Intersection of class fields

Kühne, Lars

Published in:
Acta Arithmetica

DOI:
10.4064/aa180717-9-6

Publication date:
2021

Document version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
https://doi.org/10.4064/aa180717-9-6
Intersection of class fields

by

LARS KÜHNE (Basel)

1. Introduction. The arithmetic of modular curves is essentially determined by their special points. In fact, their canonical models are defined by demanding the “right” Galois action on their special points. This Galois action can be expressed completely in terms of class field theory. This is why it is not surprising that problems in the arithmetic geometry of Shimura curves, say the André–Oort conjecture for $Y(1)^n$, can be approached by studying the class field theory associated with special points. In particular, intersections of ring class fields appear rather frequently in this situation (e.g., in [2] and [30]).

Our first result is a rather general restriction on the intersection of the maximal abelian extensions of distinct number fields. Throughout this article, we consider all number fields as subfields of a fixed algebraic closure $\overline{\mathbb{Q}}$. In addition, we denote by $K^{ab} \subset \overline{\mathbb{Q}}$ the maximal abelian extension of a number field $K \subset \overline{\mathbb{Q}}$. We say that a positive integer $n$ annihilates a profinite group $G$ if $g^n = 1$ for all $g \in G$. In other words, $n$ is said to annihilate $G$ if the profinite group $G$ has a finite exponent $e(G)$ and $n$ divides $e(G)$.

**Theorem 1.1.** Let $k$ be a number field and let $K_1/k, \ldots, K_r/k$ ($r \geq 2$) be finite normal extensions such that $K_i \cap K_j = k$. Write $K = K_1 \cdots K_r$ and $L = K_r \prod_{i=1}^{r-1} K_i^{ab}$. Then the (profinite) Galois group $\text{Gal}(K^{ab}_r \cap L/K_r^{ab})$ is annihilated by

$$e(\text{Gal}(K^{ab}_r/K_r^{ab})) \cdot \text{lcm}_{i \neq j} \{[K : K_i][K_j : k]\}.$$  

This simple theorem does not seem to have appeared in the literature so far. We deduce the following corollary concerning ring class fields. To state it, we briefly indicate our notation but postpone the details to Sections 2.1.
For a CM-field $K \subset \mathbb{Q}$ with maximal totally real subfield $F$, there is a group-theoretic transfer map $\text{Gal}(F^{ab}/F) \to \text{Gal}(K^{ab}/K)$. The fixed field of its image, which we call henceforth the “transfer field” $K^{\text{tf}} \subset \mathbb{Q}$, is closely connected to ring class fields. In fact, let $K^{\text{rcf}} \subset \mathbb{Q}$ denote the union of all ring class fields associated with orders in $K$. It is then easy to prove that $\text{Gal}(K^{\text{rcf}}/K^{\text{tf}}) \approx \text{Pic}(\mathcal{O}_F)$ (Lemma 3.2). In particular, both fields coincide for $F = \mathbb{Q}$.

**Corollary 1.2.** Given a totally real field $F$, let $K_1, \ldots, K_r$ ($r \geq 2$) be distinct CM-fields with maximal totally real subfield $F$. Write $L = K_r \prod_{i=1}^{r-1} K_i^{\text{tf}}$. Then the Galois group $\text{Gal}(K_i^{\text{tf}} \cap L/K_r)$ is annihilated by $2^{r+1}$.

This result is an improvement of [30, Proposition 18]. For the intersection of two ring class fields (i.e., $r = 2$), a slightly stronger result (cf. [10, Theorem 8.3.12]) is already known. This more precise result of Cohn, with $2^{r-1}$ instead of $2^{r+1}$, does not follow from our more general one. For general $r > 2$, we ignore the optimal bound on the exponent of $\text{Gal}(K_i^{\text{tf}} \cap L/K_r)$; a direct argument not proceeding through Theorem 1.1 may produce a better exponent. However, this numerical weakness causes probably no harm in most applications.

For comparison with the above-mentioned result of [10], let us mention that Cohn’s “ring class fields” are the finite subextensions $K'/K$ of the extension $K^{\text{rcf}}/K$ in the case where $K$ is an imaginary quadratic extension of $\mathbb{Q}$. His proof relies essentially on the fact that $\text{Gal}(K'/\mathbb{Q}) = \text{Gal}(K'/K) \rtimes \text{Gal}(K/\mathbb{Q})$ where the non-trivial element of $\text{Gal}(K'/\mathbb{Q})$ acts on the normal subgroup $\text{Gal}(K'/K)$ as inversion (cf. [11, Theorem 9.18]). It is then an easy group-theoretic argument to show that if $K'$ is a ring class field for two distinct imaginary quadratic fields $K_1$ and $K_2$ then the Galois group $\text{Gal}(K'/\mathbb{Q})$ has to have exponent 2. Cohn’s proof generalizes to arbitrary CM-fields $K_1$ and $K_2$ with the same maximal totally real subfield $F$, but it does not seem to work in the case $r > 2$.

Having established Corollary 1.2, we demonstrate its efficacy by describing its application to two problems of arithmetic geometry concerning modular curves. In these applications, there is neither need for the generality provided by Theorem 1.1 nor for Corollary 1.2 in the case $F \neq \mathbb{Q}$. However, the exposition does not simplify by dropping either generality. In addition, Theorem 1.1 seems to merit record as it may have some uses quite distant from those developed here.

Our first application of Corollary 1.2 yields a strengthening of a result on Heegner points proven by Rosen and Silverman [30]. We refer to Section 2.2 for a precise definition of the modular curves $Y_0(N)$, $N \geq 1$, and to Sec-
tion 2.3 for a discussion of CM-points. The Jacobian of the compactification $X_0(N)$ of $Y_0(N)$ is denoted by $J_0(N)$. By the work of Wiles, Taylor, and others [8, 36, 38], each elliptic curve $E/\mathbb{Q}$ of conductor $N$ admits a modular parameterization by $X_0(N)$ (i.e., a surjective homomorphism $J_0(N) \to E$ of abelian varieties).

**Theorem 1.3.** Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and $\pi : J_0(N) \to E$ a modular parameterization. Then there exists an effectively computable constant $c_1 = c_1(E, \pi, r) > 0$ for each positive integer $r$ such that the following assertion is true. Let $P_i, 1 \leq i \leq r$, be a CM-point on $Y_0(N)$ with associated CM-field $K_i$. One of the following three statements is true:

1. $K_i = K_j$ for some $1 \leq i < j \leq r$, or
2. one of the CM-points $P_i$ is associated with an order of discriminant less than $c_1$, or
3. the points $\pi(P_1), \ldots, \pi(P_r) \in E(\overline{\mathbb{Q}})$ generate a free $\mathbb{Z}$-module of rank $r$.

In the original result of Rosen and Silverman, a class of CM-fields has to be excluded. Heuristically, this class should contain infinitely many CM-fields (cf. [30, Section 10]) (1). Replacing their central result [30, Proposition 18] with our stronger Corollary 1.2, we can lift this restriction effectively. To obtain an effective constant $c_1$, we also have to replace Siegel’s class number theorem [31] with the Siegel–Tatuzawa theorem [35] as well as to use Lombardo’s effective version [22] of Serre’s open image theorem [32]. The Siegel–Tatuzawa theorem has already been used in a previous work of the author [20] for similar purposes. For comparison with [30], it should also be mentioned that we impose no Heegner condition on the orders associated with the CM-points $P_i$ (cf. [30, Section 1]). This means that the cyclic isogeny encoded within $P_i \in Y_0(N)(\overline{\mathbb{Q}})$ is not required to constitute an endomorphism of the associated CM-elliptic curve. For completeness, let us also mention that Şahinoğlu [31] has proven a result similar to [30] in the case where $E$ is a CM-elliptic curve, but under the same restriction on the CM-fields $K_i$ as in [30]. When the present article was under review, Pila and Tsimerman proved a substantial generalization [29, Corollary 1.2] of our Theorem 1.3, which is however not effective. The referee has also suggested to point out the related results [9, 37], which seem however outside the purview of our approach.

