2 \mod 3\). Then the elliptic curve \(E_0 : y^2 = x^3 + 1\) over \(\overline{\mathbb{F}_\ell}\) has complex multiplication by the order

\[
\mathbb{Z} + \mathbb{Z}[^3\zeta, \zeta + 2 + \zeta_3 + 2\pi + \zeta_3\pi + 1 + \zeta_3 - \pi - 2\zeta_3\pi]
\]
in \(\mathbb{B}_{\ell,\infty}\).

**Proof.** One could directly verify that the given order is a maximal order whose elements represent endomorphisms of the elliptic curve \(E_0\). We outline a possible strategy leading to the computation of this endomorphism ring.

Let \(O := \mathbb{Z}[^3\zeta, \pi]\) with \(\mathbb{Z}\)-basis \(\{1, \zeta_3, \zeta, \zeta_3\pi\}\) and let \(O_{E_0}\) be the image of \(A_6\) under the isomorphism (3). Then \(O_{E_0} \subseteq \mathbb{B}_{\ell,\infty}\) is a maximal order and \(O \subseteq O_{E_0}\) with index 3. Hence, \(O_E\) contains an element of the form
\[
\alpha = \frac{A + B\zeta_3 + C\pi + D\zeta_3\pi}{3}, \quad A, B, C, D \in \mathbb{Z}
\]
with \(3 \nmid \gcd(A, B, C, D)\). Since \(\alpha\) is an element of a quaternion order, it is in particular integral. This implies that its reduced trace and norm must both be integers. One has
\[
\operatorname{trd}(\alpha) = \frac{2A - B}{3},
\]
\[
\operatorname{nrd}(\alpha) = \frac{-\ell CD - AB + A^2 + B^2 + \ell(C^2 + D^2)}{9},
\]
where \(\operatorname{trd}(\cdot)\) and \(\operatorname{nrd}(\cdot)\) denote respectively the reduced trace and the reduced norm in the quaternion algebra \(\mathbb{B}_{\ell,\infty}\). Note now that, since \(O \subseteq O_{E_0}\), the integers \(A, B, C, D\) could be determined modulo 3. Hence there is just a finite number of possibilities to check. A computation shows that the possible options for the tuple \((A, B, C, D)\) are the following four:
\[
(1, 2, 1, 2), \quad (1, 2, 2, 1), \quad (2, 1, 1, 2), \quad (2, 1, 2, 1).
\]
By adding the corresponding $\alpha$’s to the order $O$ we get the following possibilities:

\[
\begin{align*}
(1, 2, 1, 2), & \quad O_1 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{1}{3} - \frac{1}{3}\zeta_3 + \frac{1}{3}\pi + \frac{2}{3}\zeta_3\pi\right) + \mathbb{Z}\left(\frac{2}{3} - \frac{1}{3}\zeta_3 - \frac{2}{3}\pi - \frac{1}{3}\zeta_3\pi\right) \\
(1, 2, 2, 1), & \quad O_2 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{1}{3} - \frac{1}{3}\zeta_3 + \frac{2}{3}\pi + \frac{1}{3}\zeta_3\pi\right) + \mathbb{Z}\left(\frac{2}{3} - \frac{1}{3}\zeta_3 - \frac{2}{3}\pi - \frac{1}{3}\zeta_3\pi\right) \\
(2, 1, 1, 2), & \quad O_3 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{2}{3} + \frac{1}{3}\zeta_3 + \frac{1}{3}\pi + \frac{2}{3}\zeta_3\pi\right) + \mathbb{Z}\left(\frac{1}{3} + \frac{1}{3}\zeta_3 - \frac{2}{3}\pi - \frac{1}{3}\zeta_3\pi\right) \\
(2, 1, 2, 1), & \quad O_4 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{2}{3} + \frac{1}{3}\zeta_3 + \frac{2}{3}\pi + \frac{1}{3}\zeta_3\pi\right) + \mathbb{Z}\left(\frac{1}{3} + \frac{1}{3}\zeta_3 - \frac{2}{3}\pi - \frac{1}{3}\zeta_3\pi\right).
\end{align*}
\]

Looking at the generators of these orders, we see that $O_1 = O_4$ and $O_2 = O_3$, so we discard the first two and we only consider $O_3$ and $O_4$. We need to decide which of these two rings is the "correct one". Indeed, the desired order must be identified to the endomorphism ring of the elliptic curve $E_0$. An element of the form $\frac{1}{3}\beta$, with $\beta \in \text{End}_\mathbb{F}_\ell(E_0)$, is an endomorphism of $E_0$ if and only if the endomorphism $\beta$ factors through the multiplication-by-$3$ morphism. This happens if and only if the $3$-torsion points of $E_0$ are in the kernel of $\beta$. The idea is then to compute the generators of the group of $3$-torsion points of $E_0$ and to test which order contains the "right" elements.

The $3$-division polynomial of $E_0$ is

\[ \Phi_3(x) = 3x(x^3 + 4), \]

so we can choose as generators of the full $3$-torsion subgroup $E_0[3](\overline{\mathbb{F}}_\ell)$ the points

\[ P = (0, 1), \quad Q = (-\sqrt{4}, \sqrt{3}) \]

for fixed choices of $\sqrt{4}, \sqrt{3} \in \overline{\mathbb{F}}_\ell$ as follows. Observe that for a prime $\ell \geq 5$ and $\ell \equiv 2 \text{ mod } 3$, all elements in $\mathbb{F}_\ell$ are cubes and $-3$ is not a square modulo $\ell$. In view of this remark, we choose $Q$ in such a way that the first coordinate lies in $\mathbb{F}_\ell$. Instead the second coordinate of $Q$ defines in any case a quadratic extension of $\mathbb{F}_\ell$, so that

\[ (\sqrt{3})^\ell = -\sqrt{3}. \]

We are ready to verify that $O_4$ is the correct order. Let

\[
\Phi = 2 + \zeta_3 + 2\pi + \zeta_3\pi \in O_E, \\
\Psi = -1 + \zeta_3 - \pi - 2\zeta_3\pi \in O_E.
\]

Then, using the fact that $2P = -P$ and $2Q = -Q$ we get that $\Phi = \Psi$ on the $3$-torsion points, so

\[
\Phi(P) = [2](0, 1) + (0, 1) + [2](0, 1) + (0, 1) = 0 \\
\Phi(Q) = (-\sqrt{4}, -\sqrt{3}) + (-\zeta\sqrt{4}, \sqrt{3}) + [2]((-\sqrt{4})^\ell, (\sqrt{3})^\ell) + (\zeta(-\sqrt{4})^\ell, (\sqrt{3})^\ell) = 0
\]

which shows that $E[3] \subseteq \ker \Phi$ and $E[3] \subseteq \ker \Psi$. One can also verify that

\[ (2 + \zeta_3 + \pi + 2\zeta_3\pi)(Q) \neq 0. \]

This proves the theorem. \[\square\]

Having determined $A_{\ell,0}$, one can make use of Serre-Tate deformation theory for abelian schemes in order to compute the rings $A_{\ell,n}$ for $n > 0$. We do this in the next theorem, which
is a very special case of [25, Formula 6.6]. We give some details on the proof. The terminology concerning formal groups follows the one present in [15].

