Separating singular moduli and the primitive
element problem

Yuri BILU, Bernadette FAYE, Huilin ZHU

March 19, 2019

Abstract
We prove that \(|x - y| \geq 800X^{-4}\), where \(x\) and \(y\) are distinct singular moduli of discriminants not exceeding \(X\). We apply this result to the “primitive element problem” for two singular moduli. In a previous article Faye and Riffaut show that the number field \(\mathbb{Q}(x, y)\), generated by two singular moduli \(x\) and \(y\), is generated by \(x - y\) and, with some exceptions, by \(x + y\) as well. In this article we fix a rational number \(\alpha \neq 0, \pm 1\) and show that the field \(\mathbb{Q}(x, y)\) is generated by \(x + \alpha y\), with a few exceptions occurring when \(x\) and \(y\) generate the same quadratic field over \(\mathbb{Q}\). Together with the above-mentioned result of Faye and Riffaut, this gives a drastic generalization of a theorem due to Allombert et al. (2015) about solution of linear equations in singular moduli.

Contents

1 Introduction 1
2 Complex analysis lemmas 4
3 Estimates for the \(j\)-invariant and its derivative 6
4 Separating distinct \(j\)-values 12
5 Separating imaginary quadratic numbers 15
6 Separating singular moduli 17
7 More on singular moduli 19
8 The primitive element 21

1 Introduction
A singular modulus is the \(j\)-invariant of an elliptic curve with complex multiplication. Given a singular modulus \(x\) we denote by \(\Delta_x\) the discriminant of the associated imaginary quadratic order. We denote by \(h(\Delta)\) the class number of the imaginary quadratic order of discriminant \(\Delta\). Recall that two singular moduli \(x\) and \(y\) are conjugate over \(\mathbb{Q}\) if and only if \(\Delta_x = \Delta_y\), and that all singular moduli of a given discriminant \(\Delta\) form a full Galois orbit over \(\mathbb{Q}\). In particular, \([\mathbb{Q}(x) : \mathbb{Q}] = h(\Delta_x)\). For all details, see, for instance, [6 §7 and §11].
In some of the recent works on Diophantine properties of singular moduli a crucial role belongs to the lower estimate for a non-zero singular modulus. Lower bounds of the the shape $|x| \gg |\Delta x|^{-c}$ with some $c > 0$ and explicit absolute constant, are obtained and used in [5, 8, 4, 3].

In this article we obtain a totally explicit lower bound for the difference $|x - y|$, where $x$ and $y$ are distinct singular moduli. Since 0 is a singular modulus, this generalizes the previous lower bounds for $|x|$.

**Theorem 1.1.** Let $x$ and $y$ be distinct singular moduli. Then

$$|x - y| \geq 800 \max\{|\Delta x|, |\Delta y|\}^{-4}.$$ 

In fact, we obtain a more precise statement, see Theorem 6.1.

We apply Theorem 1.1 to the “Primitive Element Problem” for singular moduli. From the undergraduate course of Algebra we know that, given a field $k$ of characteristic 0 and $x, y$ algebraic over $k$, the field $k(x, y)$ has a generator (called sometimes “primitive element”) of the form $x + \alpha y$, where $\alpha \in k$. Moreover, any non-zero $\alpha$ would do with finitely many exceptions, and often this set of exceptions is empty.

We consider the case $k = \mathbb{Q}$ and $x, y$ singular moduli, and we study the question “does $x + \alpha y$ generate $\mathbb{Q}(x, y)$ for all $\alpha \in \mathbb{Q}^\times$?”. To motivate this question, recall that, starting from the ground-breaking article of André [2], equations involving singular moduli were studied by many authors, see [1, 4, 11] for a historical account and further references. In particular, Kühne [10] proved that equation $x + y = 1$ has no solutions in singular moduli $x$ and $y$. This was generalized in [1], where solutions in singular moduli of a general linear equation with rational coefficients are classified.

**Theorem 1.2.** [1, Theorem 1.2] Let $A, B, C$ be rational numbers such that $AB \neq 0$. Let $x$ and $y$ be singular moduli such that $Ax + By = C$. Then either $A + B = C = 0$ and $x = y$, or the field $\mathbb{Q}(x) = \mathbb{Q}(y)$ is of degree at most 2 over $\mathbb{Q}$.

Note that lists of all imaginary quadratic discriminants $\Delta$ with $h(\Delta) \leq 2$ are widely available, so Theorem 1.2 is fully explicit.

One can re-state Theorem 1.2 as follows.

**Theorem 1.2′.** Let $\alpha$ be a non-zero rational number, and let $x, y$ be singular moduli such that $x + \alpha y \in \mathbb{Q}$. Then either $\alpha = -1$ and $x = y$ or the field $\mathbb{Q}(x) = \mathbb{Q}(y)$ is of degree at most 2 over $\mathbb{Q}$.

This raises the following natural question: what is the number field generated by $x + \alpha y$? It is clearly a subfield of $\mathbb{Q}(x, y)$, and one may wonder how smaller than $\mathbb{Q}(x, y)$ this field is. The problem is trivial when $x = y$, so we may assume that $x \neq y$.

In the special case $\alpha = \pm 1$ this question was addressed in [4]. It turns out that $x - y$ always generates $\mathbb{Q}(x, y)$, and $x + y$ generates a subfield of $\mathbb{Q}(x, y)$.
of degree at most 2, which is most often $\mathbb{Q}(x,y)$ itself. To be precise, we have the following statement.

**Theorem 1.3.** [7, Theorem 4.1] Let $x,y$ be distinct singular moduli and let $\alpha \in \{\pm 1\}$. Then $\mathbb{Q}(x,y) = \mathbb{Q}(x+\alpha y)$, unless $\alpha = 1$ and $\Delta x = \Delta y$, in which case we have $[\mathbb{Q}(x,y) : \mathbb{Q}(x+y)] \leq 2$.

In the present article we study the case $\alpha \neq \pm 1$. There is one obvious case when $x + \alpha y$ does not generate $\mathbb{Q}(x,y)$.

**Example 1.4.** Let $x$ and $y$ generate the same number field of degree 2 over $\mathbb{Q}$, and denote $x', y'$ their respective conjugates over $\mathbb{Q}$. Set

$$\alpha = -\frac{x - x'}{y - y'}.$$ (1.1)

Then $\alpha \in \mathbb{Q}$ and $x + \alpha y \in \mathbb{Q}$; hence $x + \alpha y$ cannot generate the quadratic field $\mathbb{Q}(x,y)$.

Note that when in this example $\Delta x = \Delta y$, then $\alpha = 1$, and we are in a special case of Theorem 1.3. On the other hand, if $\Delta x \neq \Delta y$, then $\alpha \neq \pm 1$ by Theorem 1.3.

All cases of Example 1.4 can be easily listed using the available lists of imaginary quadratic discriminants of class number 2.

Our principal result tells that Example 1.4 lists all cases when $x + \alpha y$ is not a primitive element of $\mathbb{Q}(x,y)$.

**Theorem 1.5.** Let $\alpha \neq 0, \pm 1$ be a rational number and $x,y$ singular moduli. Then either $\mathbb{Q}(x+\alpha y) = \mathbb{Q}(x,y)$, or $x,y, \alpha$ are as in Example 1.4, that is

1. $x$ and $y$ generate the same number field, which is of degree 2 over $\mathbb{Q}$;
2. $\Delta x \neq \Delta y$;
3. $\alpha = -(x - x')/(y - y')$, where $x', y'$ are the conjugates of $x, y$ over $\mathbb{Q}$.

Note that we do not assume $x \neq y$, because the statement holds trivially for $x = y$.

Together with Theorem 1.3 this gives a far-going generalization of Theorem 1.2.

**Acknowledgments** We thank Sasha Borichev, Lars Kühne and Ricardo Meana for very useful discussions.

All calculations were performed using PARI [12] or SAGE [13]. We thank Bill Allombert and Karim Belabas for the PARI tutorial. Our PARI scripts can be viewed here:

https://github.com/yuribilu/Separating/blob/master/scripts.gp
1.1 General conventions

Unless the contrary is stated explicitly, everywhere below the letter \( \Delta \) stands for an imaginary quadratic discriminant, that is, \( \Delta < 0 \) and satisfies \( \Delta \equiv 0, 1 \mod 4 \).

We denote by \( \mathcal{O}_\Delta \) the imaginary quadratic order of discriminant \( \Delta \), that is, \( \mathcal{O}_\Delta = \mathbb{Z}[\sqrt[2]{\Delta}] \). Then \( \Delta = Df^2 \), where \( D \) is discriminant of the number field \( K = \mathbb{Q}(\sqrt{\Delta}) \) (called the fundamental discriminant of \( \Delta \)) and \( f = [\mathcal{O}_D : \mathcal{O}_\Delta] \) is called the conductor of \( \Delta \).

We denote by \( h(\Delta) \) the class number of \( \mathcal{O}_\Delta \).

Given a singular modulus \( x \), we write \( \Delta_x = Dxf_x^2 \) with \( D_x \) the fundamental discriminant and \( f_x \) the conductor. We denote by \( \tau_x \) the only \( \tau \) is the standard fundamental domain such that \( j(\tau) = x \). Further, we denote by \( K_x \) the associated imaginary quadratic field

\[ K_x = \mathbb{Q}(\tau_x) = \mathbb{Q}(\sqrt{D_x}) = \mathbb{Q}(\sqrt{\Delta_x}). \]

We will call \( K_x \) the CM-field of the singular modulus \( x \).

2 Complex analysis lemmas

In this section and in the subsequent Sections 3 and 4 the letters \( z \) and \( w \) usually stand for complex numbers, and we will systematically write

\[ z = x + yi, \quad w = u + vi. \]

In particular, in these three sections \( x \) and \( y \) will denote real numbers, not singular moduli.