Our second application of Corollary 1.2 is a weak but effective result of André–Oort type for a product of modular curves. Recall that the com-
ponents of a special point in $Y(1)^n$ are CM-points in $Y(1)$. We can thus associate with each special point $P \in Y(1)^n$ an $n$-tuple $(K_1(P), \ldots, K_n(P))$ of CM-fields. We refer to Section 2.2 for further details. To spare additional notation, we do not fix any specific degree or height for subvarieties in $Y(1)^n$. Of course, every common choice works as we do only assert effective boundedness. For the definition of heights, the reader is referred to the textbooks \[7, 18, 40\].

**Theorem 1.4.** Let $X$ be an irreducible subvariety of $Y(1)^n$ ($n \geq 2$). Assume that there exists no coordinate permutation $\pi : Y(1)^n \rightarrow Y(1)^n$ and no algebraic subvariety $X' \subset Y(1)^{n-1}$ such that $\pi(X) = Y(1) \times X'$ or $\pi(X) = Q \times X'$ with some point $Q \in Y(1)(\overline{Q})$. Then there exists a proper algebraic subset $Z \subset X$ such that any special point $P$ in $X \setminus Z$ satisfies $K_i(P) = K_j(P)$ for some pair $(i, j)$ with $1 \leq i \neq j \leq n$. The degree, the height, and the degree of the field of definition of $Z$ can be effectively bounded in terms of the same quantities associated with $X$.

The theorem generalizes basically the first step of André’s proof \[2\] of the André–Oort conjecture for a product of two modular curves. Evidently, a non-effective version of the above theorem is also implied by Pila’s Theorem \[28\]. However, his theorem cannot be used to give effective bounds due to several non-effective arguments in his proof. In forthcoming work with Yuri Bilu \[4\], the proof of Theorem 1.4 is refined to prove the André–Oort conjecture effectively for all affine linear subvarieties of $Y(1)^n$. This is substantially beyond the currently known cases concerning curves in $Y(1)^2$ \[11, 15, 16, 20, 39\]. The above Corollary 1.2 is essential for this approach.

2. Preliminaries

2.1. Class field theory. In order to fix notations, we summarize the basics of class field theory. Our reference is \[26\]. For each number field $K$, we denote by $I_K$ its idele group, by $C_K = I_K/K^\times$ its idele class group, and by $K^{ab}$ its maximal abelian extension (in $\overline{Q}$). For an extension $L/K$ of number fields, there is a canonical inclusion $I_K \hookrightarrow I_L$, which induces an inclusion $C_K \hookrightarrow C_L$ \[26, Proposition III.2.6\]. In the other direction, the idele norm $N_{L/K} : I_L \rightarrow I_K$ induces a norm homomorphism $N_{L/K} : C_L \rightarrow C_K$.

Write $G_Q$ for the (profinite) Galois group $\text{Gal}(\overline{Q}/Q)$. For each number field $K$, every element $\sigma \in G_Q$ induces (continuous) isomorphisms $I_K \rightarrow I_{\sigma(K)}$ and $C_K \rightarrow C_{\sigma(K)}$. If $L/K$ is normal with Galois group $G = \text{Gal}(L/K)$ then $I_K = I_L^G$ \[26, Proposition III.2.5\] and $C_K = C_L^G$ \[26, Theorem III.2.7\]. The central object of global class field theory is the topological $G_Q$-module

$$C = \lim_{\longrightarrow} C_K,$$
where the direct limit is taken over all number fields $K$ with respect to the above-mentioned inclusions. Likewise, the $G_{\mathbb{Q}}$-action on $C$ is induced from the above-mentioned isomorphisms $C_K \to C_{\sigma(K)}$.

Global class field theory uses the fact that the pair $(G_{\mathbb{Q}}, C)$ is a class formation (see [26, Definition II.1.3]). With this, we have for each finite extension $L/K$ of number fields a reciprocity isomorphism (see [26, Theorem II.1.9])

$$C_K/N_{L|K}C_L \xrightarrow{\sim} \text{Gal}(L/K)^{ab}$$

and a corresponding norm residue symbol

$$(\cdot, L|K) : C_K \to \text{Gal}(L/K)^{ab}, \quad a \to (a, L|K).$$

Taking profinite limits, we obtain the universal norm residue symbol

$$(\cdot, K^{ab}|K) : C_K \to \text{Gal}(K^{ab}/K) = \text{Gal}(\overline{\mathbb{Q}}/K)^{ab}$$

for each number field $K$; its kernel is

$$D_K = \bigcap_{K \subseteq L \subseteq \overline{\mathbb{Q}}, [L:K] < \infty} N_{L|K}C_L \subset C_K.$$

We need some more information on $D_K$ in case $K$ is a CM-field with maximal totally real subfield $F$. Inspecting [3, Section IX.1] (or [27, Section 8.2]), we note that the kernel of $(\cdot, K^{ab}/K)$ equals

$$D_K = (\mathcal{C}^{\times})^{[F:Q]}\overline{\mathcal{O}_K^{\times}}K^{\times}/K^{\times} \subset C_K$$

where $\overline{\mathcal{O}_K^{\times}}$ is the topological closure of $\mathcal{O}_K^{\times}$ in $I_{K,f}$. By Dirichlet’s unit theorem, we have furthermore $[\mathcal{O}_K^{\times} : \mathcal{O}_F^{\times}] < \infty$. We infer $\overline{\mathcal{O}_K^{\times}}K^{\times} = \overline{\mathcal{O}_F^{\times}}K^{\times} \subset I_{K,f}$ and hence

$$(2.1) \quad D_K \cap I_{K,f}K^{\times}/K^{\times} = \overline{\mathcal{O}_K^{\times}}K^{\times}/K^{\times} = \overline{\mathcal{O}_F^{\times}}F^{\times}/F^{\times}.$$ 

The reciprocity isomorphism and the norm residue symbol satisfy various functoriality compatibilities that can be found in [26, Theorem II.1.11]. We state the three most important compatibilities for later use:

- Let $L/K$ be an extension of number fields. Denote by

  $$\iota_{L/K} : \text{Gal}(L^{ab}/L) \to \text{Gal}(K^{ab}/K)$$

  the homomorphism induced from $\text{Gal}(\overline{\mathbb{Q}}/L) \subseteq \text{Gal}(\overline{\mathbb{Q}}/K)$. Then the following diagram is commutative:

$$(2.2) \quad \begin{array}{ccc}
C_K & \xrightarrow{(\cdot, L^{ab}|L)} & \text{Gal}(L^{ab}/L) \\
N_{L|K} \downarrow & & \downarrow \iota_{L/K} \\
C_L & \xrightarrow{(\cdot, K^{ab}|K)} & \text{Gal}(K^{ab}/K)
\end{array}$$
Let $L/K$ be an extension of number fields. Denote by
\[ \text{Ver} : \text{Gal}(K^\text{ab}/K) \rightarrow \text{Gal}(L^\text{ab}/L) \]
the group-theoretic transfer (defined as “Verlagerung” in [26, Definition 1.4.10]). Then the following diagram is commutative:
\[
\begin{array}{ccc}
C_K & \xrightarrow{(\cdot,K^\text{ab}|K)} & \text{Gal}(K^\text{ab}/K) \\
\downarrow \text{inclusion} & & \uparrow \text{Ver} \\
C_L & \xrightarrow{(\cdot,L^\text{ab}|L)} & \text{Gal}(L^\text{ab}/L)
\end{array}
\]

Let $L/K$ be a normal extension of number fields and $\sigma \in \text{Gal}(L/K)$. Then the following diagram is commutative:
\[
\begin{array}{ccc}
C_L & \xrightarrow{(\cdot,L^\text{ab}|L)} & \text{Gal}(L^\text{ab}/L) \\
\downarrow c \mapsto \sigma(c) & & \downarrow \tau \mapsto \sigma \circ \tau \circ \sigma^{-1} \\
C_L & \xrightarrow{(\cdot,L^\text{ab}|L)} & \text{Gal}(L^\text{ab}/L)
\end{array}
\]

Finally, we make a simple observation invoking (2.2): If $L/K$ is an extension of number fields then the preimage of $\text{Gal}(L^\text{ab}/LK^\text{ab})$ under $(\cdot,L^\text{ab}|L)$ is $N^{-1}_{L/K}(D_K)$.

