Algebra & Number Theory

Volume 20
2026
No. 6

Effective multiplicative independence of three singular moduli

Yuri Bilu, Sanoli Gun and Emanuele Tron

msp

ALGEBRA AND NUMBER THEORY 20:6 (2026)
https://doi.org/10.2140/ant.2026.20.1073

Effective multiplicative independence of three singular moduli

Yuri Bilu, Sanoli Gun and Emanuele Tron

Pila and Tsimerman proved in 2017 that for every k there exist at most finitely many k-tuples $(x_1, \dots, x_k)$ of nonzero singular moduli such that $x_1, \dots, x_k$ are multiplicatively dependent, but any proper subset of them is multiplicatively independent. The proof was noneffective, using Siegel's lower bound for the class numbers. In 2019 Riffaut obtained an effective version of this result for $k = 2$. Moreover, he determined all the instances of $x^m y^n \in \mathbb{Q}^\times$, where x, y are distinct singular moduli and m, n are nonzero integers. In this article we obtain a similar result for $k = 3$. We show that $x^m y^n z^r \in \mathbb{Q}^\times$ (where x, y, z are distinct singular moduli and m, n, r nonzero integers) implies that the discriminants of x, y, z do not exceed 10^{10}.

1. Introduction

A *singular modulus* is the j-invariant of an elliptic curve with complex multiplication. Given a singular modulus x we denote by Δ_x the discriminant of the associated imaginary quadratic order. We denote by $h(\Delta)$ the class number of the imaginary quadratic order of discriminant Δ.

Recall that two singular moduli x and y are conjugate over $\mathbb{Q}$ if and only if $\Delta_x = \Delta_y$, and that there are $h(\Delta)$ singular moduli of a given discriminant Δ. In particular, $[\mathbb{Q}(x) : \mathbb{Q}] = h(\Delta_x)$. For details see, for instance, [10, §7 and §11].

There has been much work on diophantine properties of singular moduli in recent years. In particular, studying algebraic equations where the unknowns are singular moduli [2; 6; 7] is interesting by virtue of its connection with the André–Oort property for affine space [5; 16; 17].

Bilu and Gun were supported by SPARC Project P445 (India). Bilu and Tron were supported by ANR project JINVARIANT.
MSC2020: primary 11G15; secondary 11G18.
Keywords: singular moduli.

Pila and Tsimerman [20] proved that for every k there exists at most finitely many k-tuples $(x_1, \dots, x_k)$ of nonzero singular moduli such that $x_1, \dots, x_k$ are multiplicatively dependent, but any proper subset of them is multiplicatively independent. Their argument is fundamentally noneffective.

Riffaut [21, Theorem 1.7] gave an effective (and totally explicit) version of the theorem of Pila and Tsimerman in the case $k = 2$. He in fact classified all cases when $x^m y^n \in \mathbb{Q}^\times$, where x, y are singular moduli and m, n nonzero integers.

Here we obtain an effective result for $k = 3$. As Riffaut did, we prove a stronger statement: we bound explicitly discriminants of singular moduli x, y, z such that $x^m y^n z^r \in \mathbb{Q}^\times$ for some nonzero integers m, n, r. Our bound is as follows.

Theorem 1.1. *Let x, y, z be distinct nonzero singular moduli and m, n, r nonzero integers. Assume that $x^m y^n z^r \in \mathbb{Q}^\times$. Then*

$$\max\{|\Delta_x|, |\Delta_y|, |\Delta_z|\} < 10^{10}.$$

The special case $m = n = r$ has been recently settled by Fowler [13; 14].

There do exist triples of distinct singular moduli x, y, z such that $x^m y^n z^r \in \mathbb{Q}^\times$ for some nonzero $m, n, r \in \mathbb{Z}$. There are three types of currently known examples.

Rational type: Take distinct x, y, z such that

$$h(\Delta_x) = h(\Delta_y) = h(\Delta_z) = 1, \quad \Delta_x, \Delta_y, \Delta_z \neq -3.$$

Then $x, y, z \in \mathbb{Q}^\times$ and $x^m y^n z^r \in \mathbb{Q}^\times$ for any choice of m, n, r. Pila and Tsimerman [20, Example 6.2] even found an example of $x^m y^n z^r = 1$:

$$(2^6 3^3)^{10} (-2^{15})^6 (-2^{15} 3^3)^{-10} = 1,$$

the corresponding discriminants being -4, -11 and -19.

Quadratic type: Take distinct x, y, z such that

$$h(\Delta_x) = 1, \quad \Delta_x \neq -3, \quad \Delta_y = \Delta_z, \quad h(\Delta_y) = h(\Delta_z) = 2.$$

Then $x \in \mathbb{Q}^\times$ and y, z are of degree 2, conjugate over $\mathbb{Q}$. Hence $x^m y^n z^n \in \mathbb{Q}^\times$ for any choice of m, n.

Cubic type: Take distinct x, y, z such that

$$\Delta_x = \Delta_y = \Delta_z, \quad h(\Delta_x) = h(\Delta_y) = h(\Delta_z) = 3.$$

Then x, y, z are of degree 3, forming a full Galois orbit over $\mathbb{Q}$. Hence $xyz \in \mathbb{Q}^\times$.

We believe that, up to permuting x, y, z, there are no other examples, but to justify it, one needs to improve on the numerical bound 10^{10} in Theorem 1.1.

The proof of Theorem 1.1 relies on the following result, which is a partial common generalization (for big discriminants) of [21, Theorem 1.7] and [12, Theorem 1.3].

Theorem 1.2. *Let x, y be distinct nonzero singular moduli and m, n nonzero integers. Assume that*

$$\max\{|\Delta_x|, |\Delta_y|\} \geq 10^8. \tag{1-1}$$

Then $[\mathbb{Q}(x, y) : \mathbb{Q}(x^m y^n)] \leq 2$. More precisely, we have either

$$\mathbb{Q}(x^m y^n) = \mathbb{Q}(x, y) \tag{1-2}$$

or

$$\Delta_x = \Delta_y, \quad m = n, \quad [\mathbb{Q}(x, y) : \mathbb{Q}(x^m y^m)] = 2. \tag{1-3}$$

Moreover, in the latter case x and y are conjugate over the field $\mathbb{Q}(x^m y^m)$.

If $\{\Delta_x, \Delta_y\}$ is not of the form $\{\Delta, 4\Delta\}$ for some $\Delta \equiv 1 \bmod 8$, then condition (1-1) can be relaxed to

$$\max\{|\Delta_x|, |\Delta_y|\} \geq 10^6. \tag{1-4}$$

Plan of the article. In Section 2 we collect basic fact about singular moduli to be used throughout the article. In Section 3 we establish our principal tool: a linear relation between the exponents $m_1, \ldots, m_k$ stemming from the multiplicative relation $x_1^{m_1} \cdots x_k^{m_k} = 1$. Theorems 1.2 and 1.1 are proved in Sections 4 and 5, respectively.

Notation and conventions. We denote by $\mathbb{H}$ the Poincaré half-plane, and by $\mathcal{F}$ the standard fundamental domain for the action of the modular group; that is, the open hyperbolic triangle with vertices

$$\zeta_6 = \frac{1+\sqrt{-3}}{2}, \quad \zeta_3 = \frac{-1+\sqrt{-3}}{2}, \quad i\infty,$$

together with the hyperbolic geodesics $[i, \zeta_6]$ and $[\zeta_6, i\infty]$.

We denote by log the principal branch of the complex logarithm:

$$-\pi < \arg\log z \leq \pi \quad (z \in \mathbb{C}^\times).$$

We use $O_1(\cdot)$ as a quantitative version of the $O(\cdot)$ notation: $A = O_1(B)$ means that $|A| \leq B$.

We write the Galois action exponentially: $x \mapsto x^\sigma$. In particular, it is a right action: $x^{(\sigma_1\sigma_2)} = (x^{\sigma_1})^{\sigma_2}$. Most of the Galois groups occurring in this article are abelian, so this is not relevant, but in the few cases where the group is not abelian one must be vigilant.

Let R be a commutative ring, and $a \in R$. When this does not lead to confusion, we write R/a instead of R/aR.

We denote by $\mathcal{C}_m$ the cyclic group of order m.

In cross-references, item Y of Proposition X is quoted as Proposition X:Y.

2. Class numbers, denominators, isogenies

Unless the contrary is stated explicitly, the letter Δ stands for an *imaginary quadratic discriminant*, that is, $\Delta < 0$ and $\Delta \equiv 0, 1 \bmod 4$.

We denote by $\mathcal{O}_\Delta$ the imaginary quadratic order of discriminant Δ, that is,

$$\mathcal{O}_\Delta = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2].$$

Then $\Delta = Df^2$, where D is the discriminant of the number field $K = \mathbb{Q}(\sqrt{\Delta})$, called the *fundamental discriminant* of Δ, and $f = [\mathcal{O}_D : \mathcal{O}_\Delta]$ is the *conductor* of Δ.

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

Given a singular modulus x, we denote by Δ_x the discriminant of the associated CM order, and we write $\Delta_x = D_x f_x^2$ with D_x the fundamental discriminant and f_x the conductor. We denote by K_x the associated imaginary quadratic field

$$K_x = \mathbb{Q}(\sqrt{D_x}) = \mathbb{Q}(\sqrt{\Delta_x}).$$

We will call K_x the *CM field* of the singular modulus x.

It is known (see, for instance, §11 in [10]) that a singular modulus x is an algebraic integer of degree $h(\Delta_x)$, and that there are exactly $h(\Delta)$ singular moduli of given discriminant Δ, which form a full Galois orbit over $\mathbb{Q}$.

2.1. ***Class numbers and class groups.*** For a discriminant Δ and a positive integer ℓ set

$$\Psi(\ell, \Delta) = \ell \prod_{p \mid \ell} \left(1 - \frac{(\Delta/p)}{p}\right), \tag{2-1}$$

where (Δ/p) denotes the Kronecker symbol. It is useful to note that

$$\Psi(\ell, \Delta) \geq \varphi(\ell), \tag{2-2}$$

where $\varphi(\cdot)$ is Euler's totient function. Note also the multiplicativity relation

$$\Psi(\ell_1\ell_2, \Delta) = \Psi(\ell_2, \Delta\ell_1^2)\Psi(\ell_1, \Delta). \tag{2-3}$$

Recall the *class number formula*

$$h(\Delta\ell^2) = \frac{1}{[\mathcal{O}_\Delta^\times : \mathcal{O}_{\Delta\ell^2}^\times]} h(\Delta)\Psi(\ell, \Delta). \tag{2-4}$$

In [10, Theorem 7.24] this formula is proved in the case when $\Delta = D$ is a fundamental discriminant; the general case easily follows using the multiplicativity relation (2-3). Note also that

$$[\mathcal{O}_\Delta^\times : \mathcal{O}_{\Delta\ell^2}^\times] = \begin{cases} 3 & \text{if } \Delta = -3, \ell > 1, \\ 2 & \text{if } \Delta = -4, \ell > 1, \\ 1 & \text{if } \Delta \neq -3, -4. \end{cases} \tag{2-5}$$

2.1.1. *Discriminants with small class number.* Watkins [24] classified fundamental discriminants D with $h(D) \leq 100$ and found that such discriminants do not exceed 2383747 in absolute value. It turns out that the same upper bound holds true for all discriminants, not only fundamental ones.

n	1	2	3	4	5	6	7	8	10	12	16	25	50	100
max f	420	210	120	90	66	60	42	42	30	30	18	12	6	2
$D_{\max}(n)$	163	427	907	1555	2683	3763	5923	6307	13843	17803	34483	111763	462883	2383747

Table 1. Values of $D_{\max}(n)$ for arguments occurring in (2-7). The first row contains all positive integers n of the form $\lfloor 100/\varphi(f)\rfloor$ for some positive integer f. In the second row, for each n we give the biggest f with the property $100/\varphi(f) \geq n$. Finally, the third row displays $D_{\max}(n)$.

Proposition 2.1. *Let Δ be a negative discriminant with $h(\Delta) \leq 100$. Then we have $|\Delta| \leq 2383747$. If $h(\Delta) \leq 64$, then $|\Delta| \leq 991027$.*

Remark 2.2. As Guy Fowler informed us, Janis Klaise obtained the same result, with a similar proof, in his 2012 Master's thesis [15]. Apparently, this work has not been published.

Proof. Given a positive integer n, denote by

$$D_{\max}(n) := \max\{|D| : D \text{ fundamental}, h(D) \leq n\}$$

the biggest absolute value of a *fundamental* discriminant D with $h(D) \leq n$; the values of $D_{\max}$ for arguments up to 100 can be found in Watkins [24, Table 4]. For the reader's convenience, we give in Table 1 the $D_{\max}$ of the arguments occurring in equation (2-7) below.

Now let $\Delta = Df^2$ be such that $h(\Delta) \leq 100$. Using the class number formula (2-4) (applied with D as Δ and with f as ℓ), and the bound (2-2) we get

$$h(D)\varphi(f) \leq 100[\mathcal{O}_D^\times : \mathcal{O}_\Delta^\times]. \tag{2-6}$$

If $D = -3$ or -4 then this implies $\varphi(f) \leq 300$: the largest such f is $f = 1260$, so that in this case $|\Delta| \leq 6350400$.

If $D \neq -3, -4$ then we find from (2-6) that $h(D) \leq 100/\varphi(f)$, and hence

$$|\Delta| = f^2|D| \leq f^2 D_{\max}(\lfloor 100/\varphi(f)\rfloor). \tag{2-7}$$

Plugging in the values from Table 1, we find that the maximum of the right-hand side is attained for $f = 420$ and is equal to 28753200. This proves that $|\Delta| \leq 28753200$.

To complete the proof, we ran a PARI script computing the class numbers of all Δ with $|\Delta| \leq 28753200$. It confirms that the biggest Δ with $h(\Delta) \leq 100$ is -2383747, and the biggest Δ with $h(\Delta) \leq 64$ is -991027. □

2.1.2. *The 2-rank.* Given a finite abelian group G and a prime number p, the *p-rank* of G, denoted by $\rho_p(G)$, is the dimension of the $\mathbb{F}_p$-vector space G/G^p. If Δ is a discriminant, we denote by $\rho_p(\Delta)$ the p-rank of its class group.

The 2-rank of a discriminant was determined by Gauss; see [10, Proposition 3.11 and Theorem 3.15]. As usual, we denote by $\omega(n)$ the number of distinct prime divisors of a nonzero integer n.

Proposition 2.3. *Let Δ be a discriminant. Then*

$$\rho_2(\Delta) = \begin{cases} \omega(\Delta) - 1 & \text{if } \Delta \equiv 1 \bmod 4, \\ \omega(\Delta) - 2 & \text{if } \Delta \equiv 4 \bmod 16, \\ \omega(\Delta) - 1 & \text{if } \Delta \equiv 8, 12 \bmod 16, \\ \omega(\Delta) - 1 & \text{if } \Delta \equiv 16 \bmod 32, \\ \omega(\Delta) & \text{if } \Delta \equiv 0 \bmod 32. \end{cases}$$

In particular, $\rho_2(\Delta) \in \{\omega(\Delta), \omega(\Delta) - 1, \omega(\Delta) - 2\}$. If D is a fundamental discriminant, then $\rho_2(D) = \omega(D) - 1$.

2.2. ***Ring class fields.*** If x is a singular modulus with discriminant $\Delta = Df^2$ and $K = \mathbb{Q}(\sqrt{D})$ is its CM field, then $K(x)$ is an abelian extension of K such that $\mathrm{Gal}(K(x)/K)$ is isomorphic to to the class group of Δ; in particular, $[K(x) : K] = h(\Delta)$, and the singular moduli of discriminant Δ form a full Galois orbit over K as well.

This leads to the useful notion of *ring class field*. Given an imaginary quadratic field K of discriminant D and a positive integer f, the *ring class field* of K of conductor f, denoted $K[f]$, is, by definition, $K(x)$, where x is some singular modulus of discriminant Df^2. It does not depend on the particular choice of x and is an abelian extension of K.

Proofs of the statements above can be found, for instance, in [10, §§9–11].

The following properties will be systematically used.

Proposition 2.4. *Let K be an imaginary quadratic field and L a ring class field of K. Denote*

$$G = \mathrm{Gal}(L/\mathbb{Q}), \quad H = \mathrm{Gal}(L/K). \tag{2-8}$$

(As we have just seen, H is an abelian group.) *Then*:

- *Every element of $G \smallsetminus H$ is of order 2.*
- *If $\gamma \in G \smallsetminus H$ and $\eta \in H$ then $\gamma\eta\gamma = \eta^{-1}$.*

Hence, no element of $G \smallsetminus H$ commutes with any element of G of order bigger than 2.

For the proof see [10, Lemma 9.3], for instance.

Proposition 2.5. *Let K be an imaginary quadratic field of discriminant D, and ℓ, m positive integers.*

1. *Assume that either $D \neq -3, -4$ or $\gcd(\ell, m) > 1$. Then the compositum $K[\ell]K[m]$ is equal to $K[\mathrm{lcm}(\ell, m)]$.*
2. *Assume that $D = -3$ and $\gcd(\ell, m) = 1$. Then $K[\ell]K[m]$ is either equal to $K[\mathrm{lcm}(\ell, m)]$ or is a subfield of $K[\mathrm{lcm}(\ell, m)]$ of degree 3.*
3. *Assume that $D = -4$ and $\gcd(\ell, m) = 1$. Then $K[\ell]K[m]$ is either equal to $K[\mathrm{lcm}(\ell, m)]$ or is a subfield of $K[\mathrm{lcm}(\ell, m)]$ of degree 2.*

For the proof see, for instance, [2, Proposition 3.1]

2.2.1. *Two-elementary subfields of ring class fields.* We call a group 2-*elementary* if all its elements are of order dividing 2. A finite 2-elementary group is a product of cyclic groups of order 2. Let K be a field and L a finite extension of K; we say that L is 2-elementary over K if L is Galois over K, with 2-elementary Galois group. We call a number field 2-elementary if it is 2-elementary over $\mathbb{Q}$.

The following is well-known, but we include the proof for the reader's convenience.

Proposition 2.6. *Let F be a number field abelian over $\mathbb{Q}$ and contained in some ring class field. Then F is 2-elementary.*

Proof. This is an easy consequence of Proposition 2.4. Let K be an imaginary quadratic field such that its ring class field, denoted L, contains F. We use the notation of (2-8).

For $\gamma \in G$ let $\tilde{\gamma} \in \mathrm{Gal}(F/\mathbb{Q})$ denote the restriction of γ to F. Each element of $\mathrm{Gal}(F/\mathbb{Q})$ is a restriction of either some $\gamma \in G \smallsetminus H$ or some $\eta \in H$. In the former case $\tilde{\gamma}^2 = 1$ because $\gamma^2 = 1$. Now consider $\tilde{\eta}$ for some $\eta \in H$. Pick $\gamma \in G \smallsetminus H$. Then $\tilde{\gamma}\tilde{\eta}\tilde{\gamma} = \tilde{\eta}^{-1}$. But $\mathrm{Gal}(F/\mathbb{Q})$ is abelian, which implies that $\tilde{\gamma}\tilde{\eta}\tilde{\gamma} = \tilde{\gamma}^2\tilde{\eta} = \tilde{\eta}$. Hence $\tilde{\eta}^2 = 1$ as well. Thus, every element of $\mathrm{Gal}(F/\mathbb{Q})$ is of order dividing 2, as wanted. □

The only positive integers m such that the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ is 2-elementary are the divisors of 24. Hence we have the following corollary.

Corollary 2.7. *The group of roots of unity in a ring class field is of order dividing* 24.

Another important case of 2-elementary fields is the intersection $\mathbb{Q}(x) \cap \mathbb{Q}(y)$, where x and y are singular moduli with distinct fundamental discriminants. This has been known for a long time (see, for instance, the articles of André [4] or Edixhoven [11]), but we again include a proof for the reader's convenience.

Proposition 2.8. *Let x and y be singular moduli with distinct fundamental discriminants: $D_x \neq D_y$. Then the field $\mathbb{Q}(x) \cap \mathbb{Q}(y)$ is 2-elementary. In particular, if $\mathbb{Q}(x) \subset \mathbb{Q}(y)$ then $\mathbb{Q}(x)$ is 2-elementary.*

Proof. It suffices to prove that the field $\mathbb{Q}(x) \cap \mathbb{Q}(y)$ is abelian: Proposition 2.6 will then complete the job.