We denote by \([z, w]\) the straight line segment connecting \( z, w \in \mathbb{C} \):

\[ [z, w] = \{zt + w(1 - t) : t \in [0, 1]\}. \]

Lemma 2.1. Let \( z, w \in \mathbb{C} \) and let \( f \) be a holomorphic function on a neighborhood of \([z, w]\). Then

\[ |f(z) - f(w)| \leq |z - w| \max\{|f'(\xi)| : \xi \in [z, w]\}. \]

Proof. Consider the function \( g(t) = f(zt + w(1 - t)) \) on the interval \([0, 1]\). We have

\[ |g(1) - g(0)| = \left| \int_0^1 g'(t)dt \right| \leq \max\{|g'(t)| : t \in [0, 1]\}. \]

Since \( g(1) - g(0) = f(z) - f(w) \) and \( g'(t) = f'(zt + w(1 - t))(z - w) \), the result follows. \( \square \)

This lemma gives an upper estimate for the difference \( |f(z) - f(w)| \) in terms of \(|z - w|\). For the lower estimate we use the following lemma, which is Lemma 2.4 from [4].
Lemma 2.2. Let $f$ be a holomorphic function in an open neighborhood of the disc $|z - a| \leq R$ and assume that $|f(z)| \leq B$ in this disc. Further, let $\ell$ be a non-negative integer such that $f^{(k)}(a) = 0$ for $0 \leq k < \ell$ and $f^{(\ell)}(a) \neq 0$. Set $A = f^{(\ell)}(a)/\ell!$. Then in the same disc we have the estimate

$$|f(z) - A(z - a)^\ell| \leq \frac{|A|R^\ell + B}{R^{\ell+1}}|z - a|^\ell+1.$$ 

We will also need the following explicit version of the Inverse Function Theorem.

Lemma 2.3. Let $f$ be a holomorphic function in an open neighborhood of the disc $|z - a| \leq R$ and assume that $|f(z) - f(a)| \leq B$ in this disc. Assume further that $f'(a) = A \neq 0$. Set

$$C = \frac{|A|}{R} + \frac{B}{R^2},$$

and let $r$ be a positive number satisfying

$$r \leq \min \left\{ R, \frac{|A|}{3C} \right\}. \quad (2.1)$$

Then for any $w \in \mathbb{C}$ satisfying

$$|w - f(a)| \leq \frac{|A|}{2}r \quad (2.2)$$

there exists a unique $z$ in the disc $|z - a| \leq r$ such that $f(z) = w$.

Proof. Lemma 2.2 implies that in the disc $|z - a| \leq R$ we have

$$|f(z) - f(a) - A(z - a)| \leq C|z - a|^2.$$ 

Then on the circle $|z - a| = r$ we have

$$|f(z) - w - (f(a) + A(z - a) - w)| \leq Cr^2,$$

$$|f(a) + A(z - a) - w| \geq \frac{|A|}{2}r,$$

where in the second inequality we use (2.2).

From our definition of $r$ it follows that

$$|f(z) - w - (f(a) + A(z - a) - w)| < |f(a) + A(z - a) - w|$$

on the circle $|z - a| = r$. Since the equation $f(a) + A(z - a) = w$ has exactly one solution in $z$, and this solution belongs to the disc $|z - a| \leq r$ (we again use (2.2) here), the Theorem of Rouché implies that the equation $f(z) = w$ also has a unique solution in the same disc. \qed
Lemma 2.4. 1. For \( z \in \mathbb{C} \) satisfying \( |z| < 1 \) we have

\[
|e^z - 1| \geq |z| \frac{1 - |z|}{1 - |z|/2} \tag{2.3}
\]

In particular, if \( |z| \leq 1/2 \) then

\[
|e^z - 1| \geq \frac{2}{3}|z|. \quad \tag{2.4}
\]

2. Let \( z = x + yi \in \mathbb{C} \) satisfy

\[
x \leq 0, \quad |y| \leq \pi, \quad |z| \geq 1/2. \tag{2.5}
\]

Then

\[
|e^z - 1| \geq 0.27. \quad \tag{2.6}
\]

Proof. We have

\[
|e^z - 1| \geq |z| - \sum_{k=2}^{\infty} \frac{|z|^k}{k!} \geq |z| - |z| \sum_{k=1}^{\infty} \left( \frac{|z|}{2} \right)^k = |z| \frac{1 - |z|}{1 - |z|/2}.
\]

This proves (2.3) for \( |z| < 1 \), and (2.4) for \( |z| \leq 1/2 \) is an immediate consequence.

Now assume that \( z \) satisfies (2.5). If \( x \leq -0.32 \) then

\[
|e^z - 1| \geq 1 - e^{-0.32} > 0.27.
\]

Now assume that \(-0.32 \leq x \leq 0\). Then

\[
\pi \geq |y| \geq \sqrt{0.5^2 - 0.32^2} \geq 0.384.
\]

We obtain

\[
|x^y - 1| \geq e^x|e^{iy} - 1| = 2e^x \sin(y/2) \geq 2e^{-0.32} \sin(0.192) > 0.27.
\]

The lemma is proved.

\[\square\]

3 Estimates for the \( j \)-invariant and its derivative

We denote by \( \mathcal{H} \) the Poincaré plane, and by \( \mathcal{F} \) the standard fundamental domain. To be precise, \( \mathcal{F} \) is the open hyperbolic triangle with vertices \( \zeta_3, \zeta_6 \) and \( i\infty \), together with the “right” part of its boundary, that is, the geodesics \([i, \zeta_3] \) and \([\zeta_6, i\infty] \). Here

\[
\zeta_3 = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}, \quad \zeta_6 = e^{\pi i/3} = \frac{1 + \sqrt{-3}}{2}.
\]
For $z \in \mathcal{H}$ we write $q_z = e^{2\pi i z}$. When there is no risk of confusion, we omit the index and write simply $q$ instead of $q_z$. Recall that

$$j(z) = \sum_{n=-1}^{\infty} c_n q^n,$$

(3.1)

where the coefficients

$$c_{-1} = 1, \quad c_0 = 744, \quad c_1 = 196884, \quad c_2 = 21493760, \quad c_3 = 864299970, \ldots$$

are positive integers. We also denote

$$j_0(z) = c_1 q + c_2 q^2 + \ldots$$

### 3.1 Simplest estimates

We will systematically use the following trivial observations.

**Lemma 3.1.** Let $z \in \mathcal{H}$ and $v \in \mathbb{R}$ be such that $\text{Im} z \geq v$. Then

$$|j(z) - 744 - q_z^{-1}| = |j_0(z)| \leq j_0(iv),$$

(3.2)

$$|j'(z) + 2\pi i q_z^{-1}| = |j'_0(z)| \leq \frac{1}{i} j'_0(iv),$$

(3.3)

$$|j'(z)| \geq ij'(iv).$$

(3.4)

In particular, writing $z = x + yi$, we have

$$|j(z)| \leq j(iy),$$

(3.5)

$$|j'(z)| \leq 2\pi \left( 2e^{2\pi y} + \frac{1}{2\pi i} j'(iy) \right),$$

(3.6)

$$|j'(z)| \geq ij'(yi).$$

(3.7)

**Proof.** Set $w = iv$. Then $|q_z| \leq q_w$. Since the coefficients $c_n$ of the expansion (3.1) are all positive, we have

$$|j_0(z)| \leq \sum_{n=1}^{\infty} c_n |q_z|^n \leq \sum_{n=1}^{\infty} c_n q_w^n = j_m(w),$$

which proves (3.2). Similarly, using that

$$j'_0(z) = 2\pi i \sum_{n=1}^{\infty} nc_n q^n_z,$$

we obtain

$$|j'_0(z)| \leq 2\pi \sum_{n=1}^{\infty} nc_n q_w^n = \frac{1}{i} j'_0(w).$$
proving (3.3). Setting in (3.2) and (3.3) \( v = y \), we obtain (3.5) and (3.6).

We are left with (3.4) and (3.7). The real function

\[
v \mapsto ij'(v) = 2\pi \left( e^{2\pi v} - \sum_{n=1}^{\infty} nc_ne^{-2\pi nv} \right)
\]

is increasing in \( v \). Hence it suffices to prove (3.7). We have

\[
|j'(z)| = 2\pi \left| -q_z^{-1} + \sum_{n=1}^{\infty} nc_n q^n \right| \geq 2\pi \left( |q_z|^{-1} - \sum_{n=1}^{\infty} nc_n |q_z|^n \right) = ij'(iy),
\]

as wanted.

**Remark 3.2.** Estimates (3.4) and (3.7) are of interest only when \( y \geq v > 1 \), because when \( v \leq 1 \) the right-hand side of (3.4) is non-positive, as well as the right-hand side of (3.7) when \( y \leq 1 \).

Consider the functions \( f, g : \mathbb{R}_+ \rightarrow \mathbb{R}_+ \) defined by

\[
f(y) = j(iy), \quad g(y) = 2\pi \left( e^{2\pi y} + \sum_{n=1}^{\infty} nc_n e^{-2\pi ny} \right) = 4\pi e^{2\pi y} + \frac{1}{4} j'(iy) \quad (3.8)
\]

Note that the right-hand side of (3.5) is \( f(y) \) and that of (3.6) is \( g(y) \).

**Proposition 3.3.**

1. The function \( f \) is decreasing on \((0, 1]\), increasing on \([1, +\infty)\) and satisfies \( f(1/y) = f(y) \).

2. There exists \( y_0 \in [1.018, 1.019] \) such that \( g \) is decreasing on \((0, y_0]\) and increasing on \([y_0, +\infty)\).

**Proof.** Item 1 is obvious. To prove item 2, write

\[
g'(y) = (2\pi)^2 \left( e^{2\pi y} - \sum_{n=1}^{\infty} n^2 c_n e^{-2\pi ny} \right).
\]

Since the function \( y \mapsto e^{2\pi y} \) is increasing on \( \mathbb{R} \) and \( y \mapsto \sum_{n=1}^{\infty} n^2 c_n e^{-2\pi ny} \) is decreasing on \( \mathbb{R} \), the derivative vanishes at exactly one point \( y_0 \in \mathbb{R} \), being negative on the left of \( y_0 \) and positive on the right. A calculation shows that

\[
g'(1.018) = -259.31 \ldots, \quad g'(1.019) = 118.15 \ldots
\]

Whence the result.

