ON THE NUMBER OF ISOMORPHISM CLASSES OF CM ELLIPTIC CURVES DEFINED OVER A NUMBER FIELD

HARRIS B. DANIELS AND ÁLVARO LOZANO-ROBLEDO

Abstract. The theory of complex multiplication has proven to be an essential tool in number theory, mainly due to the connections with class field theory developed by Kronecker, Weber, Fricke, Hasse, Deuring, and Shimura, among others. Certain important results have been shown first in the case of complex multiplication. Thus, it is a natural question to find all the isomorphism classes of elliptic curves with complex multiplication defined over a fixed number field, for which these important results hold. In this article, we prove an upper bound on the number of isomorphism classes of CM elliptic curves defined over a number field of a fixed odd degree N, in terms of the prime factorization of N.

1. Introduction

The theory of complex multiplication has proven to be an essential tool in number theory, mainly due to the connections with class field theory developed by Kronecker, Weber, Fricke, Hasse, Deuring, and Shimura, among others. Certain important results have been shown first in the case of complex multiplication, such as the analytic continuation to the entire complex plane for the L-function of an elliptic curve (see [Sil94], Ch. III, §10), some cases of the Birch and Swinnerton-Dyer conjecture (see [CW77], [Rub99]) or the main conjectures of Iwasawa theory for elliptic curves (see for example [PR04]). Thus, it is a natural question to find all the isomorphism classes of elliptic curves with complex multiplication defined over a fixed number field, for which these important results hold. In this article, we concentrate on finding an upper bound on the number of isomorphism classes of CM elliptic curves defined over a number field of a fixed degree, and concentrate in the case of odd degree.

It is well known that there are only 13 isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with complex multiplication ([Sil09], Appendix A, §3), namely the curves with j-invariant in the list:

$$\{0,\ 2^4 3^3 5^3,\ -2^{15}\cdot 3\cdot 5^3,\ 2^6 3^3,\ 2^3 3^3 11^3,\ -3^3 5^3,\ 3^3 5^3 17^3,\ 2^6 5^3,$$
$$-2^{15},\ -2^{15}3^3,\ -2^{18}3^3 5^3,\ -2^{15}3^3 5^3 11^3,\ -2^{18}3^3 5^3 23^3 29^3\}.$$

However, the number of CM j-invariants varies wildly depending on the choice of field of definition, even in the case of quadratic number fields (see Table 1). For a number field L, we will write $\Sigma(L)$ for the set of all CM j-invariants defined over L, but not defined over $\mathbb{Q}$, so that the total number of CM j-invariants defined over L is $13+\#\Sigma(L)$. It is known that $\Sigma(L)$ is a finite set, for any number field L. In this article, we show the following simple bound for $\#\Sigma(L)$ when the degree of L is odd.

Theorem 1.1. *Let L be a number field of odd degree. Then, $\#\Sigma(L) \leq 2\log_3([L:\mathbb{Q}])$. In particular, the number of distinct CM j-invariants defined over L is bounded by $13 + 2\log_3([L:\mathbb{Q}])$.*

Remark 1.2. The simple bound given in Theorem 1.1 is essentially sharp. The bound is trivially sharp when $L=\mathbb{Q}$. Moreover, let $K=\mathbb{Q}(\sqrt{-3})$, and for any fixed $e\geq 1$, let $\mathcal{O}_e$ be an order of $\mathcal{O}_K$ with conductor $\mathfrak{f}=2\cdot 3^e$. Let E_e be an elliptic curve with CM by $\mathcal{O}$, and define $L_e=\mathbb{Q}(j(E_e))$. Then, $[L_e:\mathbb{Q}]=3^e$, and it follows from Theorem 1.3 that $\#\Sigma(L)=2e-1=2\log_3([L_e:\mathbb{Q}])-1$, which is just one unit below the bound of Theorem 1.1.

Theorem 1.1 is a consequence of more refined bounds (Theorems 1.3 and 1.4; see Remark 1.5) which we discuss below after we provide some computational data (our calculations have been performed using Sage [S$^+$14]; see also [Wat04] for some of the algorithms that Sage uses). For instance, we will show in Section 2 that, for a fixed quadratic number field $L=\mathbb{Q}(\sqrt{d})$, the number of elements in $\Sigma(L)$ is given as in Table 1 (see Remark 2.15).

In particular, $\Sigma(L)=\emptyset$ for all imaginary quadratic fields L, and in fact $\Sigma(L)=\emptyset$ for all but the 14 distinct real quadratic fields that appear in the table. Given a fixed integer $N\geq 2$, we write $\mathcal{O}(N)$ for the set of all orders of class number N in some imaginary quadratic field, and $\Sigma(N)$ for the set of CM j-invariants $j(E)$ such

2010 *Mathematics Subject Classification.* Primary: 14H52, Secondary: 14K22.

d	2	3	5	6	7	13	17	21	29	33	37	41	61	89	else
$\#\Sigma(\mathbb{Q}(\sqrt{d}))$	8	4	18	2	2	6	4	2	2	2	2	2	2	2	0

TABLE 1. The number of non-rational CM j-invariants defined over each quadratic field.

that $\mathbb{Q}(j(E))/\mathbb{Q}$ is an extension of degree N (notice that $\#\Sigma(N) = N \cdot \#\mathcal{O}(N)$). Finally, we write $\mathcal{L}(N)$ for the set of all non-isomorphic fields $L = \mathbb{Q}(j(E))$, where E is an elliptic curve with CM by an order of class number N (thus, $\#\mathcal{O}(N) \geq \#\mathcal{L}(N)$ for all N), and we write $\mathfrak{L}(N)$ for the set of all number fields of degree N. Table 1 shows that $\#\Sigma(2) = 58$ (so $\#\mathcal{O}(2) = 29$), and $\#\mathcal{L}(2) = 14$. Notice that if $L/\mathbb{Q}$ is quadratic and contains a CM j-invariant $j(E)$ not defined over $\mathbb{Q}$, then $L = \mathbb{Q}(j(E))$, and so $L \in \mathcal{L}(2)$. For similar reasons, if N is prime, and L is a number field of degree N that contains a j-invariant $j(E)$ of class number N, then $L \in \mathcal{L}(N)$, i.e., $L = \mathbb{Q}(j(E))$.

We record the sizes of $\mathcal{O}(N)$, $\Sigma(N)$, $\mathcal{L}(N)$ in Table 2, for $N = 1, \ldots, 11$, as well as the maximum number of elements of $\Sigma(L)$ for $L \in \mathcal{L}(N)$, and also the maximum of $\Sigma(L)$ over all number fields L of degree N over $\mathbb{Q}$ (and not just those fields of the form $\mathbb{Q}(j(E))$). We will explain how the data in Table 2 was collected in Section 2, Remark 2.15.

N	2	3	4	5	6	7	8	9	10	11
$\#\mathcal{O}(N)$	29	25	84	29	101	38	208	55	123	46
$\#\Sigma(N)$	58	75	336	145	606	266	1664	495	1230	506
$\#\mathcal{L}(N)$	14	23	72	25	96	32	202	50	114	42
$\max\{\#\Sigma(\mathcal{L}(N))\}$	18	2	42	2	22	2	84	3	22	2
$\max\{\#\Sigma(\mathfrak{L}(N)))\}$	18	2	42	2	22	2	84	4	22	2

TABLE 2. The number of (a) orders of class number N; (b) CM j-invariants $j(E)$ such that $\mathbb{Q}(j(E))$ is of degree N; (c) fields $\mathbb{Q}(j(E))$ as in (b), up to isomorphism; (d) maximum $\#\Sigma(L)$ for L as in (c); and maximum $\#\Sigma(L)$ for any L of degree N.

In Table 2 and in the rest of the article, we use two abbreviations:

$$\max\{\#\Sigma(\mathcal{L}(N))\} := \max\{\#\Sigma(L) : L \in \mathcal{L}(N)\} = \max\{\#\Sigma(L) : [L:\mathbb{Q}] = N, L = \mathbb{Q}(j(E)) \text{ for some CM } j(E)\},$$
$$\max\{\#\Sigma(\mathfrak{L}(N))\} := \max\{\#\Sigma(L) : L \in \mathfrak{L}(N)\} = \max\{\#\Sigma(L) : [L:\mathbb{Q}] = N\}.$$

In this paper we give upper bounds for $\max\{\#\Sigma(\mathcal{L}(N))\}$ and $\max\{\#\Sigma(\mathcal{L}(N))\}$ when N is odd. Our bounds are sharp, in the sense that we exhibit examples for arbitrarily large N that attain the bound (see Examples 5.4, 5.5, and 5.9). Our first intermediary result describes the number of CM j-invariants found in an extension of the form $L = \mathbb{Q}(j(E))$, where E is itself an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K (i.e., $L \in \mathcal{L}(N)$, where N is the class number of $\mathcal{O}$).

Theorem 1.3. *Let $j(E)$ be a j-invariant with CM by an order $\mathcal{O}$ in an imaginary quadratic field K of conductor $\mathfrak{f}$, and $j(E) \notin \mathbb{Q}$. Let $L = \mathbb{Q}(j(E))$, and suppose that $[L:\mathbb{Q}] = N > 1$ is odd. Let $\sigma_0(\mathfrak{f}) = \sum_{d|\mathfrak{f}} d^0$ be the number of positive divisors of $\mathfrak{f}$. Then, the number of j-invariants with CM defined over L is*

$$13 + \sigma_0(\mathfrak{f}) - J(K)$$

if $\mathfrak{f}$ is even, or if 2 does not split completely in K, and $13 + \sigma_0(2\mathfrak{f}) - J(K)$ otherwise, where $J(K)$ is the number of rational j-invariants of curves with CM by an order of K, i.e.,

d_K	-3	-4	-7	-8	-11	-19	-43	-67	-163	*else*
$J(K)$	3	2	2	1	1	1	1	1	1	0,

where d_K is the discriminant of K.

Our second and main result provides a bound for the number of CM j-invariants defined over any number field of odd degree N, in terms of the factorization of N. If we know the list of CM imaginary quadratic fields

that intervene in $\Sigma(L)$, and the prime factorization of their class numbers, then we can significantly improve the bound on the number of CM j-invariants defined over L, but this finer data is not required, and we also obtain a bound that only depends on the factorization of N.

Theorem 1.4. *Let $L/\mathbb{Q}$ be a number field of odd degree $N = p_1^{e_1} \cdots p_r^{e_r}$, and let $K_1, \ldots, K_t$ be the list of imaginary quadratic fields such that there is $j(E) \in \Sigma(L)$ where E has CM by an order of K_i, for some $i = 1, \ldots, t$. Further, let h_i be the class number of K_i, and suppose that $h_i > 1$ for $i = 1, \ldots, s$ and $h_i = 1$ for $i = s+1, \ldots, t$. Then,*

$$\#\Sigma(L) \leq 2s + 2\sum_{j=1}^{r} \left(e_j - \sum_{i=1}^{s} f_{i,j} \right).$$

where $h_i = p_1^{f_{i,1}} \cdots p_r^{f_{i,r}}$. In particular, $\#\Sigma(L) \leq 2\sum_{j=1}^{r} e_j$.

Remark 1.5. Let L be a number field of odd degree $N = p_1^{e_1} \cdots p_r^{e_r}$. Theorem 1.4 shows that $\#\Sigma(L) \leq 2\sum_{j=1}^{r} e_j$. Since $p_j \geq 3$, it is clear that the quantity $\sum e_j$ would be maximized if $r = 1$, $p_1 = 3$, and $e_1 = \log_3(N)$. Thus,

$$\#\Sigma(L) \leq 2\sum_{j=1}^{r} e_j \leq 2\log_3(N),$$

which shows Theorem 1.1.

The article is organized as follows. In Section 2 we include a number of well-known results on class numbers of orders in imaginary quadratic fields, and then we specialize those to the case of odd class number. In Section 3, we study the number of CM j-invariants defined over a field extension $L \in \mathcal{L}(N)$, for some fixed N, i.e., $L = \mathbb{Q}(j(E))$ for some CM curve E. In particular, we prove Theorem 1.3 (see Theorem 3.4). In Section 4 we study the intersection of ring class fields, and we use these results in Section 5 in order to prove Theorem 1.4. We also provide several explicit examples, in order to demonstrate that our bounds are, in fact, sharp in the sense that there are number fields of arbitrarily high odd degree where the bound is an equality (see Examples 5.4, 5.5, and 5.9).

Acknowledgements. The authors would like to thank Keith Conrad, David Cox, and Liang Xiao for their comments and suggestions.

2. Preliminaries

In this section we collect a number of results on orders in imaginary quadratic fields, and their class numbers. Throughout the paper K will be an imaginary quadratic field with ring of integers $\mathcal{O}_K$, and the class number of $\mathcal{O}_K$ will be denoted by h_K. The discriminant of $\mathcal{O}_K$ will be denoted by d_K. If $\mathcal{O}$ is an order of $\mathcal{O}_K$, then we denote its class number by $h(\mathcal{O})$. The basic theory of complex multiplication is summarized in the following result.