2.2. Modular curves. We introduce the modular curve $Y(1)$ as well as the modular curves $Y_0(N)$, $N \geq 1$. The reader may find all necessary details in [15, 33]. However, it is convenient for us to recast the definition of modular curves in Deligne’s terminology [13, 14] and we refer to [23] for details. The advantage of this terminology is that it is interwoven with class field theory. We also keep an embedding $\mathbb{Q} \hookrightarrow \mathbb{C}$ fixed when working with modular curves. Write $\mathbb{A}_{K,f}$ (resp. $I_{K,f}$) for the finite adeles (resp. ideles) of a number field $K$. We recall that $\text{GL}_2(\mathbb{R})$ acts on $\mathcal{H}^\pm = \{ z \in \mathbb{C} \mid \text{Im}(z) \neq 0 \}$ by fractional linear transformations, inducing a $\text{GL}_2(\mathbb{Q})$-action on $\mathcal{H}^\pm$.

Let $\mathcal{K}$ be a compact open subgroup of $\text{GL}_2(\mathbb{A}_{\mathbb{Q},f})$. Each $g' \in \text{GL}_2(\mathbb{Q})$ (resp. $k \in \mathcal{K}$) acts on $\mathcal{H}^\pm \times \text{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ by sending $(x,g)$ to $(g'x,g'g)$ (resp. to $(x,gk)$). From these actions, we obtain a double quotient set
\[ S_\mathcal{K}(\mathbb{C}) = \text{GL}_2(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \text{GL}_2(\mathbb{A}_{\mathbb{Q},f})/\mathcal{K}. \]

As usual, we write $[x,g]_\mathcal{K}$ for the element of $S_\mathcal{K}(\mathbb{C})$ that is represented by $(x,g) \in \mathcal{H}^\pm \times \text{GL}_2(\mathbb{A}_{\mathbb{Q},f})$. This set can be interpreted as the complex points of its canonical model $S_\mathcal{K}$, which is a smooth algebraic curve defined over $\mathbb{Q}$. The curve $S_\mathcal{K}$ is not geometrically connected in general. In fact, the determinant
\[ \text{det} : \text{GL}_2 \rightarrow \mathbb{G}_m \] and the sign map
\[ \mathcal{H}^\pm \rightarrow \{ \pm \}, \quad \tau \mapsto \text{sign}(\text{Im}(\tau)), \]
induce a map

$$\text{GL}_2(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \text{GL}_2(\mathbb{A}_{Q,f})/K \to \mathbb{Q}^\times \backslash \{\pm 1\} \times I_{Q,f}/\text{det}(K)$$

and the fibers of this map are the connected components of $S_K(\mathbb{C})$ in other words, the algebraic curve $S_K \times_{\mathbb{Q}} \overline{\mathbb{Q}}$ decomposes as a disjoint union of algebraic curves $S_{K,\alpha}$ indexed by $\alpha \in \mathbb{Q}^\times \backslash \{\pm 1\} \times I_{Q,f}/\text{det}(K)$. The curves $S_{K,\alpha}$ are not definable over $\mathbb{Q}$ in general, but it is easy to describe how the Galois action permutes them: Let $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $a \in I_{\mathbb{Q}}$ be such that $\sigma|_{Q^{ab}} = (a, Q^{ab}|Q)$. Furthermore, let $(\alpha_{\infty}, \alpha_f) \in \{\pm 1\} \times I_{Q,f}$ be a representative of $\alpha$ and write $a = (a_{\infty}, a_f) \in \mathbb{R}^\times \times I_{Q,f}$. With these notations, we have $\sigma(S_{K,\alpha}) = S_{K,\alpha'}$ with $\alpha'$ being represented by $(\text{sign}(a_{\infty})\alpha_{\infty}, a_f\alpha_f)$ (see [24, p. 349]). Given $(\alpha_{\infty}, \alpha_f) \in \{\pm 1\} \times I_{Q,f}$, we choose an arbitrary $\beta_f \in \text{GL}_2(\mathbb{A}_{Q,f})$ such that $\text{det}(\beta_f) = \alpha_f$ and consider the map

$$\mathcal{H}^+ \to S_K(\mathbb{C}), \quad \tau \mapsto [\alpha_{\infty} \tau, \beta_f]_K,$$

where $\mathcal{H}^+ = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$. This yields a holomorphic covering of $S_{K,\alpha}(\mathbb{C})$, inducing an isomorphism $\Gamma' \backslash \mathcal{H}^+ \to S_{K,\alpha}(\mathbb{C})$ with $\Gamma = \text{SL}_2(\mathbb{Q}) \cap \beta_fK\beta_f^{-1}$ (cf. [23, Proposition 2.7]).

We can now specialize the above observations; both $Y(1)$ and $Y_0(N)$ are geometrically connected Shimura curves $S_K$ (cf. [15, Theorem 7.6.3]). To obtain $Y(1)$, we set $K = \text{GL}_2(\hat{\mathbb{Z}})$. This implies $\text{det}(K) = \hat{\mathbb{Z}}$ and

$$\mathbb{Q}^\times \backslash \{\pm 1\} \times I_{Q,f}/\text{det}(K) \approx \hat{\mathbb{Z}}/\hat{\mathbb{Z}}$$

has a single element (cf. [23, Lemma 2.3]). Thus, $S_K$ is a geometrically connected $\mathbb{Q}$-curve and $S_K(\mathbb{C}) \approx \text{SL}_2(\mathbb{Z}) \backslash \mathcal{H}^+$. For $Y_0(N)$, we set

$$K = \tilde{\Gamma}_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\hat{\mathbb{Z}}) \mid c \equiv 0 \pmod{N} \right\}.$$

Again, we have evidently $\text{det}(K) = \hat{\mathbb{Z}}$ so that the above argument also shows that $S_K$ is a geometrically connected $\mathbb{Q}$-curve. We also note that $S_K(\mathbb{C}) \approx \tilde{\Gamma}_0(N) \backslash \mathcal{H}^+$ by the above, establishing a link to the classical definition of modular curves.