**Theorem 3.2.** Let \( \ell \geq 5 \) a prime with \( \ell \equiv 2 \mod 3 \), and let \( L := \overline{\mathbb{Q}_\ell^{ur}} \) be the completion of the maximal unramified extension of \( \mathbb{Q}_\ell \), with ring of integers \( W \) and uniformizer \( \pi \). Let \( E_0 \to \text{Spec}(W) \) be the elliptic scheme defined by the equation \( y^2 = x^3 + 1 \), and, for every \( n \in \mathbb{N} \), denote by

\[
E_n := E_0 \times_W \text{Spec}(W/\pi^{n+1}) \quad \text{and} \quad A_{\ell,n} := \text{End}_{W/\pi^{n+1}}(E_n)
\]

respectively the reduction of \( E_0 \) modulo \( \pi^{n+1} \) and its endomorphism ring. Then for every \( n \in \mathbb{N} \) we have

\[
A_{\ell,n} \cong \mathbb{Z}[\zeta_3] + \ell^n A_{\ell,0}.
\]

**Proof.** We have already determined \( A_{\ell,0} \) in Theorem 3.1. Now for every \( n \in \mathbb{N}_{>0} \) we let \( \Gamma_n \to \text{Spec}(W/\pi^{n+1}) \) be the \( \ell \)-divisible group attached to the elliptic scheme \( E_n \). Notice that in the scheme \( \text{Spec}(W/\pi^{n+1}) \) the prime \( \ell \) is locally nilpotent and the closed immersion

\[
\text{Spec}(W/\pi) \hookrightarrow \text{Spec}(W/\pi^{n+1})
\]

is given by the nilpotent ideal \( (\pi)/(\pi^{n+1}) \). We can then apply [7, Theorem 3.3] to see that the commutative diagram

\[
\begin{array}{ccc}
A_{\ell,n} & \hookrightarrow & \text{End}_{W/\pi^{n+1}}(\Gamma_n) \\
\downarrow & & \downarrow \\
A_{\ell,0} & \hookrightarrow & \text{End}_{W/\pi}(\Gamma_0)
\end{array}
\]

is a pull-back. In order to compute the endomorphism rings of the relevant \( \ell \)-divisible groups, we notice that both \( \Gamma_0 \) and \( \Gamma_1 \) are connected since \( E_0 \) is a supersingular elliptic curve. Hence by [33, Proposition 1] for every \( n \in \mathbb{N} \)

\[
\text{End}_{W/\pi^{n+1}}(\Gamma_n) \cong \text{End}_{W/\pi^{n+1}}(\mathcal{F}_n)
\]

where \( \mathcal{F}_n \) is the formal group law over \( W/\pi^{n+1} \) associated to \( \Gamma_n \) (or to \( E_n \)). These latter endomorphism rings can be computed as follows.

First of all notice that, since \( E_0 \) is a supersingular elliptic curve, the formal group \( \mathcal{F}_0 \) has height 2. Let \( \mathcal{F}_E/W \) be the formal group associated to the given integral model of \( E \) and let \( O_u \) be the ring of integers in the unique quadratic unramified extension \( F_u \) of \( \mathbb{Q}_\ell \). Notice that \( F_u = \mathbb{Q}_\ell(\zeta_3) \) because \( \ell \equiv 2 \mod 3 \). Since \( E \) has complex multiplication by \( \mathbb{Z}[\zeta_3] \), the formal group \( \mathcal{F}_E \) has a natural structure of formal \( O_u \)-module, i.e. there exists a ring homomorphism

\[
O_u \to \text{End}_W(\mathcal{F}_E)
\]

which induces the identity on the tangent space \( \text{Lie}(\mathcal{F}_E) \). Composing this isomorphism with the reduction map \( \text{End}_W(\mathcal{F}_E) \to \text{End}_W(\mathcal{F}_0) \), we obtain a ring homomorphism

\[
\alpha : O_u \to \text{End}_W(\mathcal{F}_E) \to \text{End}_W(\mathcal{F}_0)
\]

which gives \( \mathcal{F}_0 \) the structure of formal \( O_u \)-module of height 1. It is now clear that \( \mathcal{F}_E \) must be the canonical lifting of the pair \((\mathcal{F}_0, \alpha)\), as defined in [15, Proposition 2.1]. We can now deduce the endomorphism rings of its reductions modulo \( \pi^{n+1} \) using [14, Proposition 3.3]. We have, for every \( n \geq 0 \),

\[
\text{End}_{W/\pi^{n+1}}(\mathcal{F}_n) \cong O_u + \ell^n R
\]

where \( R \) is the maximal order in the unique division quaternion algebra over \( \mathbb{Q}_\ell \). Hence we can rewrite the commutative diagram (5) as
\[
A_{\ell,n} \hookrightarrow O_u + \ell^nR \\
\downarrow \\
A_{\ell,0} \hookrightarrow R \cong A_{\ell,0} \otimes \mathbb{Z}_\ell
\]

where the bottom horizontal arrow is the natural inclusion in the tensor product. Since this diagram is a pull-back, we have that

\[A_{\ell,n} = A_{\ell,0} \cap (O_u + \ell^nR)\]

where the intersection takes place in \(R\). Since \(O_u = \mathbb{Z}_\ell[\zeta_3]\), using Theorem 3.1 we see that

\[O_u + \ell^nR = \mathbb{Z}_\ell + \mathbb{Z}_\ell\zeta_3 + \mathbb{Z}_\ell\ell^n \frac{2 + \zeta_3 + 2\pi + 3\pi}{3} + \mathbb{Z}_\ell\ell^n - \frac{1 + \zeta_3 - \pi - 2\zeta_3\pi}{3}.
\]

It is now immediate to compute \(A_{\ell,n}\) and to conclude the proof of the theorem.

\[\Box\]

4. The \(\ell\)-adic valuation of a singular modulus

The main goal of this section is to prove the following theorem, which, roughly speaking, gives information about the exponents appearing in the prime factorization of a singular modulus.

**Theorem 4.1.** Let \(j \in \overline{\mathbb{Q}}\) be a singular modulus relative to the order \(O\) of discriminant \(\Delta < -3\) in an imaginary quadratic field \(K\), and let \(\ell \geq 5\) be a prime. Let \(H_O\) be the ring class field of \(K\) relative to the order \(O\) and fix a prime ideal \(\mu \subseteq O_{H,O}\) lying above \(\ell\). Then, if \(v_\mu(\cdot)\) denotes the normalized valuation associated to \(\mu\), we have

\[
v_\mu(j) \leq \begin{cases} 
3 \left( \frac{\log(3|\Delta|)}{2\log \ell} + \frac{1}{2} \right) & \text{if } \ell \nmid \Delta \\
3 & \text{otherwise.}
\end{cases}
\]

We will see at the end of this section that the order of magnitude of the bounds appearing in Theorem 4.1 cannot be significantly improved.

The dichotomy in the statement of Theorem 4.1 is reflected by its proof, which we divide according to whether \(\ell\) divides the discriminant of the order \(O\) or not. In both cases, everything boils down to the study of optimal embeddings of the order \(O\) in a certain family of nested orders \(\{B_n, n \in \mathbb{N}\}\) in the quaternion algebra \(\mathbb{B}_{\ell, \infty}\). The main problem will be determining the first index \(n_0 \in \mathbb{N}\) at which the order \(O\) does not embed anymore in \(B_n\) for \(n \geq n_0\).

In the subsequent proof, we will always use \(\mathbb{F}_\ell\) to denote the finite field with \(\ell\) elements, where \(\ell \in \mathbb{N}\) is a prime number, and by \(\overline{\mathbb{F}}_\ell\) an algebraic closure of this field.

4.1. First case: \(\ell\) does not divide \(\Delta\). Let \(j\) and \(O\) be as in the statement of the theorem, and let \(E_j\) be an elliptic curve defined over the ring class field \(H_O\) with \(j(E_j) = j\). We can always choose an integral model of \(E_j\) that has good reduction at the chosen prime ideal \(\mu\) by [30, Theorem 8 and 9], which we can apply since \(\ell \nmid \Delta\) by assumption.

Set \(H_{O,\mu}\) to be the completion of \(H_O\) at \(\mu\) and note that \(H_{O,\mu}\) is contained in the maximal unramified extension \(\mathbb{Q}_\ell^{unr}\) of \(\mathbb{Q}_\ell\). Indeed, the field extension \(\mathbb{Q} \subseteq H_O\) can ramify only at primes dividing \(\Delta\) [8, pag. 163], and this is not the case for \(\ell\) by our assumptions. We deduce that, by base-change, the elliptic curve \(E_j\) has a model with good reduction over the ring of integers \(W \subseteq L\), where \(L := \overline{\mathbb{Q}}^{unr}_\ell\) is the completion of the maximal unramified extension of \(\mathbb{Q}_\ell\). On the other hand, also the elliptic curve \(E : y^2 = x^3 + 1\) with \(j(E) = 0\) is defined over \(W\) and has good reduction, because \(\ell \geq 5\). We fix these models once for all and we let \(\pi \in W\) be a uniformizer.
Lemma 4.2. In the notation above, we have

$$v_\mu(j) = 3 \cdot \max\{n \in \mathbb{N}_{\geq 1} : \text{Iso}_{W/\pi^n}(E, E_j) \neq \emptyset\}$$

where, for every $n \in \mathbb{N}$, we denote by $\text{Iso}_{W/\pi^n}(E, E_j)$ the set of isomorphisms between $E$ mod $\pi^n$ and $E_j$ mod $\pi^n$.