Theorem 2.1 ([Sil94], Ch.2, Theorems 4.3 and 6.1; [Cox89], Theorem 11.1)**.** *Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and let E be an elliptic curve with CM by an order $\mathcal{O}$ of $\mathcal{O}_K$ of conductor $\mathfrak{f}$. Then:*

1. *The j-invariant of E, $j(E)$, is an algebraic integer.*
2. *The field $L = K(j(E))$ is the ring class field of the order $\mathcal{O}$.*
3. *$[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h(\mathcal{O})$, where $h(\mathcal{O})$ is the class number of $\mathcal{O}$.*
4. *Let $\{E_1, \ldots, E_h\}$ be a complete set of representatives of isomorphism classes of elliptic curves with CM by $\mathcal{O}$. Then $\{j(E_1), \ldots, j(E_h)\}$ is a complete set of $\mathrm{Gal}(\overline{K}/K)$ conjugates of $j(E)$.*

We shall need a formula for the class number of an arbitrary order in terms of its conductor, and the class number of the maximal order. Such a formula is given in the next theorem.

Theorem 2.2 ([Cox89], Theorem 7.24)**.** *Let $\mathcal{O}$ be the order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Then, the class number of $\mathcal{O}$ is an integer multiple of h_K, and it satisfies*

$$h(\mathcal{O}) = \frac{h_K \cdot \mathfrak{f}}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \cdot \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{d_K}{p} \right) \cdot \frac{1}{p} \right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

We remind the reader that for an odd prime p, the Kronecker symbol is just the Legendre symbol, and if $p = 2$, we have the formula

$$\left(\frac{d_K}{2}\right) = \begin{cases} 0 & \text{if } 2|d_K, \\ 1 & \text{if } d_K \equiv 1 \bmod 8, \\ -1 & \text{if } d_K \equiv 5 \bmod 8. \end{cases}$$

In this note we are specially interested in orders with odd class number. The class number formula of Theorem 2.2 shows that, for our purposes, we only need to consider imaginary quadratic fields whose ring of integers has odd class number (we will show this carefully, and improve the characterization in Theorem 2.8 below). Genus theory will tell us that we should only consider those with prime discriminant. We remind the reader that the genus field of K is the maximal unramified extension of K which is an abelian extension of $\mathbb{Q}$.

Theorem 2.3 ([Cox89], Theorem 6.1)**.** *Let K be an imaginary quadratic field of discriminant d_K, let μ be the number of primes dividing d_K, and let $p_1, \ldots, p_r$ be the odd primes dividing d_K. Set $p_i^* = (-1)^{(p_i-1)/2} p_i$. Then, the genus field of K is $K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*})$. In particular, the class number h_K is divisible by $2^{\mu-1}$.*

Corollary 2.4. *If $K/\mathbb{Q}$ is an imaginary quadratic extension with odd class number, then $K = \mathbb{Q}(\sqrt{-d})$ where $d = 1$ or 2, or a prime $q \equiv 3 \bmod 4$.*

Proof. By Theorem 2.3, if h_K is odd, then the discriminant d_K has precisely one prime divisor. In particular $d = 1$, 2, or an odd prime q. Moreover, since $d_K = -d$ or $-4d$, according to the class of $-d$ modulo 4, it follows that if $d = q$ is an odd prime, then $q \equiv 3 \bmod 4$. □

Theorem 2.5. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field with $d \neq 1$ or 2, and let $\mathcal{O}$ be the order of $\mathcal{O}_K$ of conductor $\mathfrak{f}$. Then $h(\mathcal{O})$ is odd if and only if h_K is odd, $K = \mathbb{Q}(\sqrt{-q})$ for some prime $q \equiv 3 \bmod 4$, and $\mathfrak{f} = 2^n q^m$, where $n \in \{0, 1\}$ and $m \geq 0$.*

Proof. Let us first assume that $K = \mathbb{Q}(\sqrt{-q})$ for some prime $q \equiv 3 \bmod 4$, h_K is odd, and $\mathfrak{f} = 2^n q^m$ for some $n \in \{0, 1\}$ and $m \geq 0$. Under these hypotheses $d_K = -q$. Since we are assuming that $K \neq \mathbb{Q}(i)$, we know that $[\mathcal{O}_K^\times : \mathcal{O}^\times] = 1$ or 3, so in either case $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ is odd. Thus, it suffices to check that $[\mathcal{O}_K^\times : \mathcal{O}^\times] h(\mathcal{O})$ is odd. Applying Theorem 2.2 we have that

$$\begin{aligned}
[\mathcal{O}_K^\times : \mathcal{O}^\times] h(\mathcal{O}) &= h_K \cdot \mathfrak{f} \cdot \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) = h_K \cdot 2^n \cdot q^m \prod_{p|2^n q^m} \left(1 - \left(\frac{-q}{p}\right)\frac{1}{p}\right) \\
&= \begin{cases} h_K \cdot q^m \left(1 - \left(\frac{-q}{q}\right)\frac{1}{q}\right) & \text{if } n = 0, \text{ and} \\ h_K \cdot 2 \cdot q^m \left(1 - \left(\frac{-q}{2}\right)\frac{1}{2}\right)\left(1 - \left(\frac{-q}{q}\right)\frac{1}{q}\right) & \text{if } n = 1 \end{cases} \\
&= \begin{cases} h_K \cdot q^m & \text{if } n = 0, \text{ and} \\ h_K \cdot 2 \cdot q^m \left(\frac{2 \pm 1}{2}\right) & \text{if } n = 1 \end{cases} \\
&= \begin{cases} h_K \cdot q^m & \text{if } n = 0, \text{ and} \\ h_K \cdot q^m (2 \pm 1) & \text{if } n = 1. \end{cases}
\end{aligned}$$

Therefore, $h(\mathcal{O})$ is also odd, by the assumption that h_K is odd and the fact that $q \equiv 3 \bmod 4$.

For the converse, let us assume that $h(\mathcal{O})$ is odd. By Theorem 2.2, $h(\mathcal{O})$ is a multiple of h_K, so h_K must be odd. By Corollary 2.4, and since we are assuming $d \neq 1$ or 2, we have $K = \mathbb{Q}(\sqrt{-q})$ for some prime $q \equiv 3 \bmod 4$, and so $d_K = -q$. Since $h(\mathcal{O})$ is assumed to be odd, and $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ is odd ($d \neq 1$ or 2), then $[\mathcal{O}_K^\times : \mathcal{O}^\times] h(\mathcal{O})$ is odd. By Theorem 2.2 we have that

$$[\mathcal{O}_K^\times : \mathcal{O}^\times] h(\mathcal{O}) = h_K \cdot \mathfrak{f} \cdot \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{-q}{p}\right)\frac{1}{p}\right).$$

It is clear that the 2-adic valuation of the denominator of $\prod_{p|\mathfrak{f}} \left(1 - \left(\frac{-q}{p}\right)\frac{1}{p}\right)$ is at most 1, and this occurs when $2|\mathfrak{f}$, but if $4|\mathfrak{f}$, then the 2-adic valuation of $[\mathcal{O}_K^\times : \mathcal{O}^\times] h(\mathcal{O})$ would be at least 1, and so the number would be odd.

We conclude that the 2-adic valuation of $\mathfrak{f}$ is 0 or 1. Moreover, suppose p is a prime not equal to 2 or q and such that $p|\mathfrak{f}$. Then $\left(\frac{-q}{p}\right) = \pm 1$, which implies that

$$\left(1 - \left(\frac{-q}{p}\right)\frac{1}{p}\right) = \frac{p \pm 1}{p},$$

and so the 2-adic valuation of this factor is positive, since p is odd. Hence, the 2-adic valuation of $[\mathcal{O}_K^\times : \mathcal{O}^\times]h(\mathcal{O})$ satisfies

$$\nu_2([\mathcal{O}_K^\times : \mathcal{O}^\times]h(\mathcal{O})) \geq \max\{\nu_2(\mathfrak{f}) - 1, 0\} + \#\{p : p|\mathfrak{f}, p \neq 2, q\}.$$

It follows that if $h(\mathcal{O})$ is odd, then the only primes dividing $\mathfrak{f}$ may be 2 or q, but no others. Hence, $\mathfrak{f} = 2^n q^m$, with $n \in \{0, 1\}$ and $m \geq 0$ as claimed. □

Next, we find the orders of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$ with odd class number. We remark first that the class number of the order $\mathcal{O}$ of $\mathbb{Q}(i)$ of conductor 2 is, by Theorem 2.2, given by

$$h(\mathcal{O}) = \frac{h_K \cdot \mathfrak{f}}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) = \frac{1 \cdot 2}{2}\left(1 - \left(\frac{-4}{2}\right)\frac{1}{2}\right) = 1,$$

and so $h(\mathcal{O}) = 1$ is odd. Indeed, there are elliptic curves defined over $\mathbb{Q}$ with CM by $\mathcal{O}$, namely those with $j = 2^3 3^3 11^3$.

Lemma 2.6. *Let $\mathcal{O}$ be an order of $\mathbb{Q}(i)$ of conductor $\mathfrak{f} > 2$. Then $h(\mathcal{O})$ is even.*

Proof. Notice that if $\mathfrak{f} > 2$, then $[\mathcal{O}_K^\times : \mathcal{O}^\times] = 2$. Applying Theorem 2.2, we see that

$$h(\mathcal{O}) = \frac{h_K \cdot \mathfrak{f}}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) = \frac{\mathfrak{f}}{2} \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right).$$

We will break this lemma into three cases, according to whether $\mathfrak{f}$ is a power of 2, or it has an odd prime divisor $\equiv \pm 1 \bmod 4$.

Case 1: $\mathfrak{f} > 2$ is a power of 2 (in particular, $\mathfrak{f}$ is divisible by 4). Let us write $\mathfrak{f} = 2^n$ for some $n > 1$. Applying Theorem 2.2 we obtain

$$h(\mathcal{O}) = \frac{1 \cdot 2^n}{2} \prod_{p|2^n} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right) = 2^{n-1}\left(1 - \left(\frac{-4}{2}\right)\frac{1}{2}\right) = 2^{n-1}.$$

Thus, $h(\mathcal{O})$ is even.

Case 2: The conductor of $\mathcal{O}$ is divisible by an odd prime $q \equiv 1 \bmod 4$. Let us write $\mathfrak{f} = \mathfrak{f}' \cdot q$ and again apply Theorem 2.2 to calculate

$$h(\mathcal{O}) = \frac{\mathfrak{f}}{2}\left(1 - \frac{1}{q}\right) \prod_{p|\mathfrak{f}'} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right) = \left(\frac{q-1}{2}\right) \cdot \left(\mathfrak{f}' \prod_{\substack{p|\mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right)\right).$$

Since $q \equiv 1 \bmod 4$, we have that $\dfrac{q-1}{2} \equiv 0 \bmod 2$, and since $\mathfrak{f}' \displaystyle\prod_{\substack{p|\mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right)$ is an integer, we see that $h(\mathcal{O})$ is even.

Case 3: The conductor of $\mathcal{O}$ is divisible by an odd prime $q \equiv 3 \bmod 4$. Let us write $\mathfrak{f} = \mathfrak{f}' \cdot q$. Then,

$$h(\mathcal{O}) = \left(\frac{q+1}{2}\right) \cdot \left(\mathfrak{f}' \prod_{\substack{p|\mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right)\right).$$

Since $q \equiv 3 \bmod 4$, we have that $\frac{q+1}{2} \equiv 0 \mod 2$, and again $\mathfrak{f}' \prod_{\substack{p \mid \mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right)$ is an integer, we conclude that $h(\mathcal{O})$ is even. □

Lemma 2.7. *Let $\mathcal{O}$ be an order of $\mathbb{Q}(\sqrt{-2})$ of conductor $\mathfrak{f} > 1$. Then $h(\mathcal{O})$ is even.*

Proof. Applying Theorem 2.2, we see that

$$h(\mathcal{O}) = \frac{h_K \cdot \mathfrak{f}}{[\mathcal{O}_K^\times : \mathcal{O}]} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) = \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{-8}{p}\right)\frac{1}{p}\right).$$

We consider two cases, according to whether $\mathfrak{f}$ is a power of 2.

Case 1: $\mathfrak{f}$ is a power of 2. Let us write $\mathfrak{f} = 2^n$, with $n > 0$. Then,

$$h(\mathcal{O}) = 2^n \left(1 - \left(\frac{-8}{2}\right)\frac{1}{2}\right) = 2^n.$$

Thus, $h(\mathcal{O})$ is even.

Case 2: $\mathfrak{f}$ is divisible by an odd prime q. Let us write $\mathfrak{f} = q \cdot \mathfrak{f}'$. Then,

$$\begin{aligned} h(\mathcal{O}) &= \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{-8}{p}\right)\frac{1}{p}\right) = q\left(1 - \left(\frac{-8}{q}\right)\frac{1}{q}\right) \cdot \mathfrak{f}' \prod_{\substack{p \mid \mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-8}{p}\right)\frac{1}{p}\right) \\ &= (q \pm 1)\left(\mathfrak{f}' \prod_{\substack{p \mid \mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-8}{p}\right)\frac{1}{p}\right)\right). \end{aligned}$$

Since q is an odd prime, we know that $q \pm 1$ is even, and since $\mathfrak{f}' \prod_{\substack{p \mid \mathfrak{f}' \\ p \neq q}} \left(1 - \left(\frac{-8}{p}\right)\frac{1}{p}\right)$ is an integer, we conclude that $h(\mathcal{O})$ is even. □

Putting together Theorem 2.5, Lemma 2.6, and Lemma 2.7, we show a formula for the class number of orders, in the case when the class number is odd.