**Corollary 3.4.** Let \( \alpha, \beta \) be positive real numbers and \( D \) a domain in \( \mathcal{H} \) such that for any \( z \in \mathcal{D} \) we have

\[
\alpha \leq \text{Im} z \leq \beta.
\]

Then for \( z \in \mathcal{D} \) we have

\[
|j(z)| \leq \max\{f(\alpha), f(\beta)\}, \quad |j'(z)| \leq \max\{g(\alpha), g(\beta)\}.
\]
3.2 Neighborhoods of elliptic points

Next, we want to estimate $j(z)$ and $j'(z)$ when $z$ is close to one of the elliptic points $\zeta_3$, $\zeta_6$ and $i$. Since $\zeta_3 = \zeta_6 - 1$, we restrict ourselves to $\zeta_6$ and $i$.

Let us introduce the following quantities:

$$A_0 = \frac{j'''(\zeta_6)}{3!} = -27\frac{\Gamma(1/3)^{18}}{\pi^9}i, \quad A_1 = \frac{j''(i)}{2!} = -81\frac{\Gamma(1/4)^8}{\pi^4}.$$  

For the calculation of the exact values of $j'''(\zeta_6)$ and $j''(i)$ see, for instance, [9, page 777]. The numerical values are

$$|A_0| = 45745.0806\ldots, \quad |A_1| = 24827.5650\ldots$$

**Proposition 3.5.**

1. For $0 < R < \sqrt{3}/2$ set

$$\kappa_0(R) = \frac{|A_0|}{R} + \frac{f(\sqrt{3}/2 - R)}{R^4}, \quad \lambda_0(R) = \frac{3|A_0|}{R} + \frac{\max\{g(\sqrt{3}/2 - R), g(\sqrt{3}/2 + R)\}}{R^3},$$

where $f$ and $g$ are defined in (3.8). Then in the circle $|z - \zeta_6| \leq R$ we have

$$|j(z) - A_0(z - \zeta_6)^3| \leq \kappa_0(R)|z - \zeta_6|^4, \quad (3.9)$$

$$|j'(z) - 3A_0(z - \zeta_6)^2| \leq \lambda_0(R)|z - \zeta_6|^3. \quad (3.10)$$

2. For $0 < R < 1$ set

$$\kappa_1(R) = \frac{|A_1|}{R} + \frac{f(1 - R)}{R^3}, \quad \lambda_1(R) = \frac{2|A_1|}{R} + \frac{\max\{g(1 - R), g(1 + R)\}}{R^2}.$$  

Then in the circle $|z - i| \leq R$ we have

$$|j(z) - 1728 - A_1(z - i)^2| \leq \kappa_1(R)|z - i|^3, \quad (3.11)$$

$$|j'(z) - 2A_1(z - i)| \leq \lambda_1(R)|z - i|^2. \quad (3.12)$$

**Proof.** Corollary 3.4 implies that in the circle $|z - \zeta_6| \leq R$

$$|j(z)| \leq \max\{f(\sqrt{3}/2 - R), f(\sqrt{3}/2 + R)\},$$

$$|j'(z)| \leq \max\{g(\sqrt{3}/2 - R), g(\sqrt{3}/2 + R)\}.$$  

Since

$$(\sqrt{3}/2 - R)(\sqrt{3}/2 + R) < 1,$$

we have

$$\max\{f(\sqrt{3}/2 - R), f(\sqrt{3}/2 + R)\} = f(\sqrt{3}/2 - R).$$

Now applying Lemma 2.2 we obtain (3.9) and (3.10). The proof of (3.11) and (3.12) is totally similar. □
Corollary 3.6. For \( |z - \zeta_6| \leq 0.19 \) we have
\[
|j(z) - A_0(z - \zeta_6)^3| \leq 7.26 \cdot 10^6 |z - \zeta_6|^4, \tag{3.13}
\]
\[
|j'(z) - 3A_0(z - \zeta_6)^2| \leq 2.27 \cdot 10^7 |z - \zeta_6|^3. \tag{3.14}
\]

For \( |z - i| \leq 0.2 \) we have
\[
|j(z) - 1728 - A_1(z - i)^2| \leq 4.04 \cdot 10^5 |z - i|^3, \tag{3.15}
\]
\[
|j'(z) - 2A_1(z - i)| \leq 9.1 \cdot 10^5 |z - i|^2. \tag{3.16}
\]

Proof. Set the “quasi-optimal” values \( R = 0.25 \) in (3.9), \( R = 0.19 \) in (3.10), \( R = 0.29 \) in (3.11) and \( R = 0.2 \) in (3.12). \( \square \)

3.3 Global lower estimates

Using the part of Corollary 3.6 related to \( j \) we easily obtain the following consequence.

Proposition 3.7. Let \( z \) belong to \( F \).

1. We have one of the following two options: either
\[
\min\{|z - \zeta_6|, |z - \zeta_3|\} \leq 0.001 \text{ and } |j(z)| \geq 30000 \min\{|z - \zeta_6|, |z - \zeta_3|\}^3, \tag{3.17}
\]
or
\[
\min\{|z - \zeta_6|, |z - \zeta_3|\} \geq 0.001 \text{ and } |j(z)| \geq 3 \cdot 10^{-5}. \tag{3.18}
\]

2. We have one of the following two options: either
\[
|z - i| \leq 0.01 \text{ and } |j(z) - 1728| \geq \min 20000 |z - i|^2 \tag{3.19}
\]
or
\[
|z - i| \geq 0.01 \text{ and } |j(z) - 1728| \geq 2. \tag{3.20}
\]

Proof. When \( |z - \zeta_6| \leq 0.005 \) we have
\[
|j(z)| \geq (A_0 - 7.26 \cdot 10^6 \cdot 0.001)|z - \zeta_6|^3 > 30000 |z - \zeta_6|^3.
\]

Similarly, when \( |z - \zeta_3| \leq 0.001 \) we have \( |j(z)| > 30000 |z - \zeta_3|^3 \). In particular, if \( |z - \zeta_6| = 0.001 \) or \( |z - \zeta_3| = 0.001 \) then
\[
|j(z)| \geq 30000 \cdot (0.001)^3 = 3 \cdot 10^{-5}.
\]

From the known behavior of \( j \) on the boundary of \( F \) we conclude that the estimate \( |j(z)| \geq 3 \cdot 10^{-5} \) holds for every \( z \) on the boundary of the set
\[
\{z \in F : |z - \zeta_6| \geq 0.001 \text{ and } |z - \zeta_3| \geq 0.001\}. \tag{3.21}
\]

Since \( j \) does not vanish on the set (3.21), the maximum principle implies that \( |j(z)| \geq 3 \cdot 10^{-5} \) for every \( z \) in the set (3.21). This proves part 1.

The proof of part 2 is totally similar. \( \square \)

10
Unfortunately, we cannot apply the same argument to $j'$, because we do not have enough information on its behavior on the boundary of $\mathcal{F}$. However, this can be overcome using the following simple lemma. We use the familiar notation

\[ E_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n, \quad \Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728}, \]

where $\sigma_k(n) = \sum_{d|n} d^k$ and $B_k$ the $k$th Bernoulli number.

Note that here (and until the end of Section 3.3) the letter $\Delta$ denotes the modular form $\Delta(z)$, and not an imaginary quadratic discriminant (as in the rest of the article).

**Lemma 3.8.** For any $z \in \mathcal{H}$ we have

\[ |j'(z)| \geq 2\pi \min \{ |j(z)|, |\Delta(z)|^{1/3} |j(z)|^{1/3} |j(z) - 1728| \}. \tag{3.22} \]

**Proof.** We have

\[ j(z) = \frac{E_4(z)^3}{\Delta(z)}, \quad j(z) - 1728 = \frac{E_6(z)^2}{\Delta(z)}. \]

Furthermore,

\[ \frac{1}{2\pi i} j'(z) = -\frac{E_4(z)^2 E_6(z)}{\Delta(z)} = -\frac{E_6(z)}{E_4(z)} j'(z) = -\frac{E_4(z)^2}{E_6(z)} (j(z) - 1728), \]

see, for instance, [9 page 775]. Hence

\[
\begin{align*}
\frac{|j'(z)|}{2\pi} &\geq \frac{E_6(z)}{E_4(z)} |j(z)|, \\
\frac{|j'(z)|}{2\pi} &\geq \frac{E_4(z)^2}{E_6(z)} |j(z) - 1728| \\
&= \frac{E_4(z)}{E_6(z)} \left| \Delta(z) \right|^{1/3} |j(z)|^{1/3} |j(z) - 1728|.
\end{align*}
\]

Since either $|E_6(z)/E_4(z)| \geq 1$ or $|E_4(z)/E_6(z)| \geq 1$, the result follows. \hfill \Box

**Remark 3.9.** In the neighborhoods of elliptic points one expects sharper lower bounds: there must be $|j'(z)| \geq c|j(z)|^{2/3}$ near the elliptic points of type $\zeta_6$, and $|j'(z)| \geq c|j(z) - 1728|^{1/2}$ near the elliptic points of type $i$. This can be accomplished as well, see [9 page 777]. We, however, stay with (3.22), which is neat and sufficient for our purposes.