Proof. Notice first of all that the normalized valuation on $L$, i.e the valuation $v$ satisfying $v(\pi) = 1$, extends the $\mu$-adic valuation $v_\mu$ on $H_O$ because $v_\mu(\ell) = 1$. Since $W$ is a complete discrete valuation ring whose quotient field has characteristic 0 and whose residue field $\overline{\mathbb{Q}_\ell}$ is algebraically closed of characteristic $\ell > 0$, we can apply [16, Proposition 2.3] which gives

$$v_\mu(j) = v_\mu(j - 0) = \frac{1}{2} \sum_{n=1}^{\infty} \# \text{Iso}_{W/\pi^n}(E, E_j).$$

Now, clearly $\text{Iso}_{W/\pi^{n+1}}(E, E_j) \neq \emptyset$ implies $\text{Iso}_{W/\pi^n}(E, E_j) \neq \emptyset$ for every $n \in \mathbb{N}_{\geq 0}$. Moreover, whenever the set $\text{Iso}_{W/\pi^n}(E, E_j)$ is non-empty, its cardinality equals the order of the automorphism group $\text{Aut}_{W/\pi^n}(E)$ of $E$ mod $\pi^n$. By [7, Theorem 2.1 (2)], we always have the inclusions

$$\text{End}_L(E) \hookrightarrow \text{End}_{W/\pi^n}(E) \hookrightarrow \text{End}_{W/\pi}(E)$$

induced respectively by the reduction modulo $\pi^n$ and modulo $\pi$. This means that $\# \text{Aut}_L(E) \leq \# \text{Aut}_{W/\pi^n}(E) \leq \text{Aut}_{W/\pi}(E)$, and we have

$$\# \text{Aut}_L(E) = \# \mathbb{Z} [\zeta_3]^X = 6$$

$$\# \text{Aut}_{W/\pi}(E) = \# A_0^X = 6$$

where $A_0$ is the quaternion order defined in Theorem 3.1 and the last equality follows either by a direct computation or by [32, III, Theorem 10.1]. The lemma follows.

By Lemma 4.2, in order to estimate the valuation at $\mu$ of the singular modulus $j$, we need to bound the biggest index $n$ such that the reduction modulo $\pi^n$ of the elliptic curves $E$ and $E_j$ are isomorphic. If this maximum is 0, then the two elliptic curves are not even isomorphic over $\overline{\mathbb{Q}_\ell} \cong W/\pi$, so the prime $\mu$ cannot divide $j$ and there is nothing to prove. Hence, from now on we suppose that $\mu$ divides $j$ so that $E$ mod $\pi \cong E_j$ mod $\pi$ over $\overline{\mathbb{Q}_\ell}$. Since $\ell$ does not divide the conductor of the order $O$ by assumption, [24, Theorem 13.12] ensures that $\ell$ is a prime of supersingular reduction for both $E$ and $E_j$ and, in particular, that it is congruent to 2 mod 3.

Lemma 4.3. In the setting above, for every $n \in \mathbb{N}_{\geq 1}$ the ring $\text{End}_{W/\pi^n}(E_j)$ is isomorphic to a quaternion order in $\mathbb{B}_{\ell, \infty}$ and the natural injection

$$O \cong \text{End}_W(E_j) \hookrightarrow \text{End}_{W/\pi^n}(E_j)$$

induced by the reduction modulo $\pi^n$ is an optimal embedding.

Proof. The first statement follows from the fact that $\ell$ is a prime of supersingular reduction for $E_j$ and by Serre-Tate theory, see for instance [7, Theorem 3.3]. Reductions modulo $\pi$ and $\pi^n$ give the following diagram

$$O \xleftarrow{\phi_{n-1}} \text{End}_{W/\pi^n}(E_j) \xrightarrow{\phi_0} \text{End}_{W/\pi}(E_j)$$

which clearly commutes. Since $\ell$ does not divide the conductor of the order $O$, the embedding $\phi_0$ is optimal by [25, Proposition 2.2]. It follows from the commutativity of the diagram above that also the embedding $\phi_{n-1}$ is optimal, and the lemma is proved.
Let \( n \in \mathbb{N}_{\geq 1} \) be such that \( \text{Iso}_{W/\mathbb{Q}}(E, E_1) \neq \emptyset \), and choose \( \varphi \in \text{Iso}_{W/\mathbb{Q}}(E, E_1) \). Then the isomorphism \( \varphi \) induces a ring isomorphism
\[
\tilde{\varphi}: \text{End}_{W/\mathbb{Q}}(E_1) \to \text{End}_{W/\mathbb{Q}}(E), \quad \alpha \mapsto \varphi^{-1} \circ \alpha \circ \varphi
\]
which, precomposed with the reduction map \( \mathcal{O} \hookrightarrow \text{End}_{W/\mathbb{Q}}(E_1) \), gives rise to an embedding
\[
(7) \quad \psi_{n-1}: \mathcal{O} \hookrightarrow \text{End}_{W/\mathbb{Q}}(E).
\]
By Lemma 4.3, the injection (7) is an optimal embedding. Recall now that we have explicitly described the orders \( \text{End}_{W/\mathbb{Q}}(E) \) in Theorem 3.2, so that we can identify the chain of injections
\[
\ldots \hookrightarrow \text{End}_{W/\mathbb{Q}}(E) \hookrightarrow \ldots \hookrightarrow \text{End}_{W/\mathbb{Q}}(E) \hookrightarrow \text{End}_{W/\mathbb{Q}}(E)
\]
with the filtration
\[
\ldots \subseteq A_{\ell,n-1} \subseteq \ldots \subseteq A_{\ell,1} \subseteq A_{\ell,0} \subseteq \mathcal{B}_{\ell,\infty}
\]
where \( \mathcal{B}_{\ell,\infty} \) is the unique quaternion algebra over \( \mathbb{Q} \) ramified at \( \ell \) and \( \infty \) with its explicit description given in Section 3, and the rings \( A_{\ell,i} \) have been described in Theorem 3.1 and Theorem 3.2.

We are now ready to prove the first case of Theorem 4.1. To determine whether it is possible that \( \mathcal{O} \) embeds optimally in the quaternion order \( A_{\ell,n} \) for some fixed \( n \in \mathbb{N} \), we want to use Lemma 2.1. First of all we compute, for every \( \Lambda_{\ell,n} \) of the order
\[
A_{\ell,n} := \mathbb{Z}[\zeta_3] + \ell^n A_{\ell,0} = \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\ell^n \beta_1 + \mathbb{Z}\ell^n \beta_2
\]
where
\[
\beta_1 := \frac{2 + \zeta_3 + 2\pi + \zeta_3 \pi}{3} \quad \text{and} \quad \beta_2 := \frac{-1 + \zeta_3 - \pi - 2\zeta_3 \pi}{3}.
\]
The generic element \( \alpha := A + 2B\zeta_3 + 2C\ell^n \beta_1 + 2D\ell^n \beta_2 \in \mathbb{Z} + 2A_{\ell,n} \) with \( A, B, C, D \in \mathbb{Z} \) has reduced trace
\[
\text{trd}(\alpha) = 2A - 2B + 2\ell^n C - 2\ell^n D,
\]
so, requiring that \( \alpha \) lies in the subspace of pure quaternions is equivalent to the condition
\[
A = B - \ell^n C + \ell^n D.
\]
After substituting into the expression for \( \alpha \), we find that \( \mathcal{B} = \{ 1 + 2\zeta_3, \ell^n(2\beta_1 - 1), \ell^n(2\beta_2 + 1) \} \) is a \( \mathbb{Z} \)-basis for \( \Lambda_{\ell,n} \). We obtain a slightly simpler basis if subtract the third element of \( \mathcal{B} \) from the second, reaching in this way
\[
\Lambda_{\ell,n} = \left\{ 1 + 2\zeta_3, \ell^n \cdot \frac{1 + 2\zeta_3 - 2\pi - 4\zeta_3 \pi}{3}, 2\ell^n (\pi + \zeta_3 \pi) \right\}_{\mathbb{Z}}.
\]
The reduced norm restricted to the lattice \( \Lambda_{\ell,n} \) induces the ternary quadratic form
\[
(8) \quad Q_{\ell,n}(X, Y, Z) = 3X^2 + \ell^{2n} \frac{4\ell + 1}{3} Y^2 + 4\ell^{2n+1} Z^2 + 2\ell^n X Y - 4\ell^{2n+1} Y Z
\]
and, by Lemma 2.1, the order \( \mathcal{O} \) embeds optimally in \( A_{\ell,n} \) if and only if \( |\Delta| \) is primitively represented by \( Q_{\ell,n} \) i.e. if and only if there exist \( x, y, z \in \mathbb{Z} \) coprime such that \( Q_{\ell,n}(x, y, z) = |\Delta| \). It is clear that such an equality implies a bound on the integer \( n \).

