

DISTINCT DIFFERENCES OF SINGULAR MODULI

GUY FOWLER AND EMANUELE TRON

ABSTRACT. Let $E_1, E_2/\mathbb{C}$ be non-isomorphic elliptic curves with complex multiplication. We prove that the pair (E_1, E_2) is characterised, up to isomorphism, by the difference $j(E_1) - j(E_2)$ of the respective j -invariants. In other words, we show that if x_1, x_2, x_3, x_4 are singular moduli such that $x_1 - x_2 = x_3 - x_4$, then either $(x_1, x_2) = (x_3, x_4)$ or $(x_1, x_3) = (x_2, x_4)$.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{C}$. Then E is characterised, up to isomorphism, by its j -invariant $j(E)$. In this article, we will prove that if $E_1, E_2/\mathbb{C}$ are non-isomorphic elliptic curves that both have complex multiplication (CM), then the pair (E_1, E_2) is characterised, up to isomorphism, by the difference $j(E_1) - j(E_2)$ of the respective j -invariants. The j -invariant of a CM elliptic curve is called a singular modulus. Our main result is thus the following statement.

Theorem 1.1. *Let x_1, x_2, x_3, x_4 be singular moduli. Then*

$$x_1 - x_2 = x_3 - x_4$$

if and only if either $(x_1, x_2) = (x_3, x_4)$ or $(x_1, x_3) = (x_2, x_4)$.

The classical theory of complex multiplication shows that singular moduli are algebraic integers which generate the ring class fields of imaginary quadratic fields. Gross and Zagier [20] proved, under some technical hypotheses, a factorisation formula for the absolute norm of the difference of two singular moduli. Their result shows that such differences are “highly divisible”, in the sense that the prime factors of the norm are very small compared to the size of the norm. This was generalised to non-fundamental discriminants by Lauter and Viray [25].

Known results on singular moduli also suggest that many properties that singular moduli enjoy ought to be shared more generally with differences of two singular moduli. Some examples of interest to us:

- Singular moduli are never units in the ring of algebraic integers [6, Th. 1.1], and neither are differences of singular moduli [26, Cor. 1.3].
- Singular moduli are hardly ever S -units [12, Cor. 1.1]; the same goes for differences of singular moduli [21, Th. 1].
- Multiplicative relations among singular moduli are rare [31, Th. 1.2], and similarly so are multiplicative relations among differences of singular moduli [3, Th. 1.5], [19, Cor. 1.5].

We identify the modular curve $Y(1) = \mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H}$ with the affine line over $\mathbb{C}$ by means of the j -invariant. We may then endow $\mathbb{C}^n$ with the structure of a Shimura variety in this way. A point $(x_1, \dots, x_n) \in \mathbb{C}^n$ such that $x_1, \dots, x_n$ are all singular

moduli is a special point (i.e. a zero-dimensional special subvariety) of $\mathbb{C}^n$. For a description of the positive-dimensional special subvarieties, see e.g. [29, Def. 1.3]. Solutions in singular moduli to polynomial equations therefore correspond to special points of subvarieties of $\mathbb{C}^n$.

The André–Oort conjecture for $\mathbb{C}^n$, proved by Pila [29], states that a subvariety $W \subset \mathbb{C}^n$ contains only finitely many maximal special subvarieties. In particular, a subvariety W contains only finitely many special points outside the union of the positive-dimensional special subvarieties of W . Theorem 1.1 establishes this in completely explicit form for the subvariety $W \subset \mathbb{C}^4$ given by $W = \mathbb{V}(x - y - w + z)$. Theorem 1.1 shows that the two positive-dimensional special subvarieties $\mathbb{V}(x - y, w - z)$ and $\mathbb{V}(x - w, y - z)$ of W contain all the special points of W .

Let $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$. That there are only finitely many special points $(x_1, x_2) \in \mathbb{C}^2$ such that $x_1 - x_2 = \alpha$ is a special case of André’s theorem [2]. Pila’s proof [29, Th. 13.2] of the André–Oort conjecture for $\mathbb{C}^n$ implies that the number of special points $(x_1, x_2) \in \mathbb{C}^2$ such that $x_1 - x_2 = \alpha$ may be bounded by an ineffective constant which depends only on $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Kühne [22, Th. 4] subsequently proved that this constant could be determined effectively; Edixhoven [15, Remark 7.1] (cf. [11, Th. 3.1]) had previously shown this conditionally under GRH. Scanlon’s principle of automatic uniformity, coupled with Pila’s proof of André–Oort, implies [32, Th. 4.2] that the number of special points $(x_1, x_2) \in \mathbb{C}^2$ such that $x_1 - x_2 = \alpha$ is in fact bounded by an absolute (i.e. independent of α) constant. The same result also follows from [8, Th. 1.1]; both proofs are ineffective.

A subsequent result of Pila [30, Th. 1.3] implies that there are only finitely many special points $(x_1, x_2, x_3, x_4) \in \mathbb{C}^4$ such that $x_1 - x_2 = x_3 - x_4$, but $(x_1, x_2) \neq (x_3, x_4)$ and $(x_1, x_3) \neq (x_2, x_4)$. In other words, there are only finitely many $\alpha \in \overline{\mathbb{Q}}$ for which there exist at least two distinct special points $(x_1, x_2) \in \mathbb{C}^2$ such that $x_1 - x_2 = \alpha$. This result was again ineffective.

Bilu and Kühne [7] proved the André–Oort conjecture effectively for linear subvarieties of $\mathbb{C}^n$. In particular, their result [7, Th. 1.1] implies that if $(x_1, x_2, x_3, x_4) \in \mathbb{C}^4$ is a special point such that $x_1 - x_2 = x_3 - x_4$, but $(x_1, x_2) \neq (x_3, x_4)$ and $(x_1, x_3) \neq (x_2, x_4)$, then $\max\{|\Delta_i| : i = 1, 2, 3, 4\} < 10^{88}$. Here Δ_i denotes the discriminant (defined in Section 2.1) of the singular modulus x_i . The constant here is far too large for it to be feasible to deduce Theorem 1.1 by a computation (at least with currently available resources). We therefore prove Theorem 1.1 directly, without appealing to the main result of [7].

Explicit forms of the André–Oort conjecture are known for certain curves in $\mathbb{C}^2$ and surfaces in $\mathbb{C}^3$, e.g. [1, 5, 17]. Theorem 1.1 is, to our knowledge, the first example of such a result for a subvariety of dimension 3 in $\mathbb{C}^4$.

1.1. Overview of proof. We now give a brief overview of the proof of Theorem 1.1 and an outline of the structure of the paper.

A result of the first author [18, Theorem 1.6] characterises explicitly when three singular moduli are linearly dependent over $\mathbb{Q}$. We will apply this to prove Theorem 1.1 when either x_1, x_2, x_3, x_4 are not pairwise distinct (in Section 5.1), or at least one of x_1, x_2, x_3, x_4 is rational (in Section 5.2).

Suppose then that x_1, x_2, x_3, x_4 are pairwise distinct singular moduli such that

$$x_1 - x_2 = x_3 - x_4.$$

Let Δ_i denote the discriminant of x_i . The discriminant Δ_i is a negative integer. We may assume that $|\Delta_1|$ is maximal among the $|\Delta_i|$. Our aim is to obtain a bound on $|\Delta_1|$ which is sufficiently sharp as to rule out (after some computations in PARI as necessary) there being any such x_1, x_2, x_3, x_4 .

Among the singular moduli of a given discriminant Δ , there is a unique singular modulus of largest absolute value (called the *dominant* singular modulus of that discriminant). The singular moduli of a given discriminant Δ form a complete set of Galois conjugates over $\mathbb{Q}$. We recall such background facts in Section 2. The dominant singular modulus of discriminant Δ has absolute value $\approx \exp(\pi|\Delta|^{1/2})$, while the absolute value of every other singular modulus of discriminant Δ is $\ll \exp(\pi|\Delta|^{1/2}/2)$, see Lemma 2.1.

Applying a suitable Galois automorphism, we may assume that x_1 is dominant. The proof now naturally divides into four cases, according to how many of x_2, x_3, x_4 are also dominant. If none of x_2, x_3, x_4 is dominant, then it is clear that $|\Delta_1|$ must be bounded, because $|x_1| \gg \exp(\pi|\Delta_1|^{1/2})$, while $|x_i| \ll \exp(\pi|\Delta_1|^{1/2}/2)$ for $i \geq 2$. If exactly one of x_2, x_3, x_4 is dominant, then an easy analytic lower bound (Lemma 2.4) for $e^{\pi\sqrt{n}} - e^{\pi\sqrt{n-1}}$ suffices to conclude similarly. These two easy cases are handled in Sections 5.3.1 and 5.3.2 respectively.

The remaining cases, where at least two of x_2, x_3, x_4 are dominant, are more challenging. In these cases, we would like to find an automorphism $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(x_1) = x_1$ and there are strictly fewer dominant singular moduli among $\sigma(x_2), \sigma(x_3), \sigma(x_4)$ than among x_2, x_3, x_4 . We would then be able to reduce to one of the previously-proved cases.

Unfortunately, we are not always able to find such an automorphism σ ; indeed, there are situations where no such σ can exist. Instead, in Section 3.1, we use class field theory to prove a result (Proposition 3.1) which shows that if no such automorphism σ exists, then the discriminants $\Delta_1, \Delta_2, \Delta_3, \Delta_4$ must satisfy some very strong restrictions. In Sections 3.2 and 4 we establish some consequences of these restrictions on the discriminants. We then use these to show, under these restrictions on the discriminants, that $|\Delta_1|$ must be bounded in the relevant cases. The case where two of x_2, x_3, x_4 are dominant is handled in Section 6, and the case where all of x_2, x_3, x_4 are dominant is handled in Section 7. This completes the proof of Theorem 1.1.

1.2. Solving equations in singular moduli. The reader may wonder to what extent our method could be adapted to handle other linear equations in singular moduli with rational coefficients. It would be straightforward to extend our method to handle all equations of the form

$$\epsilon_1 x_1 + \epsilon_2 x_2 + \epsilon_3 x_3 + \epsilon_4 x_4 = \alpha,$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 \in \{\pm 1\}$ and $\alpha \in \mathbb{Q}$. However equations with coefficients of unequal absolute value would pose an obstacle to our approach. For example, if x_1 and x_2 are the only dominant singular moduli occurring and $|\Delta_2| = |\Delta_1| - 1$, then our proof obtains a bound on $|\Delta_1|$ by applying Lemma 2.4. We could not do this if the coefficient of x_1 was strictly smaller than the coefficient of x_2 in absolute value, because $e^{\pi\sqrt{n}} \sim e^{\pi\sqrt{n-1}}$ as $n \rightarrow \infty$.

Moreover, another fact that necessarily complicates the casework and final answer in such extensions is that plenty of solutions in pairwise distinct singular moduli to linear equations with coefficients of unequal absolute values do exist, unlike in

Theorem 1.1. Examples of such can be generated by variously combining Galois orbits of singular moduli of degree ≤ 4 , or by more involved combinations like the solution to

$$83x_1 - 49005x_2 = 262144(x_3 + x_4)$$

with $x_1 = j((-1 + \sqrt{-115})/2)$, $x_2 = j((-1 + \sqrt{-75})/2)$, $x_3 = j((-1 + \sqrt{-55})/2)$, $x_4 = j((-3 + \sqrt{-55})/8)$.

Linear equations in more than 4 variables also seem to require new ideas beyond the methods used here. In particular, the arguments in Section 6.2 seem to make essential use of the fact that a linear equation in 4 singular moduli yields an equality between fields generated by linear combinations of 2 singular moduli, which then enables us to apply the results on such fields contained in Section 4 to this situation.