**Proposition 3.10.** Let $z$ belong to $\mathcal{F}$. Then we have one of the following three options: either

\[ \min \{ |z - \zeta_6|, |z - \zeta_3| \} \leq 0.001 \text{ and } |j'(z)| \geq 10^5 \min \{ |z - \zeta_6|, |z - \zeta_3| \}^2, \tag{3.23} \]
or

\[ |z - i| \leq 0.01 \text{ and } |j'(z)| \geq 40000|z - i|, \quad (3.24) \]

or

\[
\min\{|z - \zeta_6|, |z - \zeta_6|\} \geq 0.001, \ |z - i| \geq 0.01 \text{ and } |j'(z)| \geq 10^{-4}. \quad (3.25)
\]

**Proof.** The cases \( \min\{|z - \zeta_6|, |z - \zeta_6|\} \leq 0.001 \) and \( |z - i| \leq 0.01 \) are treated exactly as in the proof of Proposition 3.7, using the corresponding instances of Corollary 3.6. When \( \text{Im} z \geq 1.01 \) estimate (3.4) gives

\[ |j'(z)| \geq ij'(1.01i) \geq 400, \]

which is much sharper than the wanted \( |j'(z)| \geq 10^{-4}\).

We are left with proving that \( |j'(z)| \geq 10^{-4} \) in the case

\[ \min\{|z - \zeta_6|, |z - \zeta_6|\} \geq 0.001, \ |z - i| \geq 0.01, \ \text{Im} z \leq 1.01. \]

Proposition 3.7 gives

\[ |j(z)| \geq 3 \cdot 10^{-5}, \quad |j(z) - 1728| \geq 2. \quad (3.26) \]

We want to apply Lemma 3.8 and for this purpose we need a lower bound for \( |\Delta(z)|^{1/3} \). This can be easily accomplished using the familiar infinite product expansion \( \Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \). Using the inequality

\[ \log |1 + t| \geq - \frac{|t|}{1 - |t|} \]

which holds true for any complex \( t \) satisfying \( |t| < 1 \), we obtain

\[
\log |\Delta(z)|^{1/3} \geq \frac{1}{3} \log |q| - 8 \sum_{n=1}^{\infty} \frac{|q|^n}{1 - |q|} = \frac{1}{3} \log |q| - 8 \frac{|q|}{(1 - |q|)^2}.
\]

Since \( z \in F \) and \( \text{Im} z \leq 1.01 \) we have \( e^{-2.02\pi} \leq |q| \leq e^{-\pi\sqrt{3}}, \) which results in the lower estimate

\[
\log |\Delta(z)|^{1/3} \geq - \frac{2.02\pi}{3} - 8 \frac{e^{-\pi\sqrt{3}}}{(1 - e^{-\pi\sqrt{3}})^2} \geq -2.16. \quad (3.27)
\]

Now we are ready to apply Lemma 3.8. Combining it with (3.26) and (3.27), we obtain

\[ |j'(z)| \geq 2\pi \min\{3 \cdot 10^{-5}, e^{-2.16}, (3 \cdot 10^{-5})^{1/3}, 2\} \geq 10^{-4}, \]

as wanted. \( \square \)

### 4 Separating distinct \( j \)-values

In this section we bound from below the difference \( |j(z) - j(w)| \), where \( z \) and \( w \) are distinct elements from the fundamental domain \( F \).
Proposition 4.1. Let \( z, w \in \mathcal{F} \) satisfy \( \text{Im} w \geq \text{Im} z \) and \( \text{Im} w \geq 1.3 \). Then there exists \( z' \in \{ z, z+1, z-1 \} \) such that

\[
|j(z) - j(w)| \geq e^{2\pi |\text{Im} w|} \min\{0.6|z' - w|, 0.2\}. \tag{4.1}
\]

Proof. We have

\[
|j(z) - j(w)| \geq \left| q_w^{-1} - q_z^{-1} \right| - |j_0(w) - j_0(z)|.
\]

Assume first that \( \text{Im} z \leq 1.2 \). In this case

\[
\left| q_w^{-1} - q_z^{-1} \right| \geq e^{2\pi v} |1 - e^{-2\pi 0.1}| \geq 0.7 e^{2\pi v} \geq 2400,
\]

where \( v = \text{Im} w \). On the other hand, since \( z \in \mathcal{F} \) we have \( \text{Im} z \geq \sqrt{3}/2 \), and using (3.2), we find

\[
|j_0(w) - j_0(z)| \leq j_0 \left( \frac{\sqrt{3}}{2} \right) + j_0(1.3i) \leq 1400.
\]

From these two estimates we deduce that \( |j(z) - j(w)| \geq 0.25 e^{2\pi v} \), which completes the proof in the case \( \text{Im} z \leq 1.2 \).

From now on we assume that \( \text{Im} z \geq 1.2 \). Let us first estimate from above the difference \( |j_0(w) - j_0(z)| \). In the domain \( \text{Im} z \geq 1.2 \) we have

\[
|j_0'(z)| \leq \frac{1}{i} j_0'(1.2i) < 800,
\]

see (3.3). Hence

\[
|j_0(w) - j_0(z)| \leq 800|w - z|,
\]

see Lemma 2.1. Replacing here \( z \) by \( z \pm 1 \) we obtain similar inequalities with \( |w - (z \pm 1)| \) on the right. This proves that

\[
|j_0(w) - j_0(z)| \leq 800|z - z'| \tag{4.2}
\]

for every \( z' \in \{ z, z-1, z+1 \} \). In addition to this, using (3.2), we find

\[
|j_0(w) - j_0(z)| \leq j_0(1.3i) + j_0(1.2i) < 200. \tag{4.3}
\]

Now let us estimate the difference \( |q_z^{-1} - q_w^{-1}| \) from below. There exists a unique \( z' \in \{ z, z-1, z+1 \} \) such that \( |\text{Re}(z' - w)| \leq 1/2 \), and we maintain this choice of \( z' \) in the sequel. We have clearly

\[
|q_z^{-1} - q_w^{-1}| = e^{2\pi v} |e^{2\pi i(w - z')} - 1|.
\]

Our assumption \( \text{Im} w \geq \text{Im} z \) implies that

\[
\text{Re}(2\pi i(w - z')) \leq 0,
\]

and the choice of \( z' \) implies that \( |\text{Re}(w - z')| \leq 1/2 \), which can be re-written as

\[
|\text{Im}(2\pi i(w - z'))| \leq \pi.
\]
Now we want to apply Lemma 2.4 with \(2\pi i(w - z')\) as \(z\). It implies that
\[
|q_z^{-1} - q_w^{-1}| \geq \frac{2}{3}e^{2\pi v}|w - z'| \geq 2300|w - z'|, \quad (4.4)
\]
if \(|w - z'| \leq 1/(4\pi)\), and
\[
|q_z^{-1} - q_w^{-1}| \geq 0.27e^{2\pi v} \geq 900, \quad (4.5)
\]
if \(|w - z'| \geq 1/(4\pi)\). (We use the assumption \(v \geq 1.3\).) Comparing this with (4.2) and (4.3), we obtain
\[
|j(z) - j(w)| \geq \begin{cases} 
0.6e^{2\pi v}|w - z'|, & |w - z'| \leq 1/(4\pi), \\
0.7e^{2\pi v}, & |w - z'| \geq 1/(4\pi),
\end{cases} \quad \text{sharper than (4.1).} \quad \square
\]

Given \(S \subset \mathbb{C}\) and \(\varepsilon > 0\), we define the \(\varepsilon\)-neighborhood of \(S\) as the set of all \(z \in \mathbb{C}\) such that \(|z - w| < \varepsilon\) for some \(w \in S\).

**Proposition 4.2.** Assume that \(z, w \in \mathcal{F}\) and \(\text{Im} w \leq 1.3\). Then there exists \(z'\) in the \(10^{-5}\)-neighborhood of \(\mathcal{F}\) such that \(j(z') = j(z)\) and
\[
|j(z) - j(w)| \geq \min\{5 \cdot 10^{-7}, 5 \cdot 10^{-7}|j'(w)|^2, 0.6|j'(w)||z' - w|\}. \quad (4.6)
\]

**Proof.** Let \(R\) be specified later to satisfy \(0 < R < \sqrt{3}/2\). Set
\[
B = \max\{f(\sqrt{3}/2 - R), f(1.3 + R)\}, \\
r = \min\left\{R, \frac{f'(w)R^2}{3(B + R)}, \frac{R^2}{3(B + R)}\right\},
\]
where \(f\) is defined in (3.8). Corollary 3.4 implies that every \(\xi\) in the disk \(|\xi - w| \leq R\) satisfies \(|j(\xi)| \leq B\).

We will now use Lemma 2.3 with \(j\) as \(f\), with \(w\) as \(a\) and with \(j(z)\) as \(w\). Condition (2.1) translates into
\[
r \leq \min\left\{R, \frac{|j'(w)|}{3(|j'(w)|/R + B/R^2)}\right\}. \quad (4.7)
\]
We have clearly
\[
\frac{|j'(w)|}{3(|j'(w)|/R + B/R^2)} \geq \frac{\min\{|j'(w)|, 1\}R^2}{3(B + R)}.
\]
Hence (4.7) holds true by our definition of \(r\).

Lemma 2.3 implies that there are two possibilities: either
\[
|j(z) - j(w)| \geq \frac{1}{2}r|j'(w)|, \quad (4.8)
\]
or there exists \( z' \in H \) such that \( j(z') = j(z) \) and \( |z' - w| \leq r \). In the latter case Lemma 2.2 implies that
\[
|j(z') - j(w) - j'(w)(z' - w)| \leq (|j'(w)|/R + B/R^2)|z' - w|^2 \\
\leq (|j'(w)|/R + B/R^2)r|z' - w|.
\]
Using (4.7), we find that
\[
(|j'(w)|/R + B/R^2)r \leq \frac{1}{3}|j'(w)|,
\]
which implies that
\[
|j(z') - j(w)| \geq \frac{2}{3}|j'(w)||z' - w|.
\] (4.9)
Thus, we have either (4.8) or (4.9). Setting a “nearly optimal” \( R = 0.2 \), we obtain
\[
10^{-5} > \frac{R^2}{3(2B + R)} > 10^{-6};
\]
in particular,
\[
10^{-5} > r > 10^{-6}\min\{1, |j'(w)|\}.
\]
Hence (4.8) implies that
\[
|j(z) - j(w)| \geq 5 \cdot 10^{-7}\min\{1, |j'(w)|^2\}. \tag{4.10}
\]
Thus, we have either (4.10) or (4.9), which proves (4.6) with our choice of \( z' \). It remains to note that \( |z' - w| \leq r < 10^{-5} \), which shows that \( z' \) belongs to the \( 10^{-5} \)-neighborhood of \( F \).