Consider the change of variables
\[
(9) \quad \widetilde{X} = X + \frac{\ell^n}{3} Y, \quad \widetilde{Y} = Y - \frac{3}{\ell} Z, \quad \widetilde{Z} = Z
\]
that diagonalizes \( Q_{\ell,n} \) as
\[
\widetilde{Q}_{\ell,n}(\widetilde{X}, \widetilde{Y}, \widetilde{Z}) = 3\widetilde{X}^2 + \frac{4}{3} \ell^{2n+1} \widetilde{Y}^2 + \ell^{2n+1} \widetilde{Z}^2.
\]
Suppose that \( Q_{\ell,n}(X, Y, Z) = |\Delta| \) has a primitive integral solution \( (x, y, z) \in \mathbb{Z}^3 \). Then, using the change of variables (9), we see that the equation \( \widetilde{Q}_{\ell,n+1}(X, Y, Z) = |\Delta| \) has a solution
\((x, \tilde{y}, \tilde{z}) \in \left( \frac{1}{2} \mathbb{Z}, \frac{1}{2} \mathbb{Z}, \mathbb{Z} \right)\). Moreover, at least one among \(y\) and \(z\) must be non-zero; otherwise, the only possible primitive solutions to \(Q_{N}(X,Y,Z) = |\Delta|\) are \((\pm 1, 0, 0)\) which give \(\Delta = -3\), a discriminant that is excluded by the assumptions of Theorem 4.1. This implies by (9) that at least one among \(\tilde{y}\) and \(\tilde{z}\) is non-zero. Notice that if \(\tilde{y} \neq 0\) then \(|\tilde{y}| \geq 1/2\), while if \(\tilde{z} \neq 0\) then \(|\tilde{z}| \geq 1\). Hence we obtain

\[|\Delta| = 3x^2 + \frac{4}{3} t^{2n+1} \tilde{y}^2 + t^{2n+1} \tilde{z}^2 \geq \max \left\{ \frac{4}{3} t^{2n+1} \tilde{y}^2, t^{2n+1} \tilde{z}^2 \right\} \geq \frac{1}{3} t^{2n+1}\]

from which, after taking logarithms and rearranging the inequality, we get

\[n + 1 \leq \frac{\log(3|\Delta|)}{2\log t} + \frac{1}{2}.
\]

This is the wanted estimate on \(\max \{n \in \mathbb{N}_{\geq 1} : \text{Iso}_{\eta^m}(E, E_j) \neq \emptyset\}\) that, combined with Lemma 4.2, yields the desired bound for the \(\mu\)-adic valuation of the singular modulus \(j\).

4.2. Second case: \(\ell\) divides \(\Delta\). For this part of the proof, we are going to heavily rely on [25], of which we have kept the notation.

Suppose initially that \(\ell\) divides the conductor of the order \(O\). Let \(E_j\) be an elliptic curve with \(j(E_j) = j\) and let \(F\) be the minimal field extension of the ring class field \(H_O\) such that \((E_j)_{/F}\) has a model with good reduction at all primes dividing \(\ell\). Fix such a prime \(\mu_{\ell} \subseteq O_F\) lying above the prime \(\mu \subseteq H_O\) in the statement of Theorem 4.1 and consider \(L := \mathbb{F}_{\mu_{\ell}}\) (the completion of the maximal unramified extension of \(F_{\mu_{\ell}}\), with ring of integers \(A\). Both \(E\) and \(E_j\) have a model on \(A\) with good reduction at \(\mu_{\ell}\). Since \(A\) is a complete discrete valuation ring of characteristic 0 with algebraically closed residue field of characteristic \(\ell > 0\), we can use the same proof of Lemma 4.2 to see that

\[(10) \quad v_{\mu}(j) \leq 3 \cdot \max \{n \in \mathbb{N}_{\geq 1} : \text{Iso}_{A/\mu^n}(E, E_j) \neq \emptyset\}.
\]

Differently from Lemma 4.2, we only have an inequality in this case. This depends on the fact that the extension \(F \supseteq H_O\) may be ramified at \(\mu\). By [25, Proposition 4.1] one concludes immediately that \(\text{Iso}_{A/\mu^n}(E, E_j) = \emptyset\) if \(n > 1\). Together with inequality (10), this yields the theorem in this case.

Assume now that \(\ell\) divides \(\Delta\) but does not divide the conductor of the order \(O\). Then, if again \(E_j\) is an elliptic curve with \(j(E_j) = j\), we can choose \(F = H_O\) as a field where \(E_j\) has a model with good reduction at all primes dividing \(\ell\). This follows from [30, Theorem 9]. If we complete at \(\mu\), and we take \(A\) to be the ring of integers in the maximal unramified extension of \(H_{O,\mu}\) and \(W\) to be the ring of integers in the completion of the maximal unramified extension of \(Q_{\ell}\), then \(\text{Frac}(W) \subseteq \text{Frac}(A)\) is a ramified degree 2 field extension. Again by [25, Proposition 4.1], since we are assuming \(j \neq 0\) and that \(\ell\) does not divide the conunter of \(O\), for every \(n \in \mathbb{N}_{> 1}\) we have

\[(11) \quad \# \text{Iso}_{A/\mu^n}(E, E_j) \leq 2 \cdot \# S_n^{\text{Lie}}(E/A)\]

where \(S_n^{\text{Lie}}(E/A)\) is the set of all endomorphisms \(\phi \in \text{End}_{A/\mu^n}(E)\) satisfying the following three conditions:

1. \(\phi^2 - \Delta \phi + \frac{1}{4}(\Delta^2 - \Delta) = 0\);
2. The inclusion \(\mathbb{Z}[\phi] \hookrightarrow \text{End}_{A/\mu^n}(E)\) is optimal at all primes \(p \neq \ell\), see [25, Definition 2.1];
3. As endomorphism of \(\text{Lie}(E \text{ mod } \mu^n)\) we have \(\phi \equiv \delta \text{ mod } \mu^n\), where \(\delta \in A\) is a fixed root of the polynomial \(x^2 - Ax + \frac{1}{4}(x^2 - x)\).

The set \(S_n^{\text{Lie}}(E/A)\) can be partitioned as

\[S_n^{\text{Lie}}(E/A) = \bigcup_{m \in \mathbb{N}} S_{n,m}^{\text{Lie}}(E/A)\]
where \( S_{n,m}^{\text{Lie}}(E/A) \) consists of all the endomorphisms \( \varphi \in S_n^{\text{Lie}}(E/A) \) such that
\[
\text{disc } \mathbb{Z}[\zeta_3, \varphi] = m^2.
\]
Notice that, under our assumptions on \( \Delta \), the set \( S_{n,m}^{\text{Lie}}(E/A) \) is empty for every \( n \geq 1 \). Indeed, the discriminant of \( \mathbb{Z}[\zeta_3, \varphi] \) vanishes if and only if this order has rank 2 as a \( \mathbb{Z} \)-module, and this happens if and only if \( \mathbb{Z}[\varphi] \) can be embedded as a subring of \( \mathbb{Z}[\zeta_3] \). However, this cannot be the case under the current hypotheses, since the embedding \( \mathbb{Z}[\varphi] \hookrightarrow \text{End}_{\mathbb{A}^{1/2}}(E) \) is optimal at all primes \( p \neq \ell \) and \( O \) is an order of discriminant \( \Delta < -3 \) whose conductor is not divided by \( \ell \) by assumption.

