The CM class number one problem for curves of genus 2

Pınar Kılıçer, Marco Streng

The CM class number one problem for curves of genus 2

Pınar Kılıçer* and Marco Streng†

December 21, 2015

Abstract

The CM class number one problem for elliptic curves asked to find all elliptic curves defined over the rationals with non-trivial endomorphism ring. For genus-2 curves it is the problem of determining all CM curves of genus 2 defined over the *reflex field*. We solve the problem by showing that the list given in Bouyer–Streng [3, Tables 1a, 1b, 2b, and 2c] is complete.

1 Introduction

By a *curve*, we always mean a projective smooth geometrically irreducible algebraic curve. A curve C over a field k of genus g has *complex multiplication* (CM) if the endomorphism ring of its Jacobian over $\overline{k}$ is an order $\mathcal{O}$ in a *CM field* of degree $2g$, that is, a totally imaginary quadratic extension of a totally real number field of degree g. We say that C has *CM* by $\mathcal{O}$. For example, an elliptic curve E has CM if $\mathrm{End}(E_{\overline{k}})$ is an order in an imaginary quadratic field K. An elliptic curve E with CM by an order $\mathcal{O}_K$ can be defined over $\mathbb{Q}$ if and only if the class group $\mathrm{Cl}_K := I_K/P_K$

*Leiden University, LFANT, IMB, `http://pub.math.leidenuniv.nl/~kilicerp/`, pinarkilicer@gmail.com

†Leiden University, `http://pub.math.leidenuniv.nl/~strengtc/`, marco.streng@gmail.com

is trivial. The CM class number one problem for elliptic curves asks to determine all imaginary quadratic fields of class number one. This problem was solved by Heegner [7] (1952), Baker [1] (1966) and Stark [22] (1967); the fields are $K \cong \mathbb{Q}(\sqrt{-d})$ where $d \in \{1,\ 2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163\}$.

We consider the analogous problem for curves of genus 2.

In Theorem 2.2, we recall the definition of the *CM class group* $I_{K^r}/I_0(\Phi^r)$ and we call its order the *CM class number*. If a curve C has CM by a maximal order $\mathcal{O}_K$ and is defined over $\mathbb{Q}$, then the CM class group is trivial, see Theorem 2.2. In [15], Murabayashi and Umegaki listed all quartic CM fields K with curves having CM by $\mathcal{O}_K$ defined over $\mathbb{Q}$. This list contains only cyclic quartic CM fields, but not the generic dihedral quartic CM fields because curves cannot be defined over $\mathbb{Q}$ in the dihedral case, see Shimura [20, Proposition 5.17]. The simplest examples that do include the dihedral case are those defined over the reflex field, equivalently, those of CM class number one (see [3]). We give the complete list of CM class number one fields for curves of genus 2.

Theorem 1.1. *There exist exactly* 63 *isomorphism classes of non-normal quartic CM fields with CM class number one. The fields are listed in Theorem 3.17.*

Theorem 1.2. *There exist exactly* 20 *isomorphism classes of cyclic quartic CM fields with CM class number one. The fields are listed in Theorem 4.5.*

The list in Theorem 4.5 contains the list in [15].

Corollary 1.3. *There are exactly* 125 *curves of genus* 2 *defined over the reflex field with CM by* $\mathcal{O}_K$ *for some quartic non-biquadratic* K*. The fields are the fields in Theorems 1.1 and 1.2, and the curves are those of Bouyer–Streng [3, Tables 1a, 1b, 2b, and 2c].*

Proof. This follows from the list given by Bouyer–Streng in [3] and Theorems 1.1–1.2. □

Corollary 1.4. *There are exactly* 21 *absolutely simple curves of genus* 2 *defined over* $\mathbb{Q}$ *with CM. The fields and* 19 *of the curves are given in van Wamelen [24].*

The other two curves are $y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$ *and* $y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$ *given in Theorem 14 of Bisson–Streng [2].*

Proof. The 19 curves given in [3] are the curves of genus 2 defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$, see [15] or Corollary 1.3. In [2], Bisson–Streng prove that there are only 2 curves of genus 2 defined over $\mathbb{Q}$ with CM by a non-maximal order inside one of the fields of Theorem 4.5. Theorem 1.2 finishes the proof. □

Corollary 1.5. *There are finitely many curves of genus 2 with CM by an order* $\mathcal{O}$ *in a number field* K *defined over the reflex field. The fields are those of Theorems 1.1–1.2, the complete list of orders can be computed using the methods of [2] and the curves using the methods of [3].* □

In Section 2, we give some definitions and facts from CM theory, and state the CM class number one problem for curves of genus $g \leq 2$. In Section 3, we prove Theorem 1.1. The strategy is as follows. We first show that there are only finitely many such CM fields by bounding their discriminant. The bound will be too large for practical purposes, but by using ramification theory and L-functions, we improve the bound which we then use to enumerate the fields. Section 4 proves Theorem 1.2 using the same strategy as in Section 3.

Acknowledgement

The authors would like to thank Maarten Derickx and Peter Stevenhagen for useful discussions.

2 Complex Multiplication

We refer to Shimura [21] and Lang [9] as references for this section.

Let K be a CM field of degree $2g$ and N' be a number field that contains a subfield isomorphic (over $\mathbb{Q}$) to a normal closure of K. There exists an automorphism ρ of K such that for every embedding $\tau : K \to \mathbb{C}$ we have $\bar{\cdot} \circ \tau = \tau \circ \rho$; we call it *complex*

conjugation and denote it by $\bar{\cdot}$. If ϕ is an embedding of CM fields $K_1 \to K_2$, then we have $\bar{\cdot} \circ \phi = \phi \circ \bar{\cdot}$. We denote $\phi \circ \bar{\cdot}$ by $\overline{\phi}$. A *CM type* of K with values in N' is a set Φ of embeddings of K into N' such that exactly one embedding of each of the g complex conjugate pairs of embeddings $\phi,\ \overline{\phi} : K \to N'$ is in Φ.

Let Φ be a CM type of K with values in N'. Let $L \supset K$ be a CM field such that N' contains a subfield isomorphic to a normal closure of L. Then the CM type of L *induced* by Φ is $\{\phi \in \mathrm{Hom}(L, N') :\ \phi|_K \in \Phi\}$. A CM type Φ is *primitive* if it is not induced from a CM type of a proper CM subfield. We say that CM types Φ_1 and Φ_2 of K are *equivalent* if there is an automorphism σ of K such that $\Phi_1 = \Phi_2\sigma$ holds.

Let N be a normal closure of K. From now on, we identify N' with N by making a choice of isomorphism and replacing N' by a subfield. The *reflex field* of $(K,\ \Phi)$ is

$$K^r = \mathbb{Q}(\{\sum_{\phi\in\Phi} \phi(x) \mid x \in K\}) \subset N$$

and satisfies $\mathrm{Gal}(N/K^r) = \{\sigma \in \mathrm{Gal}(N/\mathbb{Q}) : \sigma\Phi = \Phi\}$. For example, if a CM field K is Galois over $\mathbb{Q}$, then the reflex field K^r of K is a subfield of K. Let Φ_N be the CM type of N induced by Φ. Then the reflex field K^r is a CM field with CM type $\Phi^r = \{\sigma^{-1}|_{K^r} :\ \sigma \in \Phi_N\}$. The pair (K^r, Φ^r) is called the *reflex* of (K, Φ). The *type norm* is the multiplicative map

$$\begin{aligned} \mathrm{N}_\Phi : K &\to K^r, \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x), \end{aligned}$$

satisfying $\mathrm{N}_\Phi\overline{\mathrm{N}_\Phi} = \mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Q}$. The type norm induces a homomorphism between the groups of fractional ideals I_K and I_{K^r} by sending $\mathfrak{b} \in I_K$ to $\mathfrak{b}' \in I_{K^r}$ such that $\mathfrak{b}'\mathcal{O}_N = \prod_{\phi\in\Phi} \phi(\mathfrak{b})\mathcal{O}_N$ (Shimura [21, Proposition 29]).

An *abelian variety* A over a field k of characteristic 0 of dimension g has CM by an order $\mathcal{O}_K$ if K has degree $2g$ and there is an embedding $\theta : K \to \mathrm{End}_{\overline{k}}(A_{\overline{k}}) \otimes \mathbb{Q}$. Let $\mathrm{Tgt}_0(A)$ be the tangent space of A over $\overline{k}$ at 0. Given A with CM by $\mathcal{O}_K$, let Φ be the set of homomorphisms $K \to \overline{k}$ occurring in the representation of K

on $\mathrm{End}_{\overline{k}}(\mathrm{Tgt}_0(A_{\overline{k}}))$. Then Φ is a CM type of K, and we say that (A,θ) is of type (K,Φ). A polarized abelian variety of type (K,Φ) is a triple $P=(A,C,\theta)$ formed by an abelian variety (A,θ) of type (K,Φ) and a polarization C of A such that $\theta(K)$ is stable under the involution of $\mathrm{End}_{\overline{k}}(A)\otimes\mathbb{Q}$ determined by C. For more details see Shimura [21, Chapter 14].

We say that an abelian variety is *absolutely simple* if it is not isogenous over $\overline{k}$ to product of abelian varieties of lower dimension.