On the other hand, the part of our approach that uses class field theory can be readily applied to other situations. Indeed, Proposition 3.1 is entirely general and does not even require that the equations being considered are linear. We therefore expect that it can be used to prove other effective André–Oort results. To prove Proposition 3.1, we use a result of Cohn [13, Th. 8.3.12]. Cohn’s result and its generalisation by Kühne [23, Cor. 1.2] have been applied previously to prove effective André–Oort results [7, 10]. In these previous applications, these results from class field theory are used to show that the size of the Galois orbit of a singular modulus x over some particular field L is $\gg c[\mathbb{Q}(x) : \mathbb{Q}]$ for some constant $c > 0$. This though leads to implied constants which are astronomical in size, even for relatively simple equations, see e.g. [7, (40)]. In contrast, our Proposition 3.1 shows only that the Galois orbit of x over L is non-trivial, but it does so without introducing such astronomical constants. It is therefore much better suited to cases where, as in Theorem 1.1, one wants to find all the solutions in singular moduli to a given equation explicitly.

2. BACKGROUND

2.1. Singular moduli. The discriminant Δ of a singular modulus x is defined to be the discriminant of the endomorphism order of an elliptic curve $E/\mathbb{C}$ with $j(E) = x$. In particular, Δ is a negative integer satisfying $\Delta \equiv 0, 1 \pmod{4}$. We may write $\Delta = f^2D$, where D is the discriminant of the quadratic imaginary field $\mathbb{Q}(\sqrt{D})$ and $f \in \mathbb{Z}_{>0}$. Call D the fundamental discriminant of x and f the conductor of x .

Singular moduli are algebraic integers. The singular moduli of a given discriminant form a complete Galois orbit over $\mathbb{Q}$, see e.g. [14, Prop. 13.2]. The number of distinct singular moduli of discriminant Δ is equal to the class number of Δ , which we denote $h(\Delta)$.

Let $j: \mathbb{H} \rightarrow \mathbb{C}$ denote the modular j -function, which has the q -expansion

$$j(z) = \frac{1}{q} + 744 + \sum_{n \geq 1} c(n)q^n,$$

where $c(n) \in \mathbb{Z}$ for all n and $q = \exp(2\pi iz)$. The map

$$(a, b, c) \mapsto j\left(\frac{-b + |\Delta|^{1/2}i}{2a}\right)$$

gives a bijection between the set

$$\{(a, b, c) \in \mathbb{Z}^3 : b^2 - 4ac = \Delta, \gcd(a, b, c) = 1, \text{ and}\}$$

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

and the set of singular moduli of discriminant Δ . Given a singular modulus x , the denominator of x is defined to be the integer a in the corresponding triple (a, b, c) . This well-known description of the singular moduli of a given discriminant corresponds to taking, for each singular modulus, its unique preimage (for j) in the standard fundamental domain for the action of $\mathrm{SL}(2, \mathbb{Z})$ on $\mathbb{H}$.

For each $\Delta < 0$ such that $\Delta \equiv 0, 1 \pmod{4}$, there exists a unique singular modulus with discriminant Δ and denominator 1, which is called the dominant singular modulus of discriminant Δ . The dominant singular modulus is given explicitly by

$$j\left(\frac{-k + |\Delta|^{1/2}i}{2}\right)$$

where $k \in \{0, 1\}$ is such that $k \equiv \Delta \pmod{4}$. It follows from the q -expansion of the j -function that $j(z) \in \mathbb{R}$ if $\Re(z) \in \{-1/2, 0\}$. Consequently, the dominant singular modulus of a given discriminant is always real. Moreover, for x the dominant singular modulus of discriminant Δ , one has that $x > 0$ if and only if $\Delta \equiv 0 \pmod{4}$.

The following bound is also a consequence of the q -expansion. Observe that both the lower and upper bounds are monotonically increasing in $|\Delta|$ and monotonically decreasing in a . More sophisticated and precise versions are known (see e.g. [28, Lemma 2.5]), but we only need this much.

Lemma 2.1. *Let x be a singular modulus of discriminant Δ and denominator a . Then*

$$e^{\pi|\Delta|^{1/2}/a} - 2079 \leq |x| \leq e^{\pi|\Delta|^{1/2}/a} + 2079.$$

Proof. This is an immediate consequence of [9, Lemma 1] and the above description of the singular moduli of a given discriminant. $\square$

Lemma 2.2. *Let $\Delta = f^2D$ be a discriminant with fundamental discriminant D and conductor f . Let x be a singular modulus with fundamental discriminant D and conductor g . If $g < f$, then*

$$|x| \leq e^{-\pi|D|^{1/2}} e^{\pi|\Delta|^{1/2}} + 2079 \leq 0.005e^{\pi|\Delta|^{1/2}} + 2079.$$

Proof. We follow the argument in [16, §4.2]. Observe that

$$e^{\pi g|D|^{1/2}} \leq e^{\pi(f-1)|D|^{1/2}} \leq e^{-\pi|D|^{1/2}} e^{\pi|\Delta|^{1/2}} \leq e^{-\pi\sqrt{3}} e^{\pi|\Delta|^{1/2}},$$

since $|D| \geq 3$. The result then follows from Lemma 2.1, since $e^{-\pi\sqrt{3}} = 0.0043\dots$ $\square$

Proposition 2.3 ([8, Lemmata 5.1 & 5.3]). *Let x_1, x_2 be distinct singular moduli of respective discriminants Δ_1, Δ_2 . Suppose that $|\Delta_2| \leq |\Delta_1|$. If x_1 is dominant, then $|x_2| < |x_1|$.*

2.2. An analytic estimate.

Lemma 2.4. *Let $d \in \mathbb{R}$. If $d \geq 5$, then*

$$e^{\pi\sqrt{d}} - e^{\pi\sqrt{d-1}} > e^{\pi\sqrt{d}}/\sqrt{d}.$$

Proof. For $x > 1$, let

$$f(x) = \sqrt{x} (1 - \exp(\pi(\sqrt{x-1} - \sqrt{x}))).$$

Note that

$$\sqrt{x-1} - \sqrt{x} = \frac{-1}{\sqrt{x-1} + \sqrt{x}},$$

so

$$f(x) = \sqrt{x} \left(1 - \exp \left(\frac{-\pi}{\sqrt{x-1} + \sqrt{x}} \right) \right) \geq \sqrt{x} \left(1 - \exp \left(\frac{-\pi}{2\sqrt{x}} \right) \right).$$

Recall that

$$e^{-y} < 1 - y + \frac{y^2}{2}$$

for every $y > 0$. Hence, for $x > 1$,

$$f(x) \geq \frac{\pi}{2} - \frac{\pi^2}{8\sqrt{x}}.$$

In particular, if $x \geq 5$, then $f(x) > 1$ as required. $\square$

3. SOME CLASS FIELD THEORY

3.1. Automorphisms of fields generated by singular moduli. Let D_1, D_2 be distinct fundamental discriminants and let x be a singular modulus of discriminant $\Delta = f^2 D_1$ for some $f \in \mathbb{Z}_{>0}$. The main result of this section (Proposition 3.1) will show that there exists an automorphism $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(x) \neq x$, but $\sigma(y) = y$ for every singular modulus y of fundamental discriminant D_2 , unless Δ is a 2-elementary discriminant (defined below). Proposition 3.1 will be vital to the proof of Theorem 1.1, because it allows us to reduce the number of dominant singular moduli of distinct fundamental discriminants that occur in an equation

$$x_1 - x_2 = x_3 - x_4.$$

In Section 3.2, we will then prove some characterisations of 2-elementary discriminants, which will enable us to handle those cases in the proof of Theorem 1.1 where no such automorphism σ exists.

Let K be an imaginary quadratic field. Write D for the discriminant of K . Let $f \in \mathbb{Z}_{>0}$. Define the ring class field of K of conductor f , which is denoted by $K[f]$, to be equal to $K(x)$, where x is any singular modulus of discriminant $\Delta = f^2 D$. This definition is independent of the choice of x , by e.g. [14, Th. 11.1]. The ring class field $K[f]$ is an abelian extension of K and a Galois extension of $\mathbb{Q}$. The Galois group $\text{Gal}(K[f]/K)$ is isomorphic to the class group of discriminant Δ , denoted $\text{cl}(\Delta)$. See [14, p. 180]. We now recall some terminology from [5].

A group G is called 2-elementary if every element of G has order ≤ 2 . Note that a 2-elementary group is always abelian and a finite 2-elementary group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$ for some $n \in \mathbb{Z}_{\geq 0}$.

A finite field extension L/K is called 2-elementary if the extension L/K is Galois and the Galois group $\text{Gal}(L/K)$ is 2-elementary. A number field L is called 2-elementary if the extension $L/\mathbb{Q}$ is 2-elementary.

A discriminant $\Delta = f^2 D$ is called 2-elementary if the finite field extension $K[f]/K$ is 2-elementary, where $K = \mathbb{Q}(\sqrt{D})$.

Proposition 3.1. *Let $\Delta = f^2 D_1$ be a discriminant, where D_1 is the corresponding fundamental discriminant. Suppose that Δ is not 2-elementary. Let D_2 be a fundamental discriminant such that $D_2 \neq D_1$. Then there exists $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that:*

- (1) if x is a singular modulus of discriminant Δ , then $\sigma(x) \neq x$.
- (2) if y is a singular modulus with fundamental discriminant D_2 , then $\sigma(y) = y$.

Note that some condition on the discriminant Δ is necessary in Proposition 3.1, because there do exist singular moduli x, y with distinct fundamental discriminants for which $\mathbb{Q}(x) = \mathbb{Q}(y)$, see [1, Table 2] for a list; the discriminants of such x, y are 2-elementary.

To prove Proposition 3.1, we will use the following result of Cohn [13]. Before stating his result, we give a definition. The transfer field of an imaginary quadratic field K , denoted by K^{tf} , is defined by

$$K^{\text{tf}} = \bigcup_{f \in \mathbb{Z}_{>0}} K[f].$$

The transfer field K^{tf} is an abelian extension of K and a Galois extension of $\mathbb{Q}$. In particular, if x is singular modulus of discriminant Δ such that $\mathbb{Q}(\sqrt{\Delta}) = K$, then $x \in K^{\text{tf}}$.

Proposition 3.2 ([13, Th. 8.3.12], cf. [23, Cor. 1.2]). *Let $K_1 \neq K_2$ be distinct, imaginary quadratic fields. Then the group*

$$\text{Gal}(K_1^{\text{tf}} \cap K_1 K_2^{\text{tf}} / K_1)$$

is 2-elementary.

Kühne [23] proved a generalisation of Cohn's result. Cohn's result was previously applied by Binyamini [10, §2.3] to obtain some effective André–Oort results.

Before proving Proposition 3.1, we first establish some auxiliary results.

Lemma 3.3. *Let $K_1 \neq K_2$ be distinct, imaginary quadratic fields with respective discriminants D_1, D_2 . Suppose that $f \in \mathbb{Z}_{>0}$ is such that*

$$K_1[f] \subset K_1 K_2^{\text{tf}}.$$

Then the discriminant $f^2 D_1$ is 2-elementary.

Proof. By assumption, $K_1[f] \subset K_1 K_2^{\text{tf}}$. Hence,

$$K_1[f] \subseteq K_1^{\text{tf}} \cap K_1 K_2^{\text{tf}}.$$

So $\text{Gal}(K_1[f]/K_1)$ is isomorphic to a quotient of the group $\text{Gal}(K_1^{\text{tf}} \cap K_1 K_2^{\text{tf}} / K_1)$. By Proposition 3.2, the group $\text{Gal}(K_1^{\text{tf}} \cap K_1 K_2^{\text{tf}} / K_1)$ is 2-elementary. Hence, the group $\text{Gal}(K_1[f]/K_1)$ is also 2-elementary, i.e. the discriminant $f^2 D_1$ is 2-elementary. $\square$

We recall the following fact from Galois theory.