Recall that we let $K_x = \mathbb{Q}(\sqrt{D_x})$ denote the CM field for x. We will denote K_{xy} the compositum of K_x and K_y, that is, the field $\mathbb{Q}(\sqrt{D_x}, \sqrt{D_y})$. Furthermore, we define

$$M = K_{xy}(x, y), \quad L = K_{xy}(x) \cap K_{xy}(y).$$

It suffices to prove that L is abelian, because $L \supset \mathbb{Q}(x) \cap \mathbb{Q}(y)$. We first prove that L is 2-elementary over the field K_{xy}.

Since $K_x \neq K_y$, there exists $\iota \in \mathrm{Gal}(M/\mathbb{Q})$ such that

$$\iota|_{K_x} = \mathrm{id} \quad \text{and} \quad \iota|_{K_y} \neq \mathrm{id}\,.$$

Proposition 2.4 implies that for $\eta \in \mathrm{Gal}(M/K_{xy})$ we have

$$\iota^{-1}\eta\iota|_{K_x(x)} = \eta|_{K_x(x)} \quad \text{and} \quad \iota^{-1}\eta\iota|_{K_y(y)} = \eta^{-1}|_{K_y(y)}.$$

We also have $\eta|_{K_{xy}} = \mathrm{id}$ by the choice of η. Hence $\eta|_L = \eta^{-1}|_L$. Since every element of $\mathrm{Gal}(L/K_{xy})$ is a restriction to L of some $\eta \in \mathrm{Gal}(M/K_{xy})$, this proves that the Galois group $\mathrm{Gal}(L/K_{xy})$ is 2-elementary.

To complete the proof of the proposition, we must show that L is abelian over $\mathbb{Q}$. Clearly, L is Galois over $\mathbb{Q}$, being the intersection of two Galois extensions. We have to show that $\mathrm{Gal}(K_{xy}/\mathbb{Q})$ acts trivially on $\mathrm{Gal}(L/K_{xy})$. This means proving the following: for every $\eta, \gamma \in \mathrm{Gal}(M/\mathbb{Q})$ such that $\eta|_{K_{xy}} = \mathrm{id}$ we have $\gamma^{-1}\eta\gamma|_L = \eta$.

We denote $\eta^\gamma = \gamma^{-1}\eta\gamma$. Proposition 2.4 implies that

$$\eta^\gamma|_{K_x(x)} \in \left\{\eta|_{K_x(x)}, \eta^{-1}|_{K_x(x)}\right\}.$$

We also have $\eta^\gamma|_{K_y} = \mathrm{id}\,|_{K_y} = \eta|_{K_y} = \eta^{-1}|_{K_y}$. It follows that

$$\eta^\gamma|_{K_{xy}(x)} \in \left\{\eta|_{K_{xy}(x)}, \eta^{-1}|_{K_{xy}(x)}\right\}.$$

In particular, $\eta^\gamma|_L \in \left\{\eta|_L, \eta^{-1}|_L\right\}$. Since $\eta|_{K_{xy}} = \mathrm{id}$ and L/K_{xy} is 2-elementary, we have $\eta|_L = \eta^{-1}|_L$. Hence $\eta^\gamma|_L = \eta|_L$. The proposition is proved. □

2.2.2. (*Almost*) 2*-elementary discriminants.* We will need a slight generalization of the notion of a 2-elementary group. A finite abelian group G will be called *almost* 2*-elementary* if it has a 2-elementary subgroup of index 2. This means that either G is 2-elementary, or it is $\mathcal{C}_4$ times a 2-elementary group. (Recall that $\mathcal{C}_m$ denotes the cyclic group of order m.)

We call a discriminant 2-elementary or almost 2-elementary if its class group has the same property. Such discriminants can be conveniently characterized in terms of the 2-rank (see Section 2.1.2):

$$\Delta \text{ is 2-elementary} \iff h(\Delta) = 2^{\rho_2(\Delta)}; \tag{2-9}$$

$$\Delta \text{ is almost 2-elementary} \iff h(\Delta) \in \{2^{\rho_2(\Delta)}, 2^{\rho_2(\Delta)+1}\}. \tag{2-10}$$

Proposition 2.9. *Let $D \neq -3, -4$ be a fundamental discriminant, and let f be such that Df^2 is an almost 2-elementary discriminant. Then*

$$f \mid 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17. \tag{2-11}$$

Proof. As before, we write $\Delta = Df^2$. Since $D \neq -3, -4$, the class number formula (2-4), together with equations (2-1) and (2-5), implies that $h(\Delta) = h(D)\Psi$, where

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

When Δ is almost 2-elementary, Ψ is a power of 2, by (2-10). More precisely, we have

$$\Psi \mid 2^{\omega(f)+2}. \tag{2-12}$$

Indeed, if Δ is almost 2-elementary, then so is D, and we have both

$$h(D) \in \{2^{\rho_2(D)}, 2^{\rho_2(D)+1}\} \quad \text{and} \quad h(\Delta) \in \{2^{\rho_2(\Delta)}, 2^{\rho_2(\Delta)+1}\}.$$

Hence,

$$\nu_2(\Psi) \le \rho_2(\Delta) - \rho_2(D) + 1. \tag{2-13}$$

Proposition 2.3 implies that

$$\rho_2(\Delta) - \rho_2(D) \le \omega(\Delta) - \omega(D) + 1 \le \omega(f) + 1, \tag{2-14}$$

which, together with (2-13), proves (2-12).

The following easily shown implications will be systematically used throughout the proof:

$$p \mid f \Longrightarrow p - (D/p) \mid \Psi,$$
$$p^2 \mid f \Longrightarrow p \mid \Psi.$$

This implies very strong constraints on the prime divisors of f.

First of all, D and f cannot have a common prime divisor other than 2. Indeed, if p divides both D and f then $(D/p) = 0$ and $p - (D/p) = p \mid \Psi$. Since Ψ is a power of 2, we must have $p = 2$.

Next, if $p \mid f$ then either $p+1$ or $p-1$ is a power of 2. Indeed, if p is odd then $p \nmid D$ (as we have just seen) which implies that $p - (D/p) \in \{p-1, p+1\}$.

Yet another observation: if $p^2 \mid f$ then $p = 2$. Indeed, in this case we again have $p \mid \Psi$.

Thus,

$$f = 2^k p_1 \cdots p_m, \tag{2-15}$$

where k and m are nonnegative integers and $p_1, \ldots, p_m$ are distinct odd primes not dividing D. We claim that

$$k = \nu_2(f) \le 4. \tag{2-16}$$

Indeed, if $k \ge 1$ then $\omega(f) = m + 1$, and

$$2^{\omega(f)+2} = 2^{m+3} \ge \Psi \ge 2^{k-1}(p_1 - 1) \cdots (p_m - 1) \ge 2^{m+k-1},$$

which proves (2-16).

To complete the proof, we have to show that the only possible prime divisors of f are 2, 3, 5, 7, 17. If $w(f) = 1$ then $\Psi \mid 8$, and $f = 2^k$ or $f = p$, an odd prime. Since $p-1$ or $p+1$ divides Ψ, this implies that $p \le 7$.

Now assume that $\omega(f) \ge 2$, and that f has a prime divisor $p \ne 2, 3, 5, 7, 17$. Then $p \ge 31$, because one of $p \pm 1$ must be a power of 2. Writing $f = 2^k p_1 \cdots p_m$ with $2 < p_1 < \cdots < p_m$ and $p_m \ge 31$, we have

$$2^{m+3} \ge 2^{\omega(f)+2} \ge \Psi \ge (p_1 - (D/p_1)) \cdots (p_m - (D/p_m)).$$

Since $p_m \ge 31$ and $p_m - (D/p_m)$ is a power of 2, we have $p_m - (D/p_m) \ge 32$.

If $m \ge 2$ then

$$(p_1 - (D/p_1)) \cdots (p_m - (D/p_m)) \ge (3-1)(5-1)^{m-2} \cdot 32 = 2^{2m+2}.$$

We obtain that $m+3 \geq 2m+2$, which is impossible for $m \geq 2$. It follows that $m = 1$, in which case $\omega(f) = 2$ and $f = 2^k p$, where $k \geq 1$ and $p \geq 31$. We obtain $16 \geq \Psi \geq 2^{k-1} \cdot 32$, a contradiction. The proof is complete. □

One can do some case-by-case analysis and show that f satisfies a stronger (but also more complicated) condition than (2-11). However, (2-11) is sufficient for our purposes.

We also need a similar result for the fundamental discriminants -3 and -4.

Proposition 2.10. *If $\Delta = -4f^2$ is an almost 2-elementary discriminant, then*

$$f \leq 8 \quad \text{or} \quad f \in \{10, 12, 15, 20\}. \tag{2-17}$$

If $\Delta = -3f^2$ is an almost 2-elementary discriminant, then

$$f \leq 5 \quad \text{or} \quad f \in \{7, 8, 11, 13, 16\}. \tag{2-18}$$

In both cases, it follows that $h(\Delta) \mid 8$.

Proof. Assume first that $\Delta = -4f^2$ is almost 2-elementary. The class number formula (2-4), together with equations (2-1) and (2-5), implies that $h(\Delta) = \Psi/2$, where

$$\Psi = \Psi(f, -4) = f \prod_{p \mid f} \left(1 - \frac{(-4/p)}{p}\right).$$

As in the proof of Proposition 2.9, this Ψ must be a power of 2; more precisely,

$$\Psi \mid 2^{\omega(f)+2}. \tag{2-19}$$

Indeed, if $2 \nmid f$, then $\Delta \equiv 12 \bmod 16$ and $\rho_2(\Delta) \leq \omega(\Delta) - 1 = \omega(f)$, while when $2 \mid f$, we have $\rho_2(\Delta) \leq \omega(\Delta) = \omega(f)$. In both cases we obtain

$$\Psi/2 = h(\Delta) \mid 2^{\omega(f)+1},$$

which is (2-19).

Let p be an odd prime divisor of f. As in the proof of Proposition 2.9, we have $p^2 \nmid f$ and $p - (-4/p) \mid \Psi$; thus $p - (-4/p)$ is a power of 2. We again write the prime factorization of f as $f = 2^k p_1 \cdots p_m$, where $2 < p_1 < \cdots < p_m$. We claim that

$$k + m \leq 3 \quad \text{and} \quad m \leq 2. \tag{2-20}$$

Indeed, if $k \geq 1$ then $\omega(f) = m + 1$, and (2-19) implies that

$$2^{m+3} \geq \Psi \geq 2^{k-1}(2 - (-4/2))(3 - (-4/3))^m = 2^{k+2m},$$

which proves (2-20) in the case $k \geq 1$. Similarly, if $k = 0$ then $2^{m+2} \geq \Psi \geq 2^{2m}$, proving (2-20) in this case as well.

In a similar fashion one proves that

$$p_m \leq 7. \tag{2-21}$$

Indeed, if $p_m > 7$ then $p_m \geq 17$, because one of $p_m \pm 1$ must be a power of 2. If $k \geq 1$ then

$$2^{m+3} \geq \Psi \geq 2^k \cdot 4^{m-1} \cdot 16 = 2^{k+2m+2},$$

which is impossible; if $k = 0$ then

$$2^{m+2} \geq \Psi \geq 4^{m-1} \cdot 16 = 2^{2m+2},$$

again impossible. This proves (2-21).

It follows from (2-20) and (2-21) that there are finitely many possible f. Checking them all using a PARI script, we obtain (2-17).

Now assume that $\Delta = -3f^2$ is almost 2-elementary. In this case $h(\Delta) = \Psi/3$, where

$$\Psi = \Psi(f, -3) = f \prod_{p \mid f} \left(1 - \frac{(-3/p)}{p}\right).$$

This time Ψ must be 3 times a power of 2. It follows again that for an odd prime p we have $p^2 \nmid f$. This is clear when $p \neq 3$, and if $9 \mid f$ then

$$3(3 - (-3/3)) = 9 \mid \Psi,$$

a contradiction.

For every $p \mid f$ the difference $p - (-3/p)$ must be either a power of 2, or 3 times a power of 2. We claim that $p - (-3/p)$ cannot be a power of 3. This is clear for $p = 2$ and for $p = 3$. Now assume that $p \neq 2, 3$ and $p - (-3/p) = 2^n$. If n is odd then $3 \mid 2^n + 1$, which means that $p = 2^n - 1$. But in this case $p \equiv 1 \bmod 3$ and $p \equiv -1 \bmod 4$, which implies that $(-3/p) = 1$. It follows that $p - (-3/p) = 2^n - 2$, a contradiction. Similarly, when n is even, we have $p = 2^n + 1$ and $(-3/p) = -1$, again a contradiction.

Thus, for every $p \mid f$ we have $p - (-3/p) = 3 \cdot 2^n$ for some n. This implies that f cannot have two distinct prime divisors: if it did, then Ψ would be divisible by 9, a contradiction.

Thus, either $f = 2^k$ for some k, or $f = p$, an odd prime. This implies that $\rho_2(\Delta) \leq \omega(\Delta) \leq 2$, and

$$\Psi/3 = h(\Delta) \mid 2^{\rho_2(\Delta)+1} \mid 8.$$

It follows that either $f \mid 16$, or $f \in \{3, 5, 7, 11, 13, 23\}$. Checking all possible f using a PARI script, we obtain (2-18). □

Proposition 2.11. *There exists a fundamental discriminant D^* such that $h(D^*) \geq 128$ and the following holds. Let $\Delta = Df^2$ be either 2-elementary or almost 2-elementary. Then either $D = D^*$ or*

$$h(\Delta) \leq \begin{cases} 16 & \text{if } \Delta \text{ is 2-elementary,} \\ 64 & \text{if } \Delta \text{ is almost 2-elementary.} \end{cases}$$

This is proved in [1, Corollary 2.5 and Remark 2.6]. It was not included in [2], the published version of the same work, so we reproduce the proof here (adding some details missing in [1]). The proof broadly follows the strategy of Weinberger [25], which rests on a classical bound of Tatuzawa, stated below.

Given a fundamental discriminant D, the *L-function attached to* D is $L(s,\chi)$, where χ is the quadratic character defined by the Kronecker symbol: $\chi(n)=(D/n)$.

Lemma 2.12 (Tatuzawa [23, Theorem 2]). *Let $0<\varepsilon<\frac{1}{2}$. There exists a fundamental discriminant D^* such that the following holds. Let D be a fundamental discriminant and $L(s,\chi)$ the attached L-function. Then $L(1,\chi)\geq 0.655\varepsilon|D|^{-\varepsilon}$ when $|D|\leq\max\{e^{1/\varepsilon},73130\}$ and $D\neq D^*$.*

Proof of Proposition 2.11. If $D=-3$ or -4 then the result follows from Proposition 2.10. Hence we may assume that $D\neq -3,-4$. In this case the analytic class number formula states that $h(D)=\pi^{-1}|D|^{1/2}L(1,\chi)$. If Δ is almost 2-elementary then so is D. By (2-10) and Proposition 2.3 we have $h(D)\leq 2^{\rho_2(D)+1}\leq 2^{\omega(D)}$.

We pick $\varepsilon=0.048$ throughout and we use the corresponding D^* from Lemma 2.12. Assuming that $D\neq D^*$, Lemma 2.12 implies that

$$2^{\omega(D)}\geq h(D)=\pi^{-1}|D|^{1/2}L(1,\chi)\geq 0.655\pi^{-1}\varepsilon|D|^{1/2-\varepsilon}$$

as long as $|D|\geq 1.2\cdot 10^9$. This implies that

$$|D|\leq\left((0.655\varepsilon)^{-1}\pi 2^{\omega(D)}\right)^{1/(1/2-\varepsilon)}\leq 26549\cdot 4.635^{\omega(D)};$$

we conclude that

$$|D|\leq\max\{26549\cdot 4.635^{\omega(D)},\,1.2\cdot 10^9\}. \tag{2-22}$$

Moreover, since D is fundamental and

$$1.2\cdot 10^9<4\cdot(3\cdot 5\cdot 7\cdot 11\cdots 37)$$

(4 times the product of the first 11 odd primes), we must have $\omega(D)\leq 11$ whenever $|D|\leq 1.2\cdot 10^9$. More generally, $|D|$ is at least 4 times the product of the first $\omega(D)-1$ odd primes. Hence, when $\omega(D)\geq 12$, we have

$$|D|\geq 4\cdot(3\cdot 5\cdot 7\cdot 11\cdots 37)\cdot 41^{\omega(D)-12}.$$

Combining this observation with the upper bound (2-22), we conclude that, when $\omega(D)\geq 12$, we have

$$4\cdot(3\cdot 5\cdot 7\cdot 11\cdots 37)\cdot 41^{\omega(D)-12}\leq|D|\leq 26549\cdot 4.635^{\omega(D)}.$$

This is easily seen to be a contradiction for $\omega(D)\geq 12$. We conclude that

$$\omega(D)\leq 11 \tag{2-23}$$

for any almost 2-elementary fundamental $D\neq D^*$.

Thus, we are now left with the task of examining discriminants $\Delta=Df^2$ such that the corresponding fundamental D satisfies conditions (2-22) and (2-23). We want to show that

- if such Δ is 2-elementary then $h(\Delta)\leq 16$, and
- if such Δ is almost 2-elementary then $h(\Delta)\leq 64$.

Proving this is a numerical check using PARI. We distinguish two cases: $\omega(D) \le 6$ and $7 \le \omega(D) \le 11$.

When $\omega(D) \le 6$ and D is almost 2-elementary then $h(D) \mid 64$. Table 4 of Watkins [24] implies that in this case $|D| \le 693067$. Using Proposition 2.9 and a PARI script, we computed all 2-elementary and all almost 2-elementary discriminants $\Delta = Df^2$ such that $|D| \le 693067$. Our script found 101 discriminants that are 2-elementary, the largest being $-7392 = -1848 \cdot 2^2$. The class numbers of all these discriminants do not exceed 16. Similarly, the script found 425 almost 2-elementary discriminants, $-87360 = -5460 \cdot 4^2$ being the largest, and their class numbers do not exceed 64. This completes the proof in the case $\omega(D) \le 6$.

When $7 \le \omega(D) \le 11$, we can no longer use [24]. To complete the proof in this case, for every $n = 7, \dots, 11$ we determine all fundamental discriminants D satisfying

$$\omega(D) = n, \quad |D| \le 26549 \cdot 4.635^n \tag{2-24}$$

(note that $26549 \cdot 4.635^n > 1.2 \cdot 10^9$ for $n \ge 7$), and for each of them we check whether it is almost 2-elementary. Our script found no almost 2-elementary fundamental discriminants satisfying (2-24) with $7 \le n \le 11$. This completes the proof of Proposition 2.11. □

Corollary 2.13. *Let x and y be singular moduli with distinct fundamental discriminants, $D_x \ne D_y$.*

(1) *Assume that $\mathbb{Q}(x) = \mathbb{Q}(y)$. Then $h(\Delta_x) = h(\Delta_y) \le 16$.*

(2) *Assume that $\mathbb{Q}(x) \subset \mathbb{Q}(y)$ and $[\mathbb{Q}(y) : \mathbb{Q}(x)] = 2$. Then $h(\Delta_x) \le 16$ and $h(\Delta_y) \le 32$.*

Proof. If $\mathbb{Q}(x) = \mathbb{Q}(y)$ then both Δ_x and Δ_y are 2-elementary by Proposition 2.8. Since $D_x \ne D_y$, one of the two is distinct from D^*; say, $D_x \ne D^*$. Then $h(\Delta_x) \le 16$. Hence $h(\Delta_y) = h(\Delta_x) \le 16$ as well. This proves item (1).

Now assume that we are in the situation of item (2). Then $\mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$ is 2-elementary by Proposition 2.8. Hence so is $\mathrm{Gal}(K_y(x)/K_y)$. Since

$$[K_y(y) : K_y(x)] \le [\mathbb{Q}(y) : \mathbb{Q}(x)] = 2,$$

the group $\mathrm{Gal}(K_y(y)/K_y)$ is almost 2-elementary. If $D_x \ne D^*$ then $h(\Delta_x) \le 16$ and $h(\Delta_y) \le 32$, so we are done. If $D_y \ne D^*$ then $h(\Delta_y) \le 64$. It follows that $h(\Delta_x) \le 32$ and we must have $D_x \ne D^*$, so we are done again. □

2.3. ***Gauss reduction theory, denominators.*** Denote by T_Δ the set of triples $(a, b, c) \in \mathbb{Z}^3$ with $\Delta = b^2 - 4ac$ satisfying

$$\gcd(a, b, c) = 1 \quad \text{and} \quad (\text{either } -a < b \le a < c \text{ or } 0 \le b \le a = c). \tag{2-25}$$

Condition (2-25) is equivalent to

$$\frac{b + \sqrt{\Delta}}{2a} \in \mathcal{F}.$$

For every singular modulus x of discriminant Δ there exists a unique triple $(a_x, b_x, c_x) \in T_\Delta$ such that, denoting

$$\tau_x = \frac{b_x + \sqrt{\Delta}}{2a_x},$$

we have $x = j(\tau_x)$. This is, essentially, due to Gauss; see [6, Section 2.2] for details.