Theorem 2.1 (Shimura [21], §8.2)**.** *An abelian variety of type (K,Φ) is simple if and only if Φ is primitive.* □

Theorem 2.2 (First Main Theorem of Complex Multiplication, [21, Main Theorem 1] in §15.3)**.** *Let (K,Φ) be a primitive CM type and (K^r,Φ^r) be the reflex of (K,Φ). Let $P=(A,C,\theta)$ be a polarized abelian variety of type (K,Φ). Let M be the field of moduli of (A,C). Then the composite $M_K=K^r\cdot M$ is the unramified class field over K^r corresponding to the ideal group*

$$I_0(\Phi^r):=\{\mathfrak{b}\in I_{K^r}:\ \mathrm{N}_{\Phi^r}(\mathfrak{b})=(\alpha),\ \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b})=\alpha\overline{\alpha},\ \text{for some } \alpha\in K^\times\}.$$

The *Jacobian* $J(C)$ of a curve C/k of genus g is an abelian variety of dimension g such that we have $J(C)(\overline{k})=\mathrm{Pic}^0(C_{\overline{k}})$; for details we refer to [13]. We say that a curve C has CM by $\mathcal{O}_K$, if there is an embedding $\theta:K\to\mathrm{End}_{\overline{k}}(J(C)_{\overline{k}})\otimes\mathbb{Q}$.

Corollary 2.3. *If a curve C has CM by $\mathcal{O}_K$ and is defined over K^r, then the CM class group $\boldsymbol{C}_{\Phi^r}:=I_{K^r}/I_0(\Phi^r)$ is trivial.* □

The CM class number one problem for CM fields of degree $2g$ asks to list all primitive CM types (K,Φ) degree $2g$ such that the CM class group $I_0(\Phi^r)$ is trivial. In the case $g=2$, these are exactly the endomorphism algebras of simple CM curves of genus 2 defined over the reflex field. Theorems 1.1 and 1.2 solve this problem for non-biquadratic quartic CM fields.

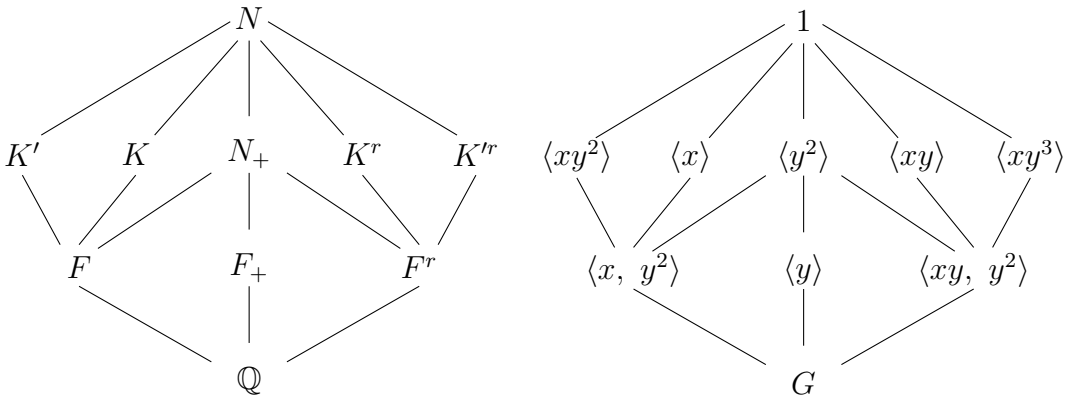
In the genus-2 case, the quartic CM field K is either cyclic Galois, biquadratic Galois, or non-Galois with Galois group D_4 (Shimura [21, Example 8.4(2)]). We re-

strict to the CM curves with simple Jacobian, which, by Theorem 2.1, have primitive types. By [21, Example 8.4(2)] their CM fields are not biquadratic.

3 The non-normal quartic CM fields

This section, which is the largest in this paper, proves the main theorem in the case of non-normal fields. The case of cyclic fields is much easier and is Section 4.

Suppose that $K/\mathbb{Q}$ is a non-normal quartic CM field with real quadratic subfield F. The normal closure N is a dihedral CM field of degree 8 with Galois group $G := \mathrm{Gal}(N/\mathbb{Q}) = \langle x,\ y : y^4 = x^2 = (xy)^2 = \mathrm{id}\rangle$. Complex conjugation $\bar{\cdot}$ is y^2 in this notation and the CM field K is the subfield of N fixed by $\langle x\rangle$. Let Φ be a CM type of K with values in N'. We can (and do) identify N with a subfield of N' in such a way that $\Phi = \{\mathrm{id}, y|_K\}$. Then the reflex field K^r of Φ is the fixed field of $\langle xy\rangle$, which is a non-normal quartic CM field non-isomorphic to K with reflex type $\Phi^r = \{\mathrm{id}, y^3|_{K^r}\}$, (see [21, Examples 8.4., 2(C)]). Denote the quadratic subfield of K^r by F^r.



Lattice of subfields and subgroups

Let N_+ be the maximal totally real subfield of N, and let F_+ be the fixed field of $\langle y\rangle$.

3.1 An effective bound for non-normal quartic CM fields with CM class number one

In this section, we find an effective upper bound for the discriminant of the non-normal quartic CM fields with CM class number one. We first prove the following relation between the relative class number $h_K^* := h_K/h_F$ and the number t_K of ramified primes in K/F.

Proposition 3.1. *Let K be a non-biquadratic quartic CM field with the real quadratic subfield F. Assuming $I_0(\Phi^r) = I_{K^r}$, we have $h_K^* = 2^{t_K-1}$, where t_K is the number of ramified primes in K/F.*

Moreover, we have $h_{K^r}^* = 2^{t_{K^r}-1}$, where t_{K^r} is the number of ramified primes in K^r/F^r.

Remark 3.2. *In the case where $K/\mathbb{Q}$ is cyclic quartic, this result is $(i) \Rightarrow (iii)$ of Proposition 4.5 in Murabayashi [14].*

On the other hand, if K is a non-normal quartic CM field, Louboutin proves $h_K^* \approx \sqrt{d_K/d_F}$ with an effective error bound, see Proposition 3.5. Putting this together with the result in Proposition 3.1 gives approximately $\sqrt{d_K/d_F} \leq 2^{t_K-1}$. As the left hand side grows more quickly than the right, this relation will give a bound on the discriminant, precisely see Proposition 3.6.

We start the proof of Proposition 3.1 with the following lemma.

Lemma 3.3. Let K be a CM field with real quadratic subfield F and group of roots of unity $\mu_K = \{\pm 1\}$. Let H denote the group $\mathrm{Gal}(K/F)$. Put $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} = \mathfrak{b}\}$. Then we have $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$, where P_K is the group of principal fractional ideals in K.

Proof. We have the exact sequence

$$1 \to I_F \to I_K^H \to \bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \to 1 \tag{3.1}$$

and

$$\bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \quad \cong \quad (\mathbb{Z}/2\mathbb{Z})^{t_K}.$$

Define $P_K^H = P_K \cap I_K^H$. The map $\varphi : I_K^H \to \frac{I_K}{P_K}$ induces an isomorphism $I_K^H/P_K^H \cong \mathrm{im}(\varphi) = I_K^H P_K/P_K$, so by (3.1), we have

$$h_F = [I_F : P_F] = \frac{[I_K^H : P_K^H][P_K^H : P_F]}{[I_K^H : I_F]} = 2^{-t_K}[I_K^H P_K : P_K][P_K^H : P_F],$$

hence

$$h_K^* := \frac{h_K}{h_F} = 2^{t_K}\frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}.$$

It now suffices to prove $[P_K^H : P_F] = 2$, for which we claim that there is a surjective group homomorphism $\phi : P_K^H \to \mu_K = \{\pm 1\}$ given by $\phi((\alpha)) = \alpha/\overline{\alpha}$ with kernel P_F.

Proof of the Claim. The map ϕ is well-defined because the image is independent of the choice of α as $\mathcal{O}_K^* = \mathcal{O}_F^*$ (cf. [10, Lemma 1]). It is clear that it is a homomorphism. If $\phi((\alpha)) = 1$, then $\alpha/\overline{\alpha} = 1$, so $\alpha = \overline{\alpha}$. This means $\alpha \in F$ and hence $(\alpha) \in P_F$. Therefore, the kernel is P_F. As $K = F(\sqrt{-\beta})$ with a totally positive element β in F, we have $\phi((\sqrt{-\beta})) = -1$, so ϕ is surjective.

Hence $[P_K^H : P_F] = |\mathrm{Im}(\phi)|$ equals 2. □

Lemma 3.4. Let K be a non-normal quartic CM field with real quadratic subfield F. Then we have $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$. Moreover, we have $[I_{K^r} : I_{K^r}^{H'} P_{K^r}] \leq [I_{K^r} : I_0(\Phi^r)]$, where $H' = \mathrm{Gal}(K^r/F^r)$.