5 Separating imaginary quadratic numbers

Call a complex number imaginary quadratic if it is algebraic of degree 2 over \( \mathbb{Q} \) and does not belong to \( \mathbb{R} \). By the discriminant of an imaginary quadratic number we mean the discriminant of its minimal polynomial over \( \mathbb{Z} \).

We want to bound from below the distance between two imaginary quadratic numbers. Of course, it is easy to do using the “Liouville inequality”: if \( \alpha \) and \( \alpha' \) are distinct complex algebraic numbers then \( |\alpha - \alpha'| \geq (2H(\alpha)H(\alpha'))^{-d} \), where \( H(\cdot) \) is the absolute (multiplicative) height and \( d = [\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}] \). However, for imaginary quadratic numbers finer bounds are possible.

**Proposition 5.1.** Let \( \alpha, \alpha' \) be distinct imaginary quadratic numbers with positive imaginary parts, and \( \Delta, \Delta' \) are their respective discriminants. Then
\[
|\alpha - \alpha'| \geq \left\{ \begin{array}{ll}
\frac{2\text{Im} \alpha \text{Im} \alpha'}{|\Delta|^{1/4}|\Delta'|^{1/4}}, & \text{Im} \alpha \neq \text{Im} \alpha', \\
\frac{\text{Im} \alpha}{|\Delta|^{1/4}|\Delta'|^{1/4}}, & \text{Im} \alpha = \text{Im} \alpha'.
\end{array} \right.
\] (5.1)
Proof. Let \( aX^2 + bX + c \in \mathbb{Z}[X] \) be the minimal polynomial of \( \alpha \) over \( \mathbb{C} \) with \( a > 0 \). Then
\[
\Delta = b^2 - 4ac, \quad \alpha = \frac{-b + |\Delta|^{1/2}i}{2a} = \beta + \delta i,
\]
with \( \beta = -b/(2a) = \text{Re} \alpha \) and \( \delta = |\Delta|^{1/2}/(2a) = \text{Im} \alpha \). Similarly,
\[
\alpha' = \frac{-b' + |\Delta'|^{1/2}i}{2a'} = \beta' + \delta' i.
\]
If \( \delta \neq \delta' \) then
\[
|\alpha - \alpha'| \geq |\delta - \delta'| \geq \frac{|(\alpha')^2|\Delta| - a^2|\Delta'|}{2aa'(\alpha'|\Delta|^{1/2} + a|\Delta'|^{1/2})} \geq \frac{1}{2aa'(\alpha'|\Delta|^{1/2} + a|\Delta'|^{1/2})} \geq \frac{4(\delta')^2}{2\delta' \min\{\delta, \delta'\}} \geq \frac{\delta|\Delta||\Delta'|}{|\Delta||\Delta'|},
\]
which proves (5.1) in the \( \text{Im} \alpha \neq \text{Im} \alpha' \).

Now assume that \( \delta = \delta' \). In this case \( \alpha \) and \( \alpha' \) generate the same imaginary quadratic field:
\[
\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\alpha') = \mathbb{Q}(\sqrt{\Delta'}).
\]
Denote by \( D \) the discriminant of this field. Then
\[
\Delta = Df^2, \quad \Delta' = D(f')^2 \quad \text{with some positive integers } f \text{ and } f'.
\]
Denote \( e = \text{gcd}(f, f') \). Since \( \delta = \delta' \) we have \( af' = \alpha' f \), and
\[
a = A\frac{f}{e}, \quad a' = A\frac{f'}{e}, \quad \delta = \delta' = \frac{e|D|^{1/2}}{2A}
\]
with some \( A \in \mathbb{Z} \). Furthermore, the relation \( \Delta = b^2 - 4ac \) implies that \( (f/e) \mid b^2 \).

Hence \( b/(f/e) = b_1/f_1 \), where \( b_1, f_1 \) are integers such that \( 0 < f_1 \leq (f/e)^{1/2} \).

Similarly, \( b'/(f'/e) = b'_1/f'_1 \), where \( 0 < f'_1 \leq (f'/e)^{1/2} \). We obtain
\[
|\alpha - \alpha'| = |\beta - \beta'| = \frac{|b_1f'_1 - b'_1f_1|}{2Af_1f'_1} \geq \frac{1}{2A(f/e)^{1/2}(f'/e)^{1/2}} = \frac{\delta}{|\Delta|^{1/2}|\Delta'|^{1/4}},
\]
which proves (5.1) in the case \( \text{Im} \alpha = \text{Im} \alpha' \).

\( \square \)

Remark 5.2. If \( \Delta = \Delta' \) then we have the sharper estimate
\[
|\alpha - \alpha'| \geq \begin{cases} 
\frac{\text{Im} \alpha' \text{Im} \alpha}{2|\Delta|^{1/2}}, & \text{Im} \alpha \neq \text{Im} \alpha', \\
\frac{\text{Im} \alpha}{|\Delta|^{1/2}}, & \text{Im} \alpha = \text{Im} \alpha'.
\end{cases}
\] (5.2)
Indeed, if $\delta = \delta'$ then (5.2) follows from (5.1). And if $\delta \neq \delta'$, then $a \neq a'$, and we obtain

$$|\alpha - \alpha'| \geq |\delta - \delta'| = \frac{|a - a'||\Delta|^{1/2}}{2aa'} \geq \frac{|\Delta|^{1/2}}{2|\Delta|^{1/2}} = \frac{|\delta||\delta'|}{2|\Delta|^{1/2}}.$$ 

Unfortunately, we cannot profit from (5.2) to refine Theorem 1.1 in the (apparently, most important) special case $\Delta_x = \Delta_y$.

**Corollary 5.3.** Let $\tau$ be an imaginary quadratic number of discriminant $\Delta$. Assume that $\tau \in \mathcal{F}$ and $\tau \neq i, \zeta_6$. Then

$$\min\{|\tau - \zeta_6|, |\tau - \zeta_3|\} \geq \frac{\sqrt{3}}{4}|\Delta|^{-1},$$

$$|\tau - i| \geq \frac{3}{8}|\Delta|^{-1}$$

$$|j(\tau)| \geq 700|\Delta|^{-3}$$

$$|j(\tau) - 1728| \geq 2000|\Delta|^{-2}$$

$$|j'(\tau)| \geq 40000|\Delta|^{-2}.$$  

**Proof.** Estimates (5.3) and (5.4) are obtained using Proposition 5.1 with $\alpha = \tau$ and $\alpha' = \zeta_6, \zeta_3, i$, respectively; note that $\text{Im}\tau \geq \sqrt{3}/2$ because $\tau \in \mathcal{F}$.

To obtain (5.5), (5.6) and (5.7) we combine Propositions 3.7 and 3.10 with estimates (5.3) and (5.4). We obtain

$$|j(\tau)| \geq \min\{10^{-3}, 700|\Delta|^{-3}\},$$

$$|j(\tau) - 1728| \geq \min\{2, 2000|\Delta|^{-2}\},$$

$$|j'(\tau)| \geq \min\{10^{-4}, 15000|\Delta|^{-1}, 40000|\Delta|^{-2}\}.$$  

Note that $10^{-3} > 700|\Delta|^{-3}$ when $|\Delta| \geq 90$. A quick PARI script shows that $|j(\tau)| \geq 700|\Delta|^{-3}$ when $\tau$ is of discriminant $\Delta$ satisfying $|\Delta| \leq 90$. This proves inequality (5.5).

In a similar fashion, using a quick calculation with PARI one gets rid of 2 in (5.8), proving (5.6).

Finally, since $|\Delta| \geq 3$ we have $15000|\Delta|^{-1} \geq 40000|\Delta|^{-2}$, and (5.7) becomes

$$|j'(\tau)| \geq \min\{10^{-4}, 40000|\Delta|^{-2}\}.$$ 

We have $10^{-4} \geq 40000|\Delta|^{-2}$ when $|\Delta| \geq 20000$, and we again use a quick PARI script to show that $|j'(\tau)| \geq 40000|\Delta|^{-2}$ when $\tau$ is of discriminant $\Delta$ satisfying $|\Delta| \leq 20000$. This proves (5.7).

## 6 Separating singular moduli

In this section we prove the first principal result of this article. Recall that we denote by $\Delta_x$ the fundamental discriminant of the singular modulus $x$.
**Theorem 6.1.** Let \( x, y \) be distinct singular moduli. Assume that \( |\Delta_x| \geq |\Delta_y| \). Then
\[
|x - y| \geq \min \{800|\Delta_y|^{-4}, 20000|\Delta_x|^{-1}|\Delta_y|^{-3}, 700|\Delta_x|^{-3}\}. \tag{6.1}
\]

**Proof.** Let \( \tau_x, \tau_y \in \mathcal{F} \) be such that \( j(\tau_x) = x \) and \( j(\tau_y) = y \). Assume first that \( \text{Im} \tau_y \geq 1.3 \). In this case Proposition 4.1 implies that
\[
|x - y| \geq e^{2\pi \text{Im} \tau_y} \min \{0.6|\tau_x - \tau_y|, 0.2\} \geq \min \{2000|\tau_x' - \tau_y|, 700\}. \tag{6.2}
\]
where \( \tau_x' \in \{\tau_x - 1, \tau_x + 1\} \). We have \( \text{Im} \tau_x' = \text{Im} \tau_x \geq \sqrt{3}/2 \) because \( \tau_x \in \mathcal{F} \). Hence, using Proposition 5.1, we obtain
\[
|\tau_x' - \tau_y| \geq |\Delta_x|^{-1}|\Delta_y|^{-1}.
\]
Combining this with (6.2) we obtain an estimate much sharper than (6.1).