Proposition 3.4 ([24, Th. VI.1.12]). *Let L/k be a Galois extension and let F/k be an arbitrary extension. Then LF/F and $L/L \cap F$ are both Galois extensions and the map $\sigma \mapsto \sigma|_L$ is an isomorphism $\text{Gal}(LF/F) \xrightarrow{\sim} \text{Gal}(L/L \cap F)$*

We need one more lemma.

Lemma 3.5. *Let $K_1 \neq K_2$ be distinct, imaginary quadratic fields with respective discriminants D_1, D_2 . Suppose that $f \in \mathbb{Z}_{>0}$ is such that the discriminant $f^2 D_1$ is not 2-elementary. Then $K_1[f] K_2^{\text{tf}} / K_1 K_2^{\text{tf}}$ is a proper Galois extension.*

Proof. The extension $K_1[f]/K_1$ is Galois. Hence, by Proposition 3.4, the extensions $K_1[f]K_2^{\text{tf}}/K_1K_2^{\text{tf}}$ and $K_1[f]/K_1[f] \cap K_1K_2^{\text{tf}}$ are both Galois and have isomorphic Galois groups.

By assumption, the discriminant f^2D_1 is not 2-elementary. Hence, by Lemma 3.3, we have that $K_1[f] \not\subset K_1K_2^{\text{tf}}$. So $K_1[f] \supsetneq K_1[f] \cap K_1K_2^{\text{tf}}$. Hence, the group $\text{Gal}(K_1[f]/K_1[f] \cap K_1K_2^{\text{tf}})$ is non-trivial, and so the group $\text{Gal}(K_1[f]K_2^{\text{tf}}/K_1K_2^{\text{tf}})$ is also non-trivial. In particular, $K_1[f]K_2^{\text{tf}}/K_1K_2^{\text{tf}}$ is a proper Galois extension. $\square$

We are now in a position to deduce Proposition 3.1.

Proof of Proposition 3.1. For $i = 1, 2$, let $K_i = \mathbb{Q}(\sqrt{D_i})$. Then $K_1 \neq K_2$. Since $\Delta = f^2D_1$ is not 2-elementary, the extension $K_1[f]K_2^{\text{tf}}/K_1K_2^{\text{tf}}$ is a proper Galois extension by Lemma 3.5. Hence there exists a non-identity element $\sigma \in \text{Gal}(K_1[f]K_2^{\text{tf}}/K_1K_2^{\text{tf}})$. In particular, σ must act non-trivially on $K_1[f]$. If x is a singular modulus of discriminant Δ , then $K_1(x) = K_1[f]$, and so we must have that $\sigma(x) \neq x$. If y is a singular modulus with fundamental discriminant D_2 , then $y \in K_2^{\text{tf}}$ and hence $\sigma(y) = y$. The proposition thus follows by taking an extension of σ to an automorphism of $\overline{\mathbb{Q}}$. $\square$

3.2. Characterising 2-elementary discriminants. We will now show that 2-elementary discriminants are of a particularly special form. We will use these facts later in Sections 6 and 7.

Tatuzawa [34, Th. 2] proved that Siegel's [33, (1)] classical, and classically ineffective, lower bound for the class number of imaginary quadratic fields can be made effective, apart from possibly a single exceptional imaginary quadratic field. The following result about 2-elementary fundamental discriminants is an explicit consequence of his theorem.

Proposition 3.6. *There exists a fundamental discriminant D_* with the following properties:*

- (1) $h(D_*) \geq 128$,
- (2) if $\Delta = f^2D$ is a 2-elementary discriminant, then either $D = D_*$ or $h(\Delta) \leq 16$.

In particular, $|D_| > 8000$. If Δ is a 2-elementary discriminant with $h(\Delta) \leq 16$, then $|\Delta| \leq 7392$.*

Proof. The first two properties are [5, Prop. 2.11]. The rest is a simple calculation in PARI. One may verify that if D is a fundamental discriminant such that $|D| \leq 8000$, then $h(D) \leq 120$. Similarly, one checks that every 2-elementary discriminant Δ with $h(\Delta) \leq 16$ satisfies $|\Delta| \leq 7392$. For the latter computation, we use the fact [18, Prop. 7.3] that $h(\Delta) \leq 32$ implies that $|\Delta| \leq 166147$. $\square$

Note that there may not exist any 2-elementary discriminants Δ with $h(\Delta) > 16$. In this case, any fundamental discriminant D_* with $h(D_*) \geq 128$ satisfies Proposition 3.6; for definiteness of notation, we set D_* to be the least (in absolute value) such fundamental discriminant, so $D_* = -8399$. If there do exist 2-elementary discriminants Δ with $h(\Delta) > 16$, then D_* is uniquely determined.

We will now show that the conductors of 2-elementary discriminants are bounded. Lemma 2.2 and Proposition 3.7 together imply a bound on the absolute value of a singular modulus x with 2-elementary discriminant $\Delta = f^2D$ solely in terms of the fundamental discriminant D .

Proposition 3.7. *Let $\Delta = f^2D$ be a 2-elementary discriminant. Then $f \leq 60$ and $f \mid 2^3 \cdot 3 \cdot 5 \cdot 7$. If $D \neq D_*$, then $f \leq 8$.*

This is a strengthening of a special case of [5, Propositions 2.9 & 2.10], which imply that any such conductor f satisfies $f \leq 28560$. The proof requires a couple of easy lemmata. The second is an immediate consequence of the first, since quotients of 2-elementary groups are themselves 2-elementary.

Lemma 3.8 ([1, Prop. 3.1]). *Let K be an imaginary quadratic field. Write D for the discriminant of K and let $f, g \in \mathbb{Z}_{>0}$. Then*

$$K[f]K[g] \subseteq K[\text{lcm}(f, g)].$$

Lemma 3.9. *Let $\Delta = f^2D$ be a 2-elementary discriminant and set $K = \mathbb{Q}(\sqrt{D})$. If $g \in \mathbb{Z}_{>0}$ is such that $K[g] \subseteq K[f]$, then the discriminant g^2D is 2-elementary. In particular, the discriminant D is 2-elementary (since $K[1] \subseteq K[f]$ by Lemma 3.8).*

Now we may prove Proposition 3.7.

Proof of Proposition 3.7. Let $\Delta = f^2D$ be a 2-elementary discriminant. If $D \neq D_*$, then $|\Delta| \leq 7392$ by Proposition 3.6. We may then verify in PARI that $f \leq 8$ by checking all such Δ . So we may assume subsequently that $D = D_*$. In particular, $D \neq -3, -4$.

The proof now follows the approach in [5, Prop. 2.9]. Since Δ is 2-elementary, D is 2-elementary by Lemma 3.9. Therefore, by [5, (2.9)], we have that

$$h(\Delta) = 2^{\rho_2(\Delta)} \text{ and } h(D) = 2^{\rho_2(D)},$$

where $\rho_2(\Delta)$ denotes the dimension of $\text{cl}(\Delta)/\text{cl}(\Delta)^2$ as an $\mathbb{F}_2$ -vector space and analogously for $\rho_2(D)$. By [5, Prop. 2.3], $\rho_2(D) = \omega(D) - 1$ and $\rho_2(\Delta) \leq \omega(\Delta)$, where $\omega(\cdot)$ denotes the number of distinct prime divisors function. Therefore,

$$\rho_2(\Delta) - \rho_2(D) \leq \omega(\Delta) - \omega(D) + 1 \leq \omega(f) + 1.$$

Let

$$\Psi = f \prod_{p|f} \left(1 - \frac{(D/p)}{p}\right),$$

where (D/p) denotes the Kronecker symbol. From the class number formula [5, (2.4) & (2.5)], we have that

$$h(\Delta) = h(D)\Psi.$$

Hence,

$$\Psi = 2^{\rho_2(\Delta) - \rho_2(D)}.$$

So Ψ is a power of 2 and $\Psi \mid 2^{\omega(f)+1}$. This certainly implies that [5, (2.12)] holds. We may thus argue as in the proof of [5, Prop. 2.9] to obtain [5, (2.15)], i.e.

$$f = 2^k p_1 \cdots p_m$$

for some non-negative integers k, m and distinct odd primes $p_1 < \cdots < p_m$ not dividing D . Note that $k = 0$ and $m = 0$ are both allowed. Further, for each p_i , either $p_i - 1$ or $p_i + 1$ divides Ψ (and hence is a power of 2).

First, we show that $k \leq 3$. Suppose that $k \geq 1$. Then $\omega(f) = m + 1$. Hence,

$$2^{m+2} = 2^{\omega(f)+1} \geq \Psi \geq 2^{k-1}(p_1 - 1) \cdots (p_m - 1) \geq 2^{m+k-1}.$$

Therefore, $m + k - 1 \leq m + 2$, and so $k \leq 3$.

Suppose that $\omega(f) = 1$. So $\Psi \mid 4$ and either $f = 2^k$ for some $k \leq 3$ or $f = p_1$ for some odd prime p_1 such that either $p_1 - 1$ or $p_1 + 1$ divides Ψ . Thus, if $f = p_1$, then $p_1 \in \{3, 5\}$. We are thus done in this case.

So we may assume that $\omega(f) \geq 2$. So $m \geq 1$. Suppose that $p_m > 7$. One of $p_m - 1$ and $p_m + 1$ is a power of 2, so $p_m \geq 17$. Therefore,

$$2^{m+2} \geq 2^{\omega(f)+1} \geq \Psi \geq (p_1 - 1) \cdots (p_m - 1).$$

If $m \geq 2$, then

$$2^{m+2} \geq (3 - 1)(5 - 1)^{m-2}16 = 2^{1+2m}$$

and so $1 + 2m \leq m + 2$, which is false since $m \geq 2$. So we must have that $m = 1$, and hence $\omega(f) = 2$. Hence, $f = 2^k p_m$ for some $k \geq 1$. We thus have that

$$8 = 2^{\omega(f)+1} \geq \Psi \geq 2^{k-1}(p_m - 1) \geq 16,$$

which is absurd. So $p_m \leq 7$.

So $p_1, \dots, p_m \in \{3, 5, 7\}$. In particular, $m \leq 3$ and so $\omega(f) \leq 4$. Suppose that $\omega(f) = 4$. Then $f = 2^k \cdot 3 \cdot 5 \cdot 7$ for some $k \geq 1$. Thus

$$2^5 = 2^{\omega(f)+1} \geq \Psi \geq 2^{k-1}(3 - 1)(5 - 1)(7 - 1) \geq 48,$$

which is false. So $\omega(f) \leq 3$.

Suppose that $\omega(f) = 3$. So $\Psi \leq 2^4$. If $k = 0$, then $f = 3 \cdot 5 \cdot 7$ and hence

$$2^4 \geq \Psi \geq (3 - 1)(5 - 1)(7 - 1) = 48,$$

which is absurd. So $k \geq 1$ and hence $m = 2$. So $f = 2^k p_1 p_2$ with $p_1, p_2 \in \{3, 5, 7\}$. If $p_1 = 5$ and $p_2 = 7$, then

$$2^4 \geq \Psi \geq 2^{k-1}(5 - 1)(7 - 1) \geq 24,$$

which is absurd. If $p_1 = 3$ and $p_2 = 7$, then

$$2^4 \geq \Psi \geq 2^{k-1}(3 - 1)(7 - 1) = 12 \cdot 2^{k-1},$$

and so $k = 1$ and $f = 2 \cdot 3 \cdot 7 = 42$. If $p_1 = 3$ and $p_2 = 5$, then

$$2^4 \geq \Psi \geq 2^{k-1}(3 - 1)(5 - 1) = 8 \cdot 2^{k-1},$$

and so $k \leq 2$ and $f \mid 2^2 \cdot 3 \cdot 5 = 60$.

If $\omega(f) = 2$, then $f \leq 2^3 \cdot 7 = 56$. This completes the proof. $\square$

Finally, we recall a helpful set of equivalent characterisations of 2-elementary discriminants, which we will use in Section 4.2.