We will call a_x the *denominator* of the singular modulus x.

Note that, alternatively, τ_x can be defined as the unique $\tau \in \mathcal{F}$ such that $j(\tau) = x$.

We will say that a positive integer a is a denominator for Δ if it is a denominator of some singular modulus of discriminant Δ; equivalently, there exist $b, c \in \mathbb{Z}$ such that $(a, b, c) \in T_\Delta$.

It will often be more convenient to use the notation $a(x)$, $b(x)$, $\tau(x)$ etc. instead of a_x, b_x, τ_x, etc.

Remark 2.14. It is useful to note that b_x and Δ_x are of the same parity: $b_x \equiv \Delta_x \bmod 2$. This is because $\Delta_x = b_x^2 - 4a_x c_x \equiv b_x^2 \bmod 4$.

For every Δ there exists exactly one singular modulus of discriminant Δ and of denominator 1, which will be called the *dominant* singular modulus of discriminant Δ. Singular moduli with denominator 2 will be called *subdominant*.

Proposition 2.15. *Let Δ be a discriminant. Then for every $a \in \{2, 3, 4, 5\}$ there exist at most 2 singular moduli x with $\Delta_x = \Delta$ and $a_x = a$. For every $A \in \{13, 18, 30\}$ there exists at most $S(A)$ singular moduli x with $\Delta_x = \Delta$ and $a_x < A$, where $S(A)$ is given in the following table*:

A	13	18	30
$S(A)$	32	48	99

Proof. Let a be a positive integer. For a residue class $r \bmod 4a$ denote $B(r)$ the number of $b \in \mathbb{Z}$ satisfying $-a < b \le a$ and $b^2 \equiv r \bmod 4a$. Denote $s(a)$ the biggest of all $B(r)$:

$$s(a) = \max\{B(r) : r \bmod 4a\}.$$

The number of triples $(a, b, c) \in T_\Delta$ with given a does not exceed $B(\Delta)$; hence it does not exceed $s(a)$ either. A quick calculation shows that $s(a) = 2$ for $a \in \{2, 3, 4, 5\}$, and

$$\sum_{a<A} s(a) = S(A)$$

for $A \in \{13, 18, 30\}$. The proposition is proved. □

We will also need miscellaneous facts about the (non)existence of singular moduli of some specific shapes. The following proposition will be used in this article only for $p = 3$. We, however, state it for general p, for the sake of further applications.

Proposition 2.16. *Let Δ be a discriminant and p an odd prime number.*

1. *Assume that $(\Delta/p)=1$. If $|\Delta|\geq 4p^2-1$ then Δ admits exactly 2 singular moduli with denominator p. More generally, if $|\Delta|\geq 4p^k-1$ then Δ admits exactly 2 singular moduli with denominator p^k.*
2. *Assume that $p^2\,|\,\Delta$, and let a be a denominator for Δ. Then either $p\nmid a$ or $p^2\,|\,a$. In particular, p is not a denominator for Δ.*

Proof. By Hensel's lemma, the assumption $(\Delta/p)=1$ implies that the congruence $b^2\equiv\Delta \bmod p^k$ has exactly two solutions b satisfying $0<b<p^k$, and exactly one of these solutions satisfies $b^2\equiv\Delta \bmod 4p^k$. If b is this solution and $|\Delta|\geq 4p^k-1$ then the two triples $(p^k,\pm b,(b^2-\Delta)/4p^k)$ belong to T_Δ. This proves item 1.

If $p^2\,|\,\Delta$ and $p\,|\,a$ then $p\,|\,b$ and $p\nmid c$. Hence $p^2\,|\,4ac=b^2-\Delta$, which implies that $p^2\,|\,a$. This proves item 2. □

Here is an analogue of Proposition 2.16 for $p=2$.

Proposition 2.17. *Let Δ be a discriminant.*

1. *Assume that $\Delta\equiv 1 \bmod 8$. If $|\Delta|>15$ then Δ admits exactly 2 subdominant singular moduli, which are $j\big((\pm 1+\sqrt{\Delta})/4\big)$. More generally, if $|\Delta|\geq 4^{k+1}-1$ then Δ admits exactly 2 singular moduli with denominator 2^k.*
2. *If $\Delta\neq 1 \bmod 8$ then it admits at most one subdominant singular modulus.*
3. *Let Δ satisfy $\Delta\equiv 4 \bmod 32$ and $|\Delta|\geq 252$. Then it admits exactly 2 singular moduli of denominator 8. These are*
$$j\left(\frac{\pm b'+\sqrt{\Delta/4}}{8}\right),\quad b'=\begin{cases}1 & \text{if } \Delta\equiv 36 \bmod 64,\\ 3 & \text{if } \Delta\equiv 4 \bmod 64.\end{cases} \tag{2-26}$$
More generally, if $k\geq 3$ and $|\Delta|\geq 4^{k+1}-4$ then Δ admits exactly 2 singular moduli with denominator 2^k.
4. *Let Δ satisfy $\Delta\equiv 4 \bmod 32$ and let a be a denominator for Δ. Then either a is odd, or $8\,|\,a$. In particular, 2, 4 and 6 are not denominators for Δ.*
5. *Let Δ be divisible by 16 and let a be a denominator for Δ. Then either a is odd, or $4\,|\,a$. In particular, 2 is not a denominator for Δ.*

   Furthermore, Δ admits at most one singular modulus with denominator 4.
6. *Assume that Δ is even, but $\Delta\neq 4 \bmod 32$, and that $|\Delta|>76$. Then 2 or 4 is a denominator for Δ.*

Proof. Items 1 and 3 are proved using Hensel's lemma exactly like item 1 of Proposition 2.16; we omit the details.

Item 2 follows from [6, Proposition 2.6], and item 6 is [9, Proposition 3.1.4]. Note that in [9] denominators are called *suitable integers*.

We are left with items 4 and 5. If $\Delta\equiv 4 \bmod 32$ and $(a,b,c)\in T_\Delta$ with $2\,|\,a$ then $2\|b$ and c is odd. Hence $b^2\equiv 4 \bmod 32$, which implies that $4ac\equiv 0 \bmod 32$. This shows that $8\,|\,a$, which proves item 4.

Finally, if $16 \mid \Delta$ and $2 \| a$ then $2 \mid b$ and $2 \nmid c$, which implies that

$$b^2 = \Delta + 4ac \equiv 8 \bmod 16,$$

a contradiction. This proves the first statement in item 5. Similarly, if $a = 4$ then $4 \mid b$ and $2 \nmid c$; in particular, $4ac \equiv 16 \bmod 32$. Hence

$$b = \begin{cases} 0 & \text{if } \Delta \equiv 16 \bmod 32, \\ 4 & \text{if } \Delta \equiv 0 \bmod 32. \end{cases}$$

Thus, in any case there is only one choice for b, which proves the second statement in item 5. □

It is useful to note that the dominant singular modulus is real; thus there exists at least one real singular modulus of every discriminant. This has the following consequence.

Proposition 2.18. *Let x be a singular modulus, and let K be a subfield of $\mathbb{Q}(x)$. Assume that K is Galois over $\mathbb{Q}$. Then K is a totally real field.*

Since $\mathbb{Q}(x)$ is Galois over $\mathbb{Q}$ when Δ_x is 2-elementary, this implies that singular moduli of 2-elementary discriminants are all real.

2.4. ***Isogenies.*** Let Λ and M be lattices in $\mathbb{C}$. We say that Λ and M are isogenous if Λ is isomorphic to a sublattice of M. Specifically, given a positive integer n, Λ and M are *n-isogenous* if M has a sublattice Λ', isomorphic to Λ, such that the quotient group M/Λ' is cyclic of order n. This relation is symmetric.

Two lattices $\langle z, 1\rangle$ and $\langle w, 1\rangle$, for z, w in the Poincaré plane $\mathbb{H}$, are n-isogenous if and only if there exists $\gamma \in \mathrm{M}_2(\mathbb{Z})$ with coprime entries and determinant n such that $w = \gamma(z)$. Imposing upon z and w certain reasonable conditions, one may assume that the matrix γ is upper triangular.

Proposition 2.19. *Let $z, w \in \mathbb{H}$ and let n be a positive integer. Assume that*

$$w \in \mathcal{F} \quad \text{and} \quad \operatorname{Im} z \geq n. \tag{2-27}$$

Then the following two conditions are equivalent.

(1) *The lattices $\langle z, 1\rangle$ and $\langle w, 1\rangle$ are n-isogenous.*

(2) *We have*

$$w = \frac{pz + q}{s},$$

where $p, q, s \in \mathbb{Z}$ satisfy

$$p, s > 0, \quad ps = n, \quad \gcd(p, q, s) = 1.$$

Proof. The implication (2) ⇒ (1) is trivial and does not require (2-27).

Now assume that (1) holds, and let $\gamma \in M_2(\mathbb{Z})$ be a matrix with coprime entries and determinant n such that $w = \gamma(z)$. There exists $\delta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\delta\gamma$ is an upper triangular matrix. Replacing δ by $\left(\begin{smallmatrix} 1 & \nu \\ 0 & 1 \end{smallmatrix}\right)\delta$ with a suitable $\nu \in \mathbb{Z}$, we may assume that $w' := \delta\gamma(z)$ satisfies

$$-\tfrac{1}{2} < \operatorname{Re} w' \leq \tfrac{1}{2}. \tag{2-28}$$

Write $\delta\gamma = \left(\begin{smallmatrix} p & q \\ 0 & s \end{smallmatrix}\right)$. Replacing δ by $-\delta$ if necessary, we may assume that $p, s > 0$. Since $ps = n$ and

$$w' = \frac{pz+q}{s},$$

we only have to prove that $w' = w$. We have $\operatorname{Im} w' = (\operatorname{Im} z)/s \geq 1$, by (2-27). Together with (2-28) this implies that $w' \in \mathcal{F}$. But w belongs to $\mathcal{F}$ as well, again by (2-27). Since $w' = \delta w$ and each $\mathrm{SL}_2(\mathbb{Z})$-orbit has exactly one point in $\mathcal{F}$, we must have $w' = w$. □

We say that two singular moduli are n-isogenous if, writing $x = j(\tau)$ and $y = j(\upsilon)$, the lattices $\langle \tau, 1\rangle$ and $\langle \upsilon, 1\rangle$ are n-isogenous.

Singular moduli x and y are n-isogenous if and only if $\Phi_n(x, y) = 0$, where $\Phi_n(X, Y)$ denotes the modular polynomial of level n. Since $\Phi_n(X, Y) \in \mathbb{Q}[X, Y]$, being n-isogenous is preserved by Galois conjugation: for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the singular moduli x^σ and y^σ are n-isogenous as long as x and y are.

For a positive integer n define

$$\mathcal{Q}(n) = \left\{ \frac{r}{s} : r, s \in \mathbb{Z}, rs = n \right\}.$$

For example,

$$\mathcal{Q}(12) = \left\{ \tfrac{1}{12}, \tfrac{1}{3}, \tfrac{3}{4}, \tfrac{4}{3}, 3, 12 \right\}.$$

The following property is an immediate consequence of Proposition 2.19.

Corollary 2.20. *Let x and y be n-isogenous singular moduli. Assume that $|\Delta_x|^{1/2} \geq 2na_x$. Then $(a_y/f_y)/(a_x/f_x) \in \mathcal{Q}(n)$. In particular,*

$$\frac{1}{n} \leq \frac{a_y/f_y}{a_x/f_x} \leq n.$$

When $n = p$ is a prime number, we have $(a_y/f_y)/(a_x/f_x) \in \{p, 1/p\}$.

The following simple facts will be repeatedly used, often without special reference.

Proposition 2.21. *Let x and y be singular moduli.*

1. *Assume that $\Delta_x = \Delta_y$ and $\gcd(a_x, a_y) = 1$. Then x and y are $a_x a_y$-isogenous.*
2. *Assume that $a_x = a_y = 1$ and $\Delta_x/e_x^2 = \Delta_y/e_y^2$, where e_x and e_y are coprime positive integers. Then x and y are $e_x e_y$-isogenous.*
3. *Two subdominant singular moduli of the same discriminant are either equal or 4-isogenous.*

Proof. To prove item 1, note that

$$\tau_y = \frac{a_x \tau_x + (b_y - b_x)/2}{a_y}.$$

Since $b_x \equiv b_y \bmod 2$ (see Remark 2.14), this proves that x and y are $a_x a_y$-isogenous.

For item 2 we have

$$\tau_x = \frac{b_x + e_x\sqrt{\Delta}}{2} \quad \text{and} \quad \tau_y = \frac{b_y + e_y\sqrt{\Delta}}{2},$$

where $\Delta = \Delta_x/e_x^2 = \Delta_y/e_y^2$. Hence

$$\tau_y = \frac{e_y\tau_x + (b_y e_x - b_x e_y)/2}{e_x}.$$

Remark 2.14 now implies that $b_x e_y \equiv b_y e_x \bmod 2$, and we conclude that x and y are $e_x e_y$-isogenous.

To prove item 3, note that distinct subdominant singular moduli of the same discriminant Δ must be of the form $j(\tau)$ and $j(\tau')$, where

$$\tau = \frac{-1+\sqrt{\Delta}}{4} \quad \text{and} \quad \tau' = \frac{1+\sqrt{\Delta}}{4};$$

see Proposition 2.17:1. We have $\tau' = (2\tau+1)/2$, which implies that $j(\tau)$ and $j(\tau')$ are 4-isogenous. □

2.5. ***Galois-theoretic lemmas.*** In this subsection we collect some lemmas with Galois-theoretic flavor that will be repeatedly used in the proofs of Theorems 1.1 and 1.2.

Lemma 2.22. *Let m be a positive integer and x a singular modulus. Then $\mathbb{Q}(x) = \mathbb{Q}(x^m)$. In other words: if x and y are distinct singular moduli of the same discriminant then $x^m \neq y^m$.*

Proof. See [21, Lemma 2.6]. □

Lemma 2.23. *Let x and y be distinct singular moduli of the same discriminant, $K = K_x = K_y$ their common CM field, $L = K(x) = K(y)$ the ring class field and $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ a Galois morphism. Assume that σ permutes x and y:*

$$x^\sigma = y \quad \text{and} \quad y^\sigma = x.$$

Then σ is of order 2.

Proof. If $\sigma \notin \mathrm{Gal}(L/K)$ then it is of order 2 because every element of $\mathrm{Gal}(L/\mathbb{Q})$ not belonging to $\mathrm{Gal}(L/K)$ is of order 2. And if $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma^2 = 1$ because $x^{\sigma^2} = x$ and $L = K(x)$. □

Lemma 2.24. *Let x, y be distinct singular moduli of the same discriminant and let K and L be as in Lemma 2.23. Let F be a proper subfield of $\mathbb{Q}(x, y)$; we write $G = \mathrm{Gal}(L/F)$. Then one of the following conditions is satisfied.*

(1) *There exists $\sigma \in G$ such that, up to switching x, y, we have $x^\sigma = x$ but $y^\sigma \neq y$.*

(2) *We have $[\mathbb{Q}(x, y) : F] = 2$ and the nontrivial automorphism of $\mathbb{Q}(x, y)/F$ permutes x and y.*

(3) *We have $L = \mathbb{Q}(x, y)$ and $[L : F] = 3$. Moreover, there exists a singular modulus z and $\sigma \in G$ such that*

$$x^\sigma = y, \quad y^\sigma = z, \quad z^\sigma = x.$$

(4) *There exists $\sigma \in G$ such that*

$$x^\sigma, y^\sigma \notin \{x, y\} \tag{2-29}$$

(Versions of this lemma were used, albeit implicitly, in [12] and elsewhere, but it does not seem to have appeared in the literature in this form.)

Proof. We may assume that every element in G which fixes x or y fixes both of them; otherwise we have item (1). We may also assume that x and y are conjugate over F; otherwise, any $\sigma \in G$ not belonging to $\mathrm{Gal}(L/\mathbb{Q}(x, y))$ satisfies (2-29).

Assume first that $L = \mathbb{Q}(x, y)$. Then the only element of G that fixes x or y is the identity. Since x and y are conjugate over F, there is exactly one $\sigma \in G$ with the property $x^\sigma = y$ and exactly one $\sigma' \in G$ with the property $y^{\sigma'} = x$. Hence (4) holds if $[L : F] \geq 4$. And if $[L : F] \leq 3$ then we have one of conditions (2) or (3) is satisfied. This completes the proof in the case $L = \mathbb{Q}(x, y)$.

Now assume that $L \neq \mathbb{Q}(x, y)$. Since $L = K(x)$, the field $\mathbb{Q}(x)$ is a subfield of L of degree 2, and so is $\mathbb{Q}(y)$. If $Q(x) \neq \mathbb{Q}(y)$ then the compositum of these fields must be L, which contradicts the assumption $L \neq \mathbb{Q}(x, y)$. Hence $\mathbb{Q}(x) = \mathbb{Q}(y)$ is a subfield of L of degree 2. (4) holds if $[\mathbb{Q}(x) : F] \geq 4$, and (2) does if $[\mathbb{Q}(x) : F] = 2$.

We are left with the case $[\mathbb{Q}(x) : F] = 3$. In this case the Galois orbit of x over F consists of 3 elements: x, y and a certain z. The group G must be either cyclic $\mathcal{C}_6$ or symmetric S_3. In the latter case G acts by permutations on the set $\{x, y, z\}$. But in this case G has an element fixing x and permuting y, z, which is impossible because $y \in \mathbb{Q}(x)$.

Thus, $G = \mathcal{C}_6$. The group $\mathrm{Gal}(L/\mathbb{Q}(x))$ is a subgroup of G; let γ be the nontrivial element of $\mathrm{Gal}(L/\mathbb{Q}(x))$. Then $\gamma \notin \mathrm{Gal}(L/K)$; otherwise, from $L = K(x)$ and $x^\gamma = x$ we would obtain that γ is the identity. It follows (see Proposition 2.4) that γ does not commute with the elements of G of order 3, which is impossible, because G is an abelian group. The lemma is proved. □

Lemma 2.25. *Let x and y be singular moduli with the same fundamental discriminant D, and let $K = \mathbb{Q}(\sqrt{D})$ be their common CM field. Assume that $K(x) = K(y)$, and that x and y do not both belong to $\mathbb{Q}$. Then*

$$\Delta_x/\Delta_y \in \{4, 1, 1/4\}.$$

Moreover, if (say) $\Delta_x = 4\Delta_y$, then $\Delta_y \equiv 1 \bmod 8$.

Proof. See [2, Proposition 4.3] and [6, Subsection 3.2.2] (where the congruence $\Delta_y \equiv 1 \bmod 8$ is proved). Note that in [2] a formally stronger hypothesis $\mathbb{Q}(x) = \mathbb{Q}(y)$ is imposed, but in the proof it is only used that $K(x) = K(y)$. □

Lemma 2.26. *Let x, x', y, y' be singular moduli. Assume that*

$$\Delta_x = \Delta_{x'}, \quad \Delta_y = \Delta_{y'} \quad \textit{and} \quad \mathbb{Q}(x, x') = \mathbb{Q}(y, y').$$

Then:

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. See [8, Lemma 7.1]. □

3. The linear relation

Let $x_1, \dots, x_k$ be nonzero singular moduli of the same fundamental discriminant D, and let $m_1, \dots, m_k \in \mathbb{Z}$. We want to show that, under some reasonable assumptions, the multiplicative relation

$$x_1^{m_1} \cdots x_k^{m_k} = 1 \tag{3-1}$$

implies the linear relation

$$\sum_{i=1}^{k} \frac{f(x_i)}{a(x_i)} m_i = 0. \tag{3-2}$$

To state those assumptions, set

$$X = \max\{|\Delta(x_i)| : 1 \le i \le k\} \quad \text{and} \quad Y = \min\{|\Delta(x_i)| : 1 \le i \le k\}, \tag{3-3}$$

and, as in Section 2.3, let f_x or $f(x)$ mean the conductor of a singular modulus x, and a_x or $a(x)$ its denominator.