Theorem 2.8. *Let K be an imaginary quadratic field, let $\mathcal{O}$ be an order of conductor $\mathfrak{f}$, and suppose that $h(\mathcal{O})$ is odd. Then, exactly one of the following occurs:*

1. *If $K = \mathbb{Q}(i)$, then $\mathcal{O} = \mathcal{O}_K$ or $\mathfrak{f} = 2$, and $h(\mathcal{O}) = 1$.*
2. *If $K = \mathbb{Q}(\sqrt{-2})$, then $\mathcal{O} = \mathcal{O}_K$ and $h(\mathcal{O}) = 1$.*
3. *If $K \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$, then $K = \mathbb{Q}(\sqrt{-q})$ for some prime $q \equiv 3 \bmod 4$, and $\mathfrak{f} = 2^n q^m$, where $n \in \{0, 1\}$ and $m \geq 0$. Thus,*
   (a) *If $K = \mathbb{Q}(\sqrt{-3})$, and $\mathcal{O} = \mathcal{O}_K$, then $h(\mathcal{O}) = 1$. Otherwise, if $\mathfrak{f} > 1$ with $\mathfrak{f} = 2^n 3^m$, then*

$$h(\mathcal{O}) = \begin{cases} 3^{m-1} & \text{if } \mathfrak{f} = 3^m, \\ 3^m & \text{if } \mathfrak{f} = 2 \cdot 3^m. \end{cases}$$

   (b) *If $K = \mathbb{Q}(\sqrt{-q}) \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, then*

$$h(\mathcal{O}) = \begin{cases} h_K \cdot q^m & \text{if } \mathfrak{f} = q^m, \\ h_K \cdot q^m & \text{if } \mathfrak{f} = 2 \cdot q^m,\ q \equiv 7 \bmod 8, \\ 3 \cdot h_K \cdot q^m & \text{if } \mathfrak{f} = 2 \cdot q^m,\ q \equiv 3 \bmod 8. \end{cases}$$

A direct consequence of the formulas for odd class numbers is that, for a fixed imaginary quadratic field, there are only finitely many orders of odd class number below a given bound. We record this as a corollary.

Corollary 2.9. *Let K be an imaginary quadratic field, and let $N \geq 1$ be fixed. Then,*

1. *There are only finitely many orders of K with odd class number $\leq N$.*

(2) *There are only finitely many isomorphism classes of elliptic curves E with CM by K, such that $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is odd and $\leq N$.*

Proof. Part (1) follows from Theorem 2.8, because the class number grows as the conductor grows. Part (2) follows from part (1) and the fact that there only finitely many elliptic curves with CM by a given order, by Theorem 2.1. □

Remark 2.10. Of course, Corollary 2.9 is true much more generally (and not just for odd class number). It is well known that there are only finitely many imaginary quadratic fields with class number less or equal than a given bound N (see [Gol85]) and, together with Theorem 2.2, this shows that there are only finitely many orders of class number $\leq N$, for any fixed $N \geq 1$.

Corollary 2.11. *Let K be an imaginary quadratic field and suppose that E_1 and E_2 have CM by orders $\mathcal{O}_1$ and $\mathcal{O}_2$ of $\mathcal{O}_K$ with conductors $\mathfrak{f}_1 \leq \mathfrak{f}_2$ respectively, such that $h(\mathcal{O}_1)$ and $h(\mathcal{O}_2)$ are odd. Let $\mathfrak{f}_g = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ and $\mathfrak{f}_l = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$, and let $\mathcal{O}_g$ and $\mathcal{O}_l$ be, respectively, orders of $\mathcal{O}_K$ with conductors $\mathfrak{f}_g$ and $\mathfrak{f}_l$. Then:*

$$h(\mathcal{O}_g) = \gcd(h(\mathcal{O}_1), h(\mathcal{O}_2)), \text{ and } h(\mathcal{O}_l) = \operatorname{lcm}(h(\mathcal{O}_1), h(\mathcal{O}_2)).$$

Proof. Throughout the proof, we will use the formulas of Theorem 2.8. If $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$, then the theorem is clear because all the class numbers involved are equal to 1, so let us assume that $K \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. If $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O}_1 = \mathcal{O}_K$ (i.e., $\mathfrak{f}_1 = 1$), then $\mathcal{O}_g = \mathcal{O}_K$ and $\mathcal{O}_l = \mathcal{O}_2$, and the formulas hold trivially. Thus, we may assume that if $K = \mathbb{Q}(\sqrt{-3})$, then neither $\mathcal{O}_1$ or $\mathcal{O}_2$ are $\mathcal{O}_K$, and therefore $\lambda = [\mathcal{O}_K^\times : \mathcal{O}_1^\times] = [\mathcal{O}_K^\times : \mathcal{O}_2^\times]$ is equal to 3 if $K = \mathbb{Q}(\sqrt{-3})$ and to 1 if $K \neq \mathbb{Q}(\sqrt{-3})$. In particular, if $\mathfrak{f}_1 = 2^{n_1} q^{m_1}$ and $\mathfrak{f}_2 = 2^{n_2} q^{m_2}$, then $\mathfrak{f}_g = \gcd(\mathfrak{f}_1, \mathfrak{f}_2) = 2^{\min\{n_1,n_2\}} 3^{\min\{m_1,m_2\}}$ and so

$$\begin{aligned} \gcd(h(\mathcal{O}_1), h(\mathcal{O}_2)) &= \begin{cases} 3 \cdot h_K \cdot q^{\min\{m_1,m_2\}}/\lambda & \text{if } n_1 = n_2 = 1 \text{ and } q \equiv 3 \bmod 8, \\ h_K \cdot q^{\min\{m_1,m_2\}}/\lambda & \text{otherwise,} \end{cases} \\ &= h(\mathcal{O}_g). \end{aligned}$$

Similarly, $\mathfrak{f}_l = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2) = 2^{\max\{n_1,n_2\}} 3^{\max\{m_1,m_2\}}$ and so

$$\begin{aligned} \operatorname{lcm}(h(\mathcal{O}_1), h(\mathcal{O}_2)) &= \begin{cases} 3 \cdot h_K \cdot q^{\max\{m_1,m_2\}}/\lambda & \text{if } n_1 \text{ or } n_2 = 1 \text{ and } q \equiv 3 \bmod 8, \\ h_K \cdot q^{\max\{m_1,m_2\}}/\lambda & \text{otherwise,} \end{cases} \\ &= h(\mathcal{O}_l). \end{aligned}$$

Thus, the proof is complete. □

We will also need a lemma about conductors in abelian extensions of imaginary quadratic fields.

Lemma 2.12. *Let $\mathcal{O}$ be an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K, and let L be the ring class field attached to $\mathcal{O}$. Then:*

(1) *Let $\mathcal{O}'$ be another order in K, with conductor $\mathfrak{f}'$, and ring class field L'. Then, $\mathcal{O} \subseteq \mathcal{O}'$ if and only if $\mathfrak{f}' | \mathfrak{f}$. Moreover, $\mathfrak{f}' | \mathfrak{f}$ implies that $L' \subseteq L$.*

(2) *Let L and L' be ring class fields attached to $\mathcal{O}$ and $\mathcal{O}'$ respectively, and let $\mathcal{C} = C(L/K)$ and $\mathcal{C}' = C(L'/K)$ be the conductors of the abelian extensions L/K and L'/K. If $L' \subseteq L$, then $\mathcal{C}'$ is a divisor of $\mathcal{C}$.*

(3) *The relationship between the conductors $\mathfrak{f}$ of $\mathcal{O}$ and $\mathcal{C} = C(L/K)$ is given by*

$$C(L/K) = \begin{cases} \mathcal{O}_K & \text{if } \mathfrak{f} = 2 \text{ or } 3, \text{ and } K = \mathbb{Q}(\sqrt{-3}), \\ \mathcal{O}_K & \text{if } \mathfrak{f} = 2, \text{ and } K = \mathbb{Q}(i), \\ (\mathfrak{f}/2)\mathcal{O}_K & \text{if } \mathfrak{f} \text{ is even and } \mathfrak{f}/2 \text{ is odd, and } 2 \text{ splits completely in } K, \\ \mathfrak{f}\mathcal{O}_K & \text{otherwise.} \end{cases}$$

In particular, $C(L/K) = (\mathfrak{f}/k)\mathcal{O}_K$ with $k = 1, 2$, or 3.

Proof. Parts (1), and (3) are shown, respectively in Exercise 9.19, and Exercise 9.20 in [Cox89]. It remains to justify (2), i.e., if L/K and L'/K are abelian extensions such that $K \subseteq L' \subseteq L$, then $\mathcal{C}' = C(L'/K)$ is a divisor of $\mathcal{C} = C(L/K)$. In order to show this, we recall that the conductor of an abelian extension F/K is the greatest common divisor of all moduli m such that $F \subseteq K_m$, where K_m is the ray class field modulo m (see Exercise 8.6 in [Cox89]). In particular $L \subseteq K_{\mathcal{C}}$, and if $L' \subseteq L$, then $L' \subseteq K_{\mathcal{C}}$ as well. From this it follows that $\mathcal{C}' = C(L'/K)$ is a divisor of $\mathcal{C}$. □

The following result is a corollary of Theorem 2.2 and Lemma 2.12.

Corollary 2.13. *Let $\mathcal{O}$ be the order of conductor $\mathfrak{f}$ in an imaginary quadratic field K, and let $\mathcal{O} \subseteq \mathcal{O}'$ be a suborder of conductor $\mathfrak{f}'$. Then, $h(\mathcal{O}')$ is a divisor of $h(\mathcal{O})$.*

Proof. If $\mathfrak{f}' = 1$, i.e., if $\mathcal{O}' = \mathcal{O}_K$, then h_K divides $h(\mathcal{O})$ by Theorem 2.2. Otherwise, assume that $\mathfrak{f}' > 1$ (and so $\mathfrak{f} > 1$ as well because $\mathfrak{f}'$ needs to be a divisor of $\mathfrak{f}$ for $\mathcal{O} \subseteq \mathcal{O}'$ to hold). In this case, $[\mathcal{O}_K^\times : \mathcal{O}^\times] = [\mathcal{O}_K^\times : \mathcal{O}'^\times]$, and the index equals 2 if $K = \mathbb{Q}(i)$, equals 3 if $K = \mathbb{Q}(\sqrt{-3})$, and 1 otherwise. Now the divisibility of class numbers is clear from the formula for $h(\mathcal{O})$ in Theorem 2.2, since $\mathfrak{f}'|\mathfrak{f}$ (by Lemma 2.12) and since the same factors in $\prod_{p|\mathfrak{f}'}\left(1 - \left(\frac{d_K}{p}\right)\cdot\frac{1}{p}\right)$ appear in the product $\prod_{p|\mathfrak{f}}\left(1 - \left(\frac{d_K}{p}\right)\cdot\frac{1}{p}\right)$. □

The result that follows characterizes extensions of K contained in a ring class field.

Theorem 2.14 ([Cox89], Theorem 9.18)**.** *Let K be an imaginary quadratic field. Then, an abelian extension L of K is generalized dihedral over $\mathbb{Q}$ if and only if L is contained in a ring class field of K.*

We finish this section with a remark about the computation of the data in Tables 1 and 2

Remark 2.15. The data in Tables 1 and 2 was gathered using SAGE version 6.1.2 ([S$^+$14]), as follows. Given a positive integer N, the command `cm_orders(N)` returns a complete list of orders of class number N, i.e., a list of all the ordered pairs $(-D, \mathfrak{f})$ such that the order $\mathcal{O}$ of $\mathbb{Q}(\sqrt{-D})$ of conductor $\mathfrak{f}$ has class number $h(\mathcal{O}) = N$. The length of this list is exactly $\#\mathcal{O}(N)$, while $\Sigma(N) = N \cdot \#\mathcal{O}(N)$. Once we had a complete list of the orders of class number N, we used `hilbert_class_polynomials(-D*f^2)` to find the minimal polynomial of the j-invariants of the elliptic curves with CM by $\mathcal{O}$. With a minimal polynomial for $j(E)$, we can define the field $L = \mathbb{Q}(j(E))$. To compute $\#\mathcal{L}(N)$, we simply compute how many of these fields are non-isomorphic for a fixed N. Last, we used the command `cm_j_invariants(L)` that returns a list of all of the j-invariants of CM elliptic curves that are defined over the number field L. Thus, in order to order to compute $\#\max\{\#\Sigma(\mathcal{L}(N)))\}$, we simply compute the length of the list returned by `cm_j_invariants(L)`, for every $L \in \mathcal{L}(N)$ and take the maximum value. To compute $\#\max\{\#\Sigma(\mathfrak{L}(N)))\}$ we do the same, but this time we take the maximum over all fields of the form $L = \mathbb{Q}(j_1, ..., j_r)$ such that $[L : \mathbb{Q}] = N$, and each j_i for $i = 1, \ldots, r$, is a j-invariant with CM by an order of class number dividing N.