Proof. To prove the first assertion, we show that the kernel of the map $\mathrm{N}_\Phi : I_K \to I_{K^r}/I_0(\Phi^r)$ is contained in $I_K^H P_K$. For any $\mathfrak{a} \in I_K$, we can compute (see [19, (3.1)])

$$\mathrm{N}_{\Phi^r}\mathrm{N}_\Phi(\mathfrak{a}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\frac{\mathfrak{a}}{\overline{\mathfrak{a}}}.$$

Suppose $\mathrm{N}_\Phi(\mathfrak{a}) \in I_0(\Phi^r)$. Then $N_{K/\mathbb{Q}}(\mathfrak{a})\frac{\mathfrak{a}}{\overline{\mathfrak{a}}} = (\alpha)$, where $\alpha \in K^\times$ and $\alpha\overline{\alpha} = N_{K^r/\mathbb{Q}}(N_\Phi(\mathfrak{a})) = N_{K/\mathbb{Q}}(\mathfrak{a})^2 \in \mathbb{Q}$. So $\frac{\mathfrak{a}}{\overline{\mathfrak{a}}} = (\beta)$, where $\beta = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})^{-1} \cdot \alpha$, and hence $\beta\overline{\beta} = 1$. There is a $\gamma \in K^\times$ such that $\beta = \frac{\overline{\gamma}}{\gamma}$ (this is a special case of Hilbert's Theorem 90, but can be seen directly by taking $\gamma = \overline{\epsilon} + \overline{\beta}\epsilon$ for any $\epsilon \in K$ with $\gamma \neq 0$.). Thus we have $\mathfrak{a} = \overline{\gamma\mathfrak{a}} \cdot (\frac{1}{\gamma}) \in I_K^H P_K$ and therefore $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$.

Now we prove the second assertion. By [19, (3.2)], we have

$$\mathrm{N}_{\Phi}\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b})\frac{\mathfrak{b}}{\overline{\mathfrak{b}}}.$$

Suppose $\mathfrak{b} \in I_0(\Phi^r)$. Then $N_{K^r/\mathbb{Q}}(\mathfrak{b})\frac{\mathfrak{b}}{\overline{\mathfrak{b}}} = (\alpha)$, where $\alpha \in K^{r\times}$ and $\alpha\overline{\alpha} = N_{\Phi}(N_{K^r/\mathbb{Q}}(\mathfrak{b}))$ $= N_{K^r/\mathbb{Q}}(\mathfrak{b})^2 \in \mathbb{Q}$. We finish the proof of $\mathfrak{b} \in I_{K^r}^{H'}P_{K^r}$ exactly as above. □

Now let us recall and prove Proposition 3.1.

Proposition 3.1. *Let K be a (non-biquadratic) quartic CM field with the real quadratic subfield F. Assuming $I_0(\Phi^r) = I_{K^r}$, we have $h_K^* = 2^{t_K-1}$, where t_K is the number of ramified primes in K/F.*

Moreover, we have $h_{K^r}^* = 2^{t_{K^r}-1}$, where t_{K^r} is the number of ramified primes in K^r/F^r.

Proof. Since $\mu_K = \{\pm 1\}$, by Lemma 3.3, we have $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$. We showed in Lemma 3.4 that, under the assumption $I_0(\Phi^r) = I_{K^r}$, the quotient $I_K/I_K^H P_K$ is trivial. Therefore, we have $h_K^* = 2^{t_K-1}$.

Similarly, by Lemma 3.3, we have $h_{K^r}^* = 2^{t_{K^r}-1}[I_{K^r} : I_{K^r}^{H^r} P_{K^r}]$ and hence $h_{K^r}^* = 2^{t_{K^r}-1}$ follows from Lemma 3.4. □

The next step is to use the following bound from analytic number theory.

Let d_M denote the discriminant of a number field M.

Proposition 3.5. *(Louboutin [12], Remark 27 (1)) Let N be the normal closure of a non-normal quartic CM field K with Galois group D_4. Assume $d_N^{1/8} \geq 222$. Then*

$$h_K^* \geq \frac{2\sqrt{d_K/d_F}}{\sqrt{e}\pi^2(\log(d_K/d_F) + 0.057)^2}. \tag{3.2}$$ □

Proposition 3.6. *Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $d_K/d_F \leq 2 \cdot 10^{15}$.*

Proof. Let

$$f(D) = \frac{2\sqrt{D}}{\sqrt{e}\pi^2(\log(D) + 0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1}f(p_t p_{t+1}\Delta_t^2),$$

where p_j is the j-th prime and $\Delta_k = \prod_{j=1}^{k} p_j$.

Here, if $D = d_K/d_F$, then f is the right hand side of the inequality (3.2) in Proposition 3.5. The quotient d_K/d_F is divisible by the product of ramified primes in K/F, so $d_K/d_F \geq \Delta_{t_K}$.

On the other hand, the function f is monotonically increasing for $D > 52$, so if $t_K \geq 4$ then $f(d_K/d_F) \geq f(\Delta_{t_K})$. Therefore, by Proposition 3.1, we get that if $I_0(\Phi^r) = I_{K^r}$, then

$$2^{t_K - 1} \geq f(d_K/d_F) \geq f(\Delta_{t_K}) \tag{3.3}$$

and hence $g(t) \leq 1$. The function g is monotonically increasing for $t \geq 4$ and is greater than 1 if $t_K > 14$. Therefore, we get $t_K \leq 14$ and $h_K^* \leq 2^{13}$, hence $d_K/d_F < 2 \cdot 10^{15}$. □

The bound that we get in Proposition 3.6 is unfortunately too large to list all the fields. In the following section we study ramification of primes in $N/\mathbb{Q}$ and find a sharper upper bound for d_{K^r}/d_{F^r}, see Proposition 3.16.

3.2 Almost all ramified primes are inert in F and F^r

In this section, under the assumption $I_0(\Phi^r) = I_{K^r}$, we study the ramification behavior of primes in $N/\mathbb{Q}$, and prove that almost all ramified primes in K^r/F^r are inert in F^r. Thus d_{K^r}/d_{F^r} grows as the square of the product of such ramified primes and we get a lower bound on $f(d_{K^r}/d_{F^r})$ of (3.3) that grows even faster with t_{K^r} than what we have had before, so, in the following section 3.3, we obtain a better upper bound on d_{K^r}/d_{F^r}.

In this section, we prove the following theorem.

Proposition 3.7. *Let K be a non-biquadratic quartic CM field of type Φ and F be its quadratic subfield. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Moreover, all the ramified primes (distinct from the ones lying above p and q) in K^r/F^r are inert in F and F^r.*

We begin the proof with exploring the ramification behavior of primes in $N/\mathbb{Q}$, under the assumption $I_0(\Phi^r) = I_{K^r}$.

3.2.1 Ramification of primes in $N/\mathbb{Q}$

Lemma 3.8. Let M/L be a Galois extension of number fields and $\mathfrak{q}$ be a prime of M over an odd prime ideal $\mathfrak{p}$ (that is, the prime $\mathfrak{p}$ lies over an odd prime in $\mathbb{Q}$) of L. Then there is no surjective homomorphism from a subgroup of $I_{\mathfrak{q}}$ to a Klein four group V_4.

Proof. For an odd prime ideal $\mathfrak{p}$ in L, suppose that there is a surjective homomorphism from a subgroup of $I_{\mathfrak{p}}$ to V_4. In other words, suppose a prime of F over $\mathfrak{p}$ is totally ramified in a biquadratic intermediate extension E/F of M/L. The biquadratic intermediate extension E/F has three quadratic intermediate extensions $E_i = F(\sqrt{\alpha_i})$ for $i = 1,\ 2,\ 3$. Without loss of generality, take $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) \in \{0, 1\}$ for each i. Note $\mathcal{O}_{E_i}$ contains $\mathcal{O}_F[\sqrt{\alpha_i}]$ of relative discriminant $4\alpha_i$ over $\mathcal{O}_F$. Since $\mathfrak{p}$ is odd, this implies that the relative discriminant D_i of $\mathcal{O}_{E_i}$ has $\mathrm{ord}_{\mathfrak{p}}(D_i) = \mathrm{ord}_{\mathfrak{p}}(\alpha_i)$. At the same time, $E_3 = F(\sqrt{\alpha_1\alpha_2})$, so $\mathfrak{p}$ ramifies in E_i for an even number of i's. In particular, $\mathfrak{p}$ is not totally ramified in E/F. □

Lemma 3.9. Let K be a non-biquadratic quartic CM field of type Φ with the real quadratic subfield F and let K^r be its reflex field with the quadratic subfield F^r. Then the following assertions hold.

(i) If a prime p is ramified in both F and F^r, then it is totally ramified in $K/\mathbb{Q}$ and $K^r/\mathbb{Q}$.

(ii) If an odd prime p is ramified in F (in F^r, respectively) as well as in F_+, then p splits in F^r (in F, respectively). Moreover, at least one of the primes above p is ramified in K^r/F^r (in K/F, respectively).

Proof. The statements (i) and (ii) are clear from Table 1 on page 17. Alternatively, one can also prove the statements as follows:

(i) Let $\mathfrak{p}_N$ be a prime of N above p that is ramified in both $F/\mathbb{Q}$ and $F^r/\mathbb{Q}$. Then the maximal unramified subextension of $N/\mathbb{Q}$ is contained in F_+. Therefore, the inertia group of $\mathfrak{p}_N$ contains $\mathrm{Gal}(N/F_+) = \langle y \rangle$. By computing ramification indices in the diagram of subfields one by one, we see that the prime p is totally ramified in K and K^r.