Proposition 3.1. *Let A be a positive number such that*

$$a(x_i) \le A \quad (1 \le i \le k). \tag{3-4}$$

Assume that

$$Y^{1/2} > \tfrac{1}{3} Ak(\log X + \log A + \log k + 20). \tag{3-5}$$

Then (3-1) implies (3-2).

It often happens that we control only a part of the denominators of $x_1, \dots, x_k$. In this case we cannot expect an identity like (3-2), but we may have good bounds for the part of the sum corresponding to the terms with small denominators.

We need some extra notation. Set $f = \gcd(f_{x_1}, \dots, f_{x_k})$ and $\Delta = Df^2$. We also define

$$e_{x_i} = e(x_i) = f(x_i)/f \quad \text{and} \quad m_i' = e(x_i) m_i \quad (i = 1, \dots, k).$$

Then we have $\Delta(x_i) = e(x_i)^2 \Delta$, and (3-2) can be rewritten as

$$\sum_{i=1}^{k} \frac{m_i'}{a(x_i)} = 0. \tag{3-6}$$

As indicated above, we want to obtain a less precise result, in the form of an inequality, which however holds true without the assumption that all the denominators are small. It will be practical to estimate separately the sums with positive and with negative exponents m_i.

Proposition 3.2. *Let A, ε be real numbers satisfying $A \ge 1$ and $0 < \varepsilon \le 0.5$. Assume that*

$$|\Delta|^{1/2} \ge \max\left\{k\varepsilon^{-1} \log X, \tfrac{1}{3} A\big(\log(k\varepsilon^{-1}) + 4\big)\right\}. \tag{3-7}$$

Then

$$\sum_{\substack{a(x_i)<A\\ m_i>0}} \frac{m_i'}{a(x_i)} \le \sum_{m_i<0} \frac{|m_i'|}{\min\{a(x_i),\, A\}} + \varepsilon\|\boldsymbol{m}'\|, \tag{3-8}$$

$$\sum_{\substack{a(x_i)<A\\ m_i<0}} \frac{|m_i'|}{a(x_i)} \le \sum_{m_i>0} \frac{m_i'}{\min\{a(x_i),\, A\}} + \varepsilon\|\boldsymbol{m}'\|. \tag{3-9}$$

Here we denote by $\|\boldsymbol{m}'\|$ *the sup-norm* $\max\{|m_1'|, \dots, |m_k'|\}$.

Propositions 3.1 and 3.2 will be our principal tools in the proofs of Theorems 1.1 and 1.2. They will be proved in Section 3.3, after some preparatory work in Sections 3.1 and 3.2.

3.1. ***Estimates for singular moduli.*** For $\tau \in \mathbb{H}$, set $q = q_\tau := e^{2\pi i\tau}$. Recall that the j-invariant function has the Fourier expansion

$$j(\tau) = \sum_{k=-1}^{\infty} c_k q^k,$$

where the c_k are positive integers, starting with $c_{-1} = 1$, $c_0 = 744$, and $c_1 = 196884$. (That they are positive integers follows from the formula

$$j(\tau) = q^{-1}\Bigl(1 + 240\sum_{k=1}^{\infty}\sigma_3(k)q^k\Bigr)^3 \prod_{n=1}^{\infty}(1-q^n)^{-24}, \quad \text{where} \quad \sigma_3(k) = \sum_{d\,|\,k} d^3;$$

see, for instance, [22, Chapter 1, Proposition 7.4 and Remark 7.4.1]. Clearly, each of the series

$$\Bigl(1 + 240\sum_{k=1}^{\infty}\sigma_3(k)q^k\Bigr)^3 \quad \text{and} \quad (1-q^n)^{-24} \quad (n = 1, 2, 3, \dots)$$

has positive integer coefficients; hence so does the Fourier expansion of j.)

Proposition 3.3. *Let* $\tau \in \mathbb{H}$, *and set* $v = \operatorname{Im}\tau$.

1. *Assume that* $v \ge 5$. *Then*

$$j(\tau) = q^{-1} + 744 + O_1(2\cdot 10^5|q|), \tag{3-10}$$

$$j(\tau) = q^{-1} + 744 + 196884q + O_1(3\cdot 10^7|q|^2), \tag{3-11}$$

$$\log|j(\tau)| = 2\pi v + O_1(800|q|), \tag{3-12}$$

$$\log(qj(\tau)) = 744q + O_1(5\cdot 10^5|q|^2), \tag{3-13}$$

$$\log(qj(\tau)) = 744q - 79884q^2 + O_1(2\cdot 10^8|q|^3). \tag{3-14}$$

2. *Assume that* $\tau \in \mathcal{F}$ *and* $v \le V$, *where* V *is a real number satisfying* $V \ge 5$. *Then*

$$\log|j(\tau)| \le 2\pi V + 3000e^{-2\pi V}. \tag{3-15}$$

We will use the following trivial lemma.

Lemma 3.4. *Let u be a complex number satisfying $|u| < 1$. Then*

$$|\log(1+u)| \le \frac{|u|}{1-|u|}.$$

Furthermore, for $n = 1, 2, \dots$ we have

$$\log(1+u) = \sum_{k=1}^{n} \frac{(-1)^{k-1}u^k}{k} + O_1\left(\frac{1}{n+1}\frac{|u|^{n+1}}{1-|u|}\right).$$

Proof of Proposition 3.3. Write $\tau = u + vi$. Then

$$q = e^{2\pi ui}e^{-2\pi v} \quad \text{and} \quad |q| = e^{-2\pi v}.$$

Let us prove item 1. We have $u \ge 5$, which implies that

$$|q| \le e^{-10\pi}.$$

For $n \ge 0$ write

$$j_n(\tau) = \sum_{k=n+1}^{\infty} c_k q^k$$

(so for example $j_0(\tau) = j(\tau) - q^{-1} - 744$ and $j_1(\tau) = j(\tau) - q^{-1} - 744 - 196884q$). Positivity of the coefficients c_k implies that

$$|j_n(\tau)q^{-n-1}| \le \sum_{k=n+1}^{\infty} c_k|q|^{k-n-1} \le \sum_{k=n+1}^{\infty} c_k e^{-10\pi(k-n-1)} = e^{10\pi(n+1)}j_n(5i).$$

In particular,

$$|j_0(\tau)q^{-1}| \le e^{10\pi}j_0(5i) < 2\cdot 10^5 \quad \text{and} \quad |j_1(\tau)q^{-2}| \le e^{20\pi}j_1(5i) < 3\cdot 10^7,$$

which proves expansions (3-10) and (3-11). Using Lemma 3.4, we deduce from them expansions (3-13) and (3-14), and (3-12) easily follows from (3-13).

Now let us prove item 2. We no longer have $v \ge 5$. However, since $\tau \in \mathcal{F}$, we have $v \ge \sqrt{3}/2$. Hence

$$|j(\tau)| \le |q|^{-1} + 744 + j_0(\sqrt{3}/2) \le e^{2\pi v} + 2079 \le e^{2\pi V}(1 + 2079e^{-2\pi V}).$$

Using Lemma 3.4, we obtain (3-15). □

We want to apply Proposition 3.3 to singular moduli. If x is a singular modulus, then there exists a unique $\tau_x \in \mathcal{F}$ such that $x = j(\tau_x)$. We have

$$\tau_x = \frac{b + \sqrt{\Delta}}{2a},$$

where $\Delta = \Delta_x$ is the discriminant, $a = a_x$ is the denominator of the singular modulus x, and $b \in \mathbb{Z}$; see Section 2.3 for details.

Corollary 3.5. *Let x be a singular modulus of discriminant Δ and denominator a.*

1. *Assume that $a \le 0.1|\Delta|^{1/2}$. Then*
$$\log|x| = \pi\frac{|\Delta|^{1/2}}{a} + O_1(e^{-2|\Delta|^{1/2}/a}).$$
2. *Let $A \ge 1$ be such that $a \ge A$ and $A \le 0.1|\Delta|^{1/2}$. Then*
$$\log|x| \le \pi\frac{|\Delta|^{1/2}}{A} + e^{-2|\Delta|^{1/2}/A}. \tag{3-16}$$
In particular, if $|\Delta| \ge 10^4$ then
$$\log|x| \le \pi|\Delta|^{1/2} + e^{-2|\Delta|^{1/2}} \le 4|\Delta|^{1/2}. \tag{3-17}$$
3. *Define τ_x as in Section 2.3. Assume that $a \le 0.1|\Delta|^{1/2}$. Then*
$$\log(xq) = 744q + O_1(5\cdot 10^5|q|^2), \tag{3-18}$$
$$\log(xq) = 744q - 79884q^2 + O_1(2\cdot 10^8|q|^3). \tag{3-19}$$
where $q = e^{2\pi i\tau_x}$.

Proof. The hypothesis that $a \le 0.1|\Delta|^{1/2}$ implies that
$$\operatorname{Im}\tau_x = \frac{|\Delta|^{1/2}}{2a} \ge 5.$$
Applying (3-12) with $\tau = \tau_x$, we obtain
$$\log|x| = \pi\frac{|\Delta|^{1/2}}{a} + O_1(800e^{-\pi|\Delta|^{1/2}/a}).$$
Since $|\Delta|^{1/2}/a \ge 10$, we have $800e^{-\pi|\Delta|^{1/2}/a} \le e^{-2|\Delta|^{1/2}/a}$. This proves item 1.

Similarly, item 2 follows by applying (3-15) with $V = |\Delta|^{1/2}/2A$. Note that (3-17) is a special case of (3-16) corresponding to $A = 1$.

Finally, (3-18) and (3-19) are obtained by setting $\tau = \tau_x$ in (3-13) and (3-14), respectively. □

We also need a lower bound. The following is a weaker version of [8, Theorem 6.1], applied with $y = 0$.

Proposition 3.6. *Let x be a singular modulus with discriminant $\Delta_x \ne -3$. Then $|x| \ge |\Delta_x|^{-3}$.*

3.2. ***Bounding the exponents.*** Let $\alpha_1, \dots, \alpha_k$ be nonzero algebraic numbers. The set of vectors $\boldsymbol{m} = (m_1, \dots, m_k) \in \mathbb{Z}^k$ such that
$$\alpha_1^{m_1}\cdots\alpha_k^{m_k} = 1$$
is a subgroup in $\mathbb{Z}^k$, denoted here by $\Gamma(\alpha_1, \dots, \alpha_k)$ (or simply Γ if this does not cause confusion).

Masser [18] showed that Γ admits a small $\mathbb{Z}$-basis. To state his result, let us introduce some notation. Let L be a number field. We denote by $\omega = \omega(L)$ the order of the group of roots of unity belonging to L, and by $\eta = \eta(L)$ the smallest positive height of the elements of L:

$$\eta = \min\{\mathrm{h}(\alpha) : \alpha \in L,\ \mathrm{h}(\alpha) > 0\}.^{1}$$

Proposition 3.7 (Masser). *Let $\alpha_1, \dots, \alpha_k$ be elements in $L^\times$. Then $\Gamma(\alpha_1, \dots, \alpha_k)$ has a $\mathbb{Z}$-basis consisting of vectors with norm bounded by $\omega(k\mathrm{h}/\eta)^{k-1}$, where*

$$\mathrm{h} = \max\{\mathrm{h}(\alpha_1), \dots, \mathrm{h}(\alpha_k), \eta\}.$$

We want to adapt this result to the case when our algebraic numbers are singular moduli.

Proposition 3.8. *Let $x_1, \dots, x_k$ be nonzero singular moduli. Set*

$$X = \max\{|\Delta_{x_1}|, \dots, |\Delta_{x_k}|\},$$

and assume that, among $D_{x_1}, \dots, D_{x_k}$, there are ℓ distinct fundamental discriminants; in symbols:

$$\ell = \#\{D_{x_1}, \dots, D_{x_k}\}.$$

Then the group $\Gamma(x_1, \dots, x_k)$ has a $\mathbb{Z}$-basis consisting of vectors with norm bounded by $24(c(\ell)kX^{1/2})^{k-1}$, where $c(\ell) = 3^{4^\ell + 2^{\ell+1}+8}$. In particular, $c(1) = 3^{16}$.

The proof uses the following result due to Amoroso and Zannier [3, Theorem 1.2].

Lemma 3.9. *Let K be a number field of degree d, and let α be an algebraic number such $K(\alpha)$ is an abelian extension of K. Then either $\mathrm{h}(\alpha) = 0$ or $\mathrm{h}(\alpha) \geq 3^{-d^2-2d-6}$.*

Proof of Proposition 3.8. Set

$$K = \mathbb{Q}(\sqrt{D_{x_1}}, \dots, \sqrt{D_{x_k}}), \quad L = K(x_1, \dots, x_k).$$

To apply Proposition 3.7, we have to estimate the quantities h, η and ω.

Since x_i is an algebraic integer, and every one of its conjugates x_i^σ satisfies $\log|x_i^\sigma| \leq 4|\Delta|^{1/2}$ (see Corollary 3.5:2), we have $\mathrm{h}(x_i) \leq 4X^{1/2}$. It follows that $\mathrm{h} \leq 4X^{1/2}$.

Since $[K : \mathbb{Q}] \leq 2^\ell$ and L is an abelian extension of K, Lemma 3.9 implies that $\eta \geq 3^{-4^\ell - 2^{\ell+1}-6}$. Finally, we have $\omega \leq 24$ from Corollary 2.7.

Putting all of this together, the result follows. □

In this article we will often work with relations of the form

$$x_1^{m_1} \cdots x_k^{m_k} = (x_1')^{m_1} \cdots (x_k')^{m_k}.$$

It is useful to have a bounded basis for the group of these relations as well.

[1] Here $\mathrm{h}(\cdot)$ is the usual absolute logarithmic height; there is no risk of confusing it with the class number $h(\cdot)$, not only because the latter is in italics, but because class numbers do not occur in this section, and heights do not occur outside this section.

Proposition 3.10. *Let $x_1, \dots, x_k, x_1', \dots, x_k'$ be singular moduli of discriminants not exceeding X, and let ℓ be the number of distinct fundamental discriminants among $D_{x_1}, \dots, D_{x_k'}$. Then the group $\Gamma(x_1/x_1', \dots, x_k/x_k')$ has a $\mathbb{Z}$-basis consisting of vectors with norm bounded by $24(c(\ell)kX^{1/2})^{k-1}$, where $c(\ell) = 3^{4^\ell+2^{\ell+1}+8}$. In particular, $c(1) = 3^{16}$.*

Proof. Same as for Proposition 3.8, only with $\mathrm{h} \le 8X^{1/2}$. □

3.3. *Proofs of Propositions 3.1 and 3.2.*

Proof of Proposition 3.1. By Proposition 3.8 we may assume that $\boldsymbol{m}$ has sup-norm

$$\|\boldsymbol{m}\| \le 24(3^{16}kX^{1/2})^{k-1}. \tag{3-20}$$

Using Corollary 3.5, we obtain

$$0 = \sum_{i=1}^{k} m_i \log|x_i| = \pi|D|^{1/2}L + O_1(k\|\boldsymbol{m}\|e^{-3Y^{1/2}/A}), \tag{3-21}$$

where L is the left-hand side of (3-2). (Recall that D denotes the common fundamental discriminant of $x_1, \dots, x_k$.) Using (3-5) and (3-20), we deduce from this the estimate $|L| \le 0.5A^{-k}$. Since L is a rational number with denominator not exceeding A^k, we must have $L = 0$. □

Proof of Proposition 3.2. We will prove only (3-8), because (3-9) is analogous.

Using Corollary 3.5 and Proposition 3.6, we obtain

$$0 = \frac{1}{\pi|\Delta|^{1/2}}\sum_{i=1}^{k} m_i \log|x_i| \ge \sum_{\substack{1\le i\le k\\ a(x_i)<A}} \frac{m_i'}{a(x_i)} - \sum_{m_i<0} \frac{|m_i'|}{\min\{a(x_i), A\}} + O_1\left(k\|\boldsymbol{m}'\|\frac{3\log X + e^{-3|\Delta|^{1/2}/A}}{\pi|\Delta|^{1/2}}\right),$$

Using our hypothesis (3-7), we obtain

$$\frac{3k\log X}{\pi|\Delta|^{1/2}} \le \frac{3}{\pi}\varepsilon, \quad \frac{ke^{-3|\Delta|^{1/2}/A}}{\pi|\Delta|^{1/2}} \le 0.01\varepsilon,$$

and the result follows. □

4. Proof of Theorem 1.2

Throughout this section, unless the contrary is stated explicitly, x and y are distinct singular moduli and m, n are nonzero integers such that $\mathbb{Q}(x^m y^n) \ne \mathbb{Q}(x, y)$.

The proof of Theorem 1.2 is organized as follows. Assuming that

$$\max\{|\Delta_x|, |\Delta_y|\} \ge 10^6, \tag{4-1}$$

we show that one of the following two conditions is satisfied: either

$$\Delta_x = \Delta_y, \quad m = n, \quad [\mathbb{Q}(x, y) : \mathbb{Q}(x^m y^m)] = 2, \quad x \text{ and } y \text{ are conjugate over } \mathbb{Q}(x^m y^m) \tag{4-2}$$

(as wanted), or

$$\{\Delta_x, \Delta_y\} = \{\Delta, 4\Delta\} \quad \text{for some } \Delta \equiv 1 \bmod 8. \tag{4-3}$$

Unfortunately, we cannot rule out (4-3) assuming merely (4-1), but we show that (4-3) is impossible under the stronger hypothesis

$$\max\{|\Delta_x|, |\Delta_y|\} \geq 10^8, \tag{4-4}$$

completing thereby the proof.

We assume that x, y have the same fundamental discriminant (in the opposite case, the argument is much simpler: see Section 4.5.) We denote by K the common CM field of x, y, and we set $L = K(x, y)$. We also set

$$\alpha = x^m y^n, \quad F = \mathbb{Q}(\alpha), \quad G = \mathrm{Gal}(L/F).$$

Since F is a proper subfield of $\mathbb{Q}(x, y)$, there exists $\sigma \in G$ such that $x^\sigma \neq x$ or $y^\sigma \neq y$. We claim that

$$x^\sigma \neq x \quad \text{and} \quad y^\sigma \neq y. \tag{4-5}$$

Indeed, if, say, $y^\sigma = y$ then $(x^\sigma)^m = x^m$, which implies $x^\sigma = x$ by Lemma 2.22.

Remark 4.1. In the course of the argument we will study multiplicative relations

$$x^m y^n (x^\sigma)^{-m} (y^\sigma)^{-n} = 1, \tag{4-6}$$

with various choices of $\sigma \in G$ satisfying (4-5), and we will use Propositions 3.1 and 3.2 with parameters satisfying the following restrictions:

$$k \leq 4; \quad X = \max\{|\Delta_x|, |\Delta_y|\} \geq \begin{Bmatrix} 10^6 \\ 10^8 \end{Bmatrix}; \quad Y \geq \tfrac{1}{4}X; \quad A \leq 9; \quad \varepsilon = \begin{Bmatrix} 0.16 \\ 0.016 \end{Bmatrix}. \tag{4-7}$$

(The top/bottom alternation will be explained momentarily.) It is easy to verify that the conditions in (4-7) ensure that (3-5) and (3-7) are satisfied, so using the propositions is justified.

From here on through Section 4.4.1 we assume (4-1), and we use Proposition 3.2 with $X \geq 10^6$ and $\varepsilon = 0.16$. Starting from Section 4.4.2 we have (4-3) and assume (4-4), which will allow us to use Proposition 3.2 with $X \geq 10^8$ and $\varepsilon = 0.016$.

4.1. ***A special case.*** In this subsection we study the special case

$$m = -n \quad \text{and} \quad \Delta_x = \Delta_y. \tag{4-8}$$

We will need the result from this case to treat the general case. It will also be a good illustration of how our method works in a simple setup.

Let $\sigma \in G$ be such that (4-5) holds. We will apply Proposition 3.2 to the multiplicative relations

$$x^m y^{-m} (x^\sigma)^{-m} (y^\sigma)^m = 1, \tag{4-9}$$

$$x^m y^{-m} (x^{\sigma^{-1}})^{-m} (y^{\sigma^{-1}})^m = 1. \tag{4-10}$$

We may assume, up to Galois conjugation, that x is dominant. Then none of $y, x^\sigma, x^{\sigma^{-1}}$ is

$$a(x) = 1, \quad a(y),\ a(x^\sigma),\ a(x^{\sigma^{-1}}) \geq 2.$$

If one of $a(y), a(x^\sigma)$ is ≥ 3, then, applying Proposition 3.2 to (4-9) with $A = 3$ and $\varepsilon = 0.16$, we obtain

$$m \leq \left(\frac{1}{\min\{3, a(y)\}} + \frac{1}{\min\{3, a(x^\sigma)\}} + 0.16 \right) m \leq \left(\tfrac{1}{2} + \tfrac{1}{3} + 0.16\right) m,$$

a contradiction.