For instance, when $N = 2$, the command `cm_orders(2)` returns the list

$$(-3,7),(-3,5),(-3,4),(-4,5),(-4,4),(-4,3),(-7,4),(-8,3),(-8,2),(-11,3),$$
$$(-15,2),(-15,1),(-20,1),(-24,1),(-35,1),(-40,1),(-51,1),(-52,1),(-88,1),(-91,1),$$
$$(-115,1),(-123,1),(-148,1),(-187,1),(-232,1),(-235,1),(-267,1),(-403,1),(-427,1).$$

Then, the command `hilbert_class_polynomials(-D*f^2)` for each pair in the list gave us minimal polynomials, which in turn allow us to define all the number fields L in $\mathcal{L}(2)$. Finally, we used `cm_j_invariants(L)`, for each L in $\mathcal{L}(2)$ to gather the data in Table 1.

3. The case when $L = \mathbb{Q}(j(E))$

In this section we consider the special case of a number field obtained by adjoining the j-invariant of a single elliptic curve with complex multiplication.

Lemma 3.1. *Let $j(E)$ be a j-invariant with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K of conductor $\mathfrak{f}$, such that the class number of $\mathcal{O}$ is $n > 1$. Then:*

1. *If $n > 1$ is odd, then the field $H = K(j(E))$ contains a unique quadratic subfield, namely K.*
2. *Suppose that $K \not\subseteq \mathbb{Q}(j(E))$, and assume the extension $K(j(E))/K$ is not 2-elementary abelian. Then $\mathbb{Q}(j(E))/\mathbb{Q}$ is not Galois.*

Proof. Let $j(E)$ be a j-invariant with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K of conductor $\mathfrak{f}$, such that the class number of $\mathcal{O}$ is odd > 1. Then, by the theory of complex multiplication the field $H = K(j(E))$ is the ring class field of $\mathcal{O}$ (Theorem 11.1 in [Cox89]). In particular, $H/\mathbb{Q}$ is Galois (Lemma 9.3 in [Cox89]), and $\mathrm{Gal}(H/\mathbb{Q})$ has order $2n$. Since n is odd, $H/\mathbb{Q}$ contains a unique quadratic subfield, namely K (note that if this was not the case, then there would be two distinct quadratic fields inside H, and therefore $\mathrm{Gal}(H/\mathbb{Q})$ would be divisible by 4). This shows (1).

For (2), let us assume that $K \not\subseteq \mathbb{Q}(j(E))$, and assume the extension $H = K(j(E))/K$ is not 2-elementary abelian. In particular, $H/\mathbb{Q}(j(E))$ is quadratic and $\mathrm{Gal}(H/\mathbb{Q}(j(E))) \cong \mathrm{Gal}(K/\mathbb{Q})$. Lemma 9.3 of [Cox89] says that

$$\mathrm{Gal}(H/\mathbb{Q}) \cong \mathrm{Gal}(H/K) \rtimes \mathrm{Gal}(H/\mathbb{Q}(j(E)))$$

is a semi-direct product, such that the non-trivial element $\tau \in \mathrm{Gal}(H/\mathbb{Q}(j(E)))$ acts by conjugation on $\mathrm{Gal}(H/K)$ and sends σ to σ^{-1}, i.e., $\tau\sigma\tau^{-1} = \sigma^{-1}$. Now, $\mathrm{Gal}(\mathbb{Q}(j(E))/\mathbb{Q})$ is Galois if and only if $\mathrm{Gal}(H/\mathbb{Q}(j(E)))$ is normal in $\mathrm{Gal}(H/\mathbb{Q})$, and Proposition 11 in Section 5.5 of [DF04] says that $\mathrm{Gal}(H/\mathbb{Q}(j(E)))$ is normal in $H/\mathbb{Q}$ if and only if the semi-direct action is trivial, i.e., $\sigma = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(H/K)$, which means that every non-trivial element of $\mathrm{Gal}(H/K)$ has order 2. However, by assumption, $\mathrm{Gal}(K(j(E))/K)$ is not 2-elementary abelian and therefore it contains an element σ such that $\sigma \neq \sigma^{-1}$. Hence, $\mathbb{Q}(j(E))/\mathbb{Q}$ cannot be Galois. □

Lemma 3.2. *Let j and j' be distinct j-invariants with complex multiplication by an order $\mathcal{O}$ of conductor $\mathfrak{f}$, within the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K, such that $h(\mathcal{O})$ is odd and > 1. Then,*

$$\mathbb{Q}(j, j') = K(j) = K(j').$$

Proof. Since j and j' have CM by the same order, they are Galois conjugates, by Theorem 2.1. By Lemma 3.1, neither $\mathbb{Q}(j)$ nor $\mathbb{Q}(j')$ are Galois extensions of $\mathbb{Q}$, but $K(j)/\mathbb{Q}$ is Galois (Theorem 11.1 in [Cox89]), and therefore

$$\mathbb{Q}(j) \subseteq \mathbb{Q}(j, j') \subseteq K(j).$$

Since $K(j)/\mathbb{Q}(j)$ is quadratic, either $\mathbb{Q}(j) = \mathbb{Q}(j, j')$ or $K(j) = \mathbb{Q}(j, j')$.

Suppose for a contradiction that $\mathbb{Q}(j) = \mathbb{Q}(j, j')$, i.e., $\mathbb{Q}(j) = \mathbb{Q}(j')$, where the last equality follows from the fact that their degrees are equal. Let $G = \mathrm{Gal}(K(j)/\mathbb{Q})$. By Lemma 9.3 of [Cox89] we can write $N = \mathrm{Gal}(K(j)/K)$ and $\langle\tau\rangle = \mathrm{Gal}(K(j)/\mathbb{Q}(j))$, so that $\mathrm{Gal}(K(j)/\mathbb{Q}) \cong N \rtimes \langle\tau\rangle$. Since $h(\mathcal{O})$ is odd, it follows that the order of N is odd, and $\langle\tau\rangle$ is a 2-Sylow subgroup of $G = \mathrm{Gal}(K(j)/\mathbb{Q})$ that fixes $\mathbb{Q}(j)$. Since j' is a conjugate of j, there exists some $g \in G$ such that $j' = g(j)$. In particular, j' is fixed by τ, because $j' \in \mathbb{Q}(j)$, but j' is also fixed by $\tau' = g\tau g^{-1}$ because

$$\tau'(j') = g\tau g^{-1}(j') = g\tau g^{-1}(g(j)) = g\tau(j) = g(j) = j',$$

where we used the fact that τ fixes j. Hence, $\mathbb{Q}(j)$ is the fixed field of $\langle\tau\rangle$ and $\mathbb{Q}(j) = \mathbb{Q}(j')$ is the fixed field of $\langle g\tau g^{-1}\rangle$, so we conclude that $\langle\tau\rangle = \langle g\tau g^{-1}\rangle$, and so $g\tau g^{-1} = \tau$, i.e., g and τ commute (recall that τ acts on g by conjugation and $\tau g\tau^{-1} = g^{-1}$). We distinguish two cases. Since $G = N \rtimes \langle\tau\rangle$, either $g \in N$, or $g = n\tau$, for some $n \in N$:

(1) If $g \in N$ commutes with τ, i.e., $g\tau = \tau g$, then $g = \tau g\tau^{-1} = g^{-1}$, so $g^2 = 1$. Since N has odd order, $g = 1$.
(2) If $g = n\tau$ for some $n \in N$, and g commutes with τ, then $n = (n\tau)\tau = \tau(n\tau)$, hence $n = \tau n\tau = \tau n\tau^{-1} = n^{-1}$, so $n = 1$ as before, and so $g = n\tau = \tau$.

In either case we find that $g = 1$ or τ, i.e., $g \in \langle\tau\rangle$, which fixed j, and so $j' = g(j) = j$, contradicting the fact that j and j' are distinct. Hence, we have reached a contradiction, and we must have $\mathbb{Q}(j) \neq \mathbb{Q}(j, j')$, which implies $\mathbb{Q}(j, j') = K(j)$ as desired. □

Lemma 3.3. *Let E be an elliptic curve with complex multiplication by an order $\mathcal{O}$ of conductor $\mathfrak{f}$, within the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K, such that $h(\mathcal{O})$ is odd. Let $\mathcal{O}'$ be another order with conductor $\mathfrak{f}'$ of odd class number, and such that there is an inclusion of ring class fields $K(\mathcal{O}') \subseteq K(\mathcal{O})$. Then, there exists a unique j-invariant j' with CM by $\mathcal{O}'$, such that any elliptic curve E' with $j(E') = j'$ satisfies $\mathbb{Q}(j(E')) \subseteq \mathbb{Q}(j(E))$.*

Proof. Let E, $\mathcal{O}$, $\mathcal{O}'$, $\mathfrak{f}$, and $\mathfrak{f}'$ be as in the statement, and let E'' for the moment be any elliptic curve with CM by the order of $\mathcal{O}'$ of conductor $\mathfrak{f}'$. Since $K(j(E))$ is the ring class field of $\mathcal{O}$ (Theorem 11.1 in [Cox89]) we have by assumption that the ring class field $K(j(E'')) = K(\mathcal{O}')$ is contained in $K(j(E)) = K(\mathcal{O})$. In particular, $\mathbb{Q}(j(E'')) \subseteq K(j(E))$. By Lemma 9.3 of [Cox89] we can write $N = \mathrm{Gal}(K(j(E))/K)$, so that $\mathrm{Gal}(K(j(E))/\mathbb{Q}) \cong N \rtimes \langle\tau\rangle$. Since $h(\mathcal{O})$ is odd, it follows that the order of N is odd, and $\langle\tau\rangle$ is a 2-Sylow subgroup of $G = \mathrm{Gal}(K(j(E))/\mathbb{Q})$.

Since $h(\mathcal{O}') = [\mathbb{Q}(j(E'')) : \mathbb{Q}]$ is odd by assumption, it follows that $\mathbb{Q}(j(E''))$ is fixed by some element τ'' of order 2 of G. Since $\langle\tau''\rangle$ is also a 2-Sylow subgroup, it follows that $\langle\tau\rangle$ and $\langle\tau''\rangle$ are conjugates, and so there is $g \in G$ such that $\tau = g\tau''g^{-1}$. Let us define $j' = g(j(E''))$. Then, j' is fixed by τ:

$$\tau(j') = g\tau''g^{-1}(j') = g\tau''g^{-1}(g(j(E''))) = g\tau''(j(E'')) = g(j(E'')) = j',$$

where we have used the fact that τ'' fixes $j(E'')$. Hence, j' is a conjugate of $j(E'')$ that is fixed by τ. Since the fixed field of $\langle\tau\rangle$ is precisely $\mathbb{Q}(j(E))$, we conclude that $j' \in \mathbb{Q}(j(E))$. Moreover, since j' is a conjugate of $j(E'')$, any elliptic curve E' with $j(E') = j'$ has CM by the order $\mathcal{O}'$ of conductor $\mathfrak{f}'$ as desired.

It remains to show that j' is the unique j-invariant with CM by $\mathcal{O}'$ contained in $\mathbb{Q}(j(E))$. Suppose that j'' is another j-invariant with CM by $\mathcal{O}'$ which is also in $\mathbb{Q}(j(E))$. Then, j'', $j(E')$ are two j-invariants with CM by $\mathcal{O}'$ contained in $\mathbb{Q}(j(E))$, and if they are distinct, then $K(j(E')) \subseteq \mathbb{Q}(j(E))$, by Lemma 3.2. However, $[K(j(E')) : \mathbb{Q}]$ is even, while $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is odd, so this is a contradiction. Hence, we must have $j'' = j(E')$, and there is a unique such j-invariant within $\mathbb{Q}(j(E))$ as claimed. □

Armed with these lemmas we are now ready to prove the following theorem.

Theorem 3.4. *Let L be a number field of degree d, and let $j(E) \in L$ be a j-invariant with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K of conductor $\mathfrak{f}$, and $j(E) \notin \mathbb{Q}$.*

1. *The class number of $\mathcal{O}$ is a divisor of $d = [L : \mathbb{Q}]$.*
2. *Let $F = \mathbb{Q}(j(E))$ be a number field of odd degree $n > 1$, and suppose $j(E') \in F$ is another j-invariant with complex multiplication, such that $j(E') \notin \mathbb{Q}$. Then, the curve E' has CM by an order $\mathcal{O}'$ also in K.*
3. *Let $F = \mathbb{Q}(j(E)) \subseteq L$, and suppose that $[F : \mathbb{Q}] = n > 1$ is odd. Let $\sigma_0(\mathfrak{f}) = \sum_{d|\mathfrak{f}} d^0$ be the number of positive divisors of $\mathfrak{f}$. Then, the number of j-invariants with CM defined over F is*

$$13 + \sigma_0(\mathfrak{f}) - J(K)$$

if $\mathfrak{f}$ is even, or if 2 does not split completely in K, and $13 + \sigma_0(2\mathfrak{f}) - J(K)$ otherwise, where $J(K)$ is the number of rational j-invariants of curves with CM by an order of K, i.e.,

d_K	-3	-4	-7	-8	-11	-19	-43	-67	-163	*else*
$J(K)$	3	2	2	1	1	1	1	1	1	0.