Now let us assume that \( \text{Im} \tau_y \leq 1.3 \) and \( y \neq 0, 1728 \). In this case Proposition 4.2 implies that
\[
|x - y| \geq \min \{5 \cdot 10^{-7}, 5 \cdot 10^{-7}|j'(\tau_y)|^2, 0.6|j'(\tau_y)||\tau_x', \tau_y|\}, \tag{6.3}
\]
where \( \tau_x' \) belongs to the \( 10^{-5} \)-neighborhood of \( \mathcal{F} \) and \( j(\tau_y) = x \).

We have
\[
\text{Im} \tau_y \geq \sqrt{3}/2, \quad \text{Im} \tau_x' \geq \sqrt{3}/2 - 10^{-5}. \tag{6.4}
\]
Hence, using Proposition 5.1 we obtain
\[
|\tau_x' - \tau_y| \geq \begin{cases}  |\Delta_x|^{-1}|\Delta_y|^{-1}, & \text{Im} \tau_x' \neq \text{Im} \tau_y, \\
(\sqrt{3}/2)|\Delta_x|^{-1/4}|\Delta_y|^{-1/4}, & \text{Im} \tau_x' = \text{Im} \tau_y, \end{cases}
\]
We have clearly \( |\Delta_x|^{3/4}|\Delta_y|^{3/4} \geq 2/\sqrt{3} \), which implies that
\[
|\tau_x' - \tau_y| \geq |\Delta_x|^{-1}|\Delta_y|^{-1} \tag{6.5}
\]
in any case. In addition to this, since \( y \neq 0, 1728 \), we have \( \tau_y \neq \zeta_6, i \). Hence Corollary 5.3 implies that
\[
|j'(\tau_y)| \geq 40000|\Delta_y|^{-2}.
\]
Combining this with (6.3) and (6.5) we obtain
\[
|x - y| \geq \min \{5 \cdot 10^{-7}, 800|\Delta_y|^{-4}, 20000|\Delta_x|^{-1}|\Delta_y|^{-3}\}.
\]
Finally, when \( y = 0 \) or \( y = 1728 \) Corollary 5.3 implies that \( |x - y| \geq 700|\Delta_x|^{-3} \).

We have proved that
\[
|x - y| \geq \min \{5 \cdot 10^{-7}, 800|\Delta_y|^{-4}, 20000|\Delta_x|^{-1}|\Delta_y|^{-3}, 700|\Delta_x|^{-3}\}, \tag{6.6}
\]
and to prove (6.1) we only have to get rid of the term \( 5 \cdot 10^{-7} \) on the right.

Note that
\[
800|\Delta_y|^{-4} \leq 5 \cdot 10^{-7} \quad \text{when } |\Delta_y| \geq 200, \\
700|\Delta_x|^{-3} \leq 5 \cdot 10^{-7} \quad \text{when } |\Delta_x| \geq 1119.
\]
Hence we have to verify that (6.1) holds true when \( |\Delta_y| \leq 200 \) and \( |\Delta_x| \leq 1119 \).

We did it using a PARI script. \( \square \)
Table 1: Data for Proposition 6.2

| $k$ | 1   | 2    | 3    | 4    |
|-----|-----|------|------|------|
| $X_k$ | 300 | 1000 | 3000 | 10000 |
| $d_k$ | 3.82 | 0.305 | 0.0292 | 0.00247 |
| $d'_k$ | 92.4 | 15.7 | 3.07 | 0.494 |

For small values of discriminants much better lower bounds hold true. Using a PARI script, we proved the following proposition, which may serve as a complement to Theorem 6.1, and will be used several times in Section 8.

**Proposition 6.2.** Let $X_k$, $d_k$ and $d'_k$ be the numbers defined in Table 1. Then for any distinct singular moduli $x, y$ with $|\Delta_x|, |\Delta_y| \leq X_k$ we have $|x - y| \geq d_k$. Moreover, if $\Delta_x = \Delta_y$ then $|x - y| \geq d'_k$.

## 7 More on singular moduli

In this section we summarize some properties of singular moduli used in the proof of Theorem 1.5.

It is well-known (see, for instance, [4, Proposition 2.5] and the references therein) that there is a one-to-one correspondence between the singular moduli of discriminant $\Delta$ and the set $T_\Delta$ of triples $(a, b, c)$ of integers satisfying

$$b^2 - 4ac = \Delta$$

and

$$\gcd(a, b, c) = 1, \quad \Delta = b^2 - 4ac,$$

either $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

If $(a, b, c) \in T_\Delta$ then $(b + \sqrt{\Delta})/2a$ belongs to the standard fundamental domain, and the corresponding singular modulus is $j((b + \sqrt{\Delta})/2a)$.

We call a singular modulus dominant if in the corresponding triple $(a, b, c)$ we have $a = 1$, and subdominant if $a = 2$. The following obvious property (see [4, Proposition 2.6]) will be crucial.

**Proposition 7.1.** There exists exactly one dominant and at most two subdominant singular moduli of a given discriminant $\Delta$. More precisely,

- there exist exactly 2 subdominant singular moduli of discriminant $\Delta$ if $\Delta \equiv 1 \mod 8, \Delta \neq -7$;
- there exists exactly 1 subdominant singular modulus of discriminant $\Delta$ if $\Delta \equiv 8, 12 \mod 16, \Delta \neq -4,-8$;
- there are no subdominant singular moduli of discriminant $\Delta$ if $\Delta \equiv 5 \mod 8$ or $\Delta \equiv 0, 4 \mod 16$. 

19
The inequality
\[ |j(z) - e^{2\pi \text{Im} z}| \leq 2079, \]
holds true for every \( z \) in the standard fundamental domain. It is proven in [5, Lemma 1], but it can also be easily deduced from (3.2) by setting \( v = \sqrt{3}/2 \) therein. In particular, if \( x \) is a singular modulus of discriminant \( \Delta \) corresponding to the triple \((a, b, c) \in T_\Delta\) then
\[ |x| - e^{\pi |\Delta_{x}|^{1/3}/4} \leq 2079. \]
This implies that
\[ |x| \leq e^{\pi |\Delta_{x}|^{1/2}} + 2079 \quad \text{in any case;} \quad (7.1) \]
\[ |x| \geq e^{\pi |\Delta_{x}|^{1/2}} - 2079 \quad \text{if } x \text{ is dominant;} \quad (7.2) \]
\[ |x| \leq e^{\pi |\Delta_{x}|^{1/2}/2} + 2079 \quad \text{if } x \text{ is not dominant;} \quad (7.3) \]
\[ |x| \leq e^{\pi |\Delta_{x}|^{1/2}/3} + 2079 \quad \text{if } x \text{ is neither dominant nor subdominant.} \quad (7.4) \]
These inequalities will be systematically used in the sequel, sometimes without special reference.

We will use the following lemmas.

Lemma 7.2. Let \( x, x', y, y' \) be singular moduli. Assume that
\[ \Delta_x = \Delta_{x'}, \quad \Delta_y = \Delta_{y'}. \]
Assume further that \( \mathbb{Q}(x, x') = \mathbb{Q}(y, y') \). Then we have the following.

1. If \( D_x \neq D_y \) then \( \mathbb{Q}(x) = \mathbb{Q}(y) \).
2. If \( D_x = D_y \) then \( K(x) = K(y) \), where \( K = K_x = K_y \) is the common CM-field for \( x \) and \( y \).

Proof. The case \( D_x \neq D_y \) is [7, Corollary 3.3].

Now assume that \( D_x = D_y \). We use the terminology of [7, Section 3]. If the field \( L = \mathbb{Q}(x, x') = \mathbb{Q}(y, y') \) is 2-elementary (that is, Galois over \( \mathbb{Q} \) with Galois group of the type \( \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z} \)), then, arguing as in the beginning of the proof of [7, Corollary 3.3], we obtain \( \mathbb{Q}(x) = \mathbb{Q}(y) \).

Now assume that \( L \) is not 2-elementary. If it is Galois over \( \mathbb{Q} \), then it is the Galois closure of both \( \mathbb{Q}(x) \) and \( \mathbb{Q}(y) \). Since the Galois closure of \( \mathbb{Q}(x) \) is \( K(x) \) and that of \( \mathbb{Q}(y) \) is \( K(y) \), we are done. Finally, if \( L \) is not Galois over \( \mathbb{Q} \) then \( x' \in \mathbb{Q}(x) \) and \( y' \in \mathbb{Q}(y) \), and so \( L = \mathbb{Q}(x) = \mathbb{Q}(y) \).

Lemma 7.3. Let \( x, y \) be singular moduli with the same fundamental discriminant \( D = D_x = D_y \), and let \( K = K_x = K_y = \mathbb{Q}(\sqrt{D}) \) be their common CM-field. Assume that \( K(x) = K(y) \neq K \). Then we have one of the following options.
1. The singular moduli $x$ and $y$ are conjugate over $\mathbb{Q}$; in other words, we have $\Delta_x = \Delta_y$.

2. There exists a discriminant $\Delta$, satisfying $\Delta \equiv 1 \mod 8$ and such that, up to swapping $x$ and $y$, we have $\Delta_x = 4\Delta$ and $\Delta_y = \Delta$.

Proof. See [1, Proposition 4.3], where everything is proved except that in option 2 we have $\Delta \equiv 1 \mod 8$. For the latter, see [4, page 407]. To be precise, both in [1] and [4] the slightly stronger assumption $\mathbb{Q}(x) = \mathbb{Q}(y)$ (in our notation) is made. But what is proved therein is exactly what we need.

8 The primitive element

In this section we prove Theorem 1.5. Thus, let $x, y$ be singular moduli and $\alpha$ a rational number, $\alpha \neq 0, \pm 1$. We will assume that $\mathbb{Q}(x + \alpha y)$ is a proper subfield of $\mathbb{Q}(x, y)$, and derive a contradiction.