Thus, we must have $a(y) = a(x^\sigma) = 2$. This means that y and x^σ are either equal or 4-isogenous; see Proposition 2.21:3. Hence so are $y^{\sigma^{-1}}$ and x. Corollary 2.20 now implies that $a(y^{\sigma^{-1}}) \leq 4$.

Applying Proposition 3.2 to (4-10) with $A = 5$ and $\varepsilon = 0.16$, we obtain

$$m + \frac{m}{a(y^{\sigma^{-1}})} \leq m \left(\frac{1}{\min\{5, a(y)\}} + \frac{1}{\min\{5, a(x^{\sigma^{-1}})\}} + 0.16 \right) \leq m\left(\tfrac{1}{2} + \tfrac{1}{2} + 0.16\right).$$

Since $a(y^{\sigma^{-1}}) \leq 4$, we get a contradiction. We have proved that (4-8) is impossible.

4.2. ***The general case: preparations.*** Now we are ready to treat the general case. Pick $\sigma \in G$ satisfying (4-5). We have $(x/x^\sigma)^m = (y^\sigma/y)^n$, and, in particular, $\mathbb{Q}((x/x^\sigma)^m) = \mathbb{Q}((y/y^\sigma)^n)$. The special case of Theorem 1.2 treated in Section 4.1 implies that

$$\mathbb{Q}((x/x^\sigma)^m) = \mathbb{Q}(x, x^\sigma), \quad \mathbb{Q}((y/y^\sigma)^n) = \mathbb{Q}(y, y^\sigma).$$

Lemma 2.26:2 now implies that $K(x) = K(y) = L$, and Lemma 2.25 implies that there exists a discriminant Δ such that

$$\Delta_x = e_x^2 \Delta, \quad \Delta_y = e_y^2 \Delta, \quad (e_x, e_y) \in \{(1,1), (2,1), (1,2)\},$$

and, moreover,

$$\text{if } (e_x, e_y) \neq (1,1) \text{ then } \Delta \equiv 1 \bmod 8. \tag{4-11}$$

We may and will assume in the sequel that

$$m > 0, \quad e_x m \geq e_y |n|, \quad a_x = 1. \tag{4-12}$$

If $(e_x, e_y) \neq (1,1)$ then x and y are not conjugate over $\mathbb{Q}$, and (4-5) becomes

$$x^\sigma, y^\sigma \notin \{x, y\}. \tag{4-13}$$

When $(e_x, e_y) = (1,1)$, Lemma 2.24 implies that σ can be redefined to satisfy either (4-13) or one of the following:

$$x^\sigma = y, \quad y^\sigma = x, \quad [\mathbb{Q}(x,y) : F] = 2; \tag{4-14}$$

$$x^\sigma = y, \quad y^\sigma = z, \quad z^\sigma = x, \quad L = \mathbb{Q}(x,y), \quad [L : F] = 3. \tag{4-15}$$

Case (4-14) is easy: relation (4-6) becomes $x^{m-n} = y^{m-n}$, and Lemma 2.22 implies that $m = n$, which means that we have (4-2).

We have to show that the other two cases are impossible. For (4-15) this is done in Section 4.3. Case (4-13) is much harder to dispose of; we deal with it in Section 4.4.

4.3. ***Case* (4-15).** We have

$$x^m y^{n-m} z^{-n} = 1.$$

Recall from (4-12) that $m \geq |n|$ and $a_x = 1$. This implies $a_y, a_z \geq 2$.

Assume first that $n > 0$. Then

$$\max\bigl\{m, |n-m|, |-n|\bigr\} = m.$$

Using Proposition 3.2 with $\varepsilon = 0.16$ and $A = 5$, we obtain

$$m \leq \frac{m-n}{\min\{5, a_y\}} + \frac{m}{\min\{5, a_z\}} n + 0.16m \leq \tfrac{1}{2}(m-n) + \tfrac{1}{2}n + 0.16m,$$

a contradiction.

Now assume that $n < 0$. Then

$$\max\bigl\{m, |n-m|, |-n|\bigr\} \leq 2m.$$

If $a_y \geq 3$ then Proposition 3.2 with $\varepsilon = 0.16$ and $A = 3$ implies that

$$m \leq \tfrac{1}{3} \cdot 2m + 0.16 \cdot 2m,$$

a contradiction. If $a_y = 2$ then x and y are 2-isogenous (see Proposition 2.21:1), and so are $y = x^\sigma$ and $z = y^\sigma$. This implies that $a_z \in \{1, 4\}$, see Corollary 2.20. But $a_z \geq 2$, and so $a_z = 4$. Proposition 3.1 now implies that

$$m + \frac{n-m}{2} - \frac{n}{4} = 0,$$

yielding $n = -2m$, again a contradiction. Thus, (4-15) is impossible.

4.4. ***Case* (4-13).** We will use the notation

$$m' = e_x m, \quad n' = e_y n.$$

Recall that $m' \geq |n'|$ and $a(x) = 1$; see (4-12). This implies, in particular, that $a(x^\sigma) \geq 2$.

4.4.1. *One of y, y^σ is dominant.* We start by showing that either y or y^σ is dominant.

Proposition 4.2. *If $n > 0$ then $a(y^\sigma) = 1$ and $\sigma^2 = 1$. If $n < 0$ then $a(y) = 1$. In both cases we have $(e_x, e_y) \neq (1, 1)$ and $\Delta \equiv 1 \bmod 8$.*

Proof. We treat separately $n > 0$ and $n < 0$.

Assume first that $n > 0$, but $a(y^\sigma) \geq 2$. We know already that $a(x^\sigma) \geq 2$. If one of $a(x^\sigma), a(y^\sigma)$ is ≥ 3 then, applying Proposition 3.2 with $A = 3$ and $\varepsilon = 0.16$ to the relation $x^m y^n (x^\sigma)^{-m} (y^\sigma)^{-n} = 1$, we obtain

$$m' \leq \frac{m}{\min\{3, a(x^\sigma)\}} + \frac{n}{\min\{3, a(y^\sigma)\}} + 0.16m \leq \left(\tfrac{1}{2} + \tfrac{1}{3} + 0.16\right)m,$$

a contradiction.

Thus, $a(x^\sigma) = a(y^\sigma) = 2$. This implies that $e_x = e_y = 1$, for otherwise $\Delta = 1 \bmod 8$ by (4-11), and one of Δ_x, Δ_y, being 4 mod 32, cannot admit singular moduli with denominator 2 (see Proposition 2.17:4).

Since $a(x^\sigma) = a(y^\sigma) = 2$ but $x^\sigma \neq y^\sigma$, the singular moduli x^σ and y^σ must be 4-isogenous; see Proposition 2.21:3. Hence so are x and y. Corollary 2.20 now implies that $a_y = 4$, and Proposition 3.1 yields

$$m' + \frac{n'}{4} - \frac{m'}{2} - \frac{n'}{2} = 0.$$

Hence $n' = 2m'$, again a contradiction. Thus, $n > 0$ implies that $a(y^\sigma) = 1$.

Note that if (4-13) holds for some $\sigma \in G$ then it also holds with σ replaced by σ^{-1}. Hence $n > 0$ implies that $a(y^{\sigma^{-1}}) = 1$ as well. Since there can be only one dominant singular modulus of a given discriminant, we must have $y^\sigma = y^{\sigma^{-1}}$. Hence $\sigma^2 = 1$ by Lemma 2.23.

Now assume that $n < 0$ but $a(y) \geq 2$. The same argument as above shows that $a(x^\sigma) = a(y) = 2$ and $e_x = e_y = 1$.

The singular moduli x^σ and y must be 4-isogenous. Hence so are x and $y^{\sigma^{-1}}$, which implies that $a(y^{\sigma^{-1}}) = 4$. Applying Proposition 3.2 with $A = 5$ and $\varepsilon = 0.16$ to

$$x^m y^{-|n|} (x^{\sigma^{-1}})^{-m} (y^{\sigma^{-1}})^{|n|} = 1,$$

we obtain

$$m' + \frac{|n'|}{4} \leq \frac{|n'|}{2} + \frac{m'}{\min\{5, a(x^{\sigma^{-1}})\}} + 0.16m'.$$

Since $|n'| \leq m'$ and $a(x^{\sigma^{-1}}) \geq 2$, this is impossible. Thus, we proved that $n < 0$ implies that $a(y) = 1$.

Finally, $(e_x, e_y) \neq (1, 1)$, because there cannot be two distinct dominant singular moduli of the same discriminant. Hence $\Delta \equiv 1 \bmod 8$ by (4-11). The proposition is proved. □

4.4.2. *Controlling the four denominators.* Thus, we know that two of the singular moduli x, y, x^σ, y^σ are dominant. Unfortunately, we have no control over the denominators of the other two.

We will now show that, with a suitably chosen Galois morphism θ, we can control the denominators of all four of $x^\theta, y^\theta, x^{\sigma\theta}, y^{\sigma\theta}$.

So far, we have assumed that $\max\{|\Delta_x|, |\Delta_y|\} \geq 10^6$ and used Proposition 3.2 with $\varepsilon = 0.16$. However, now we know that

$$\{\Delta_x, \Delta_y\} = \{\Delta, 4\Delta\} \quad \text{with } \Delta \equiv 1 \bmod 8,$$

which allows us (see Remark 4.1) to assume that $\max\{|\Delta_x|, |\Delta_y|\} \geq 10^8$ and to use Proposition 3.2 with $\varepsilon = 0.016$.

Proposition 4.3. *There exists $\theta \in \mathrm{Gal}(L/K)$ such that, when $(e_x, e_y) = (1, 2)$, we have*

$$a(x^\theta) = a(x^{\sigma\theta}) = 2, \quad a(y^\theta) = a(y^{\sigma\theta}) = 8, \tag{4-16}$$

and when $(e_x, e_y) = (2, 1)$, we have (4-16) with x and y switched.

To prove this proposition, we need to bound $|n'|$ from below.

Lemma 4.4. *Assume that $(e_x, e_y) = (2, 1)$. Then $|n'| \geq 0.85m'$.*

A similar estimate can be proved when $(e_x, e_y) = (1, 2)$, but we do not need this.

Proof. Assume first that $n < 0$. Then $a(x) = a(y) = 1$. In particular, x and y are 2-isogenous, and so are x^σ, y^σ. Write

$$x^m y^{-|n|} (x^\sigma)^{-m} (y^\sigma)^{|n|} = 1.$$

When $a(x^\sigma) \geq 8$ we use Proposition 3.2 with $A = 8$ and $\varepsilon = 0.016$ to obtain

$$m' \leq |n'| + \frac{m'}{8} + 0.016m',$$

which implies that $|n'| \geq 0.85m'$.

When $a(x^\sigma) \leq 7$, we must have $a(x^\sigma) \in \{3, 5, 7\}$ by Proposition 2.17:4, because $\Delta_x = 4\Delta \equiv 4 \bmod 32$. Since x^σ and y^σ are 2-isogenous, Corollary 2.20 implies that $a(y^\sigma) \in \{a(x^\sigma), a(x^\sigma)/4\}$, and we must have $a(y^\sigma) = a(x^\sigma)$. Using Proposition 3.1 with $A = 7$ we obtain

$$m' - |n'| - \frac{m'}{a(x^\sigma)} + \frac{|n'|}{a(x^\sigma)} = 0,$$

which shows that $|n'| = m'$. This proves the lemma in the case $n < 0$.

Now assume that $n > 0$. Then $a(x) = a(y^\sigma) = 1$ and $\sigma^2 = 1$. In particular, x and y^σ are 2-isogenous, and so are $x^{\sigma^{-1}} = x^\sigma$ and y. Arguing as above, we obtain that either $a(x^\sigma) \geq 8$ and $n' \geq 0.85m'$, or $a(x^\sigma) \in \{3, 5, 7\}$ and $n' = m'$. The lemma is proved. □

Proof of Proposition 4.3. Let us assume first that $n < 0$ and $(e_x, e_y) = (1, 2)$.

We have

$$\Delta_x = \Delta \equiv 1 \bmod 8, \quad \Delta_y = 4\Delta \equiv 4 \bmod 32. \tag{4-17}$$

By Proposition 2.17:1, there exist two distinct morphisms $\theta \in \mathrm{Gal}(L/K)$ such that $a(x^\theta) = 2$. Of the two, there can be at most one with the property $a(x^{\sigma\theta}) = 1$. Hence we may find θ satisfying

$$a(x^\theta) = 2, \quad a(x^{\sigma\theta}) \geq 2.$$

Since $n < 0$, we have $a(y) = 1$ by Proposition 4.2. Hence x and y are 2-isogenous, and so are x^θ and y^θ. It follows that $a(y^\theta) \in \{2, 8\}$. But $a(y^\theta) \neq 2$ by Proposition 2.17:4. Hence $a(y^\theta) = 8$.

Proposition 3.2, applied to

$$(x^\theta)^m (y^\theta)^{-|n|} (x^{\sigma\theta})^{-m} (y^{\sigma\theta})^{|n|} = 1$$

with $A = 9$ and $\varepsilon = 0.016$, implies that

$$\frac{m'}{2} \le \frac{|n'|}{8} + \frac{m'}{\min\{9, a(x^{\sigma\theta})\}} + 0.016m'.$$

If $a(x^{\sigma\theta}) \ge 3$ then this implies that

$$m'\left(\tfrac{1}{2} - \tfrac{1}{3}\right) \le \tfrac{1}{8}|n'| + 0.016m',$$

which is impossible because $m' \ge |n'|$. Hence $a(x^{\sigma\theta}) = 2$, and, as above, this implies that $a(y^{\sigma\theta}) = 8$.

Now assume that $n < 0$ and $(e_x, e_y) = (2, 1)$. We again have (4-17), but with x and y switched. Arguing as before, we find $\theta \in \mathrm{Gal}(L/K)$ such that

$$a(y^{\theta}) = 2, \quad a(y^{\sigma\theta}) \ge 2, \quad a(x^{\theta}) = 8.$$

As before, in the case $a(y^{\sigma\theta}) \ge 3$ we apply Proposition 3.2 to

$$(x^{\theta})^{-m}(y^{\theta})^{|n|}(x^{\sigma\theta})^{m}(y^{\sigma\theta})^{-|n|} = 1$$

and obtain

$$|n'|\left(\tfrac{1}{2} - \tfrac{1}{3}\right) \le \tfrac{1}{8}m' + 0.016m',$$

which is impossible because $|n'| \ge 0.85m'$. Hence $a(y^{\sigma\theta}) = 2$, and, as above, this implies that $a(x^{\sigma\theta}) = 8$.

Finally, let us assume that $n > 0$. Then $a(y^{\sigma}) = 1$ and $\sigma^2 = 1$. In particular, x and y^{σ} are 2-isogenous, and so are x^{σ} and $y^{\sigma^2} = y$. Now, writing

$$x^{m}(y^{\sigma})^{-n}(x^{\sigma})^{-m}y^{n} = 1,$$

we repeat the previous argument with y, y^{σ} switched, and with n replaced by $-n$. The proposition is proved. □

4.4.3. *Completing the proof.* Now we are ready to rule (4-13) out by deriving a contradiction. Let us summarize what we have. After renaming, we have distinct singular moduli x_1, x_2 of discriminant Δ and y_1, y_2 of discriminant 4Δ such that

$$a(x_1) = a(x_2) = 2, \quad a(y_1) = a(y_2) = 8,$$

and

$$x_1^{m_1}y_1^{n_1}x_2^{-m_1}y_2^{-n_1} = 1, \tag{4-18}$$

where m_1, n_1 is a permutation of m, n. We want to show that this impossible.

Proposition 3.10 implies that we may assume

$$\max\{|m_1|, |n_1|\} \le 10^{10}|\Delta|^{1/2}. \tag{4-19}$$

Note also that

$$|\Delta| \ge 10^{7} \tag{4-20}$$

by the assumption (4-4).

Proposition 2.17 implies that, after possible renumbering, we have

$$\tau(x_1)=\frac{1+\sqrt{\Delta}}{4},\quad \tau(x_2)=\frac{-1+\sqrt{\Delta}}{4},\quad \tau(y_1)=\frac{b+\sqrt{\Delta}}{8},\quad \tau(y_2)=\frac{-b+\sqrt{\Delta}}{8},$$

where $b\in\{\pm1,\pm3\}$. Set $t=e^{-\pi|\Delta|^{1/2}/4}$ and $\xi=e^{b\pi i/4}$. Then

$$e^{2\pi i\tau(x_1)}=it^2,\quad e^{2\pi i\tau(x_2)}=-it^2,\quad e^{2\pi i\tau(y_1)}=\xi t,\quad e^{2\pi i\tau(y_2)}=\bar{\xi}t.$$

We deduce from (4-18) that

$$m_1\log(it^2x_1)-m_1\log(-it^2x_2)+n_1\log(\xi ty_1)-n_1\log(\bar{\xi}ty_2)\in\tfrac{1}{4}\pi i\mathbb{Z}. \tag{4-21}$$

Corollary 3.5:3 implies that

$$\log(it^2x_1)=744it^2+O_1(5\cdot10^5t^4),\qquad \log(-it^2x_2)=-744it^2+O_1(5\cdot10^5t^4),$$
$$\log(\xi ty_1)=744\xi t+O_1(5\cdot10^5t^2),\qquad \log(\bar{\xi}ty_2)=\ 744\bar{\xi}t+O_1(5\cdot10^5t^2).$$

Transforming the left-hand side of (4-21) using these expansions, we obtain

$$744(\xi-\bar{\xi})tn_1+O_1\big(10^7t^2\max\{|m_1|,|n_1|\}\big)=\tfrac{1}{4}\pi ik$$

for some $k\in\mathbb{Z}$. An easy estimate using (4-19) and (4-20) shows that the left-hand side does not exceed 10^{-1000} in absolute value. Hence $k=0$, and we obtain, again using (4-19) and (4-20), that

$$744\,|\xi-\bar{\xi}||n_1|\le10^{17}|\Delta|^{1/2}e^{-\pi|\Delta|^{1/2}/4}<10^{-900}.$$

Hence $n_1=0$, a contradiction.

This proves the impossibility of (4-13), completing the proof of Theorem 1.2 in the case of equal fundamental discriminants.

4.5. ***Distinct fundamental discriminants.*** In this subsection $D_x\ne D_y$. Arguing as in the beginning of Section 4.2, we find a Galois morphism σ such that $\mathbb{Q}(x,x^\sigma)=\mathbb{Q}(y,y^\sigma)$. Lemma 2.26:1 implies that $\mathbb{Q}(x)=\mathbb{Q}(y)$. Corollary 2.13 implies that $h(\Delta_x)=h(\Delta_y)\le16$, and our hypothesis $\max\{|\Delta_x|,\Delta_y|\}\ge10^6$ contradicts Proposition 2.1. This concludes the proof of Theorem 1.2. □

5. Proof of Theorem 1.1

Throughout this section, unless stated otherwise, x, y, z are distinct singular moduli satisfying

$$\max\{|\Delta_x|,|\Delta_y|,|\Delta_z|\}\ge10^{10} \tag{5-1}$$

and such that there exist nonzero integers m,n,r with the property $x^my^nz^r\in\mathbb{Q}^\times$.

We assume that x, y, z have the same fundamental discriminant D; if this is not the case, then the argument is much simpler — see Section 5.5.

We denote by $K = \mathbb{Q}(\sqrt{D})$ the common CM field of x, y, z, and we set

$$L = K(x, y, z), \quad G = \mathrm{Gal}(L/K).$$

We set

$$f = \gcd(f_x, f_y, f_z), \quad e_x = \frac{f_x}{f}, \quad e_y = \frac{f_y}{f}, \quad e_z = \frac{f_z}{f}, \quad \Delta = Df^2.$$

Then $\gcd(e_x, e_y, e_z) = 1$ and

$$\Delta_x = e_x^2\Delta, \quad \Delta_y = e_y^2\Delta, \quad \Delta_z = e_z^2\Delta. \tag{5-2}$$

5.1. ***The discriminants.*** The following property, showing that the ring class fields $K(x)$, $K(y)$ and $K(z)$ are closely related, is the basis for everything.