(ii) Let p be an odd prime that is ramified in $F/\mathbb{Q}$ and $F_+/\mathbb{Q}$ and $\mathfrak{p}_N$ be a prime above p in N. The inertia group of an odd prime cannot be a biquadratic group by Lemma 3.8, so $\mathrm{I}_{\mathfrak{p}_N}$ is a proper subgroup of $\mathrm{Gal}(N/F^r)$. Since $\mathrm{I}_{\mathfrak{p}_N}$ is a normal subgroup in $\mathrm{D}_{\mathfrak{p}_N}$, the group $\mathrm{D}_{\mathfrak{p}_N}$ cannot be the full Galois group $\mathrm{Gal}(N/\mathbb{Q})$. So $\mathrm{D}_{\mathfrak{p}_N}$ is a proper subgroup of $\mathrm{Gal}(N/F^r)$ and hence p splits in F^r. Moreover, since p is ramified in F, hence in K, hence in K^r, at least one of the primes above p in F^r is ramified in K^r. Since F and F^r are symmetric in $N/\mathbb{Q}$, the same argument holds for F^r as well.

□

Lemma 3.10. Assuming $I_0(\Phi^r) = I_{K^r}$, if K^r has a prime $\mathfrak{p}$ of prime norm p with $\overline{\mathfrak{p}} = \mathfrak{p}$, then $F = \mathbb{Q}(\sqrt{p})$.

Proof. By assumption, we have

$$\mathrm{N}_{\Phi^r}(\mathfrak{p}) = (\alpha) \text{ such that } \alpha\overline{\alpha} = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{p}) = p.$$

Since $\overline{\mathfrak{p}} = \mathfrak{p}$, we have $(\alpha) = (\overline{\alpha})$, and so $\alpha = \epsilon\overline{\alpha}$ for a unit ϵ in $\mathcal{O}_K^*$ with absolute value 1 (hence a root of unity). Since $\mu_K = \{\pm 1\}$, we get $\alpha^2 = \pm p$. The case $\alpha^2 = -p$ is not possible, since K has no imaginary quadratic intermediate field. Hence we have $\alpha^2 = p$ and so $\sqrt{p} \in F$. □

Corollary 3.11. *Suppose $I_0(\Phi^r) = I_{K^r}$. If p is totally ramified in $K^r/\mathbb{Q}$, or splits in $F^r/\mathbb{Q}$ and at least one of the primes over p in F^r ramifies in K^r/F^r, then $F = \mathbb{Q}(\sqrt{p})$.* □

Proposition 3.12. *Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$, where p is a rational prime.*

Proof. Suppose that there is an odd prime p that is ramified in F. Then p is ramified either in F and F^r or in F and F_+.

If p is ramified in both F and F^r, then by Lemma 3.9-(i), the prime p is totally ramified in $K^r/\mathbb{Q}$. If p is ramified in F and F_+, then by Lemma 3.9-(ii), the prime p splits in F^r and at least one of the primes over p in F^r ramifies in K^r/F^r. In both cases, by Corollary 3.11, we have $F = \mathbb{Q}(\sqrt{p})$.

Therefore, if an odd prime p is ramified in F, then we have $F = \mathbb{Q}(\sqrt{p})$. If no odd prime ramifies in F then the only prime that ramifies in F is 2, and so we have $F = \mathbb{Q}(\sqrt{2})$. □

Lemma 3.13. Suppose $I_0(\Phi^r) = I_{K^r}$. Then the following assertions are true.

(i) If a rational prime l is unramified in both $F/\mathbb{Q}$ and $F^r/\mathbb{Q}$, but is ramified in $K/\mathbb{Q}$ or $K^r/\mathbb{Q}$, then all primes above l in F and F^r are ramified in K/F and K^r/F^r and l is inert in F^r.

(ii) If $F = \mathbb{Q}(\sqrt{p})$ with a prime number $p \equiv 3 \pmod 4$, then 2 is inert in F^r.

Proof. (i) It follows from Table 1 for except the statement that l is inert in F^r.

Suppose that l splits in F^r. Then by Corollary 3.11, we have $\sqrt{l} \in F$, but we assumed that l is unramified in F. Therefore, the prime l is inert in F^r.

(ii) If 2 is ramified in F^r, then by Lemma 3.9-(i), the prime 2 is totally ramified in K and K^r. If 2 splits in F^r, then at least one of the primes in F^r above 2 ramifies in K^r since 2 ramifies in $K/\mathbb{Q}$. Therefore, by Corollary 3.11, in both cases we have $F = \mathbb{Q}(\sqrt{2})$, contradiction. Hence the prime 2 is inert in F^r.

□

3.2.2 Equality of t_K and t_{K^r}

In the previous section, we proved that the primes that are unramified in F and F^r, but are ramified in K^r/F^r are inert in F^r. Thus these primes contribute to the number of ramified primes t_{K^r} in K^r/F^r with one prime, on the other hand they

contribute to t_K with at least one prime and exactly two if the prime splits in $F^r/\mathbb{Q}$. So if we could prove $t_K = t_{K^r}$, then that would approximately say that all such primes are inert in both F and F^r.

Proposition 3.14. *(Shimura, [19, Proposition A.7.]) Let the notation be as above. Then, we have $h_K^* = h_{K^r}^*$.*

Proof. The idea of the proof is to first show

$$\zeta_K(s)/\zeta_F(s) = \zeta_{K^r}(s)/\zeta_{F^r}(s) \tag{3.4}$$

and then use the class number formula. Louboutin [10, Theorem A] shows (3.4) by writing the Dedekind zeta functions of K, K^r, F and F^r as a product of Artin L-functions and finding relations between these combinations of L-functions (see, [10, Theorem A]).

We can also get this equality by comparing the local factors of the Euler products of the Dedekind ζ-functions of the fields. By using Table 1, we see that each ramified prime in $N/\mathbb{Q}$ has the same factors in the Euler products of the quotients of the Dedekind ζ-functions on both sides of (3.4). As an example, we take a rational prime p with ramification type (6) in Table 1, where the local factors for p of the Dedekind ζ-functions are as follows:

$$\begin{aligned}
\zeta_K(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K,1}{}^{-s}} \cdot \frac{1}{1-\mathrm{N}\mathfrak{p}_{K,y}{}^{-s}} = \frac{1}{1-(p^2)^{-s}} \cdot \frac{1}{1-p^{-s}}, \\
\zeta_F(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{F,1}{}^{-s}} \cdot \frac{1}{1-\mathrm{N}\mathfrak{p}_{F,y}{}^{-s}} = \left(\frac{1}{1-p^{-s}}\right)^2, \\
\zeta_{K^r}(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K^r,1}{}^{-s}} = \frac{1}{1-(p^2)^{-s}}, \\
\zeta_{F^r}(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K^r,1}{}^{-s}} = \frac{1}{1-p^{-s}}.
\end{aligned}$$

So for such a prime, we get

$$\zeta_K(s)_p/\zeta_F(s)_p = \frac{1}{1+p^{-s}} = \zeta_{K^r}(s)_p/\zeta_{F^r}(s)_p.$$

Similarly, by using Table 3.5.1 in [6], we can get this equality for the unramified primes as well.

The analytic class number formula at $s = 0$ (see, [25, Chapter 4]) says that the Dedekind zeta function $\zeta_M(s)$ of an algebraic number field M has a zero at $s = 0$ and the derivative of $\zeta_M(s)$ at $s = 0$ has the value

$$-\frac{h_M \cdot R_M}{w_M},$$

where h_M is the class number; R_M is the regulator; and w_M is the order of the group of roots of unity μ_M.

Since $w_K = 2 = w_F$ and $R_K = 2R_F$ (see Washington, [25, Proposition 4.16]), the analytic class number formula at $s = 0$ gives

$$\lim_{s\to 0} \frac{\zeta_K(s)}{\zeta_F(s)} = 2h_K^*.$$

Therefore, the result follows by the identity (3.4). □

Corollary 3.15. *Assuming $I_0(\Phi^r) = I_{K^r}$, we have $t := t_K = t_{K^r}$.*

Proof. By Proposition 3.1, we have $h_K^* = 2^{t_K - 1}$ and $h_{K^r}^* = 2^{t_{K^r} - 1}$. Then by Proposition 3.14, we get $t_K = t_{K^r}$. □

3.2.3 Proof of Proposition 3.7

Proposition 3.7. *Let K be a non-biquadratic quartic CM field of type Φ and F be its quadratic subfield. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Moreover, all the ramified primes (distinct from the ones lying above p and q) in K^r/F^r are inert in F and F^r.*

Proof. We first prove that if a prime l ramifies in both F and F^r, then it is equal to p, where $F = \mathbb{Q}(\sqrt{p})$.

Indeed, by Lemma 3.9-(i), the prime l is totally ramified in $K^r/\mathbb{Q}$ and hence by Corollary 3.11, we get $F = \mathbb{Q}(\sqrt{l})$, so $l = p$.

Now we see that there are four types of prime numbers that ramify in $N/\mathbb{Q}$:

(I) The prime p, which is ramified in F and possibly in F^r.

(II) The primes that are unramified in F, but ramified in F^r, say $q_1, \cdots, q_s$.

(III) The primes that are unramified in F and F^r, but ramified in K, say $r_1, \cdots, r_m$.

(IV) If $p \equiv 3 \pmod 4$, then $2 \neq p$ is ramified in F and is inert in F^r by Lemma 3.13-(ii). Let $i_2 = 1$ if $p \equiv 3 \pmod 4$, and $i_2 = 0$ if $p \not\equiv 3 \pmod 4$.

We will compute the contribution of each ramification type to the number of ramified primes t_K in K/F and t_{K^r} in K^r/F^r. Let f_p and f_p^r be the contributions of the primes over p to t_K and t_{K^r}, respectively. We claim $t_K \geq f_p + s + m + i_2$ with equality only if all primes of type (III) are inert in F and $t_{K^r} = f_p^r + m + i_2$.