Proof. Let L be a number field of degree d, and let $j(E)$ be a j-invariant with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K of conductor $\mathfrak{f}$, and $j(E) \notin \mathbb{Q}$.

1. From Theorem 2.1, we have $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$, and since $\mathbb{Q}(j(E)) \subseteq L$, it follows that $h(\mathcal{O})$ is a divisor of $d = [L : \mathbb{Q}]$.
2. Let $j(E') \in \mathbb{Q}(j(E))$ be another j-invariant with complex multiplication by an order $\mathcal{O}'$ in an imaginary quadratic field K', such that $j(E') \notin \mathbb{Q}$. Now consider $\mathbb{Q}(j(E')) \subseteq \mathbb{Q}(j(E)) \subseteq K(j(E)) = H$. Since $H/\mathbb{Q}$ is Galois, it follows that the Galois closure of $\mathbb{Q}(j(E'))$ is contained in H. Moreover, $j(E')$ is not in $\mathbb{Q}$, so $\mathbb{Q}(j(E'))/\mathbb{Q}$ is non-trivial and of odd degree (because $\mathbb{Q}(j(E))/\mathbb{Q}$ is of odd degree and $j(E') \in \mathbb{Q}(j(E))$). Since $\mathbb{Q}(j(E'))/\mathbb{Q}$ is of odd degree, K' is not a subfield of $\mathbb{Q}(j(E'))$ and $K'(j(E'))/K'$ cannot be 2-elementary abelian. Thus, by Lemma 3.1, it follows that $\mathbb{Q}(j(E'))/\mathbb{Q}$ is not Galois. Since $K'(j(E'))$ is Galois over $\mathbb{Q}$ (by Lemma 9.3 in [Cox89]), we have $K'(j(E')) \subseteq H$, and in particular, $K' \subseteq H$. But Lemma 3.1 says that $H/\mathbb{Q}$ contains a unique quadratic subfield, namely K, and so $K = K'$. Hence E and E' have complex multiplications by orders of a common imaginary quadratic field K.
3. Let $F = \mathbb{Q}(j(E)) \subseteq L$, and suppose that $[F : \mathbb{Q}] = n > 1$ is odd. Let $j(E')$ be another CM j-invariant defined over F, with CM by an order $\mathcal{O}'$ in an imaginary quadratic field K'.

   Now consider $\mathbb{Q}(j(E')) \subseteq \mathbb{Q}(j(E)) \subseteq K(j(E)) = H$. Since $H/\mathbb{Q}$ is Galois, it follows that the Galois closure of $\mathbb{Q}(j(E'))$ is contained in H. There are two possibilities. Either
   (a) $\mathbb{Q}(j(E'))/\mathbb{Q}$ is Galois. In this case, since $[\mathbb{Q}(j(E')) : \mathbb{Q}] = n'$ is a divisor of n, which is odd, then n' is also odd. Thus K' cannot be contained in $\mathbb{Q}(j(E'))$ and $K(j(E'))/K$ cannot be 2-elementary abelian. Thus, by Lemma 3.1, we must have $n' = 1$. Hence, $j(E') \in \mathbb{Q}$.
   (b) Or $\mathbb{Q}(j(E'))/\mathbb{Q}$ is not Galois. Since $K'(j(E'))$ is a ring class field, it is Galois over $\mathbb{Q}$, and therefore $K'(j(E')) \subseteq H$. In particular, $K' \subseteq H$. By Lemma 3.1, it follows that $K = K'$, and $\mathcal{O}$ and $\mathcal{O}'$ are orders within the same imaginary quadratic field K.
   Let $L = K(j(E))$ and $L' = K(j(E'))$ be ring class fields attached to $\mathcal{O}$ and $\mathcal{O}'$ respectively (of conductor $\mathfrak{f}$ and $\mathfrak{f}'$ respectively), and let $\mathcal{C} = C(L/K)$ and $\mathcal{C}' = C(L'/K)$ be the conductors of the abelian extensions L/K and L'/K. Since $L' \subseteq L$, then $\mathcal{C}'$ is a divisor of $\mathcal{C}$. We distinguish several possibilities according to the choice of K. The results below follow from Lemma 2.12, part (3):
      (i) If $K = \mathbb{Q}(i)$, then either
         - $\mathfrak{f}'|\mathfrak{f}$, so that $\mathcal{O}' \subseteq \mathcal{O}$; or

- $\mathfrak{f}' = 2$ and $\mathfrak{f} = 1$, so that $\mathcal{O}' = \mathcal{O} = \mathcal{O}_K$. Since the class number of $\mathcal{O}_K$ is 1, this means that $j(E), j(E') \in \mathbb{Q}$.

(ii) If $K = \mathbb{Q}(\sqrt{-3})$, then either
- $\mathfrak{f}'|\mathfrak{f}$, so that $\mathcal{O}' \subseteq \mathcal{O}$; or
- $\mathfrak{f}' = 2$ or 3, and $\mathfrak{f} = 1$, so that $\mathcal{O}' = \mathcal{O} = \mathcal{O}_K$. Since the class number of $\mathcal{O}_K$ is 1, this means that $j(E), j(E') \in \mathbb{Q}$.

(iii) If $K \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, then either
- $\mathfrak{f}'|\mathfrak{f}$, so that $\mathcal{O}' \subseteq \mathcal{O}$; or
- $\mathfrak{f}'|2\mathfrak{f}$, where $\mathfrak{f}$ is odd, and 2 splits completely in K.

Hence, in all cases, either $j(E') \in \mathbb{Q}$, or $\mathfrak{f}'|\mathfrak{f}$, or $\mathfrak{f}$ is odd, and 2 splits completely in K, and $\mathfrak{f}'|2\mathfrak{f}$. Since every conductor $\mathfrak{f}'$ as above corresponds to a unique order $\mathcal{O}'$ with $K(\mathcal{O}') \subseteq K(\mathcal{O})$, which in turn corresponds to a unique j-invariant $j(E') \in \mathbb{Q}(j(E))$ by Lemma 3.3, it follows that the number of $j(E') \in \mathbb{Q}(j(E))$ with $j(E') \notin \mathbb{Q}$ is precisely

$$13 + \sigma_0(\mathfrak{f}) - J(K)$$

if $\mathfrak{f}$ is even, or if 2 does not split completely in K, and

$$13 + \sigma_0(2\mathfrak{f}) - J(K)$$

otherwise, as desired. Notice, the correction factor $J(K)$ ensures that no CM elliptic curves defined over $\mathbb{Q}$ are double counted.

□

We conclude this section with a theorem about fields generated by several CM j-invariants.

Theorem 3.5. *Let K be an imaginary quadratic field and suppose that E_1 and E_2 have CM by orders $\mathcal{O}_1$ and $\mathcal{O}_2$ of $\mathcal{O}_K$ with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$ respectively. Then, if $[\mathbb{Q}(j(E_1) : \mathbb{Q}]$ and $[\mathbb{Q}(j(E_2)) : \mathbb{Q}]$ are odd, then*

1. *There exists an elliptic curve E_g with CM by an order $\mathcal{O}_g$ of $\mathcal{O}_K$ with conductor $\mathfrak{f}_g = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ such that $\mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2)) = \mathbb{Q}(j(E_g))$, and*
2. *Assume that $\mathbb{Q}(j(E_1), j(E_2))$ is an extension of odd degree. Then, there exists an elliptic curve E_l with CM by an order $\mathcal{O}_l$ of $\mathcal{O}_K$ with conductor $\mathfrak{f}_l = \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$ such that $\mathbb{Q}(j(E_1), j(E_2)) = \mathbb{Q}(j(E_l))$.*

Proof. Let $\mathfrak{f}_g = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$, and let $\mathcal{O}_g$ be the order of K with conductor $\mathfrak{f}_g$. Since $\mathfrak{f}_g$ divides $\mathfrak{f}_1$ and $\mathfrak{f}_2$, it follows from Lemma 2.12 that there are inclusions of ring class fields $K(\mathcal{O}_g) \subseteq K(\mathcal{O}_i)$ for $i = 1, 2$. By assumption $h(\mathcal{O}_1)$ and $h(\mathcal{O}_2)$ are odd, so Lemma 3.3 implies that there is a unique j-invariant j_g such that any elliptic curve E_g with $j(E_g) = j_g$ has CM by $\mathcal{O}_g$, and $\mathbb{Q}(j(E_g))$ is contained in both $\mathbb{Q}(j(E_1))$ and $\mathbb{Q}(j(E_2))$, so $\mathbb{Q}(j(E_g)) \subseteq \mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2))$. Since the degree of $\mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2))$ divides the GCD of the degrees of $\mathbb{Q}(j(E_1))$ and $\mathbb{Q}(j(E_2))$, it follows that $h(\mathcal{O}_g) = [\mathbb{Q}(j(E_g) : \mathbb{Q}]$ is a divisor of $\gcd(h(\mathcal{O}_1), h(\mathcal{O}_2))$. But Corollary 2.11 shows that $h(\mathcal{O}_g) = \gcd(h(\mathcal{O}_1), h(\mathcal{O}_2))$, and hence $\mathbb{Q}(j(E_g)) = \mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2))$. This completes the proof of part (1).

For (2), let $\mathfrak{f}_l = \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$, and let $\mathcal{O}_l$ be the order of K with conductor $\mathfrak{f}_l$. Let E_l' be for the moment any elliptic curve with CM by $\mathcal{O}_l$. Since $\mathfrak{f}_i$ divides $\mathfrak{f}_l$, for $i = 1$, or 2, it follows that $K(\mathcal{O}_i) \subseteq K(\mathcal{O}_l)$, and therefore Lemma 3.3 implies that there are elliptic curves E_1' and E_2' with CM by $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively, such that $j(E_1'), j(E_2') \in \mathbb{Q}(j(E_l'))$.

Next, from part (1) of this theorem we know that there exists an elliptic curve E_g' such that $\mathbb{Q}(j(E_1')) \cap \mathbb{Q}(j(E_2')) = \mathbb{Q}(j(E_g'))$. Thus, $K(j(E_1')) \cap K(j(E_2')) = K(j(E_g'))$ and by our previous remarks it follows that $K(j(E_1'), j(E_2')) \subseteq K(j(E_l'))$. Next we remark that $K(j(E_1'), j(E_2'))/\mathbb{Q}$ is Galois (because each $K(j(E_i'))/\mathbb{Q}$ is Galois) and compute

$$\begin{aligned}
[K(j(E_1'), j(E_2')) : \mathbb{Q}] &= \frac{[K(j(E_1')) : \mathbb{Q}] \cdot [K(j(E_2')) : \mathbb{Q}]}{[K(j(E_1')) \cap K(j(E_2')) : \mathbb{Q}]} = \frac{[K(j(E_1')) : \mathbb{Q}] \cdot [K(j(E_2')) : \mathbb{Q}]}{[K(j(E_g')) : \mathbb{Q}]} \\
&= \frac{2h(\mathcal{O}_1) \cdot 2h(\mathcal{O}_2)}{2h(\mathcal{O}_g)} = \frac{2h(\mathcal{O}_1) \cdot h(\mathcal{O}_2)}{\gcd(h(\mathcal{O}_1), h(\mathcal{O}_2))} \\
&= 2\mathrm{lcm}(h(\mathcal{O}_1), h(\mathcal{O}_2)) = 2h(\mathcal{O}_l) = [K(j(E_l')) : \mathbb{Q}],
\end{aligned}$$

where we have used Corollary 2.11 twice in the last two strings of equalities. Thus, we conclude that we have an equality $K(j(E_1'), j(E_2')) = K(j(E_l'))$. From Galois theory, we know that $\mathrm{Gal}(K(j(E_l'))/K)$ is isomorphic to

the subgroup of $\mathrm{Gal}(K(j(E_1'))/K) \times \mathrm{Gal}(K(j(E_2'))/K)$ given by

$$\left\{(\sigma_1,\sigma_2) : \sigma_1\big|_{K(j(E_1'))\cap K(j(E_2'))} = \sigma_2\big|_{K(j(E_1'))\cap K(j(E_2'))}\right\} = \left\{(\sigma_1,\sigma_2) : \sigma_1\big|_{K(j(E_g'))} = \sigma_2\big|_{K(j(E_g'))}\right\}.$$