### 2.3. CM-points.

Let $K$ be an imaginary quadratic number field. Additionally, fix an isomorphism $\varphi : K \to \mathbb{Q}^2$. This induces a $\mathbb{Q}$-algebra embedding $\rho : K \hookrightarrow \text{Mat}_{2 \times 2}(\mathbb{Q})$. Note that if $\varphi$ runs through all isomorphisms $K \to \mathbb{Q}^2$, the associated embedding $\rho$ runs through the unique $\text{GL}_2(\mathbb{Q})$-conjugacy class of embeddings $K \hookrightarrow \text{Mat}_{2 \times 2}(\mathbb{Q})$ (cf. the Skolem–Noether theorem [16, Theorem 3.3.14]). Tensoring $\rho$ with $\mathbb{A}_{Q,f}$, we obtain a homomorphism $\mathbb{A}_{K,f} \hookrightarrow \text{Mat}_{2 \times 2}(\mathbb{A}_{Q,f})$, which we also denote by $\rho$ to keep our notations simple. Clearly, we have $\rho(I_{K,f}) \subset \text{GL}_2(\mathbb{A}_{Q,f})$. There also exists a unique $x_\rho \in \mathcal{H}^+ \cap K$ whose stabilizer in $\text{GL}_2(\mathbb{Q})$ is $\rho(K^\times)$. The CM-points
with CM-field $K$ are the elements of the set 
\[ Y_K(\mathbb{C}) = \{ [x_\rho, g]_K \mid g \in \text{GL}_2(\mathbb{A}_{\mathbb{Q},f}) \} \subset S_K(\mathbb{C}); \]
this definition does not depend on $\varphi$. By Shimura’s construction of $S_K$, the points in $Y_K(\mathbb{C})$ are defined over the maximal abelian extension $K^{ab}$ and 
\[ (t, K^{ab}/K)[x_\rho, g]_K = [x_\rho, \rho(t)g]_K \]
for every $[x_\rho, g]_K \in Y_K(\mathbb{C})$ and every $t \in I_{K,f}$ (cf. [24, Definition 12.8]) \(^\dagger\)
With respect to this $I_{K,f}$-action, the CM-point $P = [x_\rho, g]_K$ has stabilizer 
\[ K^\times \cdot \mathcal{K}_{g,\rho} \subseteq I_{K,f}, \quad \mathcal{K}_{g,\rho} = \rho^{-1}(gKg^{-1}). \]
We note that $\mathcal{K}_{g,\rho}$ is a compact open subgroup of $I_{K,f}$. This subgroup depends only on the Galois orbit of $P$ since $\mathcal{K}_{g,\rho} = \mathcal{K}_{\rho(t)g,\rho}$ for any $t \in I_{K,f}$ and $\mathcal{K}_{g,\rho} = \mathcal{K}_{hg,h\rho h^{-1}}$ for any $h \in \text{GL}_2(\mathbb{Q})$. In particular, we may write $\mathcal{K}_P$ for $\mathcal{K}_{g,\rho}$ in what follows, thereby associating a compact open subgroup of $I_{K,f}$ with each CM-point $P \in S_K(\mathbb{C})$. The orbit of $P$ under $\text{Gal}(K^{ab}/K)$ can be identified with the double quotient 
\[ (2.5) \quad K^\times \backslash I_{K,f}/\mathcal{K}_P, \]
which is the set of complex points of a 0-dimensional Shimura subvariety embedded into $S_K$. In addition, the field of definition of $P$ is the fixed field of $(\mathcal{K}_P, K^{ab}/K) \subseteq \text{Gal}(K^{ab}/K)$.

Finally, we specialize to the modular curves $Y(1)$ and $Y_0(N)$ ($N \geq 1$). In this case, the identity $\text{GL}_2(\hat{\mathbb{Z}}) = \text{Stab}_{\text{GL}_2(\mathbb{A}_{\mathbb{Q},f})}(\hat{\mathbb{Z}}^2)$ implies that $\mathcal{K}_{g,\rho} = \text{Stab}_{I_{K,f}}(\varphi^{-1}(g \cdot \hat{\mathbb{Z}}^2))$. It follows that $\mathcal{K}_{g,\rho}$ is the unit group of the ring 
\[ \hat{O}_{g,\rho} = \{ r \in \mathbb{A}_{K,f} \mid r \cdot \varphi^{-1}(g \cdot \hat{\mathbb{Z}}^2) \subseteq \varphi^{-1}(g \cdot \hat{\mathbb{Z}}^2) \}, \]
which is easily seen to be an open subgroup of $\hat{O}_K$ containing $\hat{\mathbb{Z}}$. It is hence the profinite completion of the imaginary quadratic order $O_{g,\rho} = \hat{O}_{g,\rho} \cap O_K$. In this way, we can associate with each CM-point $P = [x_\rho, g]_K \in X(1)$ an order $O_P \subseteq O_K$, and the quotient (2.5) can be identified with $\text{Pic}(O_P) = K^\times \backslash I_{K,f}/\hat{O}_P^\times$. For CM-points on $Y_0(N)$, a variant of the above starting from 
\[ \hat{T}_0(N) = \text{Stab}_{\text{GL}_2(\mathbb{A}_{\mathbb{Q},f})}(\hat{\mathbb{Z}} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \hat{\mathbb{Z}} \cdot \begin{pmatrix} 0 \\ N \end{pmatrix}) \]
allows us to associate similarly an imaginary quadratic order with a CM-point $P$ on $Y_0(N)$; we again write $O_P$ for this order. Although this is not relevant for us, let us remark that this order coincides for Heegner points with the one defined in [30, Section 1].

\(^\dagger\) Note that all ideles in $\mathbb{C}^\times \times \{1\} \subset \mathbb{C}^\times \times I_{f,K}$ are norms with respect to any finite extension $L/K$. This implies $(I_{K,f}, K^{ab}/K) = \text{Gal}(K^{ab}/K)$ so that we can ignore the archimedean component of $I_K$. 
2.4. Class number bounds. To each quadratic extension $K/\mathbb{Q}$ there
is associated a Dirichlet character $\chi_K(n) = (\text{disc}(O_K)/n)$ by means of Kro-
necker’s symbol $(d/n)$; for details we refer to [11] Section 5.2. For the
associated Dirichlet $L$-function, the Siegel–Tatuzawa Theorem [35] (see also [19])
states that there exists an effectively computable constant $c_2(\varepsilon)$ and (at
most) one imaginary quadratic field $K_1$, which also depends on $\varepsilon$, such that
\[ L(1, \chi_K) > c_2(\varepsilon)|\text{disc}(O_K)|^{-\varepsilon} \]
for any other imaginary quadratic field $K \neq K_1$. Using the class number
formula [12, (15) on p. 49], we infer that
\[ \# \text{Pic}(O_K) > c_3(\varepsilon)|\text{disc}(O_K)|^{1/2-\varepsilon}. \]
Even more, we can make use of [11, Theorem 7.24] to deduce the bound
\[ \# \text{Pic}(O) > c_4(\varepsilon)|\text{disc}(O)|^{1/2-\varepsilon} \]
for any imaginary quadratic order $O$ not contained in $K_1$. Here, the constant
$c_4(\varepsilon)$ is effectively computable.

3. Intersections of class fields

3.1. General class fields. In this section, we establish Theorem 1.1.
Its Corollary 1.2 is deduced in the next section.

Proof of Theorem 1.1. We first use the following elementary argument
repeatedly: If
\[ 0 \rightarrow G_1 \rightarrow G_0 \rightarrow G_2 \rightarrow 0 \]
is an exact sequence of (neither necessarily commutative nor finite) groups
with $n_1$ (resp. $n_2$) annihilating $G_1$ (resp. $G_2$) then $G_0$ is annihilated by
$n_1n_2$. Conversely, if $G_0$ is annihilated by $n_0$ then so are $G_1$ and $G_2$. We
want to show that $\text{Gal}(KK_{r}^{ab} \cap L/K_r^{ab})$ is annihilated by (1.1). As the group
$\text{Gal}(KK_{r}^{ab} \cap L/K_r^{ab})$ surjects onto $\text{Gal}(K_r^{ab} \cap L/K_r^{ab})$, it suffices to show
that $\text{Gal}(KK_{r}^{ab} \cap L/K_r^{ab})$ is annihilated by (1.1) [3]. Furthermore, by using
the exact sequence
\[ 0 \rightarrow \text{Gal}(KK_{r}^{ab} \cap L/K_r^{ab}) \rightarrow \text{Gal}(KK_{r}^{ab} \cap L/K_r^{ab}) \rightarrow \text{Gal}(KK_{r}^{ab} / K_r^{ab}) \rightarrow 0 \]
we reduce to show that the group $\text{Gal}(KK_{r}^{ab} \cap L/K_r^{ab})$ is annihilated by
$lcm_{i \neq j}\{[K : K_i][K_j : k]\}$. In the remainder of this proof, all Galois groups