Proof of the claim: By Table 1 including Lemma 3.10, we see that for $i = 1, \cdots, s$ *exactly* one of the primes above q_i in F ramifies in K/F and the unique prime above q_i in F^r does not ramify in K^r/F^r. By Lemma 3.13-(i), we see that for $j = 1, \cdots, m$ the prime r_j is inert in F^r so contributes with *exactly* one prime to t_{K^r}, and with *at least* one prime to t_K and with exactly one if and only if r_j is inert in $F/\mathbb{Q}$. If $p \equiv 3 \pmod 4$, then by Lemma 3.13-(ii), the prime 2 is inert in F^r. As furthermore 2 is ramified in F and $F \ncong \mathbb{Q}(\sqrt{2})$, the prime 2 has the decomposition (14) in Table 1, so it contributes *exactly* with one prime to t_K and t_{K^r}. So we get $t_K \geq f_p + s + m + i_2$ with equality if and only if all primes of type (III) are inert in F and $t_{K^r} = f_p^r + m + i_2$, which proves the claim.

We observe that $s > 0$ holds. Indeed, if $s = 0$, then all primes that ramify in F^r also ramify in F. Hence d_{F^r} divides d_F, which is equal to p if $p \equiv 1 \pmod 4$ and $4p$ otherwise. So $F^r \cong F$, a contradiction.

If p ramifies in both F and F^r, then by Lemma 3.9-(i), we have $f_p = f_p^r = 1$. The same is true if p is of type (14) of Table 1. By Corollary 3.15, we have $t_K = t_{K^r}$, so in this case $m + i_2 \geq s + m + i_2$, so $s = 0$, a contradiction. Therefore, the prime p is not ramified in F^r and is not of type (14), leaving only the possibility $(q/p) = 1$. By Table 1, we see that $f_p^r - f_p = 1$. Hence $t_K = t_{K^r}$ implies that all primes of type (III) are inert in F and $s = 1$. In particular, since p is unramified in F^r, we get $F^r = \mathbb{Q}(\sqrt{q})$ for a prime $q \not\equiv 3 \pmod 4$. Moreover, Table 1 implies $(p/q) = 1$. $\square$

Table 1: Ramification table of a non-normal quartic CM field

Case	I	D	decomp. of p in N	decomp. of p in K	decomp. of p in F	decomp. of p in F_+	decomp. of p in F^r	decomp. of p in K^r	$N_{\Phi^r}(\mathfrak{p}_{K^r,1})$	$\sqrt{p} \in F$
(1)*	$\langle y^2 \rangle$	$\langle y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,x}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,xy}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	✓
(2)	$\langle y^2 \rangle$	$\langle y \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(3)	$\langle y^2 \rangle$	$\langle x,\ y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(4)*	$\langle y^2 \rangle$	$\langle xy,\ y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}$	✓
(5) (a)	$\langle x \rangle$	$\langle x \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	
(5) (b)	$\langle xy^2 \rangle$	$\langle xy^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	
(6) (a)	$\langle x \rangle$	$\langle x,\ y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2$	p	
(6) (b)	$\langle xy^2 \rangle$	$\langle x, y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2$	p	
(7) (a)	$\langle xy \rangle$	$\langle xy \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y^3}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}\mathfrak{p}_{K^r,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	✓
(7) (b)	$\langle xy^3 \rangle$	$\langle xy^3 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}\mathfrak{p}_{K^r,y^2}$	$\mathfrak{p}_{K,1}^2$	✓
(8) (a)	$\langle xy \rangle$	$\langle xy, y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}$	$\mathfrak{p}_{K,1}$	✓
(8) (b)	$\langle xy^3 \rangle$	$\langle xy, y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}^2$	p	✓
(9)	$\langle y \rangle$	$\langle y \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓
(10)	$\langle y \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓
(11)*	$\langle x, y^2 \rangle$	$\langle x, y^2 \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	✓
(12)*	$\langle x, y^2 \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}$	✓
(13)	$\langle xy, y^2 \rangle$	$\langle xy, y^2 \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}^2$	✓
(14)	$\langle xy, y^2 \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(15)	G	G	$\mathfrak{p}_{N,1}^8$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓

Table 2: This table lists all 19 pairs (I, D) where $1 \neq \mathrm{I} \triangleleft \mathrm{D} \leq D_4 = \langle x,\ y \rangle$ and D/I is cyclic, partitioned into 15 conjugacy classes (1) – (15). In particular, it contains all possible inertia and decomposition groups of ramified primes of N. This table is a corrected subset of [6, Table 3.5.1]. We restricted to $\mathrm{I} \neq 1$, added the case 8-(b), which is missing in [6, Table 3.5.1], and corrected the type norm column of some cases. The cases (11) – (15) can only occur for the prime 2, see Lemma 3.8. If there is a checkmark in the last column, then by Lemma 3.10, such splitting implies $\sqrt{p} \in F$ (i.e., $F = \mathbb{Q}(\sqrt{p})$) under the assumption $I_0(\Phi^r) = I_{K^r}$. The cases with * do not occur under the assumption $I_0(\Phi^r) = I_{K^r}$ because p is not ramified in F in these cases, but on the other hand $\sqrt{p} \in F$ by Lemma 3.10.

3.3 A sharper bound for d_{K^r}/d_{F^r}

Proposition 3.16. *Suppose $I_0(\Phi^r) = I_{K^r}$ and $d_N^{1/8} \geq 222$. Then we have $h^*_{K^r} \leq 2^5$ and $d_{K^r}/d_{F^r} \leq 3 \cdot 10^{10}$.*

Proof. Under the assumption $I_0(\Phi^r) = I_{K^r}$, in Propositions 3.12 and 3.7 we proved $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers. Additionally, we proved that at least one of the ramified primes above p in F^r is ramified in K^r/F^r, and the other ramified primes in K^r/F^r are inert in F^r, say $r_1, \cdots, r_{t-1}$. Therefore, we have $d_{K^r}/d_{F^r} \geq pqr_1^2 \cdots r_{t-1}^2$.

Let

$$f(D) = \frac{2\sqrt{D}}{\sqrt{e}\pi^2(\log(D) + 0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1} f(p_t p_{t+1} \Delta_t^2),$$

where p_j is the j-th prime and $\Delta_k = \prod_{j=1}^{k} p_j$. If $D = d_{K^r}/d_{F^r}$, then $h_{K^r} \geq f(D)$ by Proposition 3.5.

Recall that, by the proof of Proposition 3.6, the function f is monotonically increasing for $D > 52$. Therefore, if $t > 3$, then $f(d_{K^r}/d_{F^r}) > f(p_t p_{t+1} \Delta_t^2)$. So in that case by Proposition 3.1 and Corollary 3.15, we have $h^*_{K^r} = 2^{t-1}$, hence we get $g(t) \leq 1$. Further, the function g is monotonically increasing for $t \geq 4$ and is greater than 1 for $t = 7$. So we get $t \leq 6$. □

3.4 Enumerating the fields

To specify quartic CM fields, we use the following notation of the ECHIDNA database [5]. Given a quartic CM field K, let D be the discriminant of the real quadratic subfield F. Write $K = F(\sqrt{\alpha})$ where α is a totally negative element of $\mathcal{O}_F$ and take α such that $A := -\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) > 0$ is minimal and let $B := \mathrm{N}_{F/\mathbb{Q}}(\alpha)$. We choose α with minimal B if there is more than one B with the same A. We use the triple $[D, A, B]$ to uniquely represent the isomorphism class of the CM field $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B)$.

Theorem 3.17. *There exist exactly* 63 *isomorphism classes of non-normal quartic CM fields* K *that have a CM type* Φ *satisfying* $I_0(\Phi^r) = I_{K^r}$*, where* K^r *is the reflex field of* Φ*. The fields are given by* $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B) \supset \mathbb{Q}(\sqrt{D})$ *where* $[D, A, B]$ *ranges over*

$[5, 13, 41],\ [5, 17, 61],\ [5, 21, 109],\ [5, 26, 149],\ [5, 34, 269],\ [5, 41, 389],$
$[8, 10, 17],\ [8, 18, 73],\ [8, 22, 89],\ [8, 34, 281],\ [8, 38, 233],\ [13, 9, 17],$
$[13, 18, 29],\ [13, 29, 181],\ [13, 41, 157],\ [17, 5, 2],\ [17, 15, 52],\ [17, 46, 257],$
$[17, 47, 548],\ [29, 9, 13],\ [29, 26, 53],\ [41, 11, 20],\ [53, 13, 29],\ [61, 9, 5],$
$[73, 9, 2],\ [73, 47, 388],\ [89, 11, 8],\ [97, 94, 657],\ [109, 17, 45],$
$[137, 35, 272],\ [149, 13, 5],\ [157, 25, 117],\ [181, 41, 13],\ [233, 19, 32],\ [269, 17, 5],$
$[281, 17, 2],\ [389, 37, 245]$

with class number 1*;*

$[5, 11, 29],\ [5, 33, 261],\ [5, 66, 909],\ [8, 50, 425],\ [8, 66, 1017],\ [17, 25, 50],$
$[29, 7, 5],\ [29, 21, 45],\ [101, 33, 45],\ [113, 33, 18],\ [8, 14, 41],\ [8, 26, 137],$
$[12, 8, 13],\ [12, 10, 13],\ [12, 14, 37],\ [12, 26, 61],\ [12, 26, 157],\ [44, 8, 5],$
$[44, 14, 5],\ [76, 18, 5],\ [172, 34, 117],\ [236, 32, 20]$

with class number 2*;*

$[257, 23, 68]$

with class number 3*;*

$[8, 30, 153],\ [12, 50, 325],\ [44, 42, 45]$

with class number 4*.*

We start the proof by combining the ramification results into the following explicit form for K^r.