Theorem 2.1 implies that $j(E_1)$ and $j(E_1')$ are roots of the same polynomial, and so there exists an element $\sigma_1 \in \mathrm{Gal}(K(j(E_1'))/K)$ such that $\sigma_1(j(E_1')) = j(E_1)$. Similarly, there is a $\sigma_2 \in \mathrm{Gal}(K(j(E_2'))/K)$ such that $\sigma_2(j(E_2')) = j(E_2)$. Notice that for $i = 1$ or 2, the element σ_i sends $j(E_g')$ to some conjugate $\sigma_i(j(E_g'))$ of $j(E_g)$, but $\sigma_i(j(E_g')) \in \sigma_i(\mathbb{Q}(j(E_i'))) = \mathbb{Q}(j(E_i))$, and therefore $\sigma_i(j(E_g')) \in \mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2))$. Since $j(E_g)$ is the unique j-invariant with CM by $\mathcal{O}_g$ in $\mathbb{Q}(j(E_1))$ and $\mathbb{Q}(j(E_2))$ (by Lemma 3.3), it also follows that $j(E_g)$ is the unique such j-invariant in $\mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2))$. Thus, it must be that $\sigma_1(j(E_g')) = j(E_g) = \sigma_2(j(E_g'))$. Hence

$$\sigma_1\big|_{K(j(E_g'))} = \sigma_2\big|_{K(j(E_g'))}.$$

Thus there is an element $\sigma \in \mathrm{Gal}(K(j(E_l')/K)$ corresponding to the pair (σ_1,σ_2), such that $\sigma(j(E_1')) = j(E_1)$ and $\sigma(j(E_2')) = j(E_2)$. Letting $E_l = \sigma(E_l')$ we have $j(E_1), j(E_2) \in \mathbb{Q}(j(E_l))$ by construction, and E_l has CM by the order of $\mathcal{O}_K$ of conductor $\mathfrak{f}_l$. Since $K(j(E_l)) = K(j(E_1), j(E_2))$ and $\mathbb{Q}(j(E_1), j(E_2))$ is of odd degree by assumption, it must be that $\mathbb{Q}(j(E_l)) = \mathbb{Q}(j(E_1), j(E_2))$, as desired. This concludes the proof of (2). □

4. Intersections of Ring Class Fields of Different Imaginary Quadratic Fields

In this section we study the intersection of ring class fields attached to distinct imaginary quadratic fields.

Lemma 4.1. *Let $K_1, \dots, K_n$ be distinct imaginary quadratic fields of odd class number, and let $\mathcal{K}$ be the compositum $K_1 \cdots K_n$. Then, the only imaginary quadratic subfields of $\mathcal{K}$ of odd class number are $K_1, \dots, K_n$.*

Proof. By Corollary 2.4, each K_i is of the form $\mathbb{Q}(\sqrt{-q_i})$ where $q_i = 1$ or a prime, with $q_i \neq q_j$ for $i \neq j$. In particular, every quadratic subfield of the compositum $\mathcal{K} = \prod_{i=1}^n K_i$ is of the form

$$F = \mathbb{Q}\left(\sqrt{\prod_{i=1}^{n}(-q_i)^{t_i}}\right)$$

where each $t_i = 0$ or 1. But, if $t_i = 1$ for two different indices, then either F is real quadratic, or two different primes divide the discriminant and Theorem 2.3 would imply that the class number of F is even. Therefore, if $F \subseteq \mathcal{K}$ is an imaginary quadratic field of odd class number, then $t_i = 1$ for a unique index i, and so $F = K_i$ as desired. □

Lemma 4.2. *Let $K_1, \dots, K_n$ be distinct imaginary quadratic fields, and let H_i be a ring class field of K_i, for each $i = 1, \dots, n$, such that $[H_i : K_i] = n_i$ is odd. Let $\mathcal{H}$ be the compositum of all H_i. Then, any quadratic subfield $F \subseteq \mathcal{H}$ is contained in the compositum $\mathcal{K}$ of all K_i, for $i = 1, \dots, n$.*

Proof. Since the fields K_i are distinct, the compositum $\mathcal{K}$ has degree 2^n over $\mathbb{Q}$. And since $[H_i : K_i] = h_i$ is odd and $H_i/\mathbb{Q}$ Galois, it follows that $[\mathcal{H} : \mathbb{Q}]$ is a divisor of $2^n(\prod_{i=1}^n h_i)$, and therefore the power of 2 dividing $[\mathcal{H} : \mathbb{Q}]$ is precisely 2^n. If $F \subseteq \mathcal{H}$ was a quadratic field not contained in $\mathcal{K}$, then $F\mathcal{K}/\mathbb{Q}$ would be of degree 2^{n+1}, and since $F\mathcal{K} \subseteq \mathcal{H}$, it would follow that 2^{n+1} divides $[\mathcal{H} : \mathbb{Q}]$, and a contradiction arises. □

Lemma 4.3. *Let $E_1, \dots, E_n$ be elliptic curves with CM by orders $\mathcal{O}_i$ of distinct imaginary quadratic fields $K_i = \mathbb{Q}(\sqrt{-d_i})$. Assume that the extension $\mathbb{Q}(j(E_1), \dots, j(E_n))$ is of odd degree. Then, if E is a CM elliptic curve defined over $\mathbb{Q}(j(E_1), \dots, j(E_n))$, then E has CM by an order of class number 1 or an order of K_i, for some $i = 1, \dots, n$.*

Proof. Let $\mathcal{K}$ be the compositum of all K_i, for $i = 1, \dots, n$. Suppose that E has CM by an order $\mathcal{O}$ of the imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ and that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = m$. If the class number of $\mathcal{O}$ is 1, then $j(E)$ is defined over $\mathbb{Q}$, so let us assume that $m > 1$.

Since every $\mathbb{Q}(j(E_i))$ is of odd degree, we have that $\mathbb{Q}(j(E_1), \dots, j(E_n))/\mathbb{Q}$ is of odd degree, and since $j(E) \in \mathbb{Q}(j(E_1), \dots, j(E_n))$, it follows that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = m > 1$ is also odd. In particular, the Galois closure of $\mathbb{Q}(j(E))$ is the field $F(j(E))$ by Lemma 3.1. Also, we know that $K_i(j(E_i))$ is Galois, and so $\mathcal{K}(j(E_1), \dots, j(E_n))/\mathbb{Q}$ is also Galois, and so $F(j(E)) \subseteq \mathcal{K}(j(E_1), \dots, j(E_n))$. It follows that $F \subseteq \mathcal{K}$, by Lemma 4.2. But F is an imaginary quadratic field of odd class number contained in $\mathcal{K}$, and Lemma 4.1 implies that $F = K_i$ for some $i = 1, \dots, n$. □

Theorem 4.4. *Let $K_1, \dots, K_n$ be distinct imaginary quadratic fields of odd class number. Let $H_1, \dots, H_n$ be ring class fields of $K_1, \dots, K_n$ respectively, such that $[H_i : K_i] = n_i$ are all odd. Let $\mathcal{H} = \prod_{i=2}^{n} H_i$. Then $H_1 \cap \mathcal{H} = \mathbb{Q}$.*

Proof. Let $F = H_1 \cap \mathcal{H}$. Since each H_i is a ring class field, we know that $H_1/\mathbb{Q}$ and $\mathcal{H}/\mathbb{Q}$ are both Galois extensions, and therefore their intersection, F, is also Galois over $\mathbb{Q}$.

Next, we know that since $[H_1 : \mathbb{Q}] = 2n_1$ with n_1 odd, it must be that H_1 contains a unique quadratic extension (Lemma 3.1); namely, K_1, and in particular, $F \subseteq H_1$ contains at most one quadratic extension. But if $K_1 \subseteq F$, then $K_1 \subseteq \mathcal{H}$, and Lemma 4.2 would imply that K_1 is contained in the compositum $\mathcal{K} = \prod_{i=2}^{n} K_i$. By Lemma 4.1, and since all K_i are distinct of odd class number, K_1 cannot be contained in $\mathcal{K}$. It follows that F has no quadratic subextension, and in particular F is of odd degree.

Since $K_1 \cap F = \mathbb{Q}$ we get that

$$\mathrm{Gal}(FK_1/K_1) \cong \mathrm{Gal}(F/(F \cap K_1)) = \mathrm{Gal}(F/\mathbb{Q}),$$

by Galois theory, but we know that FK_1/K_1 is an abelian extension since it is a subextension of H_1/K_1. Therefore, we also have that $F/\mathbb{Q}$ is an abelian extension. Now, Galois theory implies that

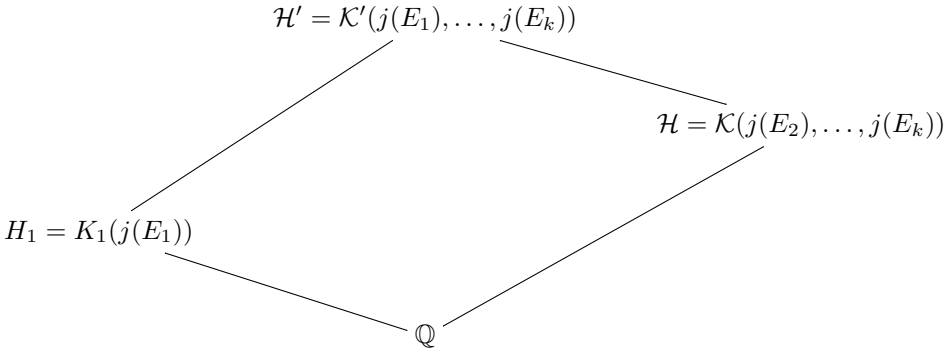
$$\mathrm{Gal}(FK_1/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q}),$$

which is clearly abelian. From Theorem 2.14 we know that FK_1/K_1 is contained in a ring class field if and only if $FK_1/\mathbb{Q}$ is generalized dihedral, but all nontrivial generalized dihedral groups are nonabelian. Thus it must be that FK_1/K_1 is a trivial extension and since $K_1 \not\subseteq F$ it follows that $F/\mathbb{Q}$ is trivial and $F = \mathbb{Q}$. □

Proposition 4.5. *Let $n \geq 1$, and suppose that E_i, for $i = 1, \dots, n$, is an elliptic curve with CM by an order $\mathcal{O}_i$ of an imaginary quadratic field K_i of odd class number, with $K_i \neq K_j$ for $i \neq j$, and such that $j(E_i) \notin \mathbb{Q}$. Further, assume that $\mathbb{Q}(j(E_1), \dots, j(E_n))/\mathbb{Q}$ is an extension of odd degree. Then:*

$$[\mathbb{Q}(j(E_1), \dots, j(E_n)) : \mathbb{Q}] = \prod_{i=1}^{n} [\mathbb{Q}(j(E_i)) : \mathbb{Q}].$$

Proof. We will prove the formula using induction on n. The statement is trivial for $n = 1$, so let us assume that it is true for $n = k - 1$, for some $k \geq 2$, and let E_i, for $i = 1, \dots, k$, be elliptic curves as in the statement of the theorem. Let $\mathcal{K}$ be the compositum of $K_2, \dots, K_k$, and let $\mathcal{K}' = K_1\mathcal{K}$ be the compositum of $K_1, \dots, K_k$. It follows from Lemma 4.1 that $[\mathcal{K}' : \mathbb{Q}] = 2^k$ and $[\mathcal{K} : \mathbb{Q}] = 2^{k-1}$. Consider the following diagram



and notice that every field in the diagram is Galois over $\mathbb{Q}$, because they are compositums of ring class fields. Since $\mathcal{H} = \mathcal{K}(j(E_2), \dots, j(E_k))$ is the compositum of all ring class fields $H_i = K_i(j(E_i))$ for $i = 2, \dots, k$, and since all the imaginary quadratic fields are distinct, it follows from Theorem 4.4 that H_1 and $\mathcal{H}$ are disjoint, and therefore

$$[\mathcal{K}'(j(E_1), \dots, j(E_k)) : \mathbb{Q}] = [K_1(j(E_1)) : \mathbb{Q}] \cdot [\mathcal{H} : \mathbb{Q}].$$

By the induction hypothesis, since $[\mathcal{K} : \mathbb{Q}] = 2^{k-1}$ and $\mathcal{K}/\mathbb{Q}$ is Galois, and $\mathbb{Q}(j(E_2), \dots, j(E_k))$ is of odd degree by assumption, it follows that

$$[\mathcal{H} : \mathbb{Q}] = 2^{k-1} \cdot [\mathbb{Q}(j(E_2), \dots, j(E_k)) : \mathbb{Q}] = 2^{k-1} \prod_{i=2}^{k} [\mathbb{Q}(j(E_i)) : \mathbb{Q}].$$

Hence, if we write $\mathcal{H}' = \mathcal{K}'(j(E_1), \ldots, j(E_k))$, we have

$$\begin{aligned} 2^k \cdot [\mathbb{Q}(j(E_1), \ldots, j(E_k)) : \mathbb{Q}] = [\mathcal{H}' : \mathbb{Q}] &= [\mathcal{K}'(j(E_1), \ldots, j(E_k)) : \mathbb{Q}] = [K_1(j(E_1)) : \mathbb{Q}] \cdot [\mathcal{H} : \mathbb{Q}] \\ &= (2 \cdot [\mathbb{Q}(j(E_1)) : \mathbb{Q}]) \cdot \left(2^{k-1} \prod_{i=2}^{k} [\mathbb{Q}(j(E_i)) : \mathbb{Q}] \right) \\ &= 2^k \cdot \prod_{i=1}^{k} [\mathbb{Q}(j(E_i)) : \mathbb{Q}], \end{aligned}$$

which shows $[\mathbb{Q}(j(E_1), \ldots, j(E_k)) : \mathbb{Q}] = \prod_{i=1}^{k} [\mathbb{Q}(j(E_i)) : \mathbb{Q}]$, as desired, as this completes the proof of the induction step, and thus the statement is true for all $n \geq 1$. □