---

(3) Although normality is not transitive in general, the normality of $K_i/k$ implies
directly that $K_i^{ab}/k$ is likewise normal. It follows that $KK_{r}^{ab} \cap L/K_r^{ab}$ is indeed a normal extension.
encountered are abelian. By Lemma 3.1, the group \( \text{Gal}(KK_r^{ab} \cap L/Kk^{ab}) \) is isomorphic to \( \text{Coker}(u) \) in the commutative diagram of abelian groups

\[
\begin{array}{ccc}
\text{Gal}(K_1^{ab} \ldots K_r^{ab}/Kk^{ab}) & \xrightarrow{u} & \text{Gal}(KK_r^{ab}/Kk^{ab}) \times \text{Gal}(L/Kk^{ab}) \\
\downarrow w & & \downarrow v \\
\text{Gal}(K_r^{ab}/K_r k^{ab}) \times \prod_{i=1}^{r-1} \text{Gal}(K_i^{ab}/K_i k^{ab}) & & \\
\end{array}
\]

where the homomorphisms are the standard ones. As \( v \) is injective, we can identify \( \text{Coker}(u) \) with a subgroup of \( \text{Coker}(w) \). In this way, \( \text{Coker}(w) \) contains an isomorphic copy of \( \text{Gal}(KK_r^{ab} \cap L/Kk^{ab}) \). Since \( K_1^{ab} \ldots K_r^{ab} \subseteq K^{ab} \), \( \text{Coker}(w) \) is the same as the cokernel \( \text{Coker}(s) \) of

\[ s : \text{Gal}(K^{ab}/Kk^{ab}) \to \prod_{i=1}^{r} \text{Gal}(K_i^{ab}/K_i k^{ab}), \quad \sigma \mapsto (\sigma|_{K_1^{ab}}, \ldots, \sigma|_{K_r^{ab}}). \]

We claim that \( \text{Coker}(s) \) is annihilated by \( \text{lcm}_{i \neq j} \{[K : K_i][K_j : k]\} \). To prove this, it suffices to show that for each \( \sigma_1 \in \text{Gal}(K_1^{ab}/K_1 k^{ab}) \) the element

\[ [K : K_1] \text{lcm}_{j \neq 1} \{[K_j : k]\} \cdot (\sigma_1, \text{id}_{K_2^{ab}}, \ldots, \text{id}_{K_r^{ab}}) \in \prod_{i=1}^{r} \text{Gal}(K_i^{ab}/K_i k^{ab}) \]

is already in the image of \( s \). By (2.2), we have a commutative diagram

\[
\begin{array}{ccc}
N_{K/k}^{-1}(D_k) & \xrightarrow{t} & \prod_{i=1}^{r} N_{K_i/k}^{-1}(D_k) \\
\downarrow (-,K^{ab}/K) & & \downarrow \prod_{i=1}^{r} (-,K_i^{ab}/K_i) \\
\text{Gal}(K^{ab}/Kk^{ab}) \xrightarrow{s} & & \prod_{i=1}^{r} \text{Gal}(K_i^{ab}/K_i k^{ab}) \\
\end{array}
\]

where the homomorphism \( t \) sends \( c \in N_{K/k}^{-1}(D_k) \) to

\[ (N_{K/K_1} c, \ldots, N_{K/K_r} c) \in \prod_{i=1}^{r} N_{K_i/k}^{-1}(D_k). \]

Choose an idele \( c_1 \in N_{K_1/k}^{-1}(D_k) \subset C_{K_1} \) that satisfies \( (c_1, N_{K_1} K_1) = \sigma_1 \). We may consider \( c_1 \) also as an element of \( C_K \) by using the canonical inclusion \( C_{K_1} \subset C_K \). By normality, the Galois group \( \text{Gal}(K/k) \) acts on each \( C_{K_i} \), \( 1 \leq i \leq r \). The idele classes \( N_{K/K_i}(c_1) \), \( 2 \leq i \leq r \), are invariant under this action; in fact, as \( \text{Gal}(K/K_i) \) is normal, each \( \sigma \in \text{Gal}(K/k) \) satisfies \( \sigma \cdot \text{Gal}(K/K_i) \sigma^{-1} = \text{Gal}(K/K_i) \). Hence, for each \( \sigma \in \text{Gal}(K/K_1) \) we have

\[
\sigma(N_{K/K_1}(c_1)) = \prod_{\tau \in \text{Gal}(K/K_1)} \sigma \cdot \tau(c_1) = \sum_{\tau' \in \text{Gal}(K/K_1)} \tau' \cdot \sigma(c_1) = \sum_{\tau \in \text{Gal}(K/K_1)} \tau(c_1) = N_{K/K_1}(c_1).
\]
Being a norm, \( N_{K/K_i}(c_1) \) is also clearly \( \text{Gal}(K/K_i) \)-invariant. From the equality \( K_1 \cap K_i = k \), we deduce the asserted \( \text{Gal}(K/k) \)-invariance by [21] Theorem VI.1.14. By Hilbert’s Satz 90, it follows that \( N_{K/K_i}(c_1) \in C^{\text{Gal}(K_i/k)} = C_k \) [26] Theorem III.2.7] and consequently
\[
N_{K/K_i}(c_1)^{[K_i:k]} = N_{K_i/k}(N_{K/K_i}(c_1)) = N_{K_i/k}(c_1)^{[K_i:k]} \in D_k.
\]
In other words, the automorphism \( (N_{K/K_i}(c_1)^{[K_i:k]}, k^{ab}|k) \in \text{Gal}(k^{ab}/k) \) is the identity \( \text{id}_{k^{ab}} \). Using [23], we conclude that also
\[
(N_{K/K_i}(c_1)^{[K_i:k]}, k^{ab}|K_i) = \text{Ver}(N_{K/K_i}(c_1)^{[K_i:k]}, k^{ab}|k) = \text{Ver}(\text{id}_{k^{ab}}) = \text{id}_{K^{ab}}.
\]
We infer that \( \prod_{i=1}^{r}(\cdot, K_i^{ab}|K_i) \) sends
\[
t(c_1)^{\text{lcm}_{j \neq 1}[[K_j:k]]} = (c_1^{[K_i:k]}, N_{K/K_2}(c_1), \ldots, N_{K/K_n}(c_1))^{\text{lcm}_{j \neq 1}[[K_j:k]]}
\]
into
\[
[K : K_1] \text{lcm}_{j \neq 1}[[K_j : k]] \cdot (\sigma_1, \text{id}_{K_2^{ab}}, \ldots, \text{id}_{K_n^{ab}}) \in \text{image}(s)
\]
as claimed. ■

The next lemma is completely elementary. Lacking references, we prove it here as a specialization of the results in [21, Section VI.1]. Note that the restriction to abelian extensions is necessary because the image of \( \Psi \) is not normal in general.

**Lemma 3.1.** Let \( k \) be a field and \( K_1/k, K_2/k \) two abelian Galois extensions contained in some common larger field. Then the cokernel of the natural map
\[
\Psi : \text{Gal}(K_1K_2/k) \to \text{Gal}(K_1/k) \times \text{Gal}(K_2/k), \quad \sigma \to (\sigma|_{K_1}, \sigma|_{K_2}),
\]
is isomorphic to \( \text{Gal}(K_1 \cap K_2/k) \).