Lemma 3.18. Suppose $I_0(\Phi^r) = I_{K^r}$. Then there exist prime numbers p, q, and $s_1 < \cdots < s_u$ with $u \in \{t_{K^r} - 1,\ t_{K^r} - 2\}$ such that all of the following hold. We have $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$ with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. There

exists a prime $\mathfrak{p}$ lying above p in F^r that ramifies in K^r, an odd $j > 0$ in $\mathbb{Z}$ and a totally positive generator π of $\mathfrak{p}^j$. Moreover, for exactly one such $\mathfrak{p}$ and each such π and j, we have $K^r \cong \mathbb{Q}(\sqrt{-\pi s_1 \cdots s_u})$.

Proof. By Proposition 3.7, we have $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$.

There exists a totally positive element β in F^{r*} such that $K^r = F^r(\sqrt{-\beta})$, where β is uniquely defined up to $(F^{r*})^2$ (without loss of generality, we can take β in $\mathcal{O}_{F^r}$).

Since $\mathcal{O}_{K^r} \supset \mathcal{O}_{F^r}[\sqrt{-\beta}] \supset \mathcal{O}_{F^r}$, the quotient of the discriminant ideals $\Delta(\mathcal{O}_{K^r}/\mathcal{O}_{F^r})/\Delta(\mathcal{O}_{F^r}[\sqrt{-\beta}]/\mathcal{O}_{F^r})$ is a square ideal in $\mathcal{O}_{F^r}$, see Cohen [4, pp.79], where $\Delta(\mathcal{O}_{F^r}[\sqrt{-\beta}]/\mathcal{O}_{F^r}) = (-4\beta)$. As β is unique up to squares, and we can take $\mathfrak{l}$-minimal $\beta' \in \beta(F^*)^2$ for each prime $\mathfrak{l}$ of $\mathcal{O}_{F^r}$, we get

$$\text{ord}_{\mathfrak{l}}((\beta)) \equiv \begin{cases} 1 \pmod 2 & \text{if } \mathfrak{l} \text{ is ramified in } K^r/F^r \text{ and } \mathfrak{l} \not| 2, \\ 0 \pmod 2 & \text{if } \mathfrak{l} \text{ is not ramified in } K^r/F^r, \\ 0 \text{ or } 1 \pmod 2 & \text{if } \mathfrak{l} \text{ is ramified in } K^r/F^r \text{ and } \mathfrak{l} | 2. \end{cases} \tag{3.5}$$

Let $\mathfrak{l}_1, \cdots, \mathfrak{l}_{t_{K^r}} \subseteq \mathcal{O}_{F^r}$ be the primes over the prime numbers $l_1, \cdots, l_{t_{K^r}}$, respectively, that ramify in K^r/F^r. Let $n_i > 0$ be minimal such that $\mathfrak{l}_i^{n_i}$ is generated by a totally positive $\lambda_i \in \mathcal{O}_{F^r}$. Since $F^r = \mathbb{Q}(\sqrt{q})$ with prime $q \not\equiv 3 \pmod 4$, genus theory implies that $\text{Cl}_{F^r} = \text{Cl}^+_{F^r}$ has odd order, and so n_i is odd. Let

$$\alpha = \prod_{i=1}^{t_{K^r}} \lambda_i^{(\text{ord}_{\mathfrak{l}_i}((\beta)) \bmod 2)}.$$

By proving the following two claims we finish the proof.

Claim 1. We have $\alpha/\beta \in (F^{r*})^2$.

Claim 2. We have $\alpha = \pi s_1 \cdots s_u$ with π, s_i and u as in the statement.

Proof of Claim 1. We first prove that $(\alpha/\beta) = (\alpha)/(\beta)$ is a square ideal.

Let $\mathfrak{l}$ be any prime of F^r. If $\mathfrak{l}$ is unramified in K^r/F^r, then by (3.5), we have $\text{ord}_{\mathfrak{l}}((\beta)) \equiv 0 \pmod 2$ so $\text{ord}_{\mathfrak{l}}((\alpha)) = 0$. If $\mathfrak{l}$ is ramified in K^r/F^r, then there exists i such that $\mathfrak{l} = \mathfrak{l}_i$, so $\text{ord}_{\mathfrak{l}}((\alpha)) \equiv \text{ord}_{\mathfrak{l}_i}((\beta)) \cdot \text{ord}_{\mathfrak{l}_i}((\lambda_i)) \equiv \text{ord}_{\mathfrak{l}_i}((\beta)) \pmod 2$ as $n_i = \text{ord}_{\mathfrak{l}_i}((\lambda_i))$ is odd. Therefore, the ideal $(\frac{\alpha}{\beta})$ is a square of an ideal $\mathfrak{a}$ in $\mathcal{O}_{F^r}$.

Thus $\mathfrak{a}^2$ is generated by the totally positive α/β. So the ideal class $[\mathfrak{a}]$ is 2-torsion in $\mathrm{Cl}^+_{F^r}$, which has an odd order, so there is a totally positive element $\mu \in F^r$ that generates $\mathfrak{a}$. So $\alpha/\beta = \mu^2 \cdot v$ for some $v \in (\mathcal{O}^*_{F^r})^+$. Since $\mathrm{Cl}_{F^r} = \mathrm{Cl}^+_{F^r}$, the norm of the fundamental unit ϵ is negative. Therefore, a unit in $\mathcal{O}_{F^r}$ is totally positive if and only if it is a square in $\mathcal{O}_{F^r}$. Hence, we have $\alpha/\beta \in (F^{r*})^2$.

Proof of Claim 2. For any given i, if l_i is inert in $F^r/\mathbb{Q}$, then $n_i = 1$ and $\lambda_i = l_i \in \mathbb{Z}_{>0}$ is prime. If l_i is not inert in $F^r/\mathbb{Q}$ then $l_i \in \{p,\ q\}$, by Proposition 3.7. If $l_i = q$, then $\mathfrak{l}_i$ is not ramified in K^r/F^r otherwise by Corollary 3.11 we get $\sqrt{q} \in F$. So $l_i = p$.

Let $\{s_1, \cdots, s_u\} = \{l_i \ :\ l_i \text{ is inert in } F^r/\mathbb{Q} \text{ and ramified in } K^r/F^r \text{ and } \mathrm{ord}_{\mathfrak{l}_i}((\beta)) \equiv 1 \pmod 2\}$. Then $u \in \{t_{K^r} - 1,\ t_{K^r} - 2,\ t_{K^r} - 3\}$ by (3.5).

Let $p\mathcal{O}_{F^r} = \mathfrak{p}\mathfrak{p}'$. Then we have $\alpha = \pi^a \pi'^{a'} \prod_{i=1}^u s_i^{(1 \bmod 2)}$, where π and π' are totally positive generators of $\mathfrak{p}^j$ and $\mathfrak{p}'^j$ for odd j. Here, we have $\prod_{i=1}^u s_i^{(1 \bmod 2)} \in \mathbb{Z}$ and $a,\ a' \in \{0,\ 1\}$. If $a = a'$, then $\alpha \in \mathbb{Z}$, which leads to contradiction since K^r is non-biquadratic. So for a unique $\mathfrak{p}$, we can take $a_1 = 1$ and $a_2 = 0$. In particular, we have $u \in \{t_{K^r} - 1,\ t_{K^r} - 2\}$. □

Combining Lemma 3.18 and the bound on the discriminant in Proposition 3.16, we now have a good way of listing the fields. Next, we need a fast way of eliminating fields from our list if they have CM class number > 1.

The following lemma is a special case of Theorem D in Louboutin [10].

Lemma 3.19. Let K be a non-biquadratic quartic CM field with real quadratic subfield F. Let d_K and d_F be the absolute values of the discriminants of K and F. Then assuming $I_0(\Phi^r) = I_{K^r}$, if a rational prime l totally splits in $K^r/\mathbb{Q}$, then $l \geq \frac{\sqrt{d_K/{d_F}^2}}{4}$.

Proof. Let l be a prime that totally splits in $K^r/\mathbb{Q}$. Let $\mathfrak{l}_{K^r}$ be a prime ideal in K^r above l. By the assumption $I_0(\Phi^r) = I_{K^r}$, there exists $\tau \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{l}_{K^r}) = (\tau)$ and $\tau\overline{\tau} = l$. Here $\tau \neq \overline{\tau}$, since $\sqrt{l} \notin K$. Then since $\mathcal{O}_K \supset \mathcal{O}_F[\tau]$ and $\Delta(\mathcal{O}_F[\tau]/\mathcal{O}_F) = (\tau - \overline{\tau})^2$, we have $d_K/d_F^2 = \mathrm{N}_{F/\mathbb{Q}}(d_{K/F}) = \mathrm{N}_{F/\mathbb{Q}}(\Delta(\mathcal{O}_K/\mathcal{O}_F)) \leq$

$\mathrm{N}_{F/\mathbb{Q}}((\tau-\overline{\tau})^2)$. Moreover, since $\tau\overline{\tau}=l$, we have $(\tau-\overline{\tau})^2 \le (2\sqrt{l})^2$ for all embeddings of F into $\mathbb{R}$, hence $d_K/d_F^2 \le \mathrm{N}_{F/\mathbb{Q}}((\tau-\overline{\tau})^2) \le 16l^2$. □

Every prime s_i as in Lemma 3.18 divides $\Delta(K^r/F^r)$ and so $s_i^2|d_{K^r}$, hence $s_i^4|d_N$. The primes p and q are ramified in F and F^r, so p^4 and q^4 divide the discriminant d_N of the normal closure N of degree 8. Hence $d_N \ge p^4q^4s_1^4\cdots s_{t-1}^4$.