Proposition 3.10 ([1, Cor. 3.3]). *Let x be a singular modulus of discriminant $\Delta = f^2 D$ and $K = \mathbb{Q}(\sqrt{D})$. The following are equivalent:*

- (1) *The discriminant Δ is 2-elementary.*
- (2) *The extension $K[f]/\mathbb{Q}$ is abelian.*
- (3) *The number field $K[f]$ is 2-elementary.*
- (4) *The extension $\mathbb{Q}(x)/\mathbb{Q}$ is Galois.*
- (5) *The extension $\mathbb{Q}(x)/\mathbb{Q}$ is abelian.*

4. FIELDS GENERATED BY SINGULAR MODULI

4.1. Some preliminary results. Here we recall some useful facts, which we will use repeatedly in the proof of Lemma 5.1 and in Section 6.2. The first is a primitive element theorem for rational linear combinations of two singular moduli. In particular, it shows that the difference $x_1 - x_2$ of distinct singular moduli x_1, x_2 is always a primitive element for the field $\mathbb{Q}(x_1, x_2)$.

Proposition 4.1 ([4, Ex. 1.4 & Th. 1.5], [16, Th. 4.1]). *Let x_1, x_2 be distinct singular moduli of respective discriminants Δ_1, Δ_2 . Let $\epsilon \in \mathbb{Q} \setminus \{0\}$. If*

$$\mathbb{Q}(x_1 + \epsilon x_2) \subsetneq \mathbb{Q}(x_1, x_2),$$

then

$$[\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1 + \epsilon x_2)] = 2$$

and

- (1) *either $\Delta_1 = \Delta_2$ and $\epsilon = 1$;*
- (2) *or all of the following hold:*
 - (a) $\Delta_1 \neq \Delta_2$,
 - (b) $\mathbb{Q}(x_1) = \mathbb{Q}(x_2)$ *and this field is a degree 2 extension of $\mathbb{Q}$,*
 - (c) $\epsilon = -(x_1 - x'_1)/(x_2 - x'_2) \notin \{\pm 1\}$, *where x'_i denotes the non-trivial conjugate of x_i over $\mathbb{Q}$.*

Proposition 4.2 ([4, Lemma 7.1]). *Let x_1, x'_1 be singular moduli of discriminant Δ_1 and let x_2, x'_2 be singular moduli of discriminant Δ_2 . Write D_1, D_2 for the respective fundamental discriminants. Suppose that $\mathbb{Q}(x_1, x'_1) = \mathbb{Q}(x_2, x'_2)$.*

- (1) *If $D_1 \neq D_2$, then $\mathbb{Q}(x_1) = \mathbb{Q}(x_2)$.*
- (2) *If $D_1 = D_2$, then $K(x_1) = K(x_2)$, where $K = \mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$.*

Proposition 4.3. *Let x_1, x_2 be distinct singular moduli with respective discriminants Δ_1, Δ_2 and fundamental discriminants D_1, D_2 .*

- (1) *If $D_1 \neq D_2$ and $\mathbb{Q}(x_1) = \mathbb{Q}(x_2)$, then the discriminants Δ_1, Δ_2 are 2-elementary and $|\Delta_1|, |\Delta_2| \leq 7392$.*
- (2) *If $D_1 = D_2$ and $K(x_1) = K(x_2)$, where $K = \mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$, then either $x_1, x_2 \in \mathbb{Q}$ or $\Delta_1/\Delta_2 \in \{1, 4, 1/4\}$.*

Proof. (1) follows from [5, Prop. 2.8 & Cor. 2.13] and Proposition 3.6. For (2), recall that the dominant singular modulus of a given discriminant is always real. Hence, every singular modulus has a real Galois conjugate over $\mathbb{Q}$. In particular, any singular modulus contained in an imaginary quadratic field must in fact be rational; hence either $K = K(x_1) = K(x_2)$ and $x_1, x_2 \in \mathbb{Q}$, or $K \neq K(x_1) = K(x_2)$, in which case the desired result follows from [4, Lemma 7.2]. $\square$

4.2. Singular moduli generating 2-elementary fields. We now introduce a further bit of terminology from [5, §2.2.2]. Call a finite abelian group G almost 2-elementary if G has a 2-elementary subgroup of index 2. A discriminant $\Delta = f^2 D$ is called almost 2-elementary if the group $\text{Gal}(K[f]/K)$ is almost 2-elementary, where $K = \mathbb{Q}(\sqrt{D})$. Note that every 2-elementary discriminant is almost 2-elementary.

In this section, we will prove the following result, which shows that if 2 of the singular moduli occurring in the equation $x_1 - x_2 = x_3 - x_4$ have 2-elementary discriminants, then the discriminants of the other two 2 singular moduli are either

2-elementary or almost 2-elementary and equal to one another. We will use this fact repeatedly in Sections 6.2, 6.3, and 7.

Proposition 4.4. *Let x_1, x_2, x_3, x_4 be pairwise distinct singular moduli with respective discriminants $\Delta_1, \Delta_2, \Delta_3, \Delta_4$. Suppose that $a_1, a_2, a_3, a_4 \in \mathbb{Q} \setminus \{0\}$ are such that*

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \in \mathbb{Q}.$$

If Δ_1, Δ_2 are both 2-elementary, then:

- (1) *either Δ_3, Δ_4 are both 2-elementary,*
- (2) *or $\Delta_3 = \Delta_4$ is almost 2-elementary and $a_3 = a_4$.*

Proof. The result follows immediately from Lemmata 4.5 and 4.6 below, since

$$\mathbb{Q} \left(x_1 + \frac{a_2}{a_1}x_2 \right) = \mathbb{Q} \left(x_3 + \frac{a_4}{a_3}x_4 \right). \quad \square$$

Lemma 4.5. *Let x_1, x_2 be singular moduli such that their respective discriminants Δ_1, Δ_2 are both 2-elementary. Let $\epsilon \in \mathbb{Q}$. Then the field $\mathbb{Q}(x_1 + \epsilon x_2)$ is 2-elementary.*

Proof. For $i = 1, 2$, Proposition 3.10 implies that the extension $\mathbb{Q}(x_i)/\mathbb{Q}$ is Galois and $\text{Gal}(\mathbb{Q}(x_i)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{n_i}$ for some $n_i \in \mathbb{Z}_{\geq 0}$. Hence, the extension $\mathbb{Q}(x_1, x_2)/\mathbb{Q}$ is Galois and has Galois group isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^{n_1} \times (\mathbb{Z}/2\mathbb{Z})^{n_2}$. In particular, the extension $\mathbb{Q}(x_1, x_2)/\mathbb{Q}$ is 2-elementary, and hence the extension $\mathbb{Q}(x_1 + \epsilon x_2)/\mathbb{Q}$ is also 2-elementary. $\square$

Lemma 4.6. *Let x_1, x_2 be distinct singular moduli with respective discriminants Δ_1, Δ_2 . Let $\epsilon \in \mathbb{Q} \setminus \{0\}$. Suppose that the field $\mathbb{Q}(x_1 + \epsilon x_2)$ is 2-elementary. If either $\Delta_1 \neq \Delta_2$ or $\epsilon \neq 1$, then the discriminants Δ_1, Δ_2 are 2-elementary. If $\Delta_1 = \Delta_2$ and $\epsilon = 1$, then this discriminant is almost 2-elementary.*

Proof. For $i \in \{1, 2\}$, let $K_i = \mathbb{Q}(\sqrt{\Delta_i})$. By assumption, the extension $\mathbb{Q}(x_1 + \epsilon x_2)/\mathbb{Q}$ is Galois and

$$\text{Gal}(\mathbb{Q}(x_1 + \epsilon x_2)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$$

for some $n \in \mathbb{Z}_{\geq 0}$. For each $i \in \{1, 2\}$, we have the following diagram of field extensions:

$$\begin{array}{ccc}
 & K_i(x_1, x_2) & \\
 & \downarrow & \\
 & K_i(x_1 + \epsilon x_2) & \\
 \swarrow & & \searrow \\
 \mathbb{Q}(x_1 + \epsilon x_2) & & K_i \\
 \searrow & & \swarrow \\
 & \mathbb{Q}(x_1 + \epsilon x_2) \cap K_i & \\
 & \downarrow & \\
 & \mathbb{Q} &
 \end{array}$$

By Proposition 3.4, we have that $K_i(x_1 + \epsilon x_2)/K_i$ is a Galois extension and

$$\text{Gal}(K_i(x_1 + \epsilon x_2)/K_i) \cong \text{Gal}(\mathbb{Q}(x_1 + \epsilon x_2)/\mathbb{Q}(x_1 + \epsilon x_2) \cap K_i) \cong (\mathbb{Z}/2\mathbb{Z})^{m_i}$$

for some $m_i \leq n$.

Suppose that $K_i(x_1 + \epsilon x_2) = K_i(x_1, x_2)$. So the extension $K_i(x_1, x_2)/K_i$ is Galois and

$$\text{Gal}(K_i(x_1, x_2)/K_i) \cong (\mathbb{Z}/2\mathbb{Z})^{m_i}.$$

In particular, the group $\text{Gal}(K_i(x_i)/K_i)$ is isomorphic to a quotient of $(\mathbb{Z}/2\mathbb{Z})^{m_i}$ and hence must be 2-elementary. Hence, the discriminant Δ_i is 2-elementary.

So we may suppose that, for some $i \in \{1, 2\}$,

$$K_i(x_1 + \epsilon x_2) \subsetneq K_i(x_1, x_2).$$

This implies that

$$\mathbb{Q}(x_1 + \epsilon x_2) \subsetneq \mathbb{Q}(x_1, x_2).$$

We thus must be in one of the two exceptional cases in Proposition 4.1. If we are in exceptional case (2) of Proposition 4.1, then

$$[\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_2) : \mathbb{Q}] = 2$$

and so certainly Δ_1, Δ_2 are 2-elementary. We may thus assume that we are in exceptional case (1) of Proposition 4.1, i.e. $\Delta_1 = \Delta_2$ and $\epsilon = 1$.

Therefore, $K_1 = K_2$ and $K_1(x_1) = K_1(x_2)$. Proposition 4.1 also implies that

$$[\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1 + x_2)] = 2,$$

and hence

$$[K_1(x_1) : K_1(x_1 + x_2)] = 2.$$

Consequently,

$$\text{Gal}(K_1(x_1)/K_1) / \text{Gal}(K_1(x_1)/K_1(x_1 + x_2)) \cong (\mathbb{Z}/2\mathbb{Z})^{m_1}.$$

In particular, the group $\text{Gal}(K_1(x_1)/K_1)$ is almost 2-elementary, and hence the discriminant Δ_1 is almost 2-elementary. $\square$

5. BEGINNING THE PROOF OF THEOREM 1.1

The “if” direction of Theorem 1.1 is obvious; we will prove the “only if”. Let x_1, x_2, x_3, x_4 be singular moduli. Suppose that

$$(1) \quad x_1 - x_2 = x_3 - x_4.$$

We want to prove that either $(x_1, x_2) = (x_3, x_4)$ or $(x_1, x_3) = (x_2, x_4)$. Suppose then that $(x_1, x_2) \neq (x_3, x_4)$ and $(x_1, x_3) \neq (x_2, x_4)$. We will show that this leads to a contradiction.

The proof splits into several cases. First, in Section 5.1, we will dispense with the case where x_1, x_2, x_3, x_4 are not pairwise distinct. Next, in Section 5.2, we handle the case where at least one of x_1, x_2, x_3, x_4 is rational. Then, in Section 5.3, we set up the proof of the general case, where x_1, x_2, x_3, x_4 are pairwise distinct and none of them is rational. The proof of this general case is then split over Sections 5.3, 6, and 7.