Let $L$ be the Galois closure of $\mathbb{Q}(x, y)$ over $\mathbb{Q}$, and denote $G = \text{Gal}(L/\mathbb{Q})$. Since $\mathbb{Q}(x + \alpha y) \neq \mathbb{Q}(x, y)$ then there exists $\sigma \in G$ such that

$$x \neq x^\sigma, \quad y \neq y^\sigma, \quad x + \alpha y = x^\sigma + \alpha y^\sigma$$

(8.1)

(we write the Galois action exponentially). Rewriting the latter equality as

$$x - x^\sigma = -\alpha(y - y^\sigma),$$

(8.2)

we obtain $\mathbb{Q}(x - x^\sigma) = \mathbb{Q}(y - y^\sigma)$. It follows that $\mathbb{Q}(x, x^\sigma) = \mathbb{Q}(y, y^\sigma)$, see Theorem 1.3.

Now, using Lemmas 7.2 and 7.3, and swapping $x$ and $y$ if necessary, we are in one of the following three options.

Equal discriminants We have $\Delta_x = \Delta_y = \Delta$.

Equal fundamental discriminants, but distinct discriminants We have $D_x = D_y = D$ and $K(x) = K(y)$, where $K = \mathbb{Q}(\sqrt{D})$ is the common CM field of $x$ and $y$. Furthermore, there exists a discriminant $\Delta$ satisfying $\Delta \equiv 1 \mod 8$ such that $\Delta_x = 4\Delta$ and $\Delta_y = \Delta$.

Distinct fundamental discriminants We have $D_x \neq D_y$ but $\mathbb{Q}(x) = \mathbb{Q}(y)$.

We study these three cases separately.

Note that in each of the three cases above we have $h(\Delta_x) = h(\Delta_y)$. We denote this quantity by $h$. In the case $h = 1$ there is nothing to prove, and the case $h = 2$ is very easy. Indeed, existence of $\sigma$ with the property (8.1) implies that $\mathbb{Q}(x) = \mathbb{Q}(y)$ and that $\alpha$ is defined by (1.1), so we are in the situation of Example 1.1.

This, in the sequel we may assume that $h \geq 3$. This will also be used systematically, usually without special reference.
8.1 Equal discriminants

We assume now that $\Delta_x = \Delta_y = \Delta$. We may also assume that $x$ is dominant as defined in Section 7.

Fix a Galois morphism $\sigma$ satisfying (8.1). Note that either $y^\sigma \neq x$ or $y^\sigma^{-1} \neq x$; indeed, if $y^\sigma = y^\sigma^{-1} = x$ then (8.2) implies $\alpha = 1$, a contradiction. Thus, replacing, if necessary, $\sigma$ by $\sigma^{-1}$, we may assume that $y^\sigma \neq x$. Using (8.2), we obtain
\[
\alpha = -\frac{x - x^\sigma}{y - y^\sigma}, \quad y, y^\sigma \neq x.
\] (8.3)

This identity will be our principal tool.

8.1.1 We have $h \geq 4$

Let us prove first that $h \geq 4$. Thus, let us assume that $h = 3$. In this case $Q(x, y)$ is the full Ring Class Field associated to the discriminant $\Delta$; denote this field $L$. In particular, it contains the imaginary quadratic CM field $K = Q(\sqrt{\Delta})$. Since $x$ is dominant, it must be real. Hence $y$ cannot be real, and the 3 singular moduli of discriminant $\Delta$ are $x, y, \bar{y}$.

The maximal proper subfields of the field $L$ are $Q(x), Q(y), Q(\bar{y})$ and $K$. The element $x + \alpha y$ cannot belong to $Q(x)$ or $Q(y)$ because $y / \notin Q(x)$ and $x / \notin Q(y)$.

Thus, either $x + \alpha y \in Q(\bar{y})$ or $x + \alpha y \in K$. The non-identical elements of the Galois group $\text{Gal}(L/K)$ are the 3-cyclic permutations of the set $\{x, y, \bar{y}\}$. In particular, there is $\theta \in \text{Gal}(L/K)$ such that
\[
x^\theta = y, \quad y^\theta = \bar{y}, \quad \bar{y}^\theta = x.
\]

If $x + \alpha y \in Q(\bar{y})$ then $y + \alpha \bar{y} = (x + \alpha y)^\theta \in Q(x) \subset \mathbb{R}$. Hence $\alpha = -1$, a contradiction. And if $x + \alpha y \in K$ then $(x + \alpha y)^{\theta^{-1}} = x + \alpha y$. But we also have $(x + \alpha y)^{\theta^{-1}} = \bar{y} + \alpha x$. Hence $\bar{y} - \alpha y \in \mathbb{R}$, which implies $\alpha = 1$, a contradiction.

8.1.2 We have $h \leq 6$

Thus, we already know that $h \geq 4$. Our next aim is proving that $h \leq 6$. In fact, we are going to prove even more than this: $\Delta$ satisfies one of the following conditions:
\[
h(\Delta) \in \{4, 5, 6\}, \quad \Delta \equiv 1 \mod 8 \quad \text{(8.4)}
\]
\[
h(\Delta) = 4, \quad \Delta \equiv 8, 12 \mod 16. \quad \text{(8.5)}
\]

Thus, assume that either $h \geq 7$ or $h \in \{4, 5, 6\}$ and none of conditions (8.4), (8.5) is satisfied, and derive a contradiction. Note that, since $h \geq 4$, we have
\[
|\Delta| \geq 39. \quad \text{(8.6)}
\]

Let $\sigma$ be as in (8.3). Since $x$ is dominant, but neither $x^\sigma$ nor $y$ nor $y^\sigma$ is, we use (7.2), (7.3), (8.3) and (8.6) to obtain the lower estimate
\[
|\alpha| \geq \frac{e^{\pi |\Delta|^{1/2}} - e^{\pi |\Delta|^{1/2}} - 4178}{2e^{\pi |\Delta|^{1/2}} + 4178} \geq 0.448 e^{\pi |\Delta|^{1/2}/2}. \quad \text{(8.7)}
\]
The group $H = \text{Gal}(L/Q(x))$ is a subgroup of the group $G = \text{Gal}(L/Q)$ of index $h = [Q(x) : Q]$. Call $\gamma \in G$ suitable if neither $x^{\gamma}$ nor $x^{\sigma \gamma}$ is dominant or subdominant. We claim that a suitable $\gamma$ exists unless $\Delta$ satisfies one of conditions (8.4), (8.5).

Since there exist exactly one dominant and at most 2 subdominant singular moduli of discriminant $\Delta$ (see Proposition 7.1), there may exist at most 3 cosets in $H \setminus G$ sending $x$ to a dominant or a subdominant element. Similarly, there exist at most 3 cosets in $\sigma^{-1} H \sigma \setminus G$ sending $x^{\sigma}$ to a dominant or a subdominant conjugate. The total cardinality of these cosets does not exceed $6|H|$. Hence a suitable $\gamma$ exists if $h \geq 7$.

Using Proposition 7.1, the same holds true if none of conditions (8.4), (8.5) is satisfied. Indeed, if $\Delta \not\equiv 1 \pmod{8}$ then there is at most one subdominant conjugate. This means that we have at most 4 “bad” cosets, and we find a suitable $\gamma$ if $h \geq 5$.

And if $\Delta \not\equiv 1 \pmod{8}$ and $\not\equiv 12 \pmod{16}$ then $\Delta$ does not admit subdominant singular moduli at all. Hence in this case we have only 2 “bad” cosets, and we find a suitable $\gamma$ if $h \geq 3$.

Thus, a suitable $\gamma$ exists. From (8.3) we deduce that

$$\alpha = \frac{x^{\gamma} - x^{\sigma \gamma}}{y^{\gamma} - y^{\sigma \gamma}}. \quad (8.8)$$

Since neither $x^{\gamma}$ nor $x^{\sigma \gamma}$ is dominant or subdominant, we may use (7.4) and (8.6) to estimate

$$|\alpha| \leq \frac{2e^{\pi |\Delta|^{1/2}/3} + 4178}{|y^{\gamma} - y^{\sigma \gamma}|} \leq \frac{8.04 e^{\pi |\Delta|^{1/2}/3}}{|y^{\gamma} - y^{\sigma \gamma}|}. \quad (8.9)$$

Theorem 1.1 implies that $|y^{\gamma} - y^{\sigma \gamma}| \geq 800|\Delta|^{-4}$. Hence

$$|\alpha| \leq 0.0101 |\Delta|^{1/3} e^{\pi |\Delta|^{1/2}/3}.$$ 

Comparing this and (8.7), we obtain $e^{\pi |\Delta|^{1/2}/6} \leq 0.0226 |\Delta|^{-4}$. This inequality is contradictory for $|\Delta| \geq 3000$.

Thus, $|\Delta| < 3000$. We again use (8.9), but this time we apply Proposition 6.2 to estimate $|y^{\gamma} - y^{\sigma \gamma}| \geq 3.07$. We obtain $|\alpha| \leq 2.62 e^{\pi |\Delta|^{1/2}/3}$. Comparing this with (8.9), we obtain $|\Delta| < 12$, a contradiction.

8.1.3 The remaining $\Delta$

We are left with $\Delta$ satisfying one of conditions (8.4), (8.5). There are 38 such discriminants, their full list (found using the SAGE function cm_orders) being

$$-39, -47, -55, -56, -63, -68, -79, -84, -87, -103, -120, -127,$$

$$-132, -135, -136, -168, -175, -180, -184, -196, -207, -228,$$

$$-247, -280, -292, -312, -328, -340, -372, -388, -408, -520,$$

$$-532, -568, -708, -760, -772, -1012. \quad (8.10)$$
Note that 16 discriminants are bold-faced. Those are of class number 4 and class group of type $[2, 2]$. If $\Delta_x$ has this property then $\mathbb{Q}(x)/\mathbb{Q}$ is a Galois extension (see, for instance, [1, Corollary 3.3]).