Algorithm 3.20. ***Output:*** *$[D,\ A,\ B]$ representations of all non-normal quartic CM fields K satisfying $I_0(\Phi^r)=I_{K^r}$.*

Step 1. Find all square-free integers smaller than $3\cdot10^{10}$ having at most 8 prime divisors and find all square-free integers smaller than 222^2.

Step 2. Order the prime factors of each of these square-free integers as tuples of primes $(p,q,s_1,\cdots,s_u)$ with $s_1<\cdots<s_u$ in $(u+1)(u+2)$-ways, then take only the tuples satisfying $q\not\equiv 3 \pmod 4$, $(p/q)=(q/p)=1$ and $(p/s_i)=(q/s_i)=-1$ for all i.

Step 3. For each $(p,q,s_1,\cdots,s_u)$, let $F^r=\mathbb{Q}(\sqrt{q})$, write $p\mathcal{O}_{F^r}=\mathfrak{p}\mathfrak{p}'$, and take $\alpha=\pi\cdot s_1\cdots s_u\in F^r$, where π is a totally positive generator of $\mathfrak{p}^j$ for an odd $j\in\mathbb{Z}_{>0}$. Construct $K^r=F^r(\sqrt{-\alpha})$.

Step 4. Eliminate the fields K^r that have totally split primes in K^r below the bound $\sqrt{d_K/d_F^2}/4$. (In this step we eliminate most of the CM fields.)

Step 5. For each $\mathfrak{q}$ with norm Q below the bound $12\log(|d_{K^r}|)^2$, check whether it is in $I_0(\Phi^r)$ as follows. List all quartic Weil Q-polynomials, that is, monic integer polynomials of degree 4 such that all roots in $\mathbb{C}$ have absolute value $\sqrt{Q}$. For each, take its roots in K and check whether $\mathrm{N}_{\Phi^r}(\mathfrak{q})$ is generated by such a root. If not, then $\mathfrak{q}$ is not in $I_0(\Phi^r)$, so we throw away the field.

Step 6. For each K^r, compute the class group of K^r and test $I_0(\Phi^r)/P_{K^r}=I_{K^r}/P_{K^r}$.

Step 7. Find $[D,\ A,\ B]$ representations for the reflex fields K of the remaining pairs (K^r,Φ^r).

Proof. Note that Step 4 and Step 5 of the algorithm above do not affect the validity of the algorithm by Lemma 3.19. These two steps are only to speed up the computation.

Suppose that a non-normal quartic CM field K satisfies $I_0(\Phi^r) = I_{K^r}$. Then by Lemma 3.18, we have $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Also by Lemma 3.18, there exist a prime $\mathfrak{p}$ lying above p in F^r that ramifies in K^r and a totally positive element $\alpha = \pi s_1 \cdots s_u$, where π is a totally positive generator of $\mathfrak{p}^j$ for an odd $j \in \mathbb{Z}_{>0}$ such that $K^r = F^r(\sqrt{-\alpha})$. By Proposition 3.7, the ramified primes in K^r/F^r that are distinct from $\mathfrak{p}$ are inert in F and F^r. As $s_1, \cdots, s_u$ are such primes, we have $(p/s_i) = -1$ and $(q/s_i) = -1$. By Lemma 3.16, we have either $h^*_{K^r} = 2^{t_{K^r}-1} \leq 2^5$ and $d_{K^r}/d_{F^r} \leq 3 \cdot 10^{10}$ or $d_N < 222^8$. Therefore, the CM field K is listed. □

We implemented the algorithm in SAGE [18, 17, 23] and obtained the list of the fields in Theorem 3.17. The implementation is available online at [8]. This proves Theorems 3.17 and 1.1. □

This computation takes few days on a computer.

Remark 3.21. *There are no fields eliminated in Step 6, because they turned out to be already eliminated in Step 5.*

4 The cyclic quartic CM fields

In [15], Murabayashi and Umegaki determined the *cyclic* CM fields whose ring of integers are isomorphic to the endomorphism rings of the (simple) Jacobians of genus-2 curves defined over $\mathbb{Q}$. Such fields have CM class number one, however there are more examples, for example, the fields in Table 1b of [3] have CM class number one, but the curves corresponding to these fields have not a model over $\mathbb{Q}$. We apply the strategy in the previous section to cyclic quartic CM fields and list all cyclic quartic CM fields with CM class number one. Murabayashi [14, Proposition 4.5] proves that the relative class group of cyclic quartic CM fields with CM class number one is 2^{t_K-1},

where t_K is the number of ramified primes in K/F. This result also follows from Proposition 3.1 in Section 3.1.

Suppose that $K/\mathbb{Q}$ is a cyclic quartic CM field with $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Since $K/\mathbb{Q}$ is normal, we consider CM types with values in K. The CM type, up to equivalence, is $\Phi = \{\mathrm{id}, \sigma\}$, which is primitive. The reflex field K^r is K and the reflex type of Φ is the CM type $\{\mathrm{id}, \sigma^3\}$ (Example 8.4(1) of [21]). In this notation complex conjugation $^-$ is σ^2.

Suppose $K \cong \mathbb{Q}(\zeta_5)$, where ζ_m denotes a primitive m-th of unity. Then the class group of K is trivial, so the equality $I_0(\Phi^r) = I_K$ holds. Hence $K = \mathbb{Q}(\zeta_5)$ will occur in the list of cyclic quartic fields satisfying $I_0(\Phi^r) = I_K$.

From now on, suppose $K \ncong \mathbb{Q}(\zeta_5)$.

Lemma 4.1. (Murabayashi [14], Lemma 4.2) If $I_0(\Phi^r) = I_K$, then there is exactly one totally ramified prime in $K/\mathbb{Q}$ (i.e., $F = \mathbb{Q}(\sqrt{p})$ with prime $p \not\equiv 3 \pmod 4$) and the other ramified primes of $K/\mathbb{Q}$ are inert in $F/\mathbb{Q}$. □

Example 4.2. *Suppose $I_0(\Phi^r) = I_K$. The relative class number h_K^* equals 1 if and only if K/F has exactly one ramified prime. This ramified prime is $\sqrt{p}$ when $F = \mathbb{Q}(\sqrt{p})$.*

Now, we determine such CM fields by using a lower bound on their relative class numbers from analytic number theory.

Theorem 4.3. *(Louboutin [11], Theorem 5) Let K be a cyclic quartic CM field of conductor f_K and discriminant d_K. Then we have*

$$h_K^* \geq \frac{2}{3e\pi^2}\left(1 - \frac{4\pi e^{1/2}}{d_K^{1/4}}\right)\frac{f_K}{(\log(f_K) + 0.05)^2}. \tag{4.1}$$

□

Proposition 4.4. *Let K be a cyclic quartic CM field satisfying $I_0(\Phi^r) = I_K$. Then we have $h_K^* \leq 2^5$ and $f_K < 2.1 \cdot 10^5$.*

Proof. Lemma 4.1 implies, under the assumption, that there is exactly one totally ramified prime in $K/\mathbb{Q}$ and the other ramified primes of $K/\mathbb{Q}$ are inert in $F/\mathbb{Q}$.

Let Δ_t be the product of the first t-primes. The ramified primes in $K/\mathbb{Q}$ divide the conductor f_K, so we have $f_K > \Delta_{t_K}$. Further, by Proposition 11.9 and 11.10 in Chapter VII [16], we have $d_K = f_K^2 \cdot d_F$ so $d_K > \Delta_{t_K}^2$. The right hand side of (4.1) is monotonically increasing with $f_K > 2$. Further, by Proposition 3.1, we have $h_K^* = 2^{t_K - 1}$, so, by dividing the both side of (4.1) by 2^{t_K-1}, we obtain

$$1 \geq \frac{2}{3e\pi^2}\left(1 - \frac{4\pi e^{1/2}}{\Delta_{t_K}^{1/2}}\right)\frac{\Delta_{t_K}}{2^{t_K}(\log(\Delta_{t_K}) + 0.05)^2}. \tag{4.2}$$

The right hand side of (4.2) is monotonically increasing with $t_K \geq 2$, and if $t_K = 7$, then the right hand side is greater than 1. Hence $t \leq 6$. So we get $h_K^* \leq 2^5$, and therefore, we get $f_K < 2.1 \cdot 10^5$. □

Theorem 4.5. *There exist exactly* 20 *isomorphism classes of cyclic quartic CM fields K with CM class number one. The fields are given by $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B) \supset \mathbb{Q}(\sqrt{D})$ where $[D, A, B]$ ranges over*

$$[5,5,5],\ [8,4,2],\ [13,13,13],\ [29,29,29],\ [37,37,333],\ [53,53,53],\ [61,61,549]$$

with class number 1*;*

$$[5,65,845],\ [5,85,1445],\ [5,10,20],\ [8,12,18],$$

$$[8,20,50],\ [13,65,325],\ [13,26,52],\ [17,119,3332]$$

with class number 2*;*

$$[5,30,180],\ [5,35,245],\ [5,15,45],\ [5,105,2205],\ [17,255,15300]$$

with class number 4*.*

We start proving with the following lemma.