5.1. The non-pairwise distinct case. Clearly, equation (1) implies that $x_1 = x_2$ if and only if $x_3 = x_4$. Similarly, $x_1 = x_3$ if and only if $x_2 = x_4$. We may thus assume that $x_1 \neq x_2$, $x_3 \neq x_4$, $x_1 \neq x_3$, and $x_2 \neq x_4$. So if x_1, x_2, x_3, x_4 are not pairwise distinct, then either $x_1 = x_4$ or $x_2 = x_3$, but not both. The equation (1) thus reduces to either $2x_1 = x_2 + x_3$ or $2x_2 = x_1 + x_4$, where the three singular moduli occurring in the equation are pairwise distinct. This though contradicts the following result.

Lemma 5.1. *The equation $2x_1 = x_2 + x_3$ has no solutions with x_1, x_2, x_3 pairwise distinct singular moduli.*

Proof. Suppose that x_1, x_2, x_3 are pairwise distinct singular moduli such that

$$(2) \quad 2x_1 = x_2 + x_3.$$

Then $|x_1| \leq \max\{|x_2|, |x_3|\}$. Since we may assume, by taking Galois conjugates, that x_1 is dominant, we must have that $|\Delta_1| < \max\{|\Delta_2|, |\Delta_3|\}$ by Proposition 2.3.

Suppose first that $x_1 \in \mathbb{Q}$. Then

$$\mathbb{Q}(x_2 + x_3) = \mathbb{Q}.$$

Hence, by Proposition 4.1, either $x_2, x_3 \in \mathbb{Q}$, or $\Delta_2 = \Delta_3$ and $h(\Delta_2) = 2$. It is straightforward to check in PARI that there are no such solutions to equation (2). So we may assume that $x_1 \notin \mathbb{Q}$.

Suppose that $x_2 \in \mathbb{Q}$. Then

$$\mathbb{Q}(x_3 - 2x_1) = \mathbb{Q}.$$

Hence, by Proposition 4.1, we must have that

$$\Delta_1 \neq \Delta_3, \mathbb{Q}(x_1) = \mathbb{Q}(x_3) \text{ is a degree 2 extension of } \mathbb{Q}, \text{ and } 2 = \frac{x_3 - x'_3}{x_1 - x'_1},$$

where x'_1, x'_3 are the non-trivial Galois conjugates of x_1, x_3 respectively. It is easy to check in PARI that there are no such Δ_1, Δ_3 . The case where $x_3 \in \mathbb{Q}$ is analogous. So assume subsequently that $x_1, x_2, x_3 \notin \mathbb{Q}$. This implies, in particular, that $\min\{|\Delta_i| : i = 1, 2, 3\} \geq 15$.

By Proposition 4.1, we thus have that

$$\mathbb{Q}(x_2) = \mathbb{Q}(2x_1 - x_3) = \mathbb{Q}(x_1, x_3)$$

and

$$\mathbb{Q}(x_3) = \mathbb{Q}(2x_1 - x_2) = \mathbb{Q}(x_1, x_2).$$

Hence $x_2 \in \mathbb{Q}(x_3)$ and $x_3 \in \mathbb{Q}(x_2)$, so that $\mathbb{Q}(x_2) = \mathbb{Q}(x_3)$. If $\Delta_2 \neq \Delta_3$, then Proposition 4.1 implies that

$$\mathbb{Q}(x_1) = \mathbb{Q}(x_2 + x_3) = \mathbb{Q}(x_2, x_3) = \mathbb{Q}(x_2) = \mathbb{Q}(x_3).$$

If $\Delta_2 = \Delta_3$, then, by Proposition 4.1 again,

$$\mathbb{Q}(x_1) = \mathbb{Q}(x_2 + x_3) \subset \mathbb{Q}(x_2, x_3) = \mathbb{Q}(x_2) = \mathbb{Q}(x_3)$$

and

$$[\mathbb{Q}(x_2) : \mathbb{Q}(x_1)] = [\mathbb{Q}(x_3) : \mathbb{Q}(x_1)] \leq 2.$$

If

$$\mathbb{Q}(x_1) = \mathbb{Q}(x_2) = \mathbb{Q}(x_3),$$

then equation (2) and [18, Th. 1.5] imply that this field must be a degree 2 extension of $\mathbb{Q}$. Hence, $\Delta_2 \neq \Delta_3$ in this case, else $x_2 + x_3 \in \mathbb{Q}$, contradicting the fact that

$x_1 \notin \mathbb{Q}$. It is then easy to verify in PARI, by making use of Lemma 2.1, that there are no such solutions to equation (2).

So we must have that

$$\mathbb{Q}(x_1) \subsetneq \mathbb{Q}(x_2) = \mathbb{Q}(x_3).$$

By equation (2) and [18, Th. 1.5] again, x_1 must be of degree 2 and x_2, x_3 of degree 4 and $\Delta_2 = \Delta_3$. Applying a suitable Galois automorphism, we may assume from now on that x_2 is dominant, and so x_3 is not dominant. If $D_1 = D_2$, then, by [18, Prop. 7.8],

$$|\Delta_2| \geq 9|\Delta_1|/4.$$

Hence, by Lemma 2.1 and equation (2), we must have that

$$e^{\pi|\Delta_2|^{1/2}} - 2079 \leq 2(e^{2\pi|\Delta_2|^{1/2}/3} + 2079) + (e^{\pi|\Delta_2|^{1/2}/2} + 2079).$$

This implies that $|\Delta_2| \leq 8$, a contradiction. So we must have that $D_1 \neq D_2$. The possible (Δ_1, Δ_2) may then be computed in PARI, as in [18, Prop. 7.6]. Applying the bound in Lemma 2.1 to equation (2) for these (Δ_1, Δ_2) , we see that the only possibility is that $(\Delta_1, \Delta_2) = (-235, -240)$ and, in this case, x_1 must be dominant as well. But then $x_1 < 0$ and $x_2 > 0$, and so $|2x_1 - x_2| > |x_2| > |x_3|$, a contradiction. $\square$

Thus we may assume subsequently that x_1, x_2, x_3, x_4 are pairwise distinct.

5.2. The case where some $x_i \in \mathbb{Q}$. Suppose $x_i \in \mathbb{Q}$ for some i . The remaining x_j, x_k, x_l then satisfy

$$(3) \quad \epsilon_1 x_j + \epsilon_2 x_k + \epsilon_3 x_l = x_i$$

for some $\epsilon_1, \epsilon_2, \epsilon_3 \in \{\pm 1\}$, precisely one of which is $= -1$. Hence, by [17, Theorem 1.1], we must have that either $x_j, x_k, x_l \in \mathbb{Q}$, or else one of x_j, x_k, x_l , say x_j , is in $\mathbb{Q}$ and the other two (i.e. x_k, x_l) are of degree 2 and conjugate over $\mathbb{Q}$ with $\epsilon_k = \epsilon_l = 1$ and $\epsilon_j = -1$. In the second case, equation (3) rearranges to

$$x_i + x_j = x_k + x_l.$$

It is an easy check in PARI to verify that both cases are impossible. Thus we may assume subsequently that $x_1, x_2, x_3, x_4 \notin \mathbb{Q}$. In particular, this implies that $|\Delta_i| \geq 15$ for every i .

5.3. Beginning the general case. We may thus assume that

$$(4) \quad x_1 - x_2 = x_3 - x_4,$$

where x_1, x_2, x_3, x_4 are pairwise distinct, non-rational singular moduli. We may further assume without loss of generality that

$$|\Delta_1| \geq |\Delta_2|, |\Delta_3|, |\Delta_4| \geq 15.$$

By taking Galois conjugates, we may also assume that x_1 is dominant.

The proof of Theorem 1.1 now divides into four cases according to how many of x_2, x_3, x_4 are also dominant. The first two cases are straightforward and are handled in Sections 5.3.1 and 5.3.2. The remaining two cases require more work and are handled in Sections 6 and 7.

5.3.1. None of x_2, x_3, x_4 is dominant. Then equation (4) and Lemma 2.1 imply that

$$e^{\pi|\Delta_1|^{1/2}} - 2079 \leq 3(e^{\pi|\Delta_1|^{1/2}/2} + 2079),$$

and this implies that $|\Delta_1| \leq 8$, a contradiction.

5.3.2. *Exactly one of x_2, x_3, x_4 is dominant.* Say $i \in \{2, 3, 4\}$ is such that x_i is dominant; write x_k, x_l for the remaining two of x_2, x_3, x_4 . Note that $|\Delta_i| < |\Delta_1|$, since there is a unique dominant singular modulus of a given discriminant. So

$$|x_1| - |x_i| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{|\Delta_1|^{1/2}} - 2 \cdot 2079,$$

by Lemmata 2.1 and 2.4. On the other hand, Lemma 2.1 also implies that

$$|x_k| + |x_l| \leq 2(e^{\pi|\Delta_1|^{1/2}/2} + 2079)$$

These bounds and equation (4) imply that $|\Delta_1| \leq 10$, a contradiction.

6. EXACTLY TWO OF x_2, x_3, x_4 ARE DOMINANT

This will be the most challenging case to handle. Write x_i, x_j for the two dominant singular moduli and x_k for the non-dominant singular modulus among x_2, x_3, x_4 . Since x_1, x_i, x_j are pairwise distinct and dominant, we have that $|\Delta_i|, |\Delta_j| < |\Delta_1|$ and $\Delta_i \neq \Delta_j$. Dominant singular moduli are real, so $x_k \in \mathbb{R}$ also. Let $\epsilon_1, \epsilon_2, \epsilon_3 \in \{\pm 1\}$ with $\#\{n : \epsilon_n = -1\} = 1$ be such that

$$(5) \quad x_1 = \epsilon_1 x_i + \epsilon_2 x_j + \epsilon_3 x_k.$$

Our first aim is to show that we can reduce this case to the following list of cases:

- (1) Δ_i, Δ_j are both 2-elementary and $|\Delta_i|, |\Delta_j| \leq 7392$;
- (2) Δ_i, Δ_j are both 2-elementary, $|\Delta_i| \leq 7392$, and $D_j = D_*$;
- (3) Δ_i, Δ_j are both 2-elementary, $D_i = D_*$, and $|\Delta_j| \leq 7392$;
- (4) Δ_i, Δ_j are both 2-elementary and $D_i = D_j = D_*$;
- (5) Δ_i is 2-elementary, Δ_j is not 2-elementary, $|\Delta_i| \leq 7392$, and $D_j = D_1$;
- (6) Δ_i is not 2-elementary, Δ_j is 2-elementary, $D_i = D_1$, and $|\Delta_j| \leq 7392$;
- (7) Δ_i is 2-elementary, Δ_j is not 2-elementary, $D_i = D_*$, and $D_j = D_1$;
- (8) Δ_i is not 2-elementary, Δ_j is 2-elementary, $D_i = D_1$, and $D_j = D_*$.

To do this, we first show in Section 6.1 that at least one of D_i, D_j must not be equal to D_1 . This part of the proof is straightforward. We then prove in Section 6.2 that if $D_i \neq D_1$, then Δ_i is 2-elementary (and analogously for j). This part of the proof will take substantially more work.

In Section 6.3, we deduce, by using these two facts, that we must be in one of the cases (1)–(8) above. We then eliminate each of these cases in turn. This elimination relies mostly on the bounds from Section 2 and on the facts about 2-elementary discriminants established in Sections 3 and 4

6.1. At least one of D_i, D_j is not equal to D_1 . Suppose that $D_1 = D_i = D_j$. Then, by Lemmata 2.1 and 2.2,

$$|x_i| + |x_j| + |x_k| \leq 2(0.005e^{\pi|\Delta_1|^{1/2}} + 2079) + (e^{\pi|\Delta_1|^{1/2}/2} + 2079).$$

Since, by Lemma 2.1 again,

$$|x_1| \geq e^{\pi|\Delta_1|^{1/2}} - 2079,$$

we thus obtain from equation (5) that $|\Delta_1| \leq 8$ and so $x_1 \in \mathbb{Q}$, a contradiction. So we may assume subsequently that at least one of D_i, D_j is not equal to D_1 .