On the other hand, in the second paragraph of [25, pag. 9247] it is proved that, for every \( m > 0 \) and \( n > 1 \), the set \( S_{n,m}^{\text{Lie}}(E/A) \) is empty. We deduce that \( S_{n,m}^{\text{Lie}}(E/A) = 0 \) for all \( n > 1 \), and combining this with inequalities (11) and (10), we conclude that \( v_\mu(j) \leq 3 \), as we wanted to show. This concludes the proof of Theorem 4.1.

4.3. **Optimality of the obtained bounds.** We now fulfill our promise of showing that the order of magnitude of the bounds appearing in Theorem 4.1 cannot be improved in general. In the case when the considered prime \( \ell \) divides the discriminant of the order \( O \) corresponding to the singular modulus \( j \), it is easy to provide examples in which the second upper-bound of (6) is reached. For instance, each of the singular moduli \( j \) of discriminant \( \Delta = -7 \cdot 5^2 \) is divided by the unique prime \( p_5 \subseteq \mathbb{Q}(j) \) above 5 and we have \( v_{p_5}(j) = 3 \). On the other hand, in the case where \( \ell \) does not divide the discriminant of \( O \) the claimed optimality follows from the following proposition.

**Proposition 4.4.** Let \( \ell \geq 5 \) be a prime with \( \ell \equiv 2 \mod 3 \). There exists an infinite family of singular moduli \( j \) whose corresponding discriminant \( \Delta_j \) is coprime with \( \ell \) and which satisfy
\[
v_\mu(j) \geq 3 \left( \frac{\log(|\Delta_j| - 3)}{2 \log \ell} + \frac{1}{2} - \frac{\log 2}{\log \ell} \right)
\]
for some prime ideal \( \mu \subseteq H\mathcal{O} \) lying above \( \ell \).

We need a preliminary result.

**Proposition 4.5.** Let \( O \) be an order in an imaginary quadratic field \( K \) and \( \ell \in \mathbb{N} \) be a prime which does not divide the conductor of \( O \) and that is inert in \( K \). Let \( W \) be the ring of integers in the completion \( \widehat{\mathbb{Q}_{\ell}}^{\text{unr}} \) of the maximal unramified extension of \( \mathbb{Q}_\ell \), with uniformizer \( \pi \in W \). Fix \( n \in \mathbb{N} \) and let \( E_0 \to \text{Spec}(W/\pi^n) \) an elliptic curve (scheme) such that the reduction modulo \( \pi \) is supersingular. If \( f : O \hookrightarrow \text{End}_{W/\pi^n}(E_0) \) is an optimal embedding, then there exists an elliptic curve \( E/W \) such that
\begin{itemize}
\item \( E \mod \pi^n \cong E_0 \);
\item \( \text{End}_W(E) \cong O \).
\end{itemize}

**Proof.** This is an application Gross and Zagier’s generalization [16, Proposition 2.7] of Deuring lifting Theorem [24, Theorem 13.14]. Note that the proof of Gross and Zagier’s result in the supersingular case does not require, in their notation, the ring \( \mathbb{Z}[\alpha_0] \) to be integrally closed but only \( \ell \) does not dividing its conductor.

Write \( O = \mathbb{Z}[\tau] \) for some imaginary quadratic \( \tau \in K \) and let \( \alpha_0 := f(\tau) \). The endomorphism \( \alpha_0 \) induces on the tangent space \( \text{Lie}(E_0) \) multiplication by an element \( w_0 \in W/\pi^n \) which is a root of the minimal polynomial \( g(x) = x^2 + Ax + B \in \mathbb{Z}[x] \) of \( \tau \) over \( \mathbb{Q} \). In order to apply [16, Proposition 2.7], we need to show that there exists \( w \in W \) such that \( w \mod \pi^n = w_0 \). Let \( \beta := \alpha_0 \mod \pi \in \mathbb{F}_\ell \). Then \( \beta \) is a root of \( g(x) \mod \pi \) lying in \( \mathbb{F}_\ell \). If \( g'(\beta) = 0 \), then \( \beta \) would actually lie in \( \mathbb{F}_\ell \). However, since \( \ell \) is inert in \( O \) and does not divide its conductor, the polynomial \( g(x) \) is irreducible over \( \mathbb{F}_\ell \) by the Kummer-Dedekind Theorem [29, Proposition 1.8.3], and this
implies that the derivative of $g(x)$ does not vanish on $\beta$ (the same argument holds for $\ell = 2$ by choosing appropriately $\tau$ in such a way that its trace is odd). Then by Hensel's lemma there exists a unique $w \in W$ lifting $\beta$. This $w$ satisfies $w \mod \pi^n = w_0$ by construction.

We now apply [16, Proposition 2.7] to deduce that there exists an elliptic curve $E_W$ and an endomorphism $\alpha \in \text{End}_W(E)$ such that $E \mod \pi^n \cong E_0$ and $\alpha \mod \pi^n = \alpha_0$. In principle, the ring $\text{End}_W(E)$ could strictly contain the order $\mathbb{Z}[\alpha]$. However, the reduction map identifies $\mathbb{Z}[\alpha]$ with $O$, and the latter optimally embeds in $\text{End}_W/\pi^n(E_0)$. Since the reduction map also embeds $\text{End}_W(E) \hookrightarrow \text{End}_W/\pi^n(E_0)$, we deduce that $\text{End}_W(E) = \mathbb{Z}[\alpha] \cong O$, as wanted.

**Proof of Proposition 4.4.** For all $n \in \mathbb{N}$ we let $Q_{\ell,n}(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ to be the quadratic form appearing in (8). Proposition 4.5 combined with Lemma 2.1 implies in particular that, for any primitive triple of integers $(x, y, z) \in \mathbb{Z}^3$ such that $-D := Q_{\ell,n}(x, y, z)$ is not divisible by $\ell$, there exists an elliptic curve $E'/w$ with complex multiplication by the order of discriminant $D$ and which is isomorphic to $E : y^2 = x^3 + 1$ modulo $\pi^{n+1}$. The primitive triple $(1, 0, 1)$ gives

$$Q_{\ell,n}(1, 0, 1) = 3 + 4\pi^{2n+1}$$

which is not divisible by $\ell$. The $j$-invariant of the corresponding elliptic curve $E$ with CM by the order of discriminant $D$ will satisfy, by Lemma 4.2, the inequality

$$v_\mu(j) \geq 3(n + 1) = 3\left(\frac{\log(|D| - 3)}{2\log \ell} + \frac{1}{2} - \frac{\log 2}{\log \ell}\right)$$

for some prime $\mu \subseteq H_0$ lying above $\ell$. This concludes the proof of the proposition. \qed

5. A conditional lower bound for the Weil height of a singular modulus

For an elliptic curve $E/L$, defined over a number field $L$, we denote by $h_F(E)$ its stable Faltings height [11, pag. 354] with Deligne’s normalization [9]. We also write $h : \overline{\mathbb{Q}} \to \mathbb{R}$ for the logarithmic Weil height of an algebraic number. The goal of this section is to provide a lower bound for the Weil height of a singular modulus relative to an order in an imaginary quadratic field $K$, under the assumption that the Legendre symbol associated to $K$ satisfies property $P(k)$ (see Definition 1.1) for some non-negative $k \in \mathbb{R}$.

**Proposition 5.1.** Let $j$ be a singular modulus of discriminant $\Delta = f^2 \Delta_K$, where $\Delta_K$ is the discriminant of the imaginary quadratic field $K$ relative to $j$. If for some $k \in \mathbb{R}_{\geq 0}$ property $P(k)$ holds for the non-principal real primitive Dirichlet character $\chi$ of discriminant $\Delta_K$, then

$$h(j) \geq 1.509 \log |\Delta| + C$$

for some absolute constant $C = C(k) \in \mathbb{R}$.