**Proof.** We establish that the image of \( \Psi \) equals the kernel of the homomorphism
\[
\Xi : \text{Gal}(K_1/k) \times \text{Gal}(K_2/k) \to \text{Gal}(K_1 \cap K_2/k), \quad (\sigma_1, \sigma_2) \mapsto \sigma_1|_{K_1 \cap K_2} \sigma_2|_{K_1 \cap K_2}^{-1}.
\]
Evidently, \( \text{image}(\Psi) \) is contained in \( \ker(\Xi) \). Assume first that both \( K_1 \) and \( K_2 \) are finite over \( k \). As \( \Xi \) is surjective, we have
\[
\# \ker(\Xi) = \frac{\# \text{Gal}(K_1/k) \cdot \# \text{Gal}(K_2/k)}{\# \text{Gal}(K_1 \cap K_2/k)} = \# \text{Gal}(K_1K_2/k) = \# \text{image}(\Psi),
\]
where we use [21] Theorem VI.1.12] for the second equality. This numerical equality shows \( \text{image}(\Psi) = \ker(\Xi) \) as claimed. The general case follows by exhausting \( K_1/k \) and \( K_2/k \) with finite subextensions. ■
3.2. Ring class fields and transfer fields. Let \( K \) be a CM-field. This means that \( K \) is an imaginary quadratic extension of a totally real number field \( F \). To any \( \mathcal{O}_F \)-order \( \mathcal{O} \subseteq \mathcal{O}_K \) is assigned its profinite completion \( \hat{\mathcal{O}} \), and its units \( \hat{\mathcal{O}}^\times \) embed diagonally into \( I_{K,f} \subset I_K \). The ring class field \( K[\mathcal{O}] \) associated with \( \mathcal{O} \) is the fixed field of \( (\hat{\mathcal{O}}^\times K^\times /K^\times, K^{ab}/K) \subset \text{Gal}(K^{ab}/K) \). Using \([2.1]\), we deduce

\[
(3.1) \quad \text{Gal}(K[\mathcal{O}]/K) = \frac{(I_{K,f} K^\times /K^\times, K^{ab}/K)}{(\hat{\mathcal{O}}^\times K^\times /K^\times, K^{ab}/K)} = K^\times \backslash I_{K,f}/\hat{\mathcal{O}}^\times = \text{Pic}(\mathcal{O}).
\]

Let \( K^{\text{ref}} \subset K^{ab} \) be the union of all ring class fields. Additionally, we can consider \( C_F = I_F/F^\times = I_F K^\times /K^\times \) as a closed subgroup of \( C_K \) and define the “transfer field” \( K^{\text{tf}} \subset K^{ab} \) to be the fixed field of \( (I_F K^\times /K^\times, K^{ab}/K) \subset \text{Gal}(K^{ab}/K) \). The fields \( K^{\text{tf}} \) and \( K^{\text{ref}} \) are intimately connected as the following lemma shows.

**Lemma 3.2.** Let \( F \) be a totally real field. For any totally imaginary quadratic extension \( K/F \), \( K^{\text{ref}} \) is a finite extension of \( K^{\text{tf}} \) and the Galois group \( \text{Gal}(K^{\text{ref}}/K^{\text{tf}}) \) is isomorphic to \( \text{Pic}(\mathcal{O}_F) \).

If \( F \) has class number one, then \( K^{\text{ref}} = K^{\text{tf}} \) for all totally imaginary extensions \( K/F \). This is hence the case for the proofs of Theorems 1.3 and 1.4 below.

**Proof of Lemma 3.2** Each ideal \( f \subseteq \mathcal{O}_F \) yields an \( \mathcal{O}_F \)-order \( \mathcal{O}_F + f \mathcal{O}_K \subseteq \mathcal{O}_K \), and the intersection of all their profinite completions \( \hat{\mathcal{O}}_F + f \hat{\mathcal{O}}_K \subseteq \hat{\mathcal{O}}_K \) equals \( \hat{\mathcal{O}}_F \). In addition, the intersection \( \mathcal{O}_1 \cap \mathcal{O}_2 \) of any two \( \mathcal{O}_F \)-orders \( \mathcal{O}_1, \mathcal{O}_2 \subseteq \mathcal{O}_K \) is again an \( \mathcal{O}_F \)-order. It follows that there is a descending chain of \( \mathcal{O}_F \)-orders \( \mathcal{O}_i \subseteq \mathcal{O}_K \) such that \( \hat{\mathcal{O}}_F^\times = \bigcap_i \hat{\mathcal{O}}_i^\times \) and \( K^{\text{ref}} = \bigcup_i K[\mathcal{O}_i] \).

We next claim the equality

\[
(3.2) \quad (\hat{\mathcal{O}}^\times_F K^\times /K^\times, K^{ab}/K) = \bigcap_i (\hat{\mathcal{O}}^\times_i K^\times /K^\times, K^{ab}/K).
\]

The inclusion “\( \subseteq \)” is trivial. For the other inclusion, we remark that by \([2.1]\) the subgroup \( \hat{\mathcal{O}}^\times_F K^\times /K^\times \subset I_{K,f} K^\times /K^\times \) contains the kernel of the restriction \( (\cdot, K^{ab}/K) \mid_{I_{K,f} K^\times /K^\times} \). Hence, the identity \((3.2)\) follows immediately from \( \hat{\mathcal{O}}^\times_F = \bigcap_i \hat{\mathcal{O}}^\times_i \).

We can now show that \( K^{\text{ref}} \) is the fixed field of \((3.2)\). Trivially, each element of \( K^{\text{ref}} \) is fixed under this group. For the other direction, let \( x \in K^{ab} \) be fixed under \((3.2)\) and let \( \overline{K(x)} \) denote the normal closure of \( K(x) \). This means that the intersection

\[
\bigcap_i (\hat{\mathcal{O}}^\times_i K^\times /K^\times, \overline{K(x)}/K) \subset \text{Gal}(\overline{K(x)}/K)
\]

contains only the identity \( \text{id}_{\overline{K(x)}} \). As \( (\mathcal{O}_i) \) is a descending chain and the group
Gal(K(x)/K) is finite, we already have (\hat{O}_i^{\times} K^{\times}/K^{\times}, K(x)/K) = \{\text{id}_{K(x)}\}
for some order \(O_i\) so that \(x \in K[O_i]\).

From this alternative presentation of \(K^{\text{rcf}}\), it follows immediately that \(K^{\text{rf}} \subseteq K^{\text{rcf}}\) and

\[
(3.3) \quad \text{Gal}(K^{\text{rcf}}/K^{\text{rf}}) = \left( \frac{I_{F,f}K^{\times}/K^{\times}, K^{\text{ab}}/K}{\hat{O}_{F}^{\times} K^{\times}/K^{\times}, K^{\text{ab}}/K} \right) = F^{\times} \backslash I_{F,f}/\hat{O}_{F}^{\times} = \text{Pic}(O_F);
\]

here, the injection \(C_F \hookrightarrow C_K\) is used in addition to (2.1). \(\blacksquare\)

A (profinite) group \(G\) is called a generalized dihedral group with respect to a normal abelian subgroup \(H\) of index 2 if \(G\) is the semidirect product \(H \rtimes \sigma H\) with \(\sigma: G/H \rightarrow \text{Aut}(H)\) sending the non-trivial element of \(G/H\) to the inversion \(H \rightarrow H, g \mapsto g^{-1}\). The following two lemmas seem to be folklore but we provide proofs here for lack of suitable references.

**Lemma 3.3.** Let \(F\) be a totally real field and \(K/F\) an imaginary quadratic extension of \(F\). Then \(K^{\text{rf}}/F\) is normal and the Galois group \(\text{Gal}(K^{\text{rf}}/F)\) is a generalized dihedral group with respect to \(\text{Gal}(K^{\text{rf}}/K)\).