6.2. If $D_i \neq D_1$, then Δ_i is 2-elementary. Suppose that $D_i \neq D_1$. Assume, towards a contradiction, that Δ_i is not 2-elementary. Then, by Proposition 3.1, there exists $\sigma_1 \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_1(x_i) \neq x_i$ and $\sigma_1(x_1) = x_1$. Write x'_n for $\sigma_1(x_n)$. Note that x'_i is not dominant. By equation (5),

$$x_1 = \epsilon_1 x'_i + \epsilon_2 x'_j + \epsilon_3 x'_k.$$

If at least one of x'_j, x'_k is also not dominant, then we have reduced to one of the cases handled in Sections 5.3.1 and 5.3.2. So we may assume that x'_j, x'_k are both dominant. In particular, $x'_j = x_j$ and $x'_k \neq x_k$, and so

$$(6) \quad x_1 = \epsilon_1 x'_i + \epsilon_2 x_j + \epsilon_3 x'_k.$$

We obtain from equations (5) and (6) that

$$(7) \quad \epsilon_1(x_i - x'_i) = -\epsilon_3(x_k - x'_k).$$

Hence

$$\mathbb{Q}(x_i - x'_i) = \mathbb{Q}(x_k - x'_k).$$

So, by Proposition 4.1,

$$\mathbb{Q}(x_i, x'_i) = \mathbb{Q}(x_k, x'_k).$$

If $D_i \neq D_k$, then $\mathbb{Q}(x_i) = \mathbb{Q}(x_k)$ by Proposition 4.2 and so Δ_i is 2-elementary by Proposition 4.3, which contradicts our assumption. So we must have that $D_i = D_k$. Then, by Propositions 4.2 and 4.3, we have that

$$\Delta_i/\Delta_k \in \{1, 4, 1/4\}.$$

Suppose $\Delta_i \neq \Delta_k$. Then $\{\Delta_i, \Delta_k\} = \{\Delta, 4\Delta\}$ for some Δ . Note that x_i, x'_i are dominant and x'_i, x_k are not dominant. Equation (7) thus implies, thanks to Lemma 2.1, that

$$e^{2\pi|\Delta|^{1/2}} - 2079 \leq 3(e^{\pi|\Delta|^{1/2}} + 2079).$$

This however is impossible for all discriminants Δ . So we must have that $\Delta_i = \Delta_k$.

If $D_j \neq D_1$ and Δ_j is not 2-elementary, then we could repeat the above argument with Δ_j in place of Δ_i to obtain that $\Delta_j = \Delta_k$ also. This would contradict the fact that $\Delta_i \neq \Delta_j$. Therefore, either $D_j = D_1$ or Δ_j is 2-elementary.

Note that $x'_k = x_i$, since both are dominant and $\Delta_i = \Delta_k$. So equation (7) yields

$$\epsilon_1(x_i - x'_i) = -\epsilon_3(x_k - x_i),$$

which rearranges to

$$x_i(\epsilon_1 - \epsilon_3) = \epsilon_1 x'_i - \epsilon_3 x_k.$$

Since x_i is dominant and x'_i, x_k are not dominant, Proposition 2.3 implies that $\epsilon_1 = \epsilon_3$. So $x'_i = x_k$ and $\epsilon_2 = -1$. Equation (5) thus rearranges to

$$(8) \quad x_1 + x_j = x_i + x_k.$$

We now split into two cases, according to whether Δ_1 is 2-elementary. We will obtain a contradiction in each case, and thus show that Δ_i must be 2-elementary.

6.2.1. *The case where Δ_1 is not 2-elementary.* The first case is relatively straightforward. Suppose that Δ_1 is not 2-elementary. Since $D_1 \neq D_i = D_k$, Proposition 3.1 implies that there exists $\sigma_2 \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_2(x_1) \neq x_1$ but $\sigma_2(x_i) = x_i$ and $\sigma_2(x_k) = x_k$. Write x_1'', x_j'' for $\sigma_2(x_1), \sigma_2(x_j)$ respectively. Applying σ_2 to equation (8) and subtracting the resulting equation from equation (8), we see that

$$(9) \quad x_1 - x_1'' = x_j'' - x_j.$$

In particular, $x_j'' \neq x_j$. So x_1'', x_j'' are not dominant. Hence, by Lemma 2.1,

$$|x_1''| + |x_j''| \leq 2(e^{\pi|\Delta_1|^{1/2}/2} + 2079)$$

On the other hand, by Lemmata 2.1 and 2.4,

$$|x_1| - |x_j| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{|\Delta_1|^{1/2}} - 2 \cdot 2079.$$

These two bounds and equation (9) then imply that $|\Delta_1| \leq 10$, which is impossible.

6.2.2. *The case where Δ_1 is 2-elementary.* The second case will require more work. Suppose then that Δ_1 is 2-elementary. Then, by Proposition 3.6, either $|\Delta_1| \leq 7392$ or $D_1 = D_*$. We now split into four subcases and derive a contradiction in each.

Subcase 1. Suppose that $|\Delta_1| \leq 7392$ and $D_j = D_1$. Since Δ_1 is 2-elementary and $|\Delta_1| \leq 7392$, Proposition 3.7 implies that $f_1 \leq 8$. Hence, by Lemmata 2.1 and 2.4,

$$|x_1| - |x_i| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{8|D_1|^{1/2}} - 2 \cdot 2079.$$

Lemmata 2.1 and 2.2 imply that

$$|x_j| + |x_k| \leq e^{-\pi|D_1|^{1/2}} e^{\pi|\Delta_1|^{1/2}} + e^{\pi|\Delta_1|^{1/2}/2} + 2 \cdot 2079.$$

These two inequalities and equation (8) together imply that

$$\begin{aligned} \frac{1}{8|D_1|^{1/2}} &\leq e^{-\pi|D_1|^{1/2}} + e^{-\pi|\Delta_1|^{1/2}/2} + (4 \cdot 2079)e^{-\pi|\Delta_1|^{1/2}} \\ &\leq 2e^{-\pi|D_1|^{1/2}} + 8316e^{-2\pi|D_1|^{1/2}}, \end{aligned}$$

where the second inequality holds since $f_1 \geq f_j + 1 \geq 2$. We obtain that $|D_1| \leq 3$ and hence $|\Delta_1| \leq 192$. We may then verify in PARI that for any $(\Delta_1, \Delta_i, \Delta_j, \Delta_k)$ satisfying these conditions, the inequality

$$(10) \quad e^{\pi|\Delta_1|^{1/2}} - 2079 > (e^{\pi|\Delta_i|^{1/2}} + 2079) + (e^{\pi|\Delta_j|^{1/2}} + 2079) + (e^{\pi|\Delta_k|^{1/2}/2} + 2079)$$

holds. This though contradicts equation (8) by Lemma 2.1.

Subcase 2. Suppose that $|\Delta_1| \leq 7392$ and $D_j \neq D_1$. Hence, as argued in the third paragraph of Section 6.2, the discriminant Δ_j must be 2-elementary. By Proposition 4.4, this implies that $\Delta_i = \Delta_k$ and this discriminant is almost 2-elementary. Lemma 2.1 and equation (8) together imply that

$$(11) \quad e^{\pi|\Delta_1|^{1/2}} - 2079 \leq (e^{\pi|\Delta_i|^{1/2}} + 2079) + (e^{\pi|\Delta_j|^{1/2}} + 2079) + (e^{\pi|\Delta_k|^{1/2}/2} + 2079).$$

In PARI, we find 19 possibilities for $(\Delta_1, \Delta_i, \Delta_j, \Delta_k)$ satisfying these conditions. For each such possibility, we verify that equation (8) does not hold with x_1, x_i, x_j the dominant singular moduli of respective discriminants $\Delta_1, \Delta_i, \Delta_j$ and x_k any non-dominant, real singular modulus of discriminant Δ_k .

Subcase 3. Suppose that $D_1 = D_*$ and $D_j \neq D_1$. As in Subcase 2, the discriminant Δ_j is 2-elementary, since $D_j \neq D_1$. Hence $|\Delta_j| \leq 7392$ by Proposition 3.6. So

$$|x_j| \leq e^{\pi\sqrt{7392}} + 2079$$

by Lemma 2.1. Also,

$$|x_1| - |x_i| - |x_k| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{|\Delta_1|^{1/2}} - e^{\pi|\Delta_1|^{1/2}/2} - 3 \cdot 2079$$

by Lemmata 2.4 and 2.1. We thus obtain from equation (8) that $|\Delta_1| \leq 7638$. Hence, $|D_*| \leq 7638$, which contradicts Proposition 3.6.

Subcase 4. Suppose that $D_j = D_1 = D_*$. Hence, by Lemmata 2.1 and 2.2,

$$\begin{aligned} |x_j| + |x_k| &\leq e^{\pi|\Delta_1|^{1/2}} e^{-\pi|D_*|^{1/2}} + e^{\pi|\Delta_1|^{1/2}/2} + 2 \cdot 2079 \\ &\leq e^{\pi|\Delta_1|^{1/2}} (e^{-\pi|D_*|^{1/2}} + e^{-\pi|\Delta_1|^{1/2}/2} + 4158e^{-\pi|\Delta_1|^{1/2}}). \end{aligned}$$

By Lemmata 2.1 and 2.4, we also have that

$$|x_1| - |x_i| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{|\Delta_1|^{1/2}} - 2 \cdot 2079 = e^{\pi|\Delta_1|^{1/2}} \left(\frac{1}{|\Delta_1|^{1/2}} - 4158e^{-\pi|\Delta_1|^{1/2}} \right).$$

Thus, equation (8) implies that

$$\frac{1}{|\Delta_1|^{1/2}} - 4158e^{-\pi|\Delta_1|^{1/2}} \leq e^{-\pi|D_*|^{1/2}} + e^{-\pi|\Delta_1|^{1/2}/2} + 4158e^{-\pi|\Delta_1|^{1/2}}.$$

Since Δ_1 is 2-elementary, Proposition 3.7 implies that $|D_*|^{1/2} \leq |\Delta_1|^{1/2} \leq 60|D_*|^{1/2}$. So,

$$\frac{1}{60|D_*|^{1/2}} \leq (2 \cdot 4158 + 1)e^{-\pi|D_*|^{1/2}} + e^{-\pi|D_*|^{1/2}/2}.$$

We thus obtain that $|D_*| \leq 22$, which contradicts Proposition 3.6.

6.3. Synthesis. By Section 6.2, if Δ_i is not 2-elementary, then $D_i = D_1$. If Δ_i is 2-elementary, then, by Proposition 3.6, either $|\Delta_i| \leq 7392$ or $D_i = D_*$. The same holds for Δ_j . Hence, at least one of Δ_i, Δ_j is 2-elementary, since D_1, D_i, D_j are not all equal by Section 6.1. We have therefore reduced to the eight cases stated at the beginning of Section 6, namely:

- (1) Δ_i, Δ_j are both 2-elementary and $|\Delta_i|, |\Delta_j| \leq 7392$;
- (2) Δ_i, Δ_j are both 2-elementary, $|\Delta_i| \leq 7392$, and $D_j = D_*$;
- (3) Δ_i, Δ_j are both 2-elementary, $D_i = D_*$, and $|\Delta_j| \leq 7392$;
- (4) Δ_i, Δ_j are both 2-elementary and $D_i = D_j = D_*$;
- (5) Δ_i is 2-elementary, Δ_j is not 2-elementary, $|\Delta_i| \leq 7392$, and $D_j = D_1$;
- (6) Δ_i is not 2-elementary, Δ_j is 2-elementary, $D_i = D_1$, and $|\Delta_j| \leq 7392$;
- (7) Δ_i is 2-elementary, Δ_j is not 2-elementary, $D_i = D_*$, and $D_j = D_1$;
- (8) Δ_i is not 2-elementary, Δ_j is 2-elementary, $D_i = D_1$, and $D_j = D_*$.

We will now obtain a contradiction in each case. We do not treat cases (3), (6), and (8), because they are evidently analogous to cases (2), (5), and (7) respectively.