Let $\Delta$ be from the list (8.10), and let $x_1, \ldots, x_h$ be the singular moduli of discriminant $\Delta$, with $x = x_1$ being the dominant. It follows from (8.3) that either $\alpha$ or $-\alpha$ belongs to the set

$$A_\Delta = \left\{ \frac{x_i - x_j}{x_j - x_k} : 2 \leq i, j \leq h, \ j < k \leq h \right\}. \quad (8.11)$$

Using PARI, we show that this set does not contain rational numbers. For those 22 discriminants which are not bold-faced, we even show that $A_\Delta$ does not contain real numbers; to be precise, we show, using a simple PARI script, that

$$\min(\{|\text{Im}z| : z \in A_\Delta\}) \geq 345$$

for every $\Delta$ in the list (8.10) except for the bold-faced ones.

For the bold-faced $\Delta$ this does not work, because all their singular moduli are real. However, for the bold-faced $\Delta$ all singular moduli are in $\mathbb{Q}(x)$, the latter field being Galois over $\mathbb{Q}$. Hence we may write, in a unique way, $x_i = f_i(x)$, each $f_i$ being a polynomial of degree not exceeding 3. It is easy to verify, using PARI, that the polynomials $f_1 - f_i$ and $f_j - f_k$ are not proportional for every choice of $i, j, k$ as above, showing that there are no rational numbers in $A_\Delta$.

This rules out all $\Delta$ from (8.10), completing the proof of Theorem 1.5 in the case of equal discriminants.

### 8.2 Equal fundamental discriminants, but distinct discriminants

Now assume that $D_x = D_y$, but $\Delta_x \neq \Delta_y$. In this case, as we have seen in the beginning of Section 8, we have $\{\Delta_x, \Delta_y\} = \{\Delta, 4\Delta\}$, where $\Delta \equiv 1 \mod 8$. We may assume that

$$\Delta_x = 4\Delta, \quad \Delta_y = \Delta,$$

and that $x$ is dominant. Since $h(\Delta) \geq 3$, we have

$$|\Delta| \geq 23. \quad (8.12)$$

Assuming that $\mathbb{Q}(x, y) \neq \mathbb{Q}(x + \alpha y)$, we find, as before, $\sigma \in G$ such that

$$\alpha = \frac{x - x^\sigma}{y - y^\sigma}. \quad (8.13)$$

Since $x$ is dominant and $x^\sigma$ is not, we use (7.1), (7.2), (7.3) and (8.12) to obtain
the estimate

\[
|\alpha| \geq \frac{e^{\pi|\Delta_{x}|^{1/2}} - e^{\pi|\Delta_{x}|^{1/2}/2} - 4178}{e^{\pi|\Delta_{x}|^{1/2}} + e^{\pi|\Delta_{x}|^{1/2}/2} + 4178} \nonumber
\]

\[
= \frac{e^{2\pi|\Delta|^{1/2}} - e^{\pi|\Delta|^{1/2}/2} - 4178}{e^{\pi|\Delta|^{1/2}} + e^{\pi|\Delta|^{1/2}/2} + 4178} \geq 0.998 e^{\pi|\Delta|^{1/2}}. \quad (8.14)
\]

Next, as in Subsection 8.1.2 we want to find \( \gamma \in G \) such that neither \( x^\gamma \) nor \( x^{\gamma y} \) is dominant or subdominant. This time, however, the task is much easier: since \( \Delta \equiv 1 \mod 8 \), we have \( \Delta_{x} = 4\Delta = 4 \mod 32 \), and Proposition 7.1 implies that there are no subdominant singular moduli of discriminant \( \Delta_{x} \). Hence we only have to assure that neither \( x^\gamma \) nor \( x^{\gamma y} \) is dominant; and such \( \gamma \) exists as soon as \( [G : H] = h \geq 3 \), which is our assumption.

We again have

\[
\alpha = -\frac{x^\gamma - x^{\gamma y}}{y^\gamma - y^{\gamma y}}.
\]

Using (7.14) and (8.12), we obtain

\[
|\alpha| \leq \frac{2e^{\pi|\Delta_{x}|^{1/2}/3} + 4178}{|y^\gamma - y^{\gamma y}|} = \frac{2e^{2\pi|\Delta|^{1/2}/3} + 4178}{|y^\gamma - y^{\gamma y}|} \leq \frac{2.19e^{2\pi|\Delta|^{1/2}/3}}{|y^\gamma - y^{\gamma y}|}. \quad (8.15)
\]

Theorem 1.1 implies that \( |y^\gamma - y^{\gamma y}| \geq 800|\Delta_{y}|^{-4} = 800|\Delta|^{-4} \). Hence

\[
|\alpha| \leq 0.00274|\Delta|^{4} e^{2\pi|\Delta|^{1/2}/3}.
\]

Comparing this with (8.14), we obtain \( e^{\pi|\Delta|^{1/2}/3} \leq 0.00275|\Delta|^{4} \). This inequality is contradictory when \( |\Delta| \geq 300 \).

Thus, \( |\Delta| < 300 \), in which case \( |y^\gamma - y^{\gamma y}| \geq 92.4 \) by Proposition 6.2. Together with (8.15), this implies \( |\alpha| \leq 0.0238e^{2\pi|\Delta|^{1/2}/3} \), which contradicts (8.14). This completes the proof in the case of equal fundamental discriminants, but distinct discriminants.

8.3 Distinct fundamental discriminants

Now we assume that \( D_{x} \neq D_{y} \). Since in this case we have \( \mathbb{Q}(x) = \mathbb{Q}(y) \), we may use Corollary 4.2 of [1], where all couples of singular moduli \((x, y)\) such that \( \mathbb{Q}(x) = \mathbb{Q}(y) \) but \( D_{x} \neq D_{y} \) are classified. Since \( h \geq 3 \), our \( \Delta_{x} \) and \( \Delta_{y} \) are featured in the six bottom lines of Table 2 on page 12 of [1]. To be precise, there are 15 (up to swapping \( x \) and \( y \)) possible pairs \((\Delta_{x}, \Delta_{y})\):

\[
(-96, -192), \quad (-96, -288), \quad (-120, -160), \quad (-120, -280), \quad (-120, -760), \quad (-160, -280), \quad (-160, -760), \quad (-180, -240), \quad (-192, -288), \quad (-195, -520), \quad (-195, -715), \quad (-280, -760), \quad (-340, -595), \quad (-480, -960), \quad (-520, -715).
\]
All of them can be disposed of using a direct calculation in a similar fashion as we disposed of the bold-faced discriminants in Subsection 8.1.3. To be precise, in all of these cases the field \( \mathbb{Q}(x) = \mathbb{Q}(y) \) is Galois over \( \mathbb{Q} \). Hence the conjugates \( x_1, \ldots, x_h \) of \( x \) and the conjugates \( y_1, \ldots, y_h \) of \( y \) can be uniquely expressed as \( x_i = f_i(x) \) and \( y_i = g_i(y) \), where \( f_i \) and \( g_i \) are polynomials over \( \mathbb{Q} \) of degree not exceeding \( h - 1 \). Now, using PARI, it is easy to verify that in each case any of the polynomials \( f_1 - f_i \) is not proportional to any of the polynomials \( g_j - g_k \). This rules out all the 15 pairs in the list above, completing the proof of Theorem 1.5.

References

[1] Bill Allombert, Yuri Bilu, and Amalia Pizarro-Madariaga, CM-points on straight lines, Analytic number theory, Springer, Cham, 2015, pp. 1–18. MR 3467387

[2] Yves André, Finitude des couples d’invariants modulaires singuliers sur une courbe algébrique plane non modulaire, J. Reine Angew. Math. 505 (1998), 203–208. MR 1662256

[3] Yuri Bilu, Philipp Habegger, and Lars Kühne, No singular moduli is a unit, IMRN (2018).

[4] Yuri Bilu, Florian Luca, and Amalia Pizarro-Madariaga, Rational products of singular moduli, J. Number Theory 158 (2016), 397–410. MR 3393559

[5] Yuri Bilu, David Masser, and Umberto Zannier, An effective “theorem of André” for CM-points on a plane curve, Math. Proc. Cambridge Philos. Soc. 154 (2013), no. 1, 145–152. MR 3002589

[6] David A. Cox, Primes of the form \( x^2 + ny^2 \), second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783

[7] Bernadette Faye and Antonin Riffaut, Fields generated by sums and products of singular moduli, J. Number Theory 192 (2018), 37–46. MR 3841544

[8] Philipp Habegger, Singular moduli that are algebraic units, Algebra Number Theory 9 (2015), no. 7, 1515–1524. MR 3404647

[9] Lars Kühne, Appendix B in [11].

[10] , An effective result of André-Oort type II, Acta Arith. 161 (2013), no. 1, 1–19. MR 3125148

[11] Antonin Riffaut, Equations with powers of singular moduli, Int. J. Number Theory, to appear, arXiv:1710.03547.

[12] The PARI Group, PARI/GP (Version 2.11.0), 2018, Bordeaux, http://pari.math.u-bordeaux.fr/

[13] The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 8.6), 2019, https://www.sagemath.org.

[14] Gisbert Wüstholz, A note on the conjectures of André-Oort and Pink, with an appendix by Lars Kühne, Bull. Inst. Math. Acad. Sin. (N.S.) 9 (2014), no. 4, 735–779. MR 3309950

Yuri BILU: Institut de Mathématiques de Bordeaux, Université de Bordeaux et CNRS, 351 cours de la Libération, 33405 Talence CEDEX, France; yuri@math.u-bordeaux.fr

Bernadette FAYE: Université Gaston-Berger de Saint-Louis, UFR SAT, BP: 234, Saint Louis, Senegal; bernadette.fayee@gmail.com

Huilin ZHU: School of Mathematical Sciences, Xiamen University, Xiamen City, Fujian Province, P.R.China; hlzhu@xmu.edu.cn