Proposition 5.1. (1) *We have*

$$L = K(x, y) = K(x, z) = K(y, z). \tag{5-3}$$

(2) *Each of the fields $K(x)$, $K(y)$, $K(z)$ is a subfield of L of degree at most 2.*

(3) *Up to permuting x, y, z (and correspondingly m, n, r) we have one of the cases from Table 2.*

Proof. By the assumption, $K(x^m) = K(y^n z^r) \subset K(y, z)$. Lemma 2.22 implies that $K(x) = K(y^n z^r)$, and Hence $x \in K(y, z)$. Hence $L = K(y, z)$. By symmetry, we obtain (5-3). This proves item (1).

From (5-1) we may assume that, for instance, $|\Delta_z| \geq 10^{10}$. Theorem 1.2 implies that the field $K(x) = K(y^n z^r)$ is a subfield of L of degree at most 2, and the same holds true for the fields $K(y)$. Unfortunately, we cannot make the same conclusion for $K(z)$, because, *a priori*, we cannot guarantee that $\max\{|\Delta_x|, |\Delta_y|\} \geq 10^8$, which is needed to apply Theorem 1.2 in this case. So a lengthy extra argument is required to prove that $[L : K(z)] \leq 2$. We split it into two cases.

Assume first that

$$\Delta \neq -3, -4 \quad \text{or} \quad \gcd(e_x, e_z) > 1. \tag{5-4}$$

In this case, setting $\ell = \mathrm{lcm}(e_x, e_y, e_z)$, Proposition 2.5 implies that $L = K[\ell f]$, the ring class field of K

e_x	$[L : K(x)]$	e_y	$[L : K(y)]$	e_z	$[L : K(z)]$	remarks
1	1	1	1	1	1	
1	1	1	1	2	1	$\Delta \equiv 1 \bmod 8$
1	1	2	1	2	1	$\Delta \equiv 1 \bmod 8$
1	2	2	1	2	1	$\Delta \equiv 0 \bmod 4$, $n = r$
1	2	3	1	3	1	$\Delta \equiv 1 \bmod 3$, $n = r$
2	2	3	1	3	1	$\Delta \equiv 1 \bmod 24$, $n = r$
1	2	4	1	4	1	$\Delta \equiv 1 \bmod 8$, $n = r$
1	2	6	1	6	1	$\Delta \equiv 1 \bmod 24$, $n = r$

Table 2. Data for Proposition 5.1.

of conductor ℓf. The class number formula (2-4) implies that

$$2 \geq [L : K(x)] = \Psi(\ell/e_x, \Delta_x), \tag{5-5}$$

which results in one of the following six cases:

$$\begin{aligned}
&\ell = e_x, && L = K(x); && \\
&\ell = 2e_x, && L = K(x), && \Delta_x \equiv 1 \bmod 8; \\
&\ell = 2e_x, && [L : K(x)] = 2, && \Delta_x \equiv 0 \bmod 4; \\
&\ell = 4e_x, && [L : K(x)] = 2, && \Delta_x \equiv 1 \bmod 8; \\
&\ell = 3e_x, && [L : K(x)] = 2, && \Delta_x \equiv 1 \bmod 3; \\
&\ell = 6e_x, && [L : K(x)] = 2, && \Delta_x \equiv 1 \bmod 24.
\end{aligned} \tag{5-6}$$

In particular, $e_x \geq \ell/6 \geq e_z/6$, which implies that $|\Delta_x| \geq |\Delta_z|/36 \geq 10^8$. Hence we may again apply Theorem 1.2 to conclude that $[L : K(z)] \leq 2$ in case (5-4).

We are left with the case

$$\Delta \in \{-3, -4\} \quad \text{and} \quad \gcd(e_x, e_z) = 1. \tag{5-7}$$

We want to show that it is impossible. We claim that in this case $\varphi(e_z) \leq 6$. Indeed, if $x \in K$ then

$$2 \geq [K(x, z) : K(x)] = [K(z) : K] = \frac{\Psi(e_z, \Delta)}{[\mathcal{O}_K^\times : \mathcal{O}_{K(z)}^\times]} \geq \frac{\Psi(e_z, \Delta)}{3},$$

which proves that $\varphi(e_z) \leq \Psi(e_z, \Delta) \leq 6$. And if $x \notin K$ then

$$\Psi(e_z, e_x^2\Delta) = \big[K[e_z e_x] : K[e_x]\big] = \big[K[e_z e_x] : K(x, z)\big] \cdot [K(x, z) : K(x)].$$

We have $\big[K[e_z e_x] : K(x, z)\big] \leq 3$ by Proposition 2.5, and

$$[K(x, z) : K(x)] = [L : K(x)] \leq 2,$$

as we have seen above. It follows that

$$\varphi(e_z) \leq \Psi(e_z, e_x^2\Delta) \leq 6.$$

From $\varphi(e_z) \leq 6$ we deduce $e_z \leq 18$. Hence $|\Delta_z| \leq 4 \cdot 18^2 < 10^{10}$, a contradiction. This shows the impossibility of (5-7), completing the proof of item (2).

We are left with part (3) of the proposition. As we have just seen, we have one of the six cases (5-6), and similarly with x replaced by y or by z. Since e_x, e_y, e_z are coprime, every prime number p does not divide one of them. If, say, $p \nmid e_x$, then

$$v_p(\ell) = v_p(\ell/e_x) \leq \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{if } p = 3, \\ 0 & \text{if } p \geq 5. \end{cases}$$

This proves that $\ell \mid 12$. Moreover,

$$\text{if } 2 \mid \ell \text{ then } \Delta \equiv 1 \bmod 8 \text{ or } \Delta \equiv 0 \bmod 4; \tag{5-8}$$

$$\text{if } 4 \mid \ell \text{ then } \Delta \equiv 1 \bmod 8; \tag{5-9}$$

$$\text{if } 3 \mid \ell \text{ then } \Delta \equiv 1 \bmod 3. \tag{5-10}$$

Indeed, assume that $2 \mid \ell$ but $\Delta \equiv 5 \bmod 8$. Since e_x, e_y, e_z are coprime, one of them, say e_x, is not divisible by 2. Then $(\Delta_x/2) = -1$, and $\Psi(\ell/e_x, \Delta_x)$ must be divisible by 3, which contradicts (5-5). This proves (5-8).

In a similar fashion, one shows that $\Psi(\ell/e_x, \Delta_x)$ is divisible by 4 in each of the cases

$$4 \mid \ell, \quad 2 \nmid e_x, \quad \Delta \equiv 0 \bmod 4,$$
$$3 \mid \ell, \quad 3 \nmid e_x, \quad \Delta \equiv 2 \bmod 3,$$

and it is divisible by 3 in the case

$$3 \mid \ell, \quad 3 \nmid e_x, \quad \Delta \equiv 0 \bmod 3.$$

This proves (5-9) and (5-10).

It also follows from Theorem 1.2 that, when, say, $K(x) \neq L$, we must have $e_y = e_z$ and $n = r$.

A little PARI script (or verification by hand) shows that, up to permuting x, y, z, all possible cases are listed in Table 2. □

Recall that $f := \gcd(f_x, f_y, f_z)$ and $G := \mathrm{Gal}(L/K)$. Set $L_0 = K[f]$.

Corollary 5.2. 1. *Either*

$$L = L_0 = K(x) = K(y) = K(z)$$

or $[L : L_0] = 2$, *in which case exactly one of the fields* $K(x), K(y), K(z)$ *is* L_0 *and the other two are* L.

2. $[L_0 : K] \geq 101$.
3. *There exists* $\sigma \in G$ *such that* $a(x^\sigma), a(y^\sigma), a(z^\sigma) \geq 13$,
4. *There exists* $\sigma \in G$ *such that* $a(x^\sigma), a(y^\sigma) \geq 18$, *and the same statement is true for* x, z *and for* y, z.
5. *There exists* $\sigma \in G$ *such that* $a(x^\sigma) \geq 30$, *and the same statement holds true for* y *and for* z.

Proof. Item 1 is proved just by exploring Table 2. To prove item 2, note that, since $\max\{e_x, e_y, e_z\} \leq 6$, we have

$$|\Delta| \geq \max\{|\Delta_x|, |\Delta_y|, |\Delta_z|\}/36 \geq 10^8 \tag{5-11}$$

by (5-1). Hence $[L_0 : K] = h(\Delta) \geq 101$ by Proposition 2.1.

In proving item 3 we must distinguish the cases $L = L_0$ and $[L : L_0] = 2$. In the former case $L = K(x) = K(y) = K(z)$ and $|G| = [L : K] \geq 101$. Proposition 2.15 implies that there exist at most 32

elements $\sigma \in G$ such that $a(x^\sigma) < 13$, and the same for y and z. Since $|G| \geq 101 > 96$, we can find $\sigma \in G$ as wanted.

If $[L : L_0] = 2$ then, say,

$$K(x) = L_0, \quad K(y) = K(z) = L,$$

and $|G| = [L : K] \geq 202$. Again using Proposition 2.15, there exist at most 32 elements $\sigma \in G$ such that $a(y^\sigma) < 13$, the same for z, and at most 64 elements $\sigma \in G$ such that $a(x^\sigma) < 13$. Since $|G| \geq 202 > 128$, we again can find a σ as wanted. This proves item 3.

Item 4 is proved similarly. In the case $L = K(x) = K(y)$ there exist at most 48 elements $\sigma \in G$ such that $a(x^\sigma) < 18$, and the same for y. Since $|G| \geq 101 > 96$, we are done. In the case when one of $K(x)$, $K(y)$ is L, the other is L_0, and $[L : L_0] = 2$, we have $48 + 96 = 144$ unsuitable $\sigma \in G$; since $|G| \geq 202$, we are done again.

Item 5 is similar as well: there exist at most 99 unsuitable σ when $L = K(x)$, and at most 198 when $[L : K(x)] = 2$; in both cases we conclude as before. □

In the sequel we set

$$m' = me_x, \quad n' = ne_y, \quad r' = re_z.$$

We may and will assume that $m > 0$ and that

$$m' \geq \max\{|n'|, |r'|\}, \quad a_x = 1. \tag{5-12}$$

In the course of the argument we will study multiplicative relations

$$x^m y^n z^r (x^\sigma)^{-m} (y^\sigma)^{-n} (z^\sigma)^{-r} = 1, \tag{5-13}$$

with various choices of $\sigma \in G$, using Propositions 3.1 and 3.2. In our usage of Propositions 3.1 and 3.2 the parameters therein will satisfy the following restrictions:

$$\begin{aligned} &k = 6, \quad X = \max\{|\Delta_x|, \Delta_y|, |\Delta_z|\} \geq 10^{10}, \quad Y = |\Delta| \geq \tfrac{1}{36} X, \\ &A \leq 162 \qquad\qquad \text{for Proposition 3.1,} \\ &A \leq 30, \quad \varepsilon = 0.01 \quad \text{for Proposition 3.2.} \end{aligned} \tag{5-14}$$

It is easy to verify that for any choice of parameters satisfying (5-14), conditions (3-5) and (3-7) are met, so using the propositions is justified.

5.2. ***The denominators.*** We already know that x is dominant, see (5-12). Our principal observation is that either one of y, z is dominant as well, or they both are subdominant. More precisely:

Proposition 5.3. *Up to interchanging y and z, one of the following conditions is satisfied*:

$$a_y = 1 \qquad \textit{and} \quad n < 0; \tag{5-15}$$

$$a_y = a_z = 2 \quad \textit{and} \quad n, r < 0. \tag{5-16}$$

Proof. With y and z possibly switched, we may assume that we are in one of the following cases:

$$n, r > 0; \tag{5-17}$$

$$n < 0 \quad \text{and} \quad r > 0; \tag{5-18}$$

$$n, r < 0. \tag{5-19}$$

We consider them separately.

Assume (5-17). Let σ be as in Corollary 5.2:3. Applying Proposition 3.2 to

$$x^m y^n z^r (x^\sigma)^{-m} (y^\sigma)^{-n} (z^\sigma)^{-r} = 1$$

with $A = 13$ and $\varepsilon = 0.01$, and using that $\max\{|m'|, |n'|, |r'|\} = m'$ by (5-12), we obtain

$$m' \le \frac{m'}{13} + \frac{n'}{13} + \frac{r'}{13} + 0.01m' \le m'\big(\tfrac{3}{13} + 0.01\big),$$

a contradiction. This shows that (5-17) is impossible.

Now assume (5-18). We want to show that $a_y = 1$ in this case. Thus, assume that $a_y \ge 2$. Using Corollary 5.2:4, we find $\sigma \in G$ such that $a(x^\sigma), a(z^\sigma) \ge 18$. Applying Proposition 3.2 to

$$x^m y^{-|n|} z^r (x^\sigma)^{-m} (y^\sigma)^{|n|} (z^\sigma)^{-r} = 1$$

with $A = 18$ and $\varepsilon = 0.01$, we obtain

$$m' \le \frac{|n'|}{\min\{18, a(y)\}} + \frac{m'}{18} + \frac{r'}{18} + 0.01m' \le m'\big(\tfrac{1}{2} + \tfrac{2}{18} + 0.01\big),$$

a contradiction. This shows that in the case (5-18) we must have (5-15).

Finally, let us assume (5-19). If one of a_y, a_z is 1 then we have (5-15), possibly after switching. If $a_y = a_z = 2$ then we have (5-16). Now let us assume that none of these is the case; that is, both a_y, a_z are ≥ 2 and one of them is ≥ 3. Again using Corollary 5.2, we may find $\sigma \in G$ such that $a(x^\sigma) \ge 30$. Applying Proposition 3.2, we obtain, in the same fashion as in the previous cases, the inequality

$$m' \le m'\big(\tfrac{1}{2} + \tfrac{1}{3} + \tfrac{1}{30} + 0.01\big),$$

a contradiction. The proposition is proved. □

We study cases (5-15) and (5-16) in Sections 5.3 and 5.4, respectively.

5.3. ***The dominant case.*** In this subsection we assume (5-15). Thus, we have

$$m > 0, \quad n < 0, \quad m' \ge \max\{|n'|, |r'|\}, \quad a_x = a_y = 1.$$

Since both x and y are dominant, we must have $e_x \ne e_y$. Exploring Table 2, we find ourselves in one of

the following cases:

$$\{e_x, e_y\} = \{1, 2\}, \quad e_z \in \{1, 2\}, \quad \Delta \equiv 1 \bmod 8, \tag{5-20}$$

$$\{e_x, e_y\} = \{1, 2\}, \quad e_z = 2, \quad \Delta \equiv 0 \bmod 4, \tag{5-21}$$

$$\{e_x, e_y\} = \{1, 3\}, \quad e_z = 3, \quad \Delta \equiv 1 \bmod 3, \tag{5-22}$$

$$\{e_x, e_y\} = \{2, 3\}, \quad e_z = 3, \quad \Delta \equiv 1 \bmod 24, \tag{5-23}$$

$$\{e_x, e_y\} = \{1, 4\}, \quad e_z = 4, \quad \Delta \equiv 1 \bmod 8, \tag{5-24}$$

$$\{e_x, e_y\} = \{1, 6\}, \quad e_z = 6, \quad \Delta \equiv 1 \bmod 24. \tag{5-25}$$

Remark 5.4. It is crucial that, in each of these cases, a nontrivial congruence condition is imposed on Δ. This allows us to use Propositions 2.16 and 2.17 to find Galois morphisms σ with well-controlled denominators of x^σ, y^σ, z^σ, which is needed for the strategy described in Section 5.3.1 to work.

Here are some more specific observations.

1. We have either $e_z = e_x$ or $e_z = e_y$, which implies that
$$a_z \neq 1. \tag{5-26}$$
2. In case (5-20) we have $K(x) = K(y) = K(z) = L$.
3. In cases (5-21)–(5-25) we have $K(z) = L$, and one of the fields $K(x)$ or $K(y)$ is L as well, while the other is a degree 2 subfield of L. More precisely:
   - If $e_x < e_y = e_z$ then $K(y) = L$ and $[L : K(x)] = 2$.
   - If $e_y < e_x = e_z$ then $K(x) = L$ and $[L : K(y)] = 2$.
4. Theorem 1.2 implies that in cases (5-21)–(5-25) we have $n = r$ when $e_x < e_y$, and $m = r$ when $e_x > e_y$.

5.3.1. *The strategy.* In each of cases (5-20)–(5-25) we apply the following strategy.

- Find possible values for a_z.
- Using Proposition 2.16 or 2.17, find several $\sigma \in G$ such that we can control the denominators
$$a(x^\sigma), \quad a(y^\sigma), \quad a(z^\sigma). \tag{5-27}$$
- For every such σ, and every possible choice of a_z and of denominators (5-27), Proposition 3.1 implies the linear equation
$$m' + n' + \frac{r'}{a_z} = \frac{m'}{a(x^\sigma)} + \frac{n'}{a(y^\sigma)} + \frac{r'}{a(z^\sigma)}.$$
With sufficiently many choices of σ, we may hope to have enough equations to conclude that $m' = n' = r' = 0$, a contradiction.

Practical implementation of this strategy differs from case to case. For instance, in cases (5-21)–(5-25) we have $m' = r'$ or $n' = r'$, so we need only two independent equations to succeed, while in case (5-20) three independent equations are needed.

Case (5-21) is somewhat special, because we get only one equation. To complete the proof in that case, we need to use an argument similar to that of Section 4.4.3.

Below details for all the cases follow.

5.3.2. *Cases* (5-22)–(5-25). In these cases $K(z) = L$, and one of the fields $K(x)$, $K(y)$ is also L while the other is a degree 2 subfield of L. In this subsection we make no use of the assumption $m' \geq |n'|$. Hence we may assume that $e_x < e_y = e_z$, in which case we have

$$K(y) = K(z) = L, \quad [L : K(x)] = 2. \tag{5-28}$$

Theorem 1.2 implies that in this case $n = r$, and that y, z are conjugate over $K(x)$:

$$y^\theta = z, \quad z^\theta = y, \tag{5-29}$$

where θ is the nontrivial element of $\mathrm{Gal}(L/K(x))$.

Let us specify the general strategy described in Section 5.3.1 for the cases (5-22)–(5-25).

1. Proposition 2.21 implies that x and y are ℓ-isogenous, where $\ell = e_x e_y$. Hence $x = x^\theta$ and $z = y^\theta$ are ℓ-isogenous as well. Using Corollary 2.20, we may now shortlist possible values of the denominator a_z. Precisely,

$$a_z \in \left(\frac{e_z}{e_x}\mathcal{Q}(\ell)\right) \cap \mathbb{Z}_{\geq 2},$$

where we use the notation $\lambda S = \{\lambda s : s \in S\}$. For instance, in case (5-23) we have $\ell = 6$, and

$$a_z \in \left(\tfrac{3}{2}\left\{\tfrac{1}{6}, \tfrac{2}{3}, \tfrac{3}{2}, 6\right\}\right) \cap \mathbb{Z}_{\geq 2} = \{9\}.$$

2. Propositions 2.16:1 and 2.17:1 imply the existence of morphisms σ_1 and σ_2 such that the three denominators $a(x)$ (which is 1), $a(x^{\sigma_1})$ and $a(x^{\sigma_2})$ are distinct. Precisely:

- If $\Delta_x \equiv 1 \bmod 3$ then 3 and 9 are denominators for Δ_x.
- If $\Delta_x \equiv 1 \bmod 8$ then 2 and 4 are denominators for Δ_x.

For instance, in case (5-23) we may find σ_1 and σ_2 to have

$$a(x^{\sigma_1}) = 3, \quad a(x^{\sigma_2}) = 9.$$

3. Using again Corollary 2.20, we may now shortlist the denominators $a(y^{\sigma_i})$ and $a(z^{\sigma_i})$. Precisely,

$$a(y^{\sigma_i}), a(z^{\sigma_i}) \in \left(a(x^{\sigma_i})\frac{e_z}{e_x}\mathcal{Q}(\ell)\right) \cap \mathbb{Z}_{\geq 1}.$$

For instance, in case (5-23) we have

$$a(y^{\sigma_1}), a(z^{\sigma_1}) \in \left(3 \cdot \tfrac{3}{2}\left\{\tfrac{1}{6}, \tfrac{2}{3}, \tfrac{3}{2}, 6\right\}\right) \cap \mathbb{Z}_{\geq 1} = \{3, 27\},$$
$$a(y^{\sigma_2}), a(z^{\sigma_2}) \in \left(9 \cdot \tfrac{3}{2}\left\{\tfrac{1}{6}, \tfrac{2}{3}, \tfrac{3}{2}, 6\right\}\right) \cap \mathbb{Z}_{\geq 1} = \{9, 81\}.$$

4. Now, Proposition 3.1 implies the system of linear equations

$$m' + \left(1 + \frac{1}{a(z)}\right) n' = \frac{m'}{a(x^{\sigma_i})} + \left(\frac{1}{a(y^{\sigma_i})} + \frac{1}{a(z^{\sigma_i})}\right) n' \quad (i = 1, 2). \tag{5-30}$$

(Recall that $n' = r'$). Solving the system, we find that $m' = n' = 0$ in every instance, a contradiction. This shows the impossibility of cases (5-22)–(5-25).