Lemma 4.6. If a cyclic quartic CM field K satisfies $I_0(\Phi^r) = I_K$, then there exist prime numbers $p,\ s_1, \cdots, s_u \in \mathbb{Z}$ such that $F = \mathbb{Q}(\sqrt{p})$ with $p \not\equiv 3 \pmod 4$ and $(p/s_i) = -1$ for all i, and we have $K^r \cong \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}})$ with $u \in \{t_K - 1,\ t_K - 2\}$ for every $\epsilon \in \mathcal{O}_F^*$ with $\epsilon\sqrt{p} >> 0$.

Proof. By Proposition 4.1, we have $F = \mathbb{Q}(\sqrt{p})$, where p is prime $p \not\equiv 3 \pmod 4$. If there are t_K ramified primes in K/F, the ones that are distinct from the one above p are inert in $F/\mathbb{Q}$, by Proposition 4.1, denote them by $s_1, \cdots, s_{t_K}$.

There exists a totally positive element β in F^* (without loss and generality, we can take β in $\mathcal{O}_F$) such that $K = F(\sqrt{-\beta})$, where β is uniquely defined up to $(F^*)^2$. As in the proof of Lemma 3.18 in the previous section, we will define a totally positive element $\alpha \in F^*$ with respect to the ramified primes in K/F and show that α and β differ by a factor in $(F^*)^2$.

Let $\epsilon \in \mathcal{O}_F^*$ such that $\epsilon\sqrt{p} >> 0$. This element exists since $p \not\equiv 3 \pmod 4$. As β is unique up to squares and we can take $\mathfrak{l}$-minimal $\beta' \in \beta(F^*)^2$ for each prime $\mathfrak{l}$ of $\mathcal{O}_F$, then we get the cases in (3.5) for $\mathrm{ord}_{\mathfrak{l}}((\beta))$.

If $p \neq 2$ and the prime (2) in $\mathcal{O}_F$ is ramified in K/F with $\mathrm{ord}_{(2)}((\beta)) \equiv 0 \pmod 2$, then take $\alpha := \epsilon s_1 \cdots s_u\sqrt{p}$ with $u = t_K - 2$. If $p = 2$ and $\mathrm{ord}_{(\sqrt{2})}((\beta)) \equiv 0 \pmod 2$, then take $\alpha := s_1 \cdots s_u$ with $u = t_K - 1$. For all other cases in (3.5), take $\alpha := \epsilon s_1 \cdots s_u\sqrt{p}$ with $u = t_K - 1$.

By construction of α, for all ideals $\mathfrak{l} \subset \mathcal{O}_F$ we have $\mathrm{ord}_{\mathfrak{l}}((\alpha/\beta)) \equiv 0 \pmod 2$. So $(\alpha/\beta) = \mathfrak{a}^2$ for a fractional $\mathcal{O}_F$-ideal $\mathfrak{a}$. The ideal $\mathfrak{a}$ is a 2-torsion element in Cl_F. Since $F = \mathbb{Q}(\sqrt{p})$ with $p \not\equiv 3 \pmod 4$, genus theory implies that $\mathrm{Cl}_F = \mathrm{Cl}_F^+$ has odd order. Therefore, there is a totally positive element μ that generates $\mathfrak{a}$. So $\alpha/\beta = \mu^2 \cdot v$ for some $v \in \mathcal{O}_F^+$. Since $\mathrm{Cl}_F = \mathrm{Cl}_F^+$, the fundamental unit has negative norm, and so $\mathcal{O}_F^+ = (\mathcal{O}_F)^2$. Hence, $\alpha/\beta \in (F^*)^2$.

In the case $p = 2$ and $\mathrm{ord}_{(\sqrt{2})}((\beta)) \equiv 0 \pmod 2$, we get $K = F(\sqrt{-s_1 \cdots s_u})$, which is a biquadratic extension of $\mathbb{Q}$. Therefore, we get $K = \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u\sqrt{p}})$ with $u \in \{t_{K-1},\ t_{K-2}\}$. □

Algorithm 4.7. ***Output:*** *$[D,\ A,\ B]$ representations of all cyclic quartic CM fields K satisfying $I_0(\Phi^r) = I_K$.*

Step 1. Find all square-free integers less than $2.1 \cdot 10^5$ and having at most 6 prime divisors.

Step 2. *Order the prime factors of each of these square-free integers as tuples of primes* $(p, s_1, \cdots, s_u)$ *with* $s_1 < \cdots < s_u$ *in* $(u+1)$*-ways, then take only the tuples satisfying* $p \not\equiv 3 \pmod 4$ *and* $(p/s_i) = -1$ *for all* i.

Step 3. *For each* $(p, s_1, \cdots, s_u)$, *let* $F = \mathbb{Q}(\sqrt{p})$ *and take a totally positive element* $\alpha = \epsilon s_1 \cdots s_u \sqrt{p}$, *where* ϵ *is a fundamental unit in* F *such that* $\epsilon\sqrt{p} >> 0$. *Construct* $K = F(\sqrt{-\alpha})$.

Step 4. *Eliminate the fields* K *that have totally split primes in* K *below the bound* $\sqrt{d_K/d_F^2}/4$. *(In this step we eliminate most of the CM fields.)*

Step 5. *For each* $\mathfrak{q}$ *with norm* Q *below the bound* $12\log(|d_{K^r}|)^2$, *check whether it is in* $I_0(\Phi^r)$ *as follows. List all quartic Weil* Q*-polynomials, that is, monic integer polynomials of degree* 4 *such that all roots in* $\mathbb{C}$ *have absolute value* $\sqrt{Q}$. *For each, take its roots in* K *and check whether* $\mathrm{N}_{\Phi^r}(\mathfrak{q})$ *is generated by such a root. If not, then* $\mathfrak{q}$ *is not in* $I_0(\Phi^r)$, *so we throw away the field.*

Step 6. *For each* K *compute the class group of the fields* K *and test* $I_0(\Phi^r)/P_K = I_K/P_K$.

Step 7. *Find* $[D,\ A,\ B]$ *representations for the quartic CM class number one fields* K.

Proof. The idea of the proof of this algorithm is exactly as the proof of Algorithm 3.20. In this algorithm, Step 1 follows from Proposition 4.4; Step 2 and 3 follow from Lemma 4.6; Step 4 follows from Lemma 3.19. □

We implemented the algorithm in SAGE [18, 17, 23] and obtained the list of the fields in Theorem 4.5. The implementation is available online at [8]. This proves Theorems 1.2 and 4.5. □

This computation takes few hours on a computer.

References

[1] Alan Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[2] Gaetan Bisson and Marco Streng. On polarised class groups of orders in quartic cm-fields. *accepted for publication in Mathematical Research Letters,* `http://arxiv.org/pdf/1302.3756v4.pdf`, 2015.

[3] Florian Bouyer and Marco Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015.

[4] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[5] David Kohel et al. Echidna algorithms for algebra and geometry experimentation. `http://echidna.maths.usyd.edu.au/~kohel/dbs/complex_multiplication2.html`.

[6] Eyal Z. Goren and Kristin E. Lauter. Genus 2 curves with complex multiplication. *Int. Math. Res. Not. IMRN*, (5):1068–1142, 2012.

[7] Kurt Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[8] Pınar Kılıçer. Sage packages for computing (non-biquadratic) quartic cm fields with cm class number one. `http://pub.math.leidenuniv.nl/~kilicerp/codes/`.

[9] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[10] Stéphane Louboutin. On the class number one problem for nonnormal quartic CM-fields. *Tohoku Math. J. (2)*, 46(1):1–12, 1994.

[11] Stéphane Louboutin. CM-fields with cyclic ideal class groups of 2-power orders. *J. Number Theory*, 67(1):1–10, 1997.

[12] Stéphane Louboutin. Explicit lower bounds for residues at $s = 1$ of Dedekind zeta functions and relative class numbers of CM-fields. *Trans. Amer. Math. Soc.*, 355(8):3079–3098, 2003.

[13] James S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[14] Naoki Murabayashi. The field of moduli of abelian surfaces with complex multiplication. *J. Reine Angew. Math.*, 470:1–26, 1996.

[15] Naoki Murabayashi and Atsuki Umegaki. Determination of all $\mathbf{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces. *Sūrikaisekikenkyūsho Kōkyūroku*, (1160):169–176, 2000. Analytic number theory and related topics (Japanese) (Kyoto, 1999).

[16] Juŕgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[17] PARI. Pari/gp computer algebra system. `http://pari.math.u-bordeaux.fr/`.

[18] SageMath. Sage mathematics software. `http://www.sagemath.org/`.

[19] Goro Shimura. On abelian varieties with complex multiplication. *Proc. London Math. Soc. (3)*, 34(1):65–86, 1977.

[20] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[21] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[22] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[23] Marco Streng. Sage package for using shimura's reciprocity law. `http://pub.math.leidenuniv.nl/~strengtc/recip/`.

[24] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.

[25] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.