Note as well that if Δ_i, Δ_j are both 2-elementary, then, by Proposition 4.4, either Δ_1, Δ_k are 2-elementary, or: $\Delta_1 = \Delta_k$ and this discriminant is almost 2-elementary and

$$x_1 + x_k = x_i + x_j.$$

6.3.1. *Case 1.* Lemma 2.1 implies that

$$|x_i| + |x_j| \leq 2(e^{\pi\sqrt{7392}} + 2079)$$

and

$$|x_1| - |x_k| \geq (e^{\pi|\Delta_1|^{1/2}} - 2079) - (e^{\pi|\Delta_1|^{1/2}/2} + 2079).$$

We thus obtain from equation (4) that $|\Delta_1| \leq 7429$.

Lemma 2.1 and equation (4) imply that

$$e^{\pi|\Delta_1|^{1/2}} - 2079 \leq (e^{\pi|\Delta_i|^{1/2}} + 2079) + (e^{\pi|\Delta_j|^{1/2}} + 2079) + (e^{\pi|\Delta_k|^{1/2}/2} + 2079).$$

We may find in PARI all the possibilities for $(\Delta_1, \Delta_i, \Delta_j, \Delta_k)$ satisfying these conditions with $|\Delta_1| \leq 7429$. For each such $(\Delta_1, \Delta_i, \Delta_j, \Delta_k)$, we may then verify that equation (4) does not hold whenever x_1, x_i, x_j are the dominant singular moduli of respective discriminants $\Delta_1, \Delta_i, \Delta_j$ and x_k is any non-dominant, real singular modulus of discriminant Δ_k .

6.3.2. *Case 2.* By Lemmata 2.1 and 2.4,

$$|x_1| - |x_j| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{|\Delta_1|^{1/2}} - 2 \cdot 2079$$

and, by Lemma 2.1,

$$|x_i| + |x_k| \leq e^{\pi\sqrt{7392}} + e^{\pi|\Delta_1|^{1/2}/2} + 2 \cdot 2079.$$

We obtain from equation (4) that $|\Delta_1| \leq 7638$. In particular, $|D_*| \leq |\Delta_j| \leq 7638$, which contradicts Proposition 3.6.

6.3.3. *Case 4.* Without loss of generality, assume that $|\Delta_j| < |\Delta_i|$. So, by Lemmata 2.4, 2.2, and 2.1,

$$|x_1| - |x_i| - |x_j| - |x_k| \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{|\Delta_1|^{1/2}} - e^{-\pi|D_*|^{1/2}} e^{\pi|\Delta_i|^{1/2}} - e^{\pi|\Delta_1|^{1/2}/2} - 4 \cdot 2079.$$

Hence, equation (4) implies that

$$e^{-\pi|D_*|^{1/2}} e^{\pi|\Delta_i|^{1/2}} \geq e^{\pi|\Delta_1|^{1/2}} \left(\frac{1}{|\Delta_1|^{1/2}} - e^{-\pi|\Delta_1|^{1/2}/2} - 8316e^{-\pi|\Delta_1|^{1/2}} \right).$$

Note that

$$\frac{1}{|\Delta_1|^{1/2}} - e^{-\pi|\Delta_1|^{1/2}/2} - 8316e^{-\pi|\Delta_1|^{1/2}} \geq \frac{1}{2|\Delta_1|^{1/2}}$$

if $|\Delta_1| \geq 13$. Since $|\Delta_1| \geq 15$, we thus must have that

$$e^{-\pi|D_*|^{1/2}} e^{\pi|\Delta_i|^{1/2}} \geq \frac{e^{\pi|\Delta_1|^{1/2}}}{2|\Delta_1|^{1/2}}.$$

The function $g(t) = \exp(\pi\sqrt{t})/2\sqrt{t}$ is increasing for $t > 1/\pi^2$. So

$$e^{-\pi|D_*|^{1/2}} e^{\pi|\Delta_i|^{1/2}} \geq \frac{e^{\pi|\Delta_i|^{1/2}}}{2|\Delta_i|^{1/2}}.$$

Since Δ_i is 2-elementary, $f_i \leq 60$ by Proposition 3.7, and so $|\Delta_i|^{1/2} \leq 60|D_*|^{1/2}$. So

$$e^{-\pi|D_*|^{1/2}} \geq \frac{1}{2|\Delta_i|^{1/2}} \geq \frac{1}{2 \cdot 60|D_*|^{1/2}},$$

which is impossible, since $|D_*| \geq 3$.

6.3.4. *Case 5.* By Lemma 2.1, we have that

$$|x_1| > e^{\pi|\Delta_1|^{1/2}} - 2079$$

and also, thanks to Lemma 2.2,

$$|x_i| + |x_j| + |x_k| \leq e^{\pi\sqrt{7392}} + 0.005e^{\pi|\Delta_1|^{1/2}} + e^{\pi|\Delta_1|^{1/2}/2} + 3 \cdot 2079.$$

We thereby obtain from equation (4) that $|\Delta_1| \leq 7392$.

Equation (4) and Lemmata 2.1 and 2.2 imply that

$$e^{\pi|\Delta_1|^{1/2}} - 2079 < (e^{\pi|\Delta_i|^{1/2}} + 2079) + (0.005e^{\pi|\Delta_1|^{1/2}} + 2079) + (e^{\pi|\Delta_k|^{1/2}/2} + 2079).$$

Thus,

$$0.995e^{\pi|\Delta_1|^{1/2}} < e^{\pi|\Delta_i|^{1/2}} + e^{\pi|\Delta_k|^{1/2}/2} + 8316.$$

Since $|\Delta_k| \leq |\Delta_1|$, we have that

$$e^{\pi|\Delta_1|^{1/2}} (0.995 - e^{-\pi|\Delta_1|^{1/2}/2} - 8316e^{-\pi|\Delta_1|^{1/2}}) < e^{\pi|\Delta_i|^{1/2}}.$$

The discriminants $\Delta_1, \Delta_i, \Delta_j$ are pairwise distinct and are all ≥ 15 in absolute value. So $|\Delta_1| \geq 19$, since discriminants are $\equiv 0, 1 \pmod{4}$. So

$$0.995 - e^{-\pi|\Delta_1|^{1/2}/2} - 8316e^{-\pi|\Delta_1|^{1/2}} > 0.995 - e^{-\pi\sqrt{19}/2} - 8316e^{-\pi\sqrt{19}} > 0.9845.$$

Hence,

$$0.9845e^{\pi|\Delta_1|^{1/2}} < e^{\pi|\Delta_i|^{1/2}}.$$

Thus,

$$|\Delta_1|^{1/2} - |\Delta_i|^{1/2} < \frac{-\log(0.9845)}{\pi} < 0.005.$$

We may therefore obtain that

$$|\Delta_1| < |\Delta_i| + 0.01|\Delta_i|^{1/2} + 0.000025 < |\Delta_i| + 1,$$

since $|\Delta_i|^{1/2} \leq \sqrt{7392} < 86$. This though contradicts the fact that $|\Delta_1| \geq |\Delta_i| + 1$.

6.3.5. *Case 7.* Since $\Delta_1 \neq \Delta_j$, Proposition 4.4 implies that Δ_k is not 2-elementary. Note also that $D_1 \neq D_*$, since D_1, D_i, D_j are not all equal. So, if Δ_1 is 2-elementary, then $|\Delta_1| \leq 7392$ by Proposition 3.6. But then $|D_*| = |D_i| \leq 7392$, which contradicts Proposition 3.6. So we may assume that Δ_1 is not 2-elementary.

Suppose that $D_k \neq D_1$. Since Δ_k is not 2-elementary, there exists, by Proposition 3.1, $\sigma_1 \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_1(x_k) \neq x_k$ but $\sigma_1(x_1) = x_1$ and $\sigma_1(x_j) = x_j$. Writing x'_n for $\sigma_1(x_n)$, we obtain from equation (5) that

$$\epsilon_1(x_i - x'_i) = -\epsilon_3(x_k - x'_k).$$

We may now obtain a contradiction by arguing as in the paragraph following equation (6). If $D_i \neq D_k$, then Δ_k is 2-elementary, a contradiction. If $D_i = D_k$, then $\Delta_i/\Delta_k \in \{1, 4, 1/4\}$. If $\Delta_i \neq \Delta_k$, then we obtain a bound $\max\{|\Delta_i|, |\Delta_k|\} \leq 11$, which is impossible. So we must have that $\Delta_i = \Delta_k$, and this contradicts the fact that Δ_k is not 2-elementary.

So $D_k = D_1 = D_j$. By Proposition 3.1, there exists $\sigma_2 \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_2(x_1) \neq x_1$ but $\sigma_2(x_i) = x_i$. We may thus obtain from equation (5) that

$$(12) \quad x_1 - x''_1 = \epsilon_2(x_j - x''_j) + \epsilon_3(x_k - x''_k),$$

where x''_n denotes $\sigma_2(x_n)$. In particular, x''_1 is not dominant. Lemma 2.1 implies that

$$(13) \quad |x_1| > e^{\pi|\Delta_1|^{1/2}} - 2079.$$

Suppose that $\Delta_k \neq \Delta_1$. Then, by Lemma 2.2, we also have that

$$|x_1''| + |x_j| + |x_j''| + |x_k| + |x_k''| \leq (e^{\pi|\Delta_1|^{1/2}/2} + 2079) + 4(0.005e^{\pi|\Delta_1|^{1/2}} + 2079).$$

These bounds and equation (12) imply that $|\Delta_1| \leq 9$, which is impossible.

So $\Delta_k = \Delta_1$. By Proposition 3.1, there exists $\sigma_3 \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_3(x_j) \neq x_j$ but $\sigma_3(x_i) = x_i$. Equation (5) thus yields that

$$(14) \quad x_1 - x_1''' = \epsilon_2(x_j - x_j''') + \epsilon_3(x_k - x_k'''),$$

where x_n''' denotes $\sigma_3(x_n)$. Suppose that $x_k = x_k'''$. Then $x_1 \neq x_1'''$, since $x_j \neq x_j'''$. So x_1''' is not dominant. Lemmata 2.1 and 2.2 imply that

$$|x_1| \geq e^{\pi|\Delta_1|^{1/2}} - 2079$$

and

$$|x_1'''| + |x_j| + |x_j'''| \leq (e^{\pi|\Delta_1|^{1/2}/2} + 2079) + 2(0.005e^{\pi|\Delta_1|^{1/2}} + 2079).$$

These bounds and equation (14) then imply that $|\Delta_1| \leq 8$, which is impossible. So $x_k \neq x_k'''$. If $x_1 = x_1'''$, then we may argue similarly (applying first a suitable automorphism to (14) to make x_k dominant) and obtain a contradiction. So $x_1 \neq x_1'''$ as well. In particular, x_1''' is not dominant.

If x_k''' is not dominant, then Lemmata 2.1 and 2.2 imply that

$$|x_1'''| + |x_j| + |x_j'''| + |x_k| + |x_k'''| \leq 3(e^{\pi|\Delta_1|^{1/2}/2} + 2079) + 2(0.005e^{\pi|\Delta_1|^{1/2}} + 2079).$$

Equation (14) and the bound (13) then imply that $|\Delta_1| \leq 9$, which is impossible.