**Proof.** Let \(\sigma\) be an automorphism of \(\overline{Q}\) fixing \(F\). Being a quadratic extension, \(K/F\) is trivially normal and \(\sigma(K) = K\). By (2.4), the field \(\sigma(K^{\text{rf}})\) is the fixed field of \((\sigma(C_F), K^{\text{ab}}/K) = (C_F, K^{\text{ab}}/K)\) and thus \(\sigma(K^{\text{rf}}) = K^{\text{rf}}\). This shows that the extension \(K^{\text{rf}}/F\) is Galois. In addition, there is an exact sequence

\[1 \rightarrow \text{Gal}(K^{\text{rf}}/K) \rightarrow \text{Gal}(K^{\text{rf}}/F) \rightarrow \text{Gal}(K/F) \rightarrow 1.\]

Let \(\iota \in \text{Gal}(K^{\text{rf}}/F)\) be a lifting of the non-trivial element of \(\text{Gal}(K/F)\). We have to show that \(\iota \circ \sigma \circ \iota^{-1} = \sigma^{-1}\) for any \(\sigma = (c, K^{\text{rf}}/K), c \in C_K\). By (2.4),

\[(c, K^{\text{rf}}/K) \circ (\iota \circ (c, K^{\text{rf}}/K) \circ \iota^{-1}) = (c, K^{\text{rf}}/K) \circ (\iota(c), K^{\text{rf}}/K) = (\iota(c), K^{\text{rf}}/K).\]

Since \(\iota(c) \in C_K^{\text{Gal}(K/F)} = C_F\) by Hilbert’s Satz 90, the automorphism \((\iota(c), K^{\text{rf}}/K)\) is the identity on \(K^{\text{rf}}\). In other words, \(\sigma \circ (\iota \circ \sigma \circ \iota^{-1}) = \text{id}_{K^{\text{rf}}}\). \(\blacksquare\)

The fact that \(\text{Gal}(K^{\text{rf}}/F)\) is a generalized dihedral group has a substantial consequence due to the following elementary lemma.

**Lemma 3.4.** Let \(G\) be a generalized dihedral group with respect to a subgroup \(H\) and let \(H_0 \subset G\) be a normal subgroup such that the quotient \(G/H_0\) is abelian. Then \(H/(H \cap H_0)\) is annihilated by 2.

**Proof.** Let \(\pi: G \rightarrow G/H_0\) be the quotient map. As \(H/(H \cap H_0) \approx HH_0/H_0\), the assertion means that \(\pi(h)^2 = 1\) for any \(h \in H\). Choose some \(g_0 \in G \setminus H\). Then \(g_0 h g_0^{-1} = h^{-1}\) and hence \(\pi(h) = \pi(h)^{-1}\) as \(G/H_0\) is abelian. This already completes the proof. \(\blacksquare\)
With the above lemmas at our disposal, we can deduce the announced corollary.

**Proof of Corollary 1.2.** By Theorem 1.1,

$$\text{Gal}\left(K_{r}^{ab} \cap \left(\prod_{i=1}^{r-1} K_i^{ab}\right)/K_r F^{ab}\right)$$

and hence $\text{Gal}(K_{r}^{tf} \cap L/K_r^{tf} \cap K_r F^{ab} \cap L)$ is annihilated by

$$n = e(\text{Gal}(KF^{ab}/K_r F^{ab})) \cdot \text{lcm}_{i \neq j}\{[K : K_i][K_j : F]\}.$$  

Since $K$ is a composite of quadratic extensions of $F$, the group $\text{Gal}(K/F)$ is abelian of exponent 2. Consequently, $K \subset F^{ab}$ and hence $KF^{ab} = F^{ab} = K_r F^{ab}$. We infer that $n = 2^r$. From Lemma 3.3 we know that $\text{Gal}(K_{r}^{tf}/F)$ is a generalized dihedral group with respect to its subgroup $\text{Gal}(K_{r}^{tf}/K_r)$. We may now apply Lemma 3.4 with the subgroup $H_0 = \text{Gal}(K_{r}^{tf} \cap F^{ab} \cap L/K_r)$ to deduce that $\text{Gal}(K_{r}^{tf} \cap F^{ab} \cap L/K_r)$ is annihilated by 2. The assertion follows straightforwardly from the exact sequence

$$0 \to \text{Gal}(K_{r}^{tf} \cap L/K_r^{tf} \cap F^{ab} \cap L) \to \text{Gal}(K_{r}^{tf} \cap L/K_r) \to \text{Gal}(K_{r}^{tf} \cap F^{ab} \cap L/K_r) \to 0. \blacksquare$$

**4. Proof of Theorem 1.3.** Our proof improves upon the original one given by Rosen and Silverman [30]. We restate the details as far as necessary to see that our Corollary 1.2 eliminates the restrictions of their proof effectively.

Assume given CM-points $P_1, \ldots, P_r$ on $Y_0(N)$ associated with distinct CM-fields $K_i$ such that

$$(4.1) \quad n_1 \cdot \pi(P_1) + n_2 \cdot \pi(P_2) + \cdots + n_r \cdot \pi(P_r) = 0, \quad (n_1, \ldots, n_r) \in \mathbb{Z}^r \setminus \{0\},$$

with respect to the group law on $E$. By using [25, Theorem 1.5], whose straightforward argument is completely effective (see the remarks in [25, Section 3]) we may assume that at least two coefficients $n_i$ are non-zero. Assume hence that $n_r \neq 0$ and $K_r \neq K_*$ where $K_*$ is the (possibly non-existent) CM-field from Section 2.4. As explained in Section 2.3 an imaginary quadratic order $O_i \subseteq O_{K_i}$ is associated with each CM-point $P_i$. Furthermore, we assign a ring class field $K[O_i]$ to each order $O_i$ (see Section 3.2).

Our next aim is to bound $|\text{disc}(O_r)|$. We do this by deriving two competing bounds on the size $\#\text{Pic}(O_r)$ of the Picard group $\text{Pic}(O_r)$. By (3.1), $\text{Pic}(O_r)$ is isomorphic to $\text{Gal}(K_r[O_r]/K_r)$. We consider the following diagram of abelian field extensions:
Intersection of class fields

\[ K_r(P_r) = K_r[\mathcal{O}_r] \]

\[ K_r(\pi(P_r)) \]

\[ K_r(n_r \cdot \pi(P_r)) \]

\[ K_r \]

As both \( E \) and the modular parameterization \( \pi : X_0(N) \to E \) are defined over \( \mathbb{Q} \), it is a direct consequence of (4.1) that

\[ K_r(n_r \cdot \pi(P_r)) \subseteq K_r[\mathcal{O}_r] \cap L \quad \text{where} \quad L = K_r \prod_{i<r} K_i[\mathcal{O}_i]. \]

By our Corollary 1.2, this implies that \( \text{Gal}(K_r(n_r \cdot \pi(P_r))/K_r) \) is annihilated by \( 2^{r+1} \). The degree \( [K_r(\pi(P_r)) : K_r(n_r \cdot \pi(P_r))] \) is bounded by some effectively computable constant \( c_5(E) \); the proof is exactly the same as that of [30, Theorem 11] noting that Serre’s open image theorem is effective by [22]. The degree \( [K_r(P_r) : K_r(\pi(P_r))]/2 \) is less than \( c_6(\pi) = \deg(\pi) \) due to an elementary argument (see [30, Proposition 6]). The group \( G = \text{Gal}(K_r[\mathcal{O}_r]/K_r) \) is abelian and hence a direct product of cyclic groups \( (\mathbb{Z}/p^n\mathbb{Z}) \) (\( p \) a prime, \( n \) a positive integer) by the elementary divisor theorem. Here, a factor of the form \( (\mathbb{Z}/2^n\mathbb{Z}) \) can only occur if

\[ n \leq c_7(E,\pi,r) = (r + 1) + \lfloor \log_2(c_5(E)c_6(\pi)) \rfloor. \]