For instance, in case (5-23), equations (5-30) become

$$m' + \left(1 + \tfrac{1}{9}\right) n' = \tfrac{1}{3} m' + \lambda n', \quad \lambda \in \left\{\tfrac{2}{3}, \tfrac{1}{3} + \tfrac{1}{27}, \tfrac{2}{27}\right\},$$
$$m' + \left(1 + \tfrac{1}{9}\right) n' = \tfrac{1}{9} m' + \mu n', \quad \mu \in \left\{\tfrac{2}{9}, \tfrac{1}{9} + \tfrac{1}{81}, \tfrac{2}{81}\right\},$$

so nine systems in total, each having $m' = n' = 0$ as its only solution.

The numerical data obtained following these steps can be found in Table 3. We have 390 linear systems to solve: nine systems in cases (5-22), (5-23), 72 systems in case (5-24), and 300 systems in case (5-25). Doing this by hand is impractical, and we used a PARI script for composing Table 3 and solving the systems.

Remark 5.5. Using Propositions 2.16 and 2.17, we can further refine the lists of possible denominators for z, y^{σ_i} and z^{σ_i}. For instance, if the discriminant $\Delta_y = \Delta_z$ is $\equiv 0 \bmod 9$ then it cannot have denominators divisible by 3 but not by 9. Thus, in case (5-23), number 3 cannot be the denominator of y^{σ_1} or of z^{σ_1}, and so we must have $a(y^{\sigma_1}) = a(z^{\sigma_1}) = 27$. Arguments of this kind, used systematically, allow one to decimate the number of systems to solve.

However, the computational time for solving our systems being insignificant, we prefer to disregard this observation.

5.3.3. *Case* (5-21). This case is similar to cases (5-22)–(5-25), but somewhat special. Let us reproduce our data for the reader's convenience:

$$\{e_x, e_y\} = \{1, 2\}, \quad e_z = 2, \quad \Delta \equiv 0 \bmod 4, \quad a_x = a_y = 1.$$

We may again assume that $e_x < e_y$, which means now that $e_x = 1$ and $e_y = 2$, and we again have (5-28) and (5-29). Step 1 of the strategy described in Section 5.3.2 works here as well: we prove that each

case	$\Delta \equiv$	e_x	e_y	ℓ	a_z	$a(x^{\sigma_1})$	$a(y^{\sigma_1}), a(z^{\sigma_1})$	$a(x^{\sigma_2})$	$a(y^{\sigma_2}), a(z^{\sigma_2})$	no. of systems
(5-22)	1 mod 3	1	3	3	9	3	$\in \{3, 27\}$	9	$\in \{9, 81\}$	9
(5-23)	1 mod 24	2	3	6	9	3	$\in \{3, 27\}$	9	$\in \{9, 81\}$	9
(5-24)	1 mod 8	1	4	4	$\in \{4, 16\}$	2	$\in \{2, 8, 32\}$	4	$\in \{4, 16, 64\}$	72
(5-25)	1 mod 24	1	6	6	$\in \{4, 9, 36\}$	2	$\in \{2, 8, 18, 72\}$	3	$\in \{3, 12, 27, 108\}$	300
(5-21)	4 mod 32	1	2	2	4	8	$\in \{8, 32\}$	16	$\in \{16, 64\}$	9

Table 3. Cases (5-22)–(5-25) and case (5-21) with $\Delta \equiv 4 \bmod 32$.

of y, z is 2-isogenous to x, which allows us to determine that $a_z = 4$. For later use, let us note that

$$\tau_x = \frac{\sqrt{\Delta}}{2}, \quad \tau_y = \sqrt{\Delta}, \quad \tau_z = \frac{b' + \sqrt{\Delta}}{4}, \tag{5-31}$$

where

$$b' = \begin{cases} 0 & \text{if } \Delta \equiv 4 \bmod 8, \\ 2 & \text{if } \Delta \equiv 0 \bmod 8. \end{cases} \tag{5-32}$$

The rest of the argument splits into two subcases. If $\Delta \equiv 4 \bmod 32$ then we may proceed as in Section 5.3.2. Proposition 2.17 implies that there exist $\sigma_1, \sigma_2 \in G$ such that $a(x^{\sigma_1}) = 8$ and $a(x^{\sigma_2}) = 16$. As before, we can now determine possible denominators of $y^{\sigma_i}, z^{\sigma_i}$ (see the bottom line of Table 3) and solve the resulting systems (5-30), concluding that $m = n = 0$.

Now assume that $\Delta \not\equiv 4 \bmod 32$. In this case 2 or 4 is a denominator for Δ; see Proposition 2.17:6. Since $\Delta_x = \Delta$, there exists $\sigma \in G$ such that $a(x^\sigma) \in \{2, 4\}$. We claim that

$$y^\sigma, z^\sigma \notin \{y, z\}. \tag{5-33}$$

Indeed, if, say, $y^\sigma = y$ then $\sigma = \mathrm{id}$ because $L = K(y)$; but $x^\sigma \neq x$, a contradiction. For the same reason, $z^\sigma \neq z$. Now assume that $y^\sigma = z$. Theorem 1.2 implies that y and z are conjugate over $K(x)$. Hence there exists $\theta \in G$ such that

$$x^\theta = x, \quad y^\theta = z, \quad z^\theta = y.$$

Then $z^{\theta\sigma} = z$, and, as before, $\theta\sigma = \mathrm{id}$, which is again a contradiction because $x^{\theta\sigma} = x^\sigma \neq x$. Similarly one shows that $z^\sigma \neq y$. This proves (5-33).

The cases $a(x^\sigma) = 2$ and $a(x^\sigma) = 4$ are very similar, but each one has some peculiarities, so we consider them separately.

Assume that $a(x^\sigma) = 2$. Then $a(y^\sigma) = a(z^\sigma) = 8$. Proposition 3.1 gives

$$m' + n'\left(1 + \tfrac{1}{4}\right) = \tfrac{1}{2}m' + n'\left(\tfrac{1}{8} + \tfrac{1}{8}\right),$$

which is just $m' = -2n'$. Hence $m = -4n$. It follows that $(x/x^\sigma)^4 (y^\sigma/y)(z^\sigma/z)$ is a root of unity. Since the roots of unity in L are of order dividing 24 (see Corollary 2.7), we obtain

$$\left(x^4 (x^\sigma)^{-4} y^{-1} z^{-1} y^\sigma z^\sigma\right)^{24} = 1. \tag{5-34}$$

Now we are going to argue as in Section 4.4.3. This means:

- We give explicit expressions for the τ- and q-parameters of all the six singular moduli occurring in (5-34). The τ-parameters for x, y, z are already given in (5-31), so we need to determine them only for $x^\sigma, y^\sigma, z^\sigma$.
- Taking the logarithm of (5-34), we deduce that a certain linear combination of logarithms is a multiple of $\pi i/12$.
- Using the q-expansion from Corollary 3.5, we obtain a contradiction.

Note, however, that in Section 4.4.3 the first order expansion (3-18) was sufficient, while now we would need the second order expansion (3-19).

Since y, z, x^σ are distinct and 2-isogenous to x, we must have, in addition to (5-31), (5-32),

$$\tau(x^\sigma) = \frac{b_2 + \sqrt{\Delta}}{4}, \quad \text{where} \quad b_2 = \begin{cases} 0 & \text{if } b' = 2, \\ 2 & \text{if } b' = 0. \end{cases} \tag{5-35}$$

Since x, y^σ, z^σ are distinct and 2-isogenous to x^σ, we must have

$$\{\tau(y^\sigma), \tau(z^\sigma)\} = \left\{ \frac{b_2+\sqrt{\Delta}}{8}, \frac{b_2'+\sqrt{\Delta}}{8} \right\}, \quad b_2' \in \{b_2+4, b_2-4\}.$$

Set $t = e^{-\pi|\Delta|^{1/2}/4}$ and $\xi = e^{\pi i b_2/4}$. Note that $\xi \in \{1, i\}$, and that

$$e^{\pi i b'/2} = -\xi^2, \quad e^{\pi i b_2'/4} = -\xi.$$

We obtain

$$e^{2\pi i \tau_x} = t^4, \quad e^{2\pi i \tau_y} = t^8, \quad e^{2\pi i \tau_z} = -\xi^2 t^2, \quad e^{2\pi i \tau(x^\sigma)} = \xi^2 t^2, \quad \{e^{2\pi i \tau(y^\sigma)}, e^{2\pi i \tau(z^\sigma)}\} = \{\xi t, -\xi t\}.$$

Taking the logarithm of (5-34), we obtain

$$4\log(t^4 x) - 4\log(\xi^2 t^2 x^\sigma) - \log(t^8 y) - \log(-\xi^2 t^2 z) + \log(-\xi t \cdot \xi t \cdot y^\sigma \cdot z^\sigma) \in \frac{\pi i}{12}\mathbb{Z}.$$

The q-expansion (3-19) from Corollary 3.5 implies that for some $k \in \mathbb{Z}$ we have

$$\frac{\pi i}{12} k = -162000\xi^2 t^2 + O_1(10^{10} t^3).$$

This easily leads to a contradiction, exactly as in Section 4.4.3.

Now assume that $a(x^\sigma) = 4$. Since x^σ is 2-isogenous to y^σ and to z^σ, Corollary 2.20 and Proposition 2.17 imply that $a(y^\sigma), a(z^\sigma) \in \{4, 16\}$. Note however that

$$\Delta_y = \Delta_z = 4\Delta \equiv 0 \bmod 16,$$

and Proposition 2.17:5 implies that there may be at most one singular modulus of this discriminant with denominator 4. But we already have $a_z = 4$, and so neither of $a(y^\sigma), a(z^\sigma)$ can equal 4 by (5-33).

Thus, $a(y^\sigma) = a(z^\sigma) = 16$. Proposition 3.1 gives

$$m' + n'\left(1 + \tfrac{1}{4}\right) = \tfrac{1}{4}m' + n'\left(\tfrac{1}{16} + \tfrac{1}{16}\right),$$

which is $m = -3n$. Arguing as before, we obtain

$$\left(x^3 (x^\sigma)^{-3} y^{-1} z^{-1} y^\sigma z^\sigma\right)^{24} = 1. \tag{5-36}$$

We have

$$\tau(x^\sigma) = \frac{b_4 + \sqrt{\Delta}}{8},$$

and we want to specify this b_4. Since $(b_4)^2 \equiv \Delta \bmod 16$, we must have

$$\Delta \equiv 0, 4 \bmod 16 \quad \text{and} \quad b_4 = \begin{cases} 0 & \text{if } \Delta \equiv 16 \bmod 32, \\ 4 & \text{if } \Delta \equiv 0 \bmod 32, \\ \pm 2 & \text{if } \Delta \equiv 4 \bmod 16. \end{cases}$$

Hence,

$$b' \in \{b_4 + 2, b_4 - 2\}.$$

Finally, since both y^σ, z^σ have denominators 16 and are 2-isogenous to x^σ, we have

$$\{\tau(y^\sigma), \tau(z^\sigma)\} = \left\{ \frac{b_4+\sqrt{\Delta}}{16}, \frac{b_4'+\sqrt{\Delta}}{16} \right\} \quad \text{and} \quad b_4' \in \{b_4 + 8, b_4 - 8\}.$$

Set $t = e^{-\pi|\Delta|^{1/2}/8}$ and $\xi = e^{\pi i b_4/8}$. Note that $\xi \in \{1, i, e^{\pm \pi i/4}\}$, and that

$$e^{\pi i b'/4} = \pm i \xi^2, \quad e^{\pi i b_4'/8} = -\xi.$$

We obtain

$$e^{2\pi i \tau_x} = t^8, \quad e^{2\pi i \tau_y} = t^{16}, \quad e^{2\pi i \tau_z} = \varepsilon i \xi^2 t^4, \quad e^{2\pi i \tau(x^\sigma)} = \xi^2 t^2, \quad \left\{ e^{2\pi i \tau(y^\sigma)}, e^{2\pi i \tau(z^\sigma)} \right\} = \{\xi t, -\xi t\},$$

where $\varepsilon \in \{1, -1\}$. Taking the logarithm of (5-36), we obtain

$$3\log(t^8 x) - 3\log(\xi^2 t^2 x^\sigma) - \log(t^{16} y) - \log(-\varepsilon i \xi^2 t^4 z) + \log(-\xi t \cdot \xi t \cdot y^\sigma \cdot z^\sigma) \in \frac{\pi i}{12}\mathbb{Z}.$$

The q-expansion (3-19) implies that for some $k \in \mathbb{Z}$ we have

$$\frac{\pi i}{12} k = -162000 \xi^2 t^2 + O_1(10^{10} t^3),$$

which again leads to a contradiction.

5.3.4. *Case* (5-20). We want to adapt the procedure described in Section 5.3.2 to this case. We reproduce our data for the reader's convenience:

$$\{e_x, e_y\} = \{1, 2\}, \quad e_z \in \{1, 2\}, \quad \Delta \equiv 1 \bmod 8, \quad a_x = a_y = 1. \tag{5-37}$$

The singular moduli x and y are 2-isogenous by Proposition 2.21. However, now we have $K(x) = K(y) = K(z) = L$, which means that there does not exist $\theta \in G$ with the properties $x^\theta = x$ and $y^\theta = z$. Hence, a priori we have no control of the degree of isogeny between x and z. To gain such control we need to determine the denominator a_z.

Proposition 5.6. *Assume* (5-37). *Then* $(e_x, e_y) = (1, 2)$ *and*

$$\textit{either} \quad e_z = 1, \quad a_z = 4 \quad \textit{or} \quad e_z = 2, \quad a_z = 3. \tag{5-38}$$

The proof consists of several steps. To start with, we eliminate the subcase $(e_x, e_y) = (2, 1)$.

Proposition 5.7. *In case* (5-37) *we must have* $(e_x, e_y) = (1, 2)$.

Proof. Note that $a_z > 1$; see (5-26). We will assume that $(e_x, e_y) = (2, 1)$ and get a contradiction.

Since $\Delta_y = \Delta \equiv 1 \bmod 8$, Proposition 2.17 implies that there are two elements $\sigma \in G$ such that $a(y^\sigma) = 2$. Since $L = K(z)$, at most one of them may satisfy $a(z^\sigma) = 1$. Hence there exists $\sigma \in G$ such that $a(y^\sigma) = 2$ and $a(z^\sigma) \geq 2$.

Since x and y are 2-isogenous, we must have $a(x^\sigma) \in \{2, 8\}$. But 2 is not a denominator for $\Delta_x = 4\Delta$ by Proposition 2.17, which implies that $a(x^\sigma) = 8$. Thus, we have found σ such that

$$a(x^\sigma) = 8, \quad a(y^\sigma) = 2, \quad a(z^\sigma) \geq 2.$$

We now want to derive a contradiction in each of the following cases:

$$\text{One of } a(z), a(z^\sigma) \text{ is } 2. \tag{5-39}$$

$$\text{Both } a(z), a(z^\sigma) \text{ are at least } 3. \tag{5-40}$$

Assume (5-39). Then $e_z = 1$, again by the same reason: 2 is not a denominator for 4Δ. Hence there exists $\theta \in G$ such that $y^\theta = z$. Since y, y^σ are 2-isogenous, so are $z = y^\theta$ and $z^\sigma = y^{\theta\sigma} = y^{\sigma\theta}$. It follows that if one of the denominators $a(z), a(z^\sigma)$ is 2, the other must be 4. Proposition 3.1 now implies that

$$m' + n' + \frac{r'}{a'} = \frac{m'}{8} + \frac{n'}{2} + \frac{r'}{a''} \quad \text{and} \quad \{a', a''\} = \{2, 4\}.$$

Hence

$$\frac{7}{8}m' = \frac{|n'|}{2} + r'\left(\frac{1}{a''} - \frac{1}{a'}\right) \leq m'\left(\frac{1}{2} + \frac{1}{4}\right),$$

a contradiction. This eliminates (5-39).

In case (5-40) we use Proposition 3.2 with $A = 9$ to obtain

$$m' + \frac{|n'|}{2} \leq \frac{m'}{8} + |n'| + \frac{|r'|}{d} + 0.01m' \quad \text{and} \quad d = \begin{cases} \min\{9, a(z^\sigma)\}, & r > 0, \\ \min\{9, a(z)\}, & r < 0. \end{cases}$$

Since $d \geq 3$, we obtain

$$\left(\frac{7}{8} - 0.01\right)m' \leq \frac{|n'|}{2} + \frac{|r'|}{3} \leq m'\left(\frac{1}{2} + \frac{1}{3}\right),$$

a contradiction. This rules (5-40) out as well. The proposition is proved. □

Next, we show the impossibility of $a_z = 2$.

Proposition 5.8. *In case (5-37) we must have $a_z \geq 3$.*

Proof. We already know that $a_z \geq 2$ and that $(e_x, e_y) = (1, 2)$. We also note the statement is immediate for $e_z = 2$, because 2 is not a denominator for 4Δ; see Proposition 2.17. Thus, let us assume that

$$(e_x, e_y, e_z) = (1, 2, 1), \quad a_z = 2,$$

and show that this is impossible.

Arguing as in the proof of Proposition 5.7 but with the roles of x and y interchanged, we find σ

satisfying

$$a(x^\sigma) = 2, \quad a(y^\sigma) = 8, \quad a(z^\sigma) \geq 2.$$

Since x, z are 2-isogenous, we have $a(z^\sigma) \in \{1, 4\}$, and we must have $a(z^\sigma) = 4$ because $a(z^\sigma) \geq 2$.

Next, let $\theta \in G$ be defined by $z^\theta = x$. Since x, z are 2-isogenous, we must have $a(x^\theta) = 2$, which implies that $a(y^\theta) = 8$.

Applying Proposition 3.1 to the relation

$$(x^\sigma)^m (y^\sigma)^n (z^\sigma)^r = (x^\theta)^m (y^\theta)^n (z^\theta)^r,$$

we obtain

$$\frac{m'}{2} + \frac{n'}{8} + \frac{r'}{4} = \frac{m'}{2} + \frac{n'}{8} + \frac{r'}{1},$$

which implies $r = 0$, a contradiction. □

We also need to know that $|n'|$ is not much smaller than m'.

Proposition 5.9. *When $r > 0$ we have $|n'| > 0.87m'$. When $r < 0$ and $a_z \geq a$ we have $|n'| > \lambda(a)m'$, where*

$$\lambda(a) = 0.956 - \frac{1}{\min\{30, a\}}.$$

Here are lower bounds for $\lambda(a)$ for some values of a that will emerge below:

a	3	5	6	24	30
$\lambda(a)$	> 0.62	> 0.75	> 0.78	> 0.91	> 0.92

Proof. When $r > 0$ we use Corollary 5.2 to find σ such that $a(x^\sigma), a(z^\sigma) \geq 18$. Now Proposition 3.2 gives

$$m' \leq |n'| + \frac{m'}{18} + \frac{r'}{18} + 0.01m' \leq |n'| + m'\Big(\frac{2}{18} + 0.01\Big),$$

which implies $|n'| > 0.87m'$.

When $r < 0$ we use Corollary 5.2 to find σ such that $a(x^\sigma) \geq 30$. When $a_z \geq a$, we obtain

$$m' \leq |n'| + \frac{m'}{30} + \frac{|r'|}{\min\{30, a\}} + 0.01m' \leq |n'| + m'\left(\frac{1}{30} + \frac{1}{\min\{30, a\}} + 0.01\right),$$

which implies $|n'| > \lambda(a)m'$. □

Proof of Proposition 5.6. The proof is similar to that of Proposition 5.7, but with the roles of x and y interchanged. This means that, instead of the inequality $m' \geq |n'|$, we have to use weaker inequalities from Proposition 5.9. This is why we cannot rule out (5-38).