So assume that x_k''' is dominant, i.e. $x_k''' = x_1$. Lemmata 2.1 and 2.2 then yield that

$$|x_1'''| + |x_j| + |x_j'''| + |x_k| \leq 2(e^{\pi|\Delta_1|^{1/2}/2} + 2079) + 2(0.005e^{\pi|\Delta_1|^{1/2}} + 2079).$$

If $\epsilon_3 = 1$, then

$$|x_1 + \epsilon_3 x_k'''| \geq 2(e^{\pi|\Delta_1|^{1/2}} - 2079).$$

And so equation (14) implies that $|\Delta_1| \leq 7$, a contradiction. If $\epsilon_3 = -1$, then $\epsilon_2 = 1$ and equation (14) rearranges to

$$(15) \quad x_k - x_1''' = x_j - x_j'''.$$

Since $x_j \neq x_j'''$, we have that $x_k \neq x_1'''$. Taking suitable Galois conjugates, we may now assume that x_k is dominant, and so x_1''' is not dominant. Thus, by Lemma 2.1,

$$|x_k| - |x_1'''| \geq (e^{\pi|\Delta_1|^{1/2}} - 2079) - (e^{\pi|\Delta_1|^{1/2}/2} + 2079),$$

while, by Lemma 2.2,

$$|x_j| + |x_j'''| \leq 2(0.005e^{\pi|\Delta_1|^{1/2}} + 2079).$$

These bounds and equation (15) together imply that $|\Delta_1| \leq 8$, a contradiction.

7. ALL OF x_2, x_3, x_4 ARE DOMINANT

In this case, $\Delta_1, \Delta_2, \Delta_3, \Delta_4$ are pairwise distinct, since x_1, x_2, x_3, x_4 are dominant and pairwise distinct.

7.1. Equal fundamental discriminants. If $D_1 = D_2 = D_3 = D_4$, then Lemmata 2.1 and 2.2 and equation (4) together imply that

$$e^{\pi|\Delta_1|^{1/2}} - 2079 \leq 3(0.005e^{\pi|\Delta_1|^{1/2}} + 2079),$$

and hence $|\Delta_1| \leq 8$, a contradiction. We may thus assume that the fundamental discriminants D_1, D_2, D_3, D_4 are not all equal.

7.2. An inductive argument. Let $i \in \{2, 3, 4\}$ be such that $D_i \neq D_1$. Suppose that Δ_i is not 2-elementary. Then, by Proposition 3.1, there exists $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(x_i) \neq x_i$ and $\sigma(x_1) = x_1$. In particular, $\sigma(x_i)$ is not dominant, and so applying σ to equation (4) reduces us to one of the previously proved cases where at most two of x_2, x_3, x_4 are dominant.

We may thus assume subsequently that, for every $i \in \{2, 3, 4\}$, either $D_i = D_1$ or Δ_i is 2-elementary. In particular, at least one of $\Delta_2, \Delta_3, \Delta_4$ is 2-elementary, since D_1, D_2, D_3, D_4 are not all equal. To finish the proof of Theorem 1.1, we distinguish two final cases, according to whether or not Δ_1 is 2-elementary.

7.3. The case where Δ_1 is not 2-elementary. Suppose Δ_1 is not 2-elementary. Then, by Proposition 4.4, at most one of $\Delta_2, \Delta_3, \Delta_4$ is 2-elementary, since the four discriminants are pairwise distinct. Therefore, there exists a unique $i \in \{2, 3, 4\}$ such that $D_i \neq D_1$, since Δ_i is 2-elementary for any such i by Section 7.2. For the remaining $j, k \in \{2, 3, 4\}$, we have that $D_j = D_k = D_1$ and hence, by Lemma 2.2,

$$(16) \quad |x| \leq 0.005e^{\pi|\Delta_1|^{1/2}} + 2079$$

for every singular modulus x of discriminant Δ_j or Δ_k .

Since Δ_1 is not 2-elementary, by Proposition 3.1 there exists $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(x_1) \neq x_1$ and $\sigma(x_i) = x_i$. In particular, $\sigma(x_1)$ is not dominant. Write x'_n for $\sigma(x_n)$. There are $\epsilon_1, \epsilon_2, \epsilon_3 \in \{\pm 1\}$ such that

$$x_1 = \epsilon_1 x_i + \epsilon_2 x_j + \epsilon_3 x_k$$

and

$$x'_1 = \epsilon_1 x_i + \epsilon_2 x'_j + \epsilon_3 x'_k.$$

Hence,

$$x_1 = x'_1 + \epsilon_2(x_j - x'_j) + \epsilon_3(x_k - x'_k).$$

This equation, Lemma 2.1, and equation (16) together imply that

$$e^{\pi|\Delta_1|^{1/2}} - 2079 \leq (e^{\pi|\Delta_1|^{1/2}/2} + 2079) + 4(0.005e^{\pi|\Delta_1|^{1/2}} + 2079).$$

From this we obtain that $|\Delta_1| \leq 9$, a contradiction.

7.4. The case where Δ_1 is 2-elementary. So we may assume subsequently that Δ_1 is 2-elementary. Since the fundamental discriminants D_1, D_2, D_3, D_4 are not all equal, there exists $i \in \{2, 3, 4\}$ such that $D_i \neq D_1$. Then Δ_i is 2-elementary by Section 7.2. Therefore, Proposition 4.4 implies that all of $\Delta_1, \Delta_2, \Delta_3, \Delta_4$ must be 2-elementary, since they are pairwise distinct.

Suppose that $D_1 = D_*$. Then, for each $j \geq 2$, either

$$D_j = D_1 \text{ and } |x_j| \leq 0.005e^{\pi|\Delta_1|^{1/2}} + 2079$$

by Lemmata 2.1 and 2.2, or

$$D_j \neq D_1 \text{ and } |\Delta_j| \leq 7392$$

by Proposition 3.6. These bounds, Lemma 2.1, and equation (4) then imply that $|\Delta_1| \leq 7452$ and thus $|D_*| \leq 7452$, which contradicts Proposition 3.6.

So we may assume that $D_1 \neq D_*$. Hence, $|\Delta_1| \leq 7392$ by Proposition 3.6. Further, Lemma 2.1 and equation (4) imply that

$$(17) \quad e^{\pi|\Delta_1|^{1/2}} - 2079 \leq (e^{\pi|\Delta_2|^{1/2}} + 2079) + (e^{\pi|\Delta_3|^{1/2}} + 2079) + (e^{\pi|\Delta_4|^{1/2}} + 2079)$$

We may then find in PARI all the possible $(\Delta_1, \Delta_2, \Delta_3, \Delta_4)$ satisfying the above conditions and, for each possibility, verify that equation (4) does not hold for the corresponding dominant singular moduli. This completes the proof of Theorem 1.1.

Acknowledgments. This work was supported by ANR project JINVARIANT. The authors would like to thank the referee for their helpful comments. On behalf of all authors, the corresponding author states that there is no conflict of interest.

Supporting data. All computations in this paper were performed using the open-source computer algebra system PARI/GP [27]; the scripts are available from: https://github.com/guyfowler/distinct_differences.

REFERENCES

- [1] B. Allombert, Yu. Bilu, and A. Pizarro-Madariaga, *CM-points on straight lines*, Analytic number theory, Springer, Cham, 2015, pp. 1–18.
- [2] Y. André, *Finitude des couples d’invariants modulaires singuliers sur une courbe algébrique plane non modulaire*, J. Reine Angew. Math. **505** (1998), 203–208.
- [3] V. Aslanyan, S. Eterović, and G. Fowler, *Multiplicative relations among differences of singular moduli*, [arXiv:2308.12244v2](https://arxiv.org/abs/2308.12244), to appear in Ann. Sc. Norm. Super. Pisa Cl. Sci.
- [4] Yu. Bilu, B. Faye, and H. Zhu, *Separating singular moduli and the primitive element problem*, Q. J. Math. **71** (2020), no. 4, 1253–1280.
- [5] Yu. Bilu, S. Gun and E. Tron, *Effective multiplicative independence of three singular moduli*, Algebra & Number Theory **20** (2026), no. 6, 1073–1123.
- [6] Yu. Bilu, P. Habegger, and L. Kühne, *No singular modulus is a unit*, Int. Math. Res. Not. IMRN (2020), no. 24, 10005–10041.
- [7] Yu. Bilu and L. Kühne, *Linear Equations in Singular Moduli*, Int. Math. Res. Not. IMRN (2020), no. 21, 7617–7643.
- [8] Yu. Bilu, F. Luca, and D. Masser, *Collinear CM-points*, Algebra & Number Theory **11** (2017), no. 5, 1047–1087.
- [9] Yu. Bilu, D. Masser, and U. Zannier, *An effective “theorem of André” for CM-points on a plane curve*, Math. Proc. Cambridge Philos. Soc. **154** (2013), no. 1, 145–152.
- [10] G. Binyamini, *Some effective estimates for André–Oort in $Y(1)^n$* , J. Reine Angew. Math. **767** (2020), 17–35, with an appendix by E. Kowalski.
- [11] F. Breuer, *Heights of CM points on complex affine curves*, Ramanujan J. **5** (2001), no. 3, 311–317.
- [12] F. Campagna, *On singular moduli that are S-units*, Manuscripta Math. **166** (2021), 73–90.
- [13] H. Cohn, *Introduction to the construction of class fields*, Dover Publications, Inc., New York, 1994, Corrected reprint of the 1985 original.
- [14] D. Cox, *Primes of the form $x^2 + ny^2$* , John Wiley & Sons, Inc., New York, 1989.
- [15] B. Edixhoven, *Special points on the product of two modular curves*, Compositio Math. **114** (1998), no. 3, 315–328.
- [16] B. Faye and A. Riffaut, *Fields generated by sums and products of singular moduli*, J. Number Theory **192** (2018), 37–46.
- [17] G. Fowler, *Equations in three singular moduli: the equal exponent case*, J. Number Theory **243** (2023), 256–297.
- [18] G. Fowler, *Some uniform effective results on André–Oort for sums of powers in $\mathbb{C}^n$* , Math. Proc. Cambridge Philos. Soc. **180** (2026), no. 3, 607–641.

- [19] Y. Fu and R. Zhao, *Algebraic independence of special points on Shimura varieties*, preprint, [arXiv:2405.14084v2](https://arxiv.org/abs/2405.14084v2) (2024).
- [20] B. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.
- [21] S. Herrero, R. Menares, and J. Rivera-Letelier, *There are at most finitely many singular moduli that are S -units*, Compos. Math. **160.4** (2024), 732–770.
- [22] L. Kühne, *An effective result of André–Oort type II*, Acta Arith. **161** (2013), no. 1, 1–19.
- [23] L. Kühne, *Intersection of class fields*, Acta Arith. **198** (2021), no. 2, 109–127.
- [24] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
- [25] K. Lauter and B. Viray, *On singular moduli for arbitrary discriminants*, Int. Math. Res. Not. IMRN (2015), no. 19, 9206–9250.
- [26] Y. Li, *Singular units and isogenies between CM elliptic curves*, Compos. Math. **157** (2021), no. 5, 1022–1035.
- [27] The PARI Group, PARI/GP version 2.18.0, Univ. Bordeaux, 2024, <http://pari.math.u-bordeaux.fr/>.
- [28] F. Pazuki, *Modular invariants and isogenies*, Int. J. Number Theory **15.3** (2019), 569–584.
- [29] J. Pila, *O-minimality and the André–Oort conjecture for $\mathbb{C}^n$* , Ann. of Math. (2) **173** (2011), no. 3, 1779–1840.
- [30] J. Pila, *Special point problems with elliptic modular surfaces*, Mathematika **60** (2014), no. 1, 1–31.
- [31] J. Pila and J. Tsimerman, *Multiplicative relations among singular moduli*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **17** (2017), no. 4, 1357–1382.
- [32] T. Scanlon, *Automatic uniformity*, Int. Math. Res. Not. (2004), no. 62, 3317–3326.
- [33] C. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83–86.
- [34] T. Tatuzawa, *On a theorem of Siegel*, Jpn. J. Math. **21** (1951), 163–178.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MANCHESTER, M13 9PL, UK
 HEILBRONN INSTITUTE FOR MATHEMATICAL RESEARCH, BRISTOL, UK
Email address: guy.fowler@manchester.ac.uk

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UNIVERSITÉ DE BORDEAUX
 351 COURS DE LA LIBÉRATION, 33405 TALENCE, FRANCE
Email address: emanuele.tron@math.u-bordeaux.fr