**Proof.** Let $E/\mathbb{Q}(j)$ be an elliptic curve defined with $j(E) = j$. Using [13, Lemma 7.9], the logarithmic Weil height of $j$ can be bounded from below by the stable Faltings height of $E$ as follows

$$h(j) \geq 12 h_F(E) + 8.64.$$  \hspace{1cm} (12)

The stable Faltings height of $E$ can be explicitly computed using the well-known results of Colmez [6] and Nakkajima-Taguchi [28]. One has

$$h_F(E) = \frac{1}{4} \log(|\Delta|) + \frac{1}{2} L'(\chi, 1) - \frac{1}{2} \sum_{p | \ell} e_\ell(p) \log p - \frac{1}{2} (\gamma + \log(2\pi))$$
where $\chi$ is the Kronecker symbol relative to the CM field $K$, $\gamma$ is the Euler-Mascheroni constant, $f$ is the conductor of the CM order and for a prime $p$

$$e_f(p) := \frac{1 - \chi(p)}{p - \chi(p)} \frac{1 - p^{-\omega_p(f)}}{1 - p^{-1}}.$$ 

Using property $P(k)$ we then get

$$h_F(E) > \frac{1}{4} \log(\vert \Delta \vert) + \frac{1}{2} \left( -\frac{1}{2485} \log \vert \Delta_K \vert - k \right) - \frac{1}{2} \left( \sum_{p \mid f} e_f(p) \log p \right) - \frac{1}{2} \left( \frac{1}{2} \gamma + \log(2\pi) \right)$$

$$= \frac{1}{4} \log(\vert \Delta \vert) + \frac{1}{2} \left( -\frac{1}{2485} \log \vert \Delta \vert - 0.2485 \log f^{-2} - k \right) - \frac{1}{2} \left( \sum_{p \mid f} e_f(p) \log p \right) - \frac{1}{2} \left( \frac{1}{2} \gamma + \log(2\pi) \right)$$

$$= 0.12575 \log \vert \Delta \vert + 0.2485 \log f - \frac{1}{2} \left( \sum_{p \mid f} e_f(p) \log p \right) - \frac{1}{2} \left( \frac{1}{2} \gamma + \log(2\pi) + k \right).$$

We want to bound from below the quantity

$$A(f) := 0.2485 \log f - \frac{1}{2} \left( \sum_{p \mid f} e_f(p) \log p \right).$$

To do this, one can proceed exactly as in [2, Section 4]. First, one notices that

$$e_f(p) \leq \frac{2}{p + 1} \cdot \frac{1 - p^{-\omega_p(f)}}{1 - p^{-1}}$$

by considering all the possible values of the Dirichlet character $\chi(p)$. Setting now for all $n \in \mathbb{N}_{>0}$

$$\delta(n) := 0.2485 \log n - \left( \sum_{p \mid n} \frac{\log p}{p + 1} \cdot \frac{1 - p^{-\omega_p(n)}}{1 - p^{-1}} \right),$$

one notices that $\delta(n)$ is an additive function and satisfies $\delta(p^{k+1}) \geq \delta(p^k)$ for all primes $p \in \mathbb{N}$ and integers $k > 0$. Since one has $\delta(2), \delta(3) < 0$ and $\delta(p) > 0$ for all primes $p \geq 5$, we deduce that $\delta(n) \geq \delta(2) + \delta(3)$ for all $n \in \mathbb{N}_{>0}$. We then have

$$A(f) \geq \delta(f) \geq \delta(2) + \delta(3) = 0.2485(\log 2 + \log 3) - \left( \frac{\log 2}{3} + \frac{\log 3}{4} \right) \geq -0.0605.$$

In conclusion, we obtain

(13) $$h_F(E) > 0.12575 \log \vert \Delta \vert - C_0$$

where we set

$$C_0 = \frac{1}{2} \left( \frac{1}{2} \gamma + \log(2\pi) + k \right) + 0.0605.$$

Combining now (12) with (13) we obtain

$$h(j) > 1.509 \log \vert \Delta \vert - 12C_0 + 8.64$$

and this concludes the proof. \qed
6. Proof of Theorem 1.2

We now begin the proof of Theorem 1.2. First of all, we show that it is sufficient to prove that, under the assumptions of the theorem, the set of singular \(\ell\)-units is finite and its cardinality can be effectively bounded. Indeed, suppose that \(j \in \mathbb{Q}\) is a singular \(S\)-unit and assume that \(p \in S_0\) is a prime dividing its norm \(N_{\mathbb{Q}(j)/\mathbb{Q}}(j)\). It has been proved in [5, Theorem 1.2] that in this case, there are at least other 3 primes not congruent to 1 modulo 3 dividing its norm. In particular, \(j\) cannot be a singular \(S\)-unit (the existence of this argument is also remarked in [22, Section 1.1]).

Hence we are reduced to bound the number of singular \(\ell\)-units for \(\ell \geq 5\) a prime congruent to 2 modulo 3. To this aim, we follow the strategy used in [2] to prove the emptiness of the set of singular units. Let \(j\) be a singular \(\ell\)-unit relative to the order \(O\) of discriminant \(\Delta\), and let \(h(j)\) be its logarithmic Weil height. By the usual properties of height functions [4, Lemma 1.5.18], we have

\[
\begin{align*}
\sum_{\nu | \ell} d_{\nu} \log |j^{-1}|_{\nu} = A + N
\end{align*}
\]

where \(d_{\nu} := [\mathbb{Q}_{\nu}(j) : \mathbb{Q}_{\nu}]\) is the local degree at the place \(\nu\) and

\[
A := \sum_{\nu | \ell} d_{\nu} \log |j^{-1}|_{\nu} \quad \text{and} \quad N := \sum_{\nu | \ell} d_{\nu} \log |j^{-1}|_{\nu}
\]

are, respectively, the archimedean and non-archimedean components of the height. Notice that the expression for \(N\) follows from our assumption of \(j\) being an \(\ell\)-unit.

The archimedean component \(A\) has been studied in [2, Corollary 3.2]. Here it is proved that, for \(|\Delta| \geq 10^{14}\), we have

\[
A \leq \frac{12 F \log |\Delta|}{h_\Delta} + 3 \log \frac{F |\Delta|^{1/2} \log |\Delta|}{h_\Delta} - 3.77
\]

where \(h_\Delta\) is the class number of the order of discriminant \(\Delta\) and \(F = \max\{2^{\omega(a)} : a \leq \sqrt{|\Delta|}\}\).

As far as the non-archimedean part is concerned, we have

\[
N = \sum_{\nu | \ell} d_{\nu} \log |j^{-1}|_{\nu} = \sum_{\nu | \ell} \nu_p(j) \log \ell_\nu = \frac{\log \ell}{[\mathbb{Q}(j) : \mathbb{Q}]} \sum_{\nu | \ell} \nu_p(j) f_p
\]

where \(f_p\) denotes the residue degree of the prime \(\nu \subseteq \mathbb{Q}(j)\) lying above \(\ell\). For every such \(p\), we choose a prime ideal \(\mu \subseteq H_O\) that divides \(p\). Using Theorem 4.1 we have

\[
\nu_p(j) \leq \nu_p(\ell) \leq \max \left\{ 3 \left( \frac{\log 3 |\Delta|}{2 \log \ell} + \frac{1}{2} \right), 3 \right\}
\]

and, combining this estimate with equality (16), we get

\[
N \leq \log \ell \cdot \max \left\{ 3 \left( \frac{\log 3 |\Delta|}{2 \log \ell} + \frac{1}{2} \right), 3 \right\} \frac{1}{[\mathbb{Q}(j) : \mathbb{Q}]} \sum_{\nu | \ell} f_p \leq \max \left\{ \frac{3}{2} \log 3 |\Delta| + \log \ell, 3 \log \ell \right\}.
\]