Theorem 4.6. *Suppose that E_i, for $i = 1, 2, 3, \ldots, n$, is an elliptic curve with CM by an order $\mathcal{O}_i$ of an imaginary quadratic field K_i of odd class number. Further suppose that the extension $\mathbb{Q}(j(E_1), \ldots, j(E_n))/\mathbb{Q}$ is of odd degree, and $K_i \neq K_j$ if $i \neq j$. Then,*

1. *$\mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2), \ldots, j(E_n)) = \mathbb{Q}$, and*
2. *If E is an elliptic curve with CM by $\mathcal{O}$ an order of an imaginary quadratic field K such that $j(E) \in \mathbb{Q}(j(E_1), j(E_2), \ldots, j(E_n))$, then $K = K_i$ and $j(E) \in \mathbb{Q}(j(E_i))$, for some $i = 1, 2, 3, \ldots, n$.*

Proof. Let $\mathcal{K}$ be the compositum of K_2 through K_n. Consider $\mathbb{Q}(j(E_1)) \subseteq K(j(E_1)) = H_1$ and

$$\mathbb{Q}(j(E_2), \ldots, j(E_n)) \subseteq \mathcal{K}(j(E_2), \ldots, j(E_n)) = \mathcal{H}.$$

By Theorem 4.4, we have $H_1 \cap \mathcal{H} = \mathbb{Q}$, and therefore $\mathbb{Q}(j(E_1)) \cap \mathbb{Q}(j(E_2), \ldots, j(E_n)) = \mathbb{Q}$. This shows part (1).

Suppose that E is an elliptic curve with CM such that $j(E) \in \mathbb{Q}(j(E_1), \ldots, j(E_n))$. From Lemma 4.3 we know that E must have CM by an order of class number 1 (and thus $j(E) \in \mathbb{Q}$) or an order of K_i, for some $i = 1, \ldots, n$. Without loss of generality assume that E has CM by $\mathcal{O} \subset K_1$. Now, by Proposition 4.5 we have

$$[\mathbb{Q}(j(E_1), \ldots, j(E_n)) : \mathbb{Q}] = \prod_{i=1}^{n} [\mathbb{Q}(j(E_i)) : \mathbb{Q}].$$

Since E and E_1 have CM by orders of odd class number of the same imaginary quadratic field, and $\mathbb{Q}(j(E), j(E_1))$ is contained in an extension of odd degree by assumption, Theorem 3.5 implies that there is an elliptic curve E_l with CM by an order of K_1 such that $\mathbb{Q}(j(E), j(E_1)) = \mathbb{Q}(j(E_l))$. Thus,

$$\mathbb{Q}(j(E_1), j(E_2), \ldots, j(E_n)) = \mathbb{Q}(j(E), j(E_1), j(E_2), \ldots, j(E_n)) = \mathbb{Q}(j(E_l), j(E_2), \ldots, j(E_n))$$

and so, using Proposition 4.5 once again, we obtain

$$[\mathbb{Q}(j(E_1), \ldots, j(E_n)) : \mathbb{Q}] = [\mathbb{Q}(j(E_l), \ldots, j(E_n)) : \mathbb{Q}] = [\mathbb{Q}(j(E_l)) : \mathbb{Q}] \cdot \prod_{i=2}^{n} [\mathbb{Q}(j(E_i)) : \mathbb{Q}].$$

It follows that $[\mathbb{Q}(j(E_1)) : \mathbb{Q}] = [\mathbb{Q}(j(E_l)) : \mathbb{Q}]$, and since $\mathbb{Q}(j(E_1)) \subseteq \mathbb{Q}(j(E), j(E_1)) = \mathbb{Q}(j(E_l))$, we conclude that $\mathbb{Q}(j(E_1)) = \mathbb{Q}(j(E_l)) = \mathbb{Q}(j(E), j(E_1))$ and so $j(E) \in \mathbb{Q}(j(E_1))$ as desired. □

5. A Sharp Upper Bound

We are finally ready to find an upper bound on the number of elliptic curves with CM defined over a number L of odd degree over $\mathbb{Q}$. In order to simplify the situation further, we introduce the following notation.

Definition 5.1. *Given a number field $L/\mathbb{Q}$ and an imaginary quadratic field K, let $\Sigma(L, K)$ be the set j-invariants of elliptic curves defined over L with CM by an order of $\mathcal{O}_K$ that are not defined over $\mathbb{Q}$. We define the field of definition of $\Sigma(L, K)$ as $\mathbb{Q}(\Sigma(L, K)) = \mathbb{Q}(\{j : j \in \Sigma(L, K)\})$. Also, let $\Sigma(L)$ be the set of j-invariants of elliptic curves defined over L with CM that are not defined over $\mathbb{Q}$. The field of definition of $\Sigma(L)$ will be denoted by $\mathbb{Q}(\Sigma(L)) = \mathbb{Q}(\{j : j \in \Sigma(L)\})$.*

We begin by showing that $\Sigma(L, K)$ is a finite set.

Lemma 5.2. *If L is a number field of odd degree over $\mathbb{Q}$, then*

1. *$\Sigma(L, K)$ is a finite set, and*
2. *There exists an elliptic curve E with CM by an order $\mathcal{O}$ of $\mathcal{O}_K$ such that $\mathbb{Q}(\Sigma(L, K)) = \mathbb{Q}(j(E))$.*

Proof. If E is an elliptic curve with CM by K and $j(E) \in L$, then $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is a divisor of $N = [L : \mathbb{Q}]$. Since $L/\mathbb{Q}$ is assumed to have odd degree, it follows that $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is odd and $\leq N$. Hence, Corollary 2.9 implies that there are only finitely many possibilities for $j(E)$. Hence $\Sigma(L, K)$ is finite. This shows (1).

Now, part (2) follows by induction on the size of $\Sigma(L, K)$ by Theorem 3.5. □

It is worth pointing out that the previous finiteness result (Lemma 5.2, part (1)) is also true in even degree (see Remark 2.10).

Proposition 5.3. *Let $L/\mathbb{Q}$ be a number field of odd degree and let K be an imaginary quadratic field such that $\Sigma(L, K) \neq \emptyset$. Further, suppose that $d = [\mathbb{Q}(\Sigma(L, K)) : \mathbb{Q}] = p_1^{e_1} \cdots p_r^{e_r}$, and $h_K = p_1^{f_1} \cdots p_r^{f_r}$, for some distinct primes p_i, and some $e_i, f_i \geq 0$. Then,*

(1) *If $h_K = 1$, we have $\#\Sigma(L, K) \leq 2\sum_{i=1}^{r} e_i$, and*

(2) *If $h_K > 1$, then $\#\Sigma(L, K) \leq 2\left(1 + \sum_{i=1}^{r}(e_i - f_i)\right) \leq 2\sum_{i=1}^{r} e_i$.*

In all cases, $\#\Sigma(L, K) \leq 2\sum_{i=1}^{r} e_i$.

Proof. Notice first that the assumption that $L/\mathbb{Q}$ is an odd degree extension guarantees that d is also odd since $\mathbb{Q}(\Sigma(L, K))$ is a subfield of L. From Lemma 5.2, we know that there is an elliptic curve with CM by an order $\mathcal{O}$ of $\mathcal{O}_K$ such that $\mathbb{Q}(\Sigma(L, K)) = \mathbb{Q}(j(E))$. Suppose that the conductor of $\mathcal{O}$ is $\mathfrak{f}$. Therefore, $d = [\mathbb{Q}(\Sigma(L, K)) : \mathbb{Q}] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$ and so it must be that h_K divides d and so h_K must be odd. In particular, $0 \leq f_i \leq e_i$ for $i = 1, \ldots, r$. Also, Lemmas 2.6 and 2.7 show that $K \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$ because $\Sigma(L, K) = \emptyset$ in those cases. Combining all of this we get that $K = \mathbb{Q}(\sqrt{-q})$ and $\mathfrak{f} = 2^n q^m$, with $q \equiv 3 \bmod 4$, $n \in \{0, 1\}$, and $m \geq 0$. Further, we have that $d_K = -q$.

Assume that $h_K \neq 1$, so that at least one exponent $f_i > 0$ in the prime factorization of h_K. Applying Theorem 3.4, and noting that $J(K) = 0$ because we are assuming $h_K \neq 1$, we can see that

$$\begin{aligned}
\#\Sigma(L, K) &= \begin{cases} \sigma_0(\mathfrak{f}) & \text{if } n = 1, \text{ or } 2 \text{ does not split completely in } K, \\ \sigma_0(2\mathfrak{f}) & \text{otherwise (in particular } n = 0), \end{cases} \\
&= \begin{cases} \sigma_0(2q^m) & \text{if } n = 1, \text{ or } 2 \text{ does not split completely in } K, \\ \sigma_0(2 \cdot q^m) & \text{otherwise (in particular } n = 0), \end{cases} \\
&\leq 2(m + 1).
\end{aligned}$$

By Theorem 2.8 we have that

$$\begin{aligned}
p_1^{e_1} \cdots p_r^{e_r} = d = [\mathbb{Q}(\Sigma(L, K)) : \mathbb{Q}] = h(\mathcal{O}) &= \begin{cases} h_K \cdot \mathfrak{f} & \text{if } \mathfrak{f} \text{ is odd}, \\ h_K \cdot \frac{\mathfrak{f}}{2} & \text{if } \mathfrak{f} \text{ is even and } d_K \equiv 1 \bmod 8, \\ h_K \cdot \frac{3 \cdot \mathfrak{f}}{2} & \text{if } \mathfrak{f} \text{ is even and } d_K \equiv 5 \bmod 8. \end{cases} \\
&= \begin{cases} p_1^{f_1} \cdots p_r^{f_r} q^m & \text{if } \mathfrak{f} \text{ is odd, or } d_K \equiv 1 \bmod 8, \\ 3p_1^{f_1} \cdots p_r^{f_r} q^m & \text{otherwise.} \end{cases}
\end{aligned}$$

In particular, $\sum_{i=1}^{r} e_i \geq m + \sum_{i=1}^{r} f_i$, and therefore $m \leq \sum_{i=1}^{r}(e_i - f_i)$. It follows that

$$\#\Sigma(L, K) \leq 2(m + 1) \leq 2\left(1 + \sum_{i=1}^{r}(e_i - f_i)\right).$$

Since we are assuming $h_K > 1$, we know that at least one index $f_i > 0$. Thus,

$$\#\Sigma(L, K) \leq 2(m + 1) \leq 2\left(1 + \sum_{i=1}^{r}(e_i - f_i)\right) \leq 2\left(1 + \sum_{i=1}^{r} e_i - \sum_{i=1}^{r} f_i\right) \leq 2\left(1 + \sum_{i=1}^{r} e_i - 1\right) = 2\sum_{i=1}^{r} e_i.$$

This proves (2) in the case of $h_K > 1$. If $h_K = 1$, then we distinguish three cases according to whether $q = 3$, $q = 7$, or $q \in D = \{11, 19, 43, 67, 163\}$. For each of these 3 cases we also need to consider if $n = 0$ or 1. In all six

possible cases we calculate $d = h(\mathcal{O})$ and the corresponding sum of the exponents, as well as $\#\Sigma(L,K)$:

$$d = h(\mathcal{O}) = \begin{cases} q^{m-1} & \text{if } q=3, n=0, \\ q^m & \text{if } q=3, n=1, \\ q^m & \text{if } q=7, n=0, \\ q^m & \text{if } q=7, n=1, \\ q^m & \text{if } q\in D, n=0, \\ 3q^m & \text{if } q\in D, n=1, \end{cases}, \quad 2\sum_{i=1}^{r} e_i = \begin{cases} 2(m-1) & \text{if } q=3, n=0, \\ 2m & \text{if } q=3, n=1, \\ 2m & \text{if } q=7, n=0, \\ 2m & \text{if } q=7, n=1, \\ 2m & \text{if } q\in D, n=0, \\ 2(m+1) & \text{if } q\in D, n=1, \end{cases} = \begin{cases} 2m-2 & \text{if } q=3, n=0, \\ 2m & \text{if } q=3, n=1, \\ 2m & \text{if } q=7, n=0, \\ 2m & \text{if } q=7, n=1, \\ 2m & \text{if } q\in D, n=0, \\ 2m+2 & \text{if } q\in D, n=1, \end{cases}$$

$$\#\Sigma(L,K) = \begin{cases} \sigma_0(\mathfrak{f})-3 & \text{if } q=3, n=0, \\ \sigma_0(\mathfrak{f})-3 & \text{if } q=3, n=1, \\ \sigma_0(2\mathfrak{f})-2 & \text{if } q=7, n=0, \\ \sigma_0(\mathfrak{f})-2 & \text{if } q=7, n=1, \\ \sigma_0(\mathfrak{f})-1 & \text{if } q\in D, n=0, \\ \sigma_0(\mathfrak{f})-1 & \text{if } q\in D, n=1, \end{cases} = \begin{cases} (m+1)-3 & \text{if } q=3, n=0, \\ 2(m+1)-3 & \text{if } q=3, n=1, \\ 2(m+1)-2 & \text{if } q=7, n=0, \\ 2(m+1)-2 & \text{if } q=7, n=1, \\ (m+1)-1 & \text{if } q\in D, n=0, \\ 2(m+1)-1 & \text{if } q\in D, n=1, \end{cases} = \begin{cases} m-2 & \text{if } q=3, n=0, \\ 2m-1 & \text{if } q=3, n=1, \\ 2m & \text{if } q=7, n=0, \\ 2m & \text{if } q=7, n=1, \\ m & \text{if } q\in D, n=0, \\ 2m+1 & \text{if } q\in D, n=1. \end{cases}$$