We already know that $a_z \geq 3$ and that $(e_x, e_y) = (1, 2)$. We also note that 4 is not a denominator for 4Δ; see Proposition 2.17. Hence it suffices to show that each of the cases

$$e_z = 1, \quad a_z \geq 3, \quad a_z \neq 4, \tag{5-41}$$

$$e_z = 2, \quad a_z \geq 5, \tag{5-42}$$

leads to a contradiction. As in the proof of Proposition 5.8, we fix $\sigma \in G$ satisfying

$$a(x^\sigma) = 2, \quad a(y^\sigma) = 8, \quad a(z^\sigma) \geq 2.$$

Assume (5-41). As in the proof of Proposition 5.7, we show that z, z^σ are 2-isogenous. Hence $\{a(z), a(z^\sigma)\} = \{a', 2a'\}$, where $a' \geq 3$. If $a' \geq 6$ then, using Proposition 3.2, we obtain

$$\frac{m'}{2} + |n'| \leq m' + \frac{|n'|}{8} + \frac{|r'|}{6} + 0.01m',$$

which implies that

$$|n'| \leq \tfrac{8}{7} m' \left(\tfrac{1}{2} + \tfrac{1}{6} + 0.01\right) < 0.78m',$$

contradicting the lower bound $|n'| > 0.78m'$ from Proposition 5.9.

If $a' \in \{3, 4, 5\}$ then Proposition 3.1 gives

$$m' + n' + \frac{r'}{a(z)} = \frac{m'}{2} + \frac{n'}{8} + \frac{r'}{a(z^\sigma)}.$$

This can be rewritten as

$$|n'| = \frac{8}{7}\left(\frac{m'}{2} + r'\left(\frac{1}{a(z)} - \frac{1}{a(z^\sigma)}\right)\right), \tag{5-43}$$

which implies

$$|n'| \leq \tfrac{8}{7} m' \left(\tfrac{1}{2} + \tfrac{1}{6}\right) < 0.77m', \tag{5-44}$$

When $r > 0$ this contradicts the lower bound $|n'| > 0.87m'$ from Proposition 5.9. When $r < 0$ and $a_z = 2a'$ this contradicts the lower bound $|n'| > 0.78m'$ from Proposition 5.9. Finally, when $r < 0$ and $a_z = a'$, we deduce from (5-43) the sharper upper bound $|n'| \leq \frac{4}{7}m'$, contradicting the lower bound $|n'| \geq 0.62m'$ from Proposition 5.9. This shows the impossibility of (5-41).

Now let us assume (5-42). Proposition 3.2 implies that

$$\frac{m'}{2} + |n'| \leq m' + \frac{|n'|}{8} + \frac{|r'|}{d} + 0.01m' \quad \text{and} \quad d = \begin{cases} \min\{9, a(z)\} & \text{if } r > 0, \\ \min\{9, a(z^\sigma)\} & \text{if } r < 0. \end{cases}$$

If $r > 0$ then $d \geq 5$, and we obtain

$$|n'| \leq \tfrac{8}{7} m' \left(\tfrac{1}{2} + \tfrac{1}{5} + 0.01\right) < 0.82m',$$

contradicting the lower bound $|n'| > 0.87m'$ from Proposition 5.9.

If $r < 0$ and $d \geq 8$ then

$$|n'| \leq \tfrac{8}{7} m' \left(\tfrac{1}{2} + \tfrac{1}{8} + 0.01\right) < 0.73m',$$

contradicting the lower bound $|n'| > 0.75m'$ from Proposition 5.9.

Thus,

$$r < 0, \quad 3 \leq a(z^\sigma) \leq 7.$$

Since $e_z = 2$, we must have $a(z^\sigma) = p \in \{3, 5, 7\}$. Hence y^σ and z^σ are $8p$-isogenous, and so are y and z. It follows that $a_z = 8p \geq 24$, and Proposition 5.9 implies the lower bound $|n'| > 0.91m'$. On the other

i	$a(x^{\sigma_i})$	$a(y^{\sigma_i})$	$a(z^{\sigma_i})$
1	2	8	$\in \{2, 8\}$
2	4	16	1
3	$\in \{2, 8\}$	$\in \{8, 32\}$	2

i	$a(x^{\sigma_i})$	$a(y^{\sigma_i})$	$a(z^{\sigma_i})$
1	2	8	24
2	3	3	1
3	$\in \{6, 24\}$	24	8

Table 4. Denominators for case (5-20). The table on the left refers to $(e_x, e_y, e_z) = (1, 2, 1)$ and $a_z = 4$; there are 8 systems in total. On the right, $(e_x, e_y, e_z) = (1, 2, 2)$ and $a_z = 3$, with 2 systems in total.

hand, Proposition 3.1 implies that

$$m' + n' + \frac{r'}{8p} = \frac{m'}{2} + \frac{n'}{8} + \frac{r'}{p},$$

which yields

$$|n'| = \frac{4m'}{7} + \frac{|r'|}{p} < 0.91\, m',$$

a contradiction. This shows impossibility of (5-42). The proposition is proved. □

Now it is easy to dispose of case (5-20), alias (5-37). We define σ_1 as σ from the proof of Proposition 5.6; that is, $a(x^{\sigma_1}) = 2$ and $a(z^{\sigma_1}) \neq 1$. Next, we define σ_2 from

$$z^{\sigma_2} = \begin{cases} x & \text{if } e_z = 1, \\ y & \text{if } e_z = 2. \end{cases}$$

Finally, we set $\sigma_3 = \sigma_2\sigma_1$.

Using Proposition 2.17 and Corollary 2.20, we calculate the possible denominators; see Table 4. A verification shows that, in each case, the system of 3 linear equations

$$m' + n' + \frac{r'}{a_z} = \frac{m'}{a(x^{\sigma_i})} + \frac{n'}{a(y^{\sigma_i})} + \frac{r'}{a(z^{\sigma_i})} \quad (i = 1, 2, 3) \tag{5-45}$$

has only the trivial solution.

5.4. ***The subdominant case.*** In this subsection we assume (5-16). Thus, we have

$$m > 0, \quad n, r < 0, \quad m' \geq \max\{|n'|, |r'|\}, \quad a_x = 1, \quad a_y = a_z = 2.$$

To start with, note that

$$e_y = e_z \quad \text{and} \quad \Delta_y = \Delta_z \equiv 1 \bmod 8. \tag{5-46}$$

Indeed, among the three numbers e_x, e_y, e_z there are only two distinct integers, see Table 2. If $e_y \neq e_z$ then, switching, if necessary, x and y, we may assume that $e_x = e_y$. Hence $K(x) = K(y)$, and we have one of two possibilities:

$$K(x) = K(y) = K(z) = L \tag{5-47}$$

or

$$K(x) = K(y) = L, \quad [L : K(z)] = 2.$$

In the latter case we must have $m = n$ by Theorem 1.2, which is impossible because $m > 0$ and $n < 0$. Thus, we have (5-47). Lemma 2.25 now implies that $e_z = 2$ and $\Delta_x = \Delta_y = \Delta \equiv 1 \bmod 8$. But then $\Delta_z \equiv 4 \bmod 32$, and we cannot have $a_z = 2$ by Proposition 2.17:4. Thus, $e_x = e_y$ is impossible, which proves that $e_y = e_z$. Now Proposition 2.17:2 implies that $\Delta_y = \Delta_z \equiv 1 \bmod 8$, which completes the proof of (5-46).

Exploring Table 2 and taking note of (5-46), we end up with one of the following cases:

$$e_x \in \{1, 2\}, \quad e_y = e_z = 1, \quad \Delta \equiv 1 \bmod 8, \quad L = K(x) = K(y) = K(z); \tag{5-48}$$

$$e_x \in \{1, 2\}, \quad e_y = e_z = 3, \quad \Delta \equiv 1 \bmod 24, \quad [L : K(x)] = 2, \quad n = r. \tag{5-49}$$

We cannot have $e_y = e_z = 4$ or $e_y = e_z = 6$, because in these cases $\Delta_y = \Delta_z \equiv 0 \bmod 4$, contradicting (5-46).

Each of the cases (5-48) and (5-49) can be disposed of using the strategy described in Section 5.3.1; moreover, the very first step of that strategy can be skipped, because a_z is already known.

Case (5-48) is analogous to case (5-20), but is much simpler, because, as indicated above, we already know a_z. We define $\sigma_1, \sigma_2, \sigma_3$ by

$$a(y^{\sigma_1}) = 1, \quad a(z^{\sigma_2}) = 1, \quad a(y^{\sigma_3}) = 8.$$

There can be several candidates for σ_3, we just pick one of them. The possible denominators, determined using Corollary 2.20 and Proposition 2.17:4, are given in Table 5. A verification with PARI shows that each of the 12 possible systems

$$m' + \frac{n'}{2} + \frac{r'}{2} = \frac{m'}{a(x^{\sigma_i})} + \frac{n'}{a(y^{\sigma_i})} + \frac{r'}{a(z^{\sigma_i})} \quad (i = 1, 2, 3)$$

has only the trivial solution $m' = n' = r' = 0$.

In case (5-49) we have $n = r$ (and also $n' = r'$), and so we need only σ_1 and σ_2. We do as in Section 5.3.2. Since $\Delta_x \equiv 1 \bmod 3$, we can find σ_1, σ_2 satisfying $a(x^{\sigma_1}) = 3$ and $a(y^{\sigma_2}) = 9$. Defining

$$\ell = \begin{cases} 6 & \text{when } e_x = 1, \\ 12 & \text{when } e_x = 2, \end{cases}$$

a quick verification shows that singular moduli x, y are ℓ-isogenous, and so are x, z. Using Corollary 2.20 and Proposition 2.16:2, we determine the possible denominators: in both cases $e_x = 1$ and $e_x = 2$ we find

$$a(y^{\sigma_1}), a(z^{\sigma_1}) = 54, \quad a(y^{\sigma_2}), a(z^{\sigma_2}) \in \{18, 162\}.$$

i	$a(x^{\sigma_i})$	$a(y^{\sigma_i})$	$a(z^{\sigma_i})$
1	2	1	4
2	2	4	1
3	$\in \{4, 16\}$	8	$\in \{2, 8, 32\}$

i	$a(x^{\sigma_i})$	$a(y^{\sigma_i})$	$a(z^{\sigma_i})$
1	8	1	4
2	8	4	1
3	$\in \{16, 64\}$	8	$\in \{2, 8, 32\}$

Table 5. Denominators for case (5-48), with (e_x, e_y, e_z) taking the values (1, 1, 1) (left) and (2, 1, 1) (right). In either case, there are 6 systems in total.

It follows that m', n' satisfy one of the three linear systems

$$\begin{cases} m' + n'\left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{3}m' + \left(\frac{1}{54} + \frac{1}{54}\right)n', \\ m' + n'\left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{9}m' + \lambda n', \end{cases} \qquad \text{where } \lambda \in \left\{\tfrac{1}{18} + \tfrac{1}{18},\ \tfrac{1}{18} + \tfrac{1}{162},\ \tfrac{1}{162} + \tfrac{1}{162}\right\}.$$

A verification shows that each of these systems has only the trivial solution $m' = n' = 0$. This completes the proof of Theorem 1.1 for equal fundamental discriminants.

5.5. ***Distinct fundamental discriminants.*** We are left with the case when the fundamental discriminants D_x, D_y, D_z are not all equal. We may assume that $|\Delta_z| \geq |\Delta_y| \geq |\Delta_x|$. In particular, $|\Delta_z| \geq 10^{10}$ and $\Delta_z \neq \Delta_x$. Theorem 1.2 and Lemma 2.22 imply that $\mathbb{Q}(y) = \mathbb{Q}(y^n) = \mathbb{Q}(x^m z^r) = \mathbb{Q}(x, z)$, and so

$$\mathbb{Q}(x), \mathbb{Q}(z) \subset \mathbb{Q}(y). \tag{5-50}$$

Theorem 1.2 and Lemma 2.22 imply that $\mathbb{Q}(x) = \mathbb{Q}(x^m) = \mathbb{Q}(y^n z^r)$ is a subfield of $\mathbb{Q}(y, z)$ of degree at most 2. Since $z \in \mathbb{Q}(y)$, this implies that

$$[\mathbb{Q}(y) : \mathbb{Q}(x)] \leq 2.$$

Unfortunately, we cannot claim similarly that $[\mathbb{Q}(y) : \mathbb{Q}(z)] \leq 2$, because we do not know whether the singular moduli x, y satisfy the hypotheses of Theorem 1.2.

The rest of the proof splits into two cases: $D_x \neq D_y$ and $D_y \neq D_z$.

5.5.1. *The case $D_x \neq D_y$.* Since $[\mathbb{Q}(y) : \mathbb{Q}(x)] \leq 2$, Corollary 2.13 implies that $[\mathbb{Q}(y) : \mathbb{Q}] \leq 32$. It follows that $h(\Delta_z) = [\mathbb{Q}(z) : \mathbb{Q}] \leq 32$ as well. This contradicts Proposition 2.1 because $|\Delta_z| \geq 10^{10}$.

5.5.2. *The case $D_y \neq D_z$.* Since $z \in \mathbb{Q}(y)$, the field $\mathbb{Q}(z)$ must be 2-elementary by Proposition 2.8. Hence the proof in this case will be complete if we show either that

$$\rho_2(\Delta_z) \leq 6 \tag{5-51}$$

or that

$$[\mathbb{Q}(y) : \mathbb{Q}(z)] \leq 2. \tag{5-52}$$

Recall that $\rho_2(\,\cdot\,)$ is the 2-rank; see Section 2.1.2.

Indeed, assume that (5-51) holds. Since $\mathbb{Q}(z)$ is 2-elementary, we have $h(\Delta_z) = 2^{\rho_2(\Delta_z)} \leq 64$, contradicting Proposition 2.1.

Similarly, if (5-52) holds then $h(\Delta_z) \leq 16$ by Corollary 2.13, again contradicting Proposition 2.1.

We will show that, depending on the size of Δ_y, one of (5-51) or (5-52) holds.

If $|\Delta_y| \geq 10^8$, then Theorem 1.2 applies to the singular moduli x, y. It follows that $\mathbb{Q}(z) = \mathbb{Q}(z^r) = \mathbb{Q}(x^m y^n)$ is a subfield of $\mathbb{Q}(x, y)$ of degree at most 2. Since $x \in \mathbb{Q}(y)$, we obtain $[\mathbb{Q}(y) : \mathbb{Q}(z)] \leq 2$, which is (5-52).

Next, let us assume that $10^6 \leq |\Delta_y| \leq 10^8$. If $\Delta_y \not\equiv 4 \bmod 32$ then Theorem 1.2 again applies to the singular moduli x, y, and we may argue as above, obtaining (5-52).

If $\Delta_y \equiv 4 \bmod 32$, then $\rho_2(\Delta_y) = \omega(\Delta_y) - 2$; see Proposition 2.3. Since

$$10^8 < 4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 446185740,$$

we have $\omega(\Delta_y) \le 8$. Hence $\rho_2(\Delta_y) \le 6$. Now let $K = \mathbb{Q}(\sqrt{\Delta_y})$ be the CM field of y. Since $\mathbb{Q}(z)$ is 2-elementary, K is not contained in $\mathbb{Q}(z)$ by Proposition 2.18. Since both K and $\mathbb{Q}(z)$ are Galois extensions of $\mathbb{Q}$, the group $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ is isomorphic to $\mathrm{Gal}(K(z)/K)$, which is a quotient group of $\mathrm{Gal}(K(y)/K)$. In particular,

$$\rho_2(\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})) \le \rho_2(\mathrm{Gal}(K(y)/K)) \le 6,$$

which is (5-51).

Finally, let us assume that $|\Delta_y| \le 10^6$. Since

$$10^6 < 4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 1021020,$$

we have $\rho_2(\Delta_y) \le \omega(\Delta) \le 6$, again by Proposition 2.3. As we have seen, this implies (5-51). Theorem 1.1 is proved.

Acknowledgments

We thank Guy Fowler and the referee for many comments that helped us to correct inaccuracies and improve the presentation. We also thank Francesco Amoroso, Margaret Bilu, Igor Rapinchuk and Anatoly Vorobey for useful suggestions. Finally, we thank Bill Allombert and Amalia Pizarro, who allowed us to borrow Proposition 2.11 from [1].

All calculations were performed using PARI [19]. We thank Bill Allombert and Karim Belabas for the PARI tutorial. The reader may consult https://github.com/yuribilu/multiplicative to view the PARI scripts used for this article.

References

[1] B. Allombert, Y. Bilu, and A. Pizarro-Madariaga, "CM-points on straight lines", 2014. An early version of [2]. arXiv 1406.1274v1

[2] B. Allombert, Y. Bilu, and A. Pizarro-Madariaga, "CM-points on straight lines", pp. 1–18 in *Analytic number theory*, Springer, 2015. MR

[3] F. Amoroso and U. Zannier, "A uniform relative Dobrowolski's lower bound over abelian extensions", *Bull. Lond. Math. Soc.* **42**:3 (2010), 489–498. MR

[4] Y. André, "Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire", *J. Reine Angew. Math.* **505** (1998), 203–208. MR

[5] Y. Bilu, D. Masser, and U. Zannier, "An effective 'theorem of André' for CM-points on a plane curve", *Math. Proc. Cambridge Philos. Soc.* **154**:1 (2013), 145–152. MR

[6] Y. Bilu, F. Luca, and A. Pizarro-Madariaga, "Rational products of singular moduli", *J. Number Theory* **158** (2016), 397–410. MR

[7] Y. Bilu, F. Luca, and D. Masser, "Collinear CM-points", *Algebra Number Theory* **11**:5 (2017), 1047–1087. MR

[8] Y. Bilu, B. Faye, and H. Zhu, "Separating singular moduli and the primitive element problem", *Q. J. Math.* **71**:4 (2020), 1253–1280. MR

[9] Y. Bilu, F. Luca, and A. Pizarro-Madariaga, "Trinomials, singular moduli and Riffaut's conjecture", *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **23**:4 (2022), 2003–2048. MR

[10] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2nd ed., Wiley, Hoboken, NJ, 2013. MR

[11] B. Edixhoven, "Special points on the product of two modular curves", *Compositio Math.* **114**:3 (1998), 315–328. MR

[12] B. Faye and A. Riffaut, "Fields generated by sums and products of singular moduli", *J. Number Theory* **192** (2018), 37–46. MR

[13] G. Fowler, "Triples of singular moduli with rational product", *Int. J. Number Theory* **16**:10 (2020), 2149–2166. MR

[14] G. Fowler, "Equations in three singular moduli: the equal exponent case", *J. Number Theory* **243** (2023), 256–297. MR

[15] J. Klaise, *Orders in quadratic imaginary fields of small class number*, Master's thesis, University of Warwick, 2012, available at https://warwick.ac.uk/fac/cross_fac/complexity/people/students/dtc/students2013/klaise/janis_klaise_ug_report.pdf.

[16] L. Kühne, "An effective result of André–Oort type", *Ann. of Math.* (2) **176**:1 (2012), 651–671. MR

[17] L. Kühne, "An effective result of André–Oort type, II", *Acta Arith.* **161**:1 (2013), 1–19. MR

[18] D. W. Masser, "Linear relations on algebraic groups", pp. 248–262 in *New advances in transcendence theory* (Durham, 1986), Cambridge Univ. Press, 1988. MR

[19] "PARI/GP version 2.11.4", software, 2020, available at http://pari.math.u-bordeaux.fr.

[20] J. Pila and J. Tsimerman, "Multiplicative relations among singular moduli", *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **17**:4 (2017), 1357–1382. MR

[21] A. Riffaut, "Equations with powers of singular moduli", *Int. J. Number Theory* **15**:3 (2019), 445–468. MR

[22] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR

[23] T. Tatuzawa, "On a theorem of Siegel", *Jpn. J. Math.* **21** (1951), 163–178. MR

[24] M. Watkins, "Class numbers of imaginary quadratic fields", *Math. Comp.* **73**:246 (2004), 907–938. MR

[25] P. J. Weinberger, "Exponents of the class groups of complex quadratic fields", *Acta Arith.* **22** (1973), 117–124. MR

Communicated by Jonathan Pila
Received 2022-08-03 Revised 2024-07-05 Accepted 2025-05-02

yuri@math.u-bordeaux.fr *Institut de Mathématiques de Bordeaux, Université de Bordeaux & CNRS, Talence, France*

sanoli@imsc.res.in *Institute of Mathematical Sciences, CIT Campus, Tharamani, Chennai, India*

emanuele.tron@math.u-bordeaux.fr *Institut de Mathématiques de Bordeaux, Université de Bordeaux & CNRS, Talence, France*

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2026 is US $590/year for the electronic version, and $865/year (+$75, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, is published continuously online.

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

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 20 No. 6 2026