Using now (15) and (17) in (14), we obtain

\[
\begin{align*}
\sum_{\nu | \ell} d_{\nu} \log |j^{-1}|_{\nu} &= A + N \\
&\leq \frac{12 F \log |\Delta|}{h_\Delta} + 3 \log \frac{F |\Delta|^{1/2} \log |\Delta|}{h_\Delta} - 3.77 + \max \left\{ \frac{3}{2} \log 3 |\Delta| + \log \ell, 3 \log \ell \right\}
\end{align*}
\]
for $|\Delta| \geq 10^{14}$. As far as lower bounds for the height are concerned, Proposition 5.1 gives a first conditional estimate. In order to have a good lower bound also in the case the class number $h_\Delta$ is small, we will use [2, Proposition 4.1], where it is proved that

\begin{equation}
\frac{\pi |\Delta|^{1/2} - 0.01}{h_\Delta} \leq h(j)
\end{equation}

for $|\Delta| \geq 16$. Combining then the lower bounds in Proposition 5.1 and (19) with the upper bound (18) we obtain

\begin{align*}
Y(\Delta) &\leq \frac{12F \log |\Delta|}{h_\Delta} + 3 \log \frac{F |\Delta|^{1/2} \log |\Delta|}{h_\Delta} - 3.76 + \max \left\{ \frac{3}{2} (\log 3|\Delta| + \log \ell), 3 \log \ell \right\}
\end{align*}

for $|\Delta| \geq 10^{14}$, where

\begin{align*}
Y(\Delta) &:= \max \left\{ \frac{\pi |\Delta|^{1/2}}{h_\Delta}, 1.509 \log |\Delta| + C \right\}
\end{align*}

and $C \in \mathbb{R}$ is the constant appearing in Proposition 5.1. Then dividing both sides of the inequality by $Y(\Delta)$ and rearranging the terms we get

\begin{equation}
1 \leq A(\Delta) + B(\Delta) + C(\Delta) + D(\Delta)
\end{equation}

where

\begin{align*}
A(\Delta) &= \frac{12F \log |\Delta|}{h_\Delta Y(\Delta)} \\
B(\Delta) &= \frac{3}{Y(\Delta)} \log (F \log |\Delta|) - \frac{3.76}{Y(\Delta)} \\
C(\Delta) &= \frac{3}{Y(\Delta)} \log \left( \frac{|\Delta|^{1/2}}{h_\Delta} \right) \\
D(\Delta) &= \frac{1}{Y(\Delta)} \max \left\{ \frac{3}{2} (\log 3|\Delta| + \log \ell), 3 \log \ell \right\}
\end{align*}

The quantities $A(\Delta), B(\Delta)$ and $C(\Delta)$ can be studied as in [2, Section 5]. More precisely, suppose that $|\Delta| \geq 10^{15}$. One has

\begin{equation}
A(\Delta) = \frac{12F \log |\Delta|}{h_\Delta Y(\Delta)} \leq \frac{12}{\pi} \frac{F \log |\Delta|}{|\Delta|^{1/2}} \leq \frac{12}{\pi} 0.0014 < 0.0054
\end{equation}

where the second inequality is the same appearing at the end of [2, Section 5.3]. Moreover using

\begin{equation}
\log (F \log |\Delta|) \leq \frac{\log 2}{2} \cdot \frac{\log |\Delta|}{\log \log |\Delta| - c_1 - \log 2} + \log \log |\Delta|
\end{equation}

which is [2, Inequality (5.8)] (here $c_1 \in \mathbb{R}$ is a fixed constant), we have that, for every $\varepsilon_B > 0$, the inequality

\begin{equation}
B(\Delta) \leq \frac{3}{1.509 \log |\Delta| + C} \left( \frac{\log 2}{2} \cdot \frac{\log |\Delta|}{\log \log |\Delta| - c_1 - \log 2} + \log \log |\Delta| \right) < \varepsilon_B
\end{equation}

holds for $|\Delta|$ sufficiently large. Finally, using the fact that $x \mapsto \log(x)/x$ is a decreasing function when $x \geq 4$, for every $\varepsilon_C > 0$ one has
Finally, as in \([2, \text{Proposition 4.3}]\) one gets the lower bound for the Weil height of a singular modulus of discriminant \(\Delta\), and is not sufficient for our purposes.

Since \(j\) for every \(\Delta\) holds for
\[\text{Lemma 14 (ii)},\] the lower bound
\[\text{derivative known to the author can be deduced from [1, Theorem 1]}, \text{which yields, as in [18, Lemma 14 (ii)]}, \text{the lower bound}\]
\[(20)\]
\[
D(\Delta) = \frac{3}{2} \left( \log |\Delta| + \log \ell \right) = \frac{3}{2} \left( \log |\Delta| + \log 3 + \log \ell \right).
\]

Since
\[
\log |\Delta| = \frac{\log |\Delta|}{Y(\Delta)} \leq \frac{\log |\Delta|}{1.509 \log |\Delta| + C} = (1.509)^{-1} \frac{1.509^{-1} \log |\Delta| + C}{1.509 \log |\Delta| + C}
\]
for every \(\epsilon_D > 0\), we have
\[(24) D(\Delta) \leq \frac{3}{2} \left( (1.509)^{-1} - \frac{(1.509)^{-1} \log |\Delta| + C}{1.509 \log |\Delta| + C} \right) \leq 0.9941 + \epsilon_D
\]
for \(|\Delta| \gg \ell\).

We can now combine (21), (22), (23), (24) with (20) to obtain
\[1 \leq 0.0054 + \epsilon_B + \epsilon_C + 0.9941 + \epsilon_D = 0.9996 + \epsilon_B + \epsilon_C + \epsilon_D
\]
which holds for \(|\Delta| \gg \ell\). Choosing \(\epsilon_B, \epsilon_C, \epsilon_D\) small enough, the inequality cannot be verified for arbitrary large \(|\Delta|\). This proves that there are finitely many singular \(\ell\)-units and concludes the proof of Theorem 1.2.

7. Conclusions and remarks

We make here some comments concerning Theorem 1.2 and its proof. First of all, the proof of Theorem 1.2 is in principle completely explicit. However, the bounds on the number of singular \(S_F\)-units that one obtains from the argument are clearly too big to be used for any numerical search. On the other hand, a precise answer to a question such as “How many singular \(11\)-units exist?” would in all probability require the development of an efficient algorithm to test whether a given singular modulus is an \(S\)-unit for a specified finite set of primes \(S\). We are not aware of the existence of such an algorithm.

Ultimately, the reason why we are forced to rely on property \(P(k)\) to prove our bounds is the fact that the elliptic curve \(E : y^2 = x^3 + 1\) has too many automorphisms in characteristic \(\ell \geq 5\) (in characteristic \(\ell = 2\) or \(\ell = 3\) there are even more automorphisms, which is the reason why these two primes are excluded even conditionally). This leads to a coefficient \(3/2\) in the first estimate of Theorem 4.1, and the known lower bounds on the logarithmic derivative of an \(L\)-function attached to an imaginary quadratic field become too weak in order to prove, using our methods, that estimate (20) does not hold for \(|\Delta|\) big. The best bound on this logarithmic derivative known to the author can be deduced from [1, Theorem 1], which yields, as in [18, Lemma 14 (ii)], the lower bound
\[h_F(E) \geq \frac{\sqrt{5}}{20} \log |\Delta| - 5.93 \approx 0.1118 \log |\Delta| - 5.93
\]
on the stable Faltings height of an elliptic curve \(E\) with CM by an order of discriminant \(\Delta\). Finally, as in [2, Proposition 4.3] one gets the lower bound
\[(25) h(j) \geq \frac{3}{\sqrt{5}} \log |\Delta| - 9.79 \approx 1.3416 \log |\Delta| - 9.79
\]
for the Weil height of a singular modulus of discriminant \(\Delta\). This bound is slightly weaker than the one present in Proposition 5.1, and is not sufficient for our purposes.
However, it appears that the same strategy used in this manuscript could actually yield effective unconditional results on the finiteness of the set of singular moduli \( j \) such that \( j - j_0 \) is an \( S \)-unit, for a fixed singular modulus \( j_0 \neq 0 \) and specific sets of primes \( S \) depending on \( j_0 \). This is because CM elliptic curves \( E \) with \( j(E) = j_0 \neq 0 \) do not have many automorphisms in positive characteristic. These ideas will be object of future research.