Here it is worth noting that the condition $\Sigma(L,K)\neq\emptyset$ imposes some lower bounds on m, so that $\#\Sigma(L,K)>0$. In all of these cases, we have that $\#\Sigma(L,K) \leq 2\sum_{i=1}^{r} e_i$, as claimed (and there is equality in certain cases!). □

Example 5.4. Let $K=\mathbb{Q}(\sqrt{-7})$. Let E be an elliptic curve with complex multiplication by the order $\mathcal{O}$ of $\mathcal{O}_K$ of conductor $\mathfrak{f}=2\cdot 7^m$. In this case $h_k=1$ and $h(\mathcal{O})=7^m$, so if we define $L=\mathbb{Q}(j(E))$, then $[L:\mathbb{Q}]=7^m$. Since $\mathbb{Q}(\Sigma(L,K))\subseteq L$, and $\mathbb{Q}(j(E))\subseteq\mathbb{Q}(\Sigma(L,K))$, it follows that $L=\mathbb{Q}(\Sigma(L,K))$. Thus, Proposition 5.3 says that $\#\Sigma(L,K)\leq 2m$. While Theorem 3.4 part (3) says that $\#\Sigma(L,K)=\sigma_0(\mathfrak{f})-J(K)=\sigma_0(2\cdot 3^m)-2=2m$. Therefore, the upper bound established in Proposition 5.3 is sharp.

Example 5.5. Let $K=\mathbb{Q}(\sqrt{-23})$. Let E be an elliptic curve with complex multiplication by the order of $\mathcal{O}_K$ with conductor $\mathfrak{f}=2\cdot 23^m$. In this case, we have that $h_K=3$ and so if we define $L=\mathbb{Q}(j(E))$, then $[L:\mathbb{Q}]=3\cdot 23^m$. Since $\mathbb{Q}(\Sigma(L,K))\subseteq L$ by definition, and $\mathbb{Q}(j(E))\subseteq\mathbb{Q}(\Sigma(L,K))$, it follows that $L=\mathbb{Q}(\Sigma(L,K))$. Thus, Proposition 5.3, part (2), says that $\#\Sigma(L,K)\leq 2(1+(m+1)-1)=2(m+1)$. While Theorem 3.4 part (3) says that $\#\Sigma(L,K)=\sigma_0(\mathfrak{f})=\sigma_0(2\cdot 23^m)=2(m+1)$. Therefore, the upper bound established in Proposition 5.3 is again sharp.

Remark 5.6. Examples 5.4 and 5.5 show that the bound established in Proposition 5.3 is sharp when the class number of K is 1 or if the class number of K is greater than 1. In the proof of Proposition 5.3, however, one can see that when the class number of K is 1, then the bound can be sharp only for $K=\mathbb{Q}(\sqrt{-7})$.

Next, we will show that $\Sigma(L)$ is a union of sets of the form $\Sigma(L,K)$, for a finite number of quadratic fields K.

Lemma 5.7. *Given a number field $L/\mathbb{Q}$ of odd degree n, there exists a finite list of imaginary quadratic fields $K_1,\ldots,K_t$ of odd class number such that $\Sigma(L)=\bigcup_{i=1}^{t}\Sigma(L,K_i)$ with $\Sigma(L,K_i)\cap\Sigma(L,K_j)=\emptyset$ if $i\neq j$, and $\Sigma(L,K_i)\neq\emptyset$ for each $i=1,\ldots,t$.*

Proof. Let L be a number field of odd degree, and let $\widehat{L}$ be the Galois closure of L. Let $\mathcal{K}_L$ be the largest 2-elementary abelian extension contained in L, and let $K_1,\ldots,K_u$, for some $u\geq 1$, be all the imaginary quadratic fields of odd class number contained in $\mathcal{K}_L\subseteq\widehat{L}$.

Let K be an imaginary quadratic field such that there is an elliptic curve E with CM by an order $\mathcal{O}$ in K, and such that $j(E)\in L$ but not in $\mathbb{Q}$. Since $[L:\mathbb{Q}]$ is odd, and $\mathbb{Q}(j(E))\subseteq L$, it follows that $h(\mathcal{O})$ is odd, and therefore Lemma 3.1 implies that the Galois closure of $\mathbb{Q}(j(E))$ is $K(j(E))$. In particular, $K(j(E))\subseteq\widehat{L}$ and so $K\subseteq\widehat{L}$. Since the class number $h(\mathcal{O})$ is odd, and h_K divides $h(\mathcal{O})$, it follows that h_K is odd, and therefore K is one of $K_1,\ldots,K_u$. If we let $K_1,\ldots,K_t$, for some $t\leq u$, be the subset of fields such that $\Sigma(L,K_i)\neq\emptyset$ for $i=1,\ldots,t$, then we have shown that $\Sigma(L)\subseteq\bigcup_{i=1}^{t}\Sigma(L,K_i)$. Clearly $\Sigma(L,K_i)\subseteq\Sigma(L)\subseteq L$ for each i, and so we have an equality $\Sigma(L)=\bigcup_{i=1}^{t}\Sigma(L,K_i)$.

The disjointness $\Sigma(L,K_i)\cap\Sigma(L,K_j)=\emptyset$ if $i\neq j$ follows from the fact that an elliptic curve cannot have CM by orders of two different imaginary quadratic fields. □

Theorem 5.8. *Let $L/\mathbb{Q}$ be a number field of odd degree $n=p_1^{e_1}\cdots p_r^{e_r}$, and let $K_1,\dots,K_t$ be the list of those imaginary quadratic fields given by Lemma 5.7, such that $K_1,\dots,K_s$, for some $0\leq s\leq t$, are those with odd class number >1. Let h_i be the class number of K_i, and write $h_i=p_1^{f_{i,1}}\cdots p_r^{f_{i,r}}$, for $i=1,\dots,s$. Then,*

$$\#\Sigma(L)\leq 2s+2\sum_{j=1}^{r}\left(e_j-\sum_{i=1}^{s}f_{i,j}\right)\leq 2\sum_{j=1}^{r}e_j.$$

Moreover, if $t=s=0$, then $\Sigma(L)$ is empty.

Proof. From Lemma 5.7 we know that there is a finite list of imaginary quadratic fields of odd class number $K_1,K_2,\dots,K_t$ such that $\Sigma(L)=\bigcup_{i=1}^{t}\Sigma(L,K_i)$ with $\Sigma(L,K_i)\cap\Sigma(L,K_j)=\emptyset$ if $i\neq j$, and $\Sigma(L,K_i)\neq\emptyset$ for each $i=1,\dots,t$ (in particular, if $t=0$, then $\Sigma(L)=\emptyset$). Assume that $t\geq 1$, and let $K_1,\dots,K_s$, for some $0\leq s\leq t$, be the subset of those fields with odd class number >1. By Lemma 5.2, for each i there is an elliptic curve E_i with CM by an order in K_i such that $\mathbb{Q}(\Sigma(L,K_i))=\mathbb{Q}(j(E_i))$. Moreover, by Theorem 4.6, we have that for fixed i,

$$\mathbb{Q}(j(E_i))\cap\mathbb{Q}(\{j(E_k):1\leq k\leq t,\ k\neq i\})=\mathbb{Q},$$

and Proposition 4.5 shows that

$$[\mathbb{Q}(j(E_1),\dots,j(E_n)):\mathbb{Q}]=\prod_{i=1}^{t}[\mathbb{Q}(j(E_i)):\mathbb{Q}].$$

Hence,

$$\begin{aligned}[\mathbb{Q}(\Sigma(L)):\mathbb{Q}]&=\left[\mathbb{Q}\left(\bigcup_{i=1}^{t}\Sigma(L,K_i)\right):\mathbb{Q}\right]=\left[\prod_{i=1}^{t}\mathbb{Q}\left(\Sigma(L,K_i)\right):\mathbb{Q}\right]\\&=\left[\prod_{i=1}^{t}\mathbb{Q}\left(j(E_i)\right):\mathbb{Q}\right]=[\mathbb{Q}(j(E_1),\dots,j(E_t)):\mathbb{Q}]\\&=\prod_{i=1}^{t}[\mathbb{Q}(j(E_i)):\mathbb{Q}]=\prod_{i=1}^{t}[\mathbb{Q}(\Sigma(L,K_i)):\mathbb{Q}].\end{aligned}$$

Let us write $[\mathbb{Q}(\Sigma(L,K_i)):\mathbb{Q}]=n_i=p_1^{e_{i,1}}p_2^{e_{i,2}}\dots p_r^{e_{i,r}}$. Since $\mathbb{Q}(\Sigma(L))\subseteq L$, the previous equations show that $\prod_{i=1}^{t}n_i$ divides n. Hence, $e_j\geq\sum_{i=1}^{t}e_{i,j}$. Now it follows from Proposition 5.3 that

$$\begin{aligned}\#\Sigma(L)=\sum_{i=1}^{t}\#\Sigma(L,K_i)&\leq\sum_{i=1}^{s}\#\Sigma(L,K_i)+\sum_{i=s+1}^{t}\#\Sigma(L,K_i)\\&\leq\sum_{i=1}^{s}2\left(1+\sum_{j=1}^{r}(e_{i,j}-f_{i,j})\right)+\sum_{i=s+1}^{t}\left(2\sum_{j=1}^{r}e_{i,j}\right)\\&=2s+2\sum_{j=1}^{r}\left(\sum_{i=1}^{t}e_{i,j}-\sum_{i=1}^{s}f_{i,j}\right)\\&\leq 2s+2\sum_{j=1}^{r}\left(e_j-\sum_{i=1}^{s}f_{i,j}\right).\end{aligned}$$

Moreover, by Proposition 5.3 we also know

$$\#\Sigma(L)=\sum_{i=1}^{t}\#\Sigma(L,K_i)\leq\sum_{i=1}^{t}\left(2\sum_{j=1}^{r}e_{i,j}\right)=2\sum_{j=1}^{r}\sum_{i=1}^{t}e_{i,j}\leq 2\sum_{j=1}^{r}e_j,$$

as desired. □

Example 5.9. Let $K_1 = \mathbb{Q}(\sqrt{-7})$, $K_2 = \mathbb{Q}(\sqrt{-31})$, and $K_3 = \mathbb{Q}(\sqrt{-47})$. Let E_i, for $i = 1, 2, 3$, be an elliptic curve with complex multiplication by an order $\mathcal{O}_i$ of $\mathcal{O}_{K_i}$, respectively. Further, suppose that the conductor of the orders $\mathcal{O}_1$, $\mathcal{O}_2$, and $\mathcal{O}_3$ are $\mathfrak{f}_1 = 2 \cdot 7^{m_1}$, $\mathfrak{f}_2 = 2 \cdot 31^{m_2}$, and $\mathfrak{f}_3 = 2 \cdot 47^{m_3}$ with $m_1, m_2, m_3 \geq 1$ respectively. In this case, we have that $h(\mathcal{O}_1) = 7^{m_1}$, $h(\mathcal{O}_2) = 3 \cdot 31^{m_2}$, and $h(\mathcal{O}_3) = 5 \cdot 47^{m_3}$, by Theorem 2.8. Let $L = \mathbb{Q}(j(E_1), j(E_2), j(E_3))$. From the proof of Theorem 5.8, we know that

$$[L : \mathbb{Q}] = \prod_{i=1}^{3} [\mathbb{Q}(j(E_i)) : \mathbb{Q}] = 3 \cdot 5 \cdot 7^{m_1} \cdot 31^{m_2} \cdot 47^{m_3}.$$

Since $\mathbb{Q}(\Sigma(L)) \subseteq L$ and $L = \mathbb{Q}(j(E_1), j(E_2), j(E_3)) \subset \mathbb{Q}(\Sigma(L))$ by definition, we know that $L = \mathbb{Q}(\Sigma(L))$ and that $\Sigma(L) = \Sigma(L, K_1) \cup \Sigma(L, K