Genus theory (cf. [41, Proposition 6.3]) yields the bound

\[ \dim_{\mathbb{F}_2}(\text{Pic}(\mathcal{O}_r)[2]) \leq c_8(\varepsilon_1)|\text{disc}(\mathcal{O}_r)|^{\varepsilon_1} \]

for some effective constant \( c_8(\varepsilon_1) > 0 \). As \( \dim_{\mathbb{F}_2}(\text{Pic}(\mathcal{O}_r)[2]) \) is also the number of factors \( (\mathbb{Z}/2^n\mathbb{Z}) \) occurring in \( G \), it follows that

\[ \# \text{Pic}(\mathcal{O}_r)^{\text{even}} \leq (c_8(\varepsilon_1)|\text{disc}(\mathcal{O}_r)|^{\varepsilon_1}c_7(E,\pi,r). \]

Furthermore, we infer that

\[ (4.2) \quad \# \text{Pic}(\mathcal{O}_r)^{\text{odd}} = [K_r[\mathcal{O}_r] : K_r]^{\text{odd}} \leq [K_r[\mathcal{O}_r] : K_r(n_r \cdot \pi(P_r))] \leq c_5(E)c_6(\pi) \]

from the fact that \( [K_r(n_r \cdot \pi(P_r)) : K_r] \) is a power of 2. By assumption, we have \( K_r \neq K_* \) so that we may use (2.6) with \( \mathcal{O} = \mathcal{O}_r \). Combining this with the above two inequalities, we obtain

\[ c_4(\varepsilon_2)|\text{disc}(\mathcal{O}_r)|^{1/2-\varepsilon_2} < \# \text{Pic}(\mathcal{O}_r) \leq c_5(E)c_6(\pi)c_8(\varepsilon_1)c_7(E,\pi,r)|\text{disc}(\mathcal{O}_r)|^{\varepsilon_1c_7(E,\pi,r)}. \]
Choosing both $\varepsilon_1$ and $\varepsilon_2$ sufficiently small, we derive an upper bound on $|\text{disc}(O_r)|$.

5. Proof of Theorem 1.4. Let $pr_i : Y(1)^n \to Y(1)^{n-1}$ denote the projection omitting the $i$th factor of $Y(1)^n$. We claim that the generic fiber dimension of $pr_i|_X$ is zero; otherwise upper semicontinuity of the fiber dimension \cite[Théorème 13.1.3]{L} would imply that each fiber has dimension $\geq 1$. This is only possible if $\pi(X) = Y(1)^n \times pr_i(X)$ for an appropriate coordinate permutation $\pi : Y(1)^n \to Y(1)^n$, which contradicts our assumptions. It follows that the closed points $P \in X$ such that $\dim(pr^{-1}_i(P)) \cap X \geq 1$ are all contained in a proper Zariski closed subset $Z_i \subset X$. Working with explicit equations, we ascertain that the height and the degree of $Z' = Z_1 \cup \cdots \cup Z_n$ can be effectively bounded in terms of the degree and height of $X$.

The closed set $Z'$ is part of the exceptional set $Z$ whose existence is claimed in the theorem. To describe the other part, let $P = (P_1, \ldots, P_n) \in (X \setminus Z')(\overline{\mathbb{Q}})$ be a special point such that $K_i(P) \neq K_j(P)$ for all $i \neq j$. There exists some $i_0 \in \{1, \ldots, n\}$ such that $K_{i_0}(P) \neq K_*$. Furthermore, denote by $O_i$ the quadratic order associated with the CM-point $P_i$ as in Section 2.3. Recall that $K_i(P_i) = K_i[O_i]$. There exists some effectively computable constant $c_9(X)$, depending only on the degree of $X$ and the degree of its field of definition, such that

$$[K_{i_0}[O_{i_0}] \cdot L : L] \leq c_9(X) \quad \text{where} \quad L = K_{i_0} \prod_{1 \leq i \leq n, i \neq i_0} K_i[O_i].$$

Consider the following diagram of abelian field extensions:

\[ \begin{array}{ccc}
K_{i_0}[O_{i_0}] \cdot L & \to & L \\
\downarrow & & \downarrow \\
K_{i_0}[O_{i_0}] \cap L & \to & K_{i_0}
\end{array} \]

By \cite[Theorem VI.1.12]{L}, we have an equality

$$[K_{i_0}[O_{i_0}] \cdot L : L] = [K_{i_0}[O_{i_0}] : K_{i_0}[O_{i_0}] \cap L].$$

Furthermore, Corollary 1.2 implies that $\text{Gal}(K_{i_0}[O_{i_0}] \cap L/K_{i_0})$ is annihilated by $2^{n+1}$. 

Analogous to the proof of Theorem 1.3, we can derive an upper bound for $|\text{disc}(\mathcal{O}_{i_0})|$ from this information. As there, genus theory yields
\[
\# \text{Pic}(\mathcal{O}_{i_0})^{\text{even}} \leq (\dim F_2(\text{Pic}(\mathcal{O}_{i_0})[2]))^{c_{10}(X)} \leq (c_8(\varepsilon_1)|\text{disc}(\mathcal{O}_{i_0})|^{\varepsilon_1})^{c_{10}(X)}
\]
with $c_{10}(X) = n + 1 + \lfloor \log_2(c_9(X)) \rfloor$. Furthermore, $\# \text{Pic}(\mathcal{O}_{i_0})^{\text{odd}} \leq c_9(X)$. Using the Siegel–Tatuzawa Theorem (2.6), we obtain
\[
c_4(\varepsilon_2)|\text{disc}(\mathcal{O}_{i_0})|^{1/2-\varepsilon_2} < \# \text{Pic}(\mathcal{O}_{i_0}) \leq c_8(\varepsilon_1)^{c_{10}(X)}c_9(X)|\text{disc}(\mathcal{O}_{i_0})|^{\varepsilon_1c_{10}(X)}.
\]

For $\varepsilon_1, \varepsilon_2 \to 0$, this leads to an effective upper bound $c_{11}(X)$ on $|\text{disc}(\mathcal{O}_{i_0})|$. There exist only finitely many CM-points $Q_1, \ldots, Q_m \in Y(1)$ whose associated imaginary quadratic order has discriminant less than $c_{11}(X)$. By assumption, the $i$th coordinate function $x_i : Y(1)^n \to Y(1)$, $i \in \{1, \ldots, n\}$, restricts to a non-constant regular function on $X$. This implies that
\[
Z'' = X \cap \bigcup_{1 \leq i \leq n} \bigcup_{1 \leq j \leq m} (x_i^{-1}(Q_j))
\]
is a proper algebraic subset of $X$. The above argument shows that the CM-points $P$ contradicting the assertion of the theorem with $Z = Z'$ must be contained in $Z''$. Finally, the height and degree of $Z''$ can evidently be effectively bounded so that the assertion of the theorem is true for $Z = Z' \cup Z''$.

**Acknowledgements.** The author thanks, for their helpful remarks and for the discussions he had with them, Yuri Bilu, Philipp Habegger, Jonathan Pila, Harry Schmidt, Joseph Silverman, and Gisbert Wüstholz. He also thanks the referee for critical reading and valuable suggestions. In addition, he thanks both the Max Planck Institute for Mathematics and the Fields Institute for their supportive hospitality during the composition of this article. Finally, he acknowledges financial support by an Ambizione Grant of the Swiss National Science Foundation.

**References**


---

Lars Kühne  
Departement Mathematik und Informatik  
Spiegelgasse 1  
4051 Basel, Switzerland  
E-mail: lars.kuehne@unibas.ch

Current address:  
Institut for Matematiske Fag  
Universitetsparken 5  
2100 København Ø, Denmark  
E-mail: lk@math.ku.dk