We conclude by proving Theorem 1.3.

**Proof of Theorem 1.3.** Let \( \ell \geq 5 \) be any prime. Again using [5, Theorem 1.2] we can reduce to study only the set of singular \( \ell \)-units. If \( j \in \mathbb{Q} \) is a singular \( \ell \)-unit of discriminant \( \Delta \) and \( \ell \mid \Delta \), Theorem 4.1 ensures that \( v_\mu(j) \leq 3 \) for every prime \( \mu \subseteq \mathbb{Q}(j) \) lying above \( \ell \). Then we see that the non-archimedean part \( N \) of the Weil height \( h(j) \) is bounded by \( 3 \log \ell \). Under these circumstances, the unconditional lower bound (25) is enough to make the proof in Section 6 work in exactly the same way. \( \square \)

**Acknowledgments**

The author would like to thank Fabien Pazuki for his constant support and for the comments on previous versions of this manuscript. He would also like to thank Philipp Habegger for the many discussions had during and after the author’s stay at the University of Basel, and for his comments. Finally he would like to thank Jared Asuncion, Yuri Bilu, Florent Jouve, Riccardo Pengo and Emanuele Tron for the useful discussions.

This project has received funding from the European Union Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 801199.

**References**

[1] A. I. Badzyan. “The Euler-Kronecker constant”. In: *Mat. Zametki* 87.1 (2010), pp. 35–47 (cit. on pp. 2, 19).

[2] Y. Bilu, P. Habegger, and L. Kühne. “No singular modulus is a unit”. In: *International Mathematics Research Notices* (2018) (cit. on pp. 1, 3, 16–19).

[3] Y. Bilu, D. Masser, and U. Zannier. “An effective “theorem of André” for CM-points on a plane curve”. In: *Math. Proc. Cambridge Philos. Soc.* 154.1 (2013), pp. 145–152 (cit. on p. 1).

[4] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*. Vol. 4. New Mathematical Monographs. Cambridge University Press, Cambridge, 2006, pp. xvi+652 (cit. on p. 17).

[5] F. Campagna. “On singular moduli that are \( S \)-units”. In: *manuscripta mathematica* (2020), pp. 1–18 (cit. on pp. 1, 3, 17, 20).

[6] P. Colmez. “Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe”. In: *Compositio Math.* 111.3 (1998), pp. 359–368 (cit. on pp. 3, 15).

[7] B. Conrad. “Gross-Zagier revisited”. In: *Heegner points and Rankin L-series*. Vol. 49. Math. Sci. Res. Inst. Publ. With an appendix by W. R. Mann. Cambridge Univ. Press, Cambridge, 2004, pp. 67–163 (cit. on pp. 6, 9, 11).

[8] D. A. Cox. *Primes of the form \( x^2 + ny^2 \).* Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013, pp. xviii+356 (cit. on pp. 1, 4, 10).

[9] P. Deligne. “Preuve des conjectures de Tate et de Shafarevitch (d’après G. Faltings)”. In: 121-122. Seminar Bourbaki, Vol. 1983/84. 1985, pp. 25–41 (cit. on p. 15).

[10] M. Deuring. “Die typen der multiplikatorenringe elliptischer funktionenkörper”. In: *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*. Vol. 14. 1. Springer. 1941, pp. 197–272 (cit. on p. 4).
[11] G. Faltings. “Erratum: “Finiteness theorems for abelian varieties over number fields””. In: Invent. Math. 75.2 (1984), p. 381 (cit. on p. 15).
[12] G. Frei. “Heinrich Weber and the emergence of class field theory”. In: The history of modern mathematics, Vol. I (Poughkeepsie, NY, 1989). Academic Press, Boston, MA, 1989, pp. 425–450 (cit. on p. 1).
[13] É. Gaudron and G. Rémond. “Théorème des périodes et degrés minimaux d’isogénies”. In: Comment. Math. Helv. 89.2 (2014), pp. 343–403 (cit. on p. 15).
[14] B. H. Gross. “Heights and the special values of L-series”. In: Number theory (Montreal, Que., 1985). Vol. 7. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1987, pp. 115–187 (cit. on pp. 5, 9).
[15] B. H. Gross. “On canonical and quasicanonical liftings”. In: Invent. Math. 84.2 (1986), pp. 321–326 (cit. on pp. 6, 9).
[16] B. H. Gross and D. B. Zagier. “On singular moduli”. In: J. Reine Angew. Math. 355 (1985), pp. 191–220 (cit. on pp. 3, 6, 11, 14, 15).
[17] P. Habegger. “Weakly bounded height on modular curves”. In: Acta Math. Vietnam. 35.1 (2010), pp. 43–69 (cit. on p. 2).
[18] P. Habegger, G. Jones, and D. Masser. “Six unlikely intersection problems in search of effectivity”. In: Math. Proc. Cambridge Philos. Soc. 162.3 (2017), pp. 447–477 (cit. on p. 19).
[19] P. Habegger. “Singular moduli that are algebraic units”. In: Algebra Number Theory 9.7 (2015), pp. 1515–1524 (cit. on p. 1).
[20] S. Herrero, R. Menares, and J. Rivera-Letelier. “p-adic distribution of CM points and Hecke orbits I: Convergence towards the Gauss point”. In: Algebra Number Theory 14.5 (2020), pp. 1239–1290 (cit. on p. 1).
[21] S. Herrero, R. Menares, and J. Rivera-Letelier. “p-Adic distribution of CM points and Hecke orbits. II: Linnik equidistribution on the supersingular locus”. In: arXiv e-prints, arXiv:2102.04865 (Feb. 2021), arXiv:2102.04865. arXiv: 2102 . 04865 [math . NT] (cit. on p. 1).
[22] S. Herrero, R. Menares, and J. Rivera-Letelier. “There are at most finitely many singular moduli that are S-units”. In: arXiv e-prints, arXiv:2102.05041 (Feb. 2021), arXiv:2102.05041. arXiv: 2102 . 05041 [math . NT] (cit. on pp. 1, 3, 17).
[23] L. Kühne. “An effective result of André-Oort type”. In: Ann. of Math. (2) 176.1 (2012), pp. 651–671 (cit. on p. 1).
[24] S. Lang. Elliptic functions. Second edition. Vol. 112. Springer, New York, NY, 1987 (cit. on pp. 4, 6, 11, 14).
[25] K. Lauter and B. Viray. “On singular moduli for arbitrary discriminants”. In: Int. Math. Res. Not. IMRN 19 (2015), pp. 9206–9250 (cit. on pp. 3, 6, 9, 11, 13, 14).
[26] Y. Li. “Singular Units and Isogenies Between CM Elliptic Curves”. In: arXiv e-prints, arXiv:1810.13214 (Oct. 2018), arXiv:1810.13214. arXiv: 1810 . 13214 [math . NT] (cit. on p. 1).
[27] M. Mourtada and V. Kumar Murty. “Omega theorems for $L_F(1, \chi_D)$”. In: Int. J. Number Theory 9.3 (2013), pp. 561–581 (cit. on p. 2).
[28] Y. Nakkajima and Y. Taguchi. “A generalization of the Chowla-Selberg formula”. In: J. Reine Angew. Math. 419 (1991), pp. 119–124 (cit. on pp. 3, 15).
[29] J. Neukirch. Algebraic number theory. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571 (cit. on p. 14).
[30] J.-P. Serre and J. Tate. “Good reduction of abelian varieties”. In: Ann. of Math. (2) 88 (1968), pp. 492–517 (cit. on pp. 10, 13).
[31] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525 (cit. on p. 4).

[32] J. H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513 (cit. on pp. 4, 11).

[33] J. T. Tate. “p-divisible groups”. In: *Proc. Conf. Local Fields* (Driebergen, 1966). Springer, Berlin, 1967, pp. 158–183 (cit. on p. 9).

[34] J. Voight. *Quaternion algebras*. v.0.9.23, August 2, 2020 (cit. on pp. 4, 7).

Francesco Campagna - Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

Email address: campagna@math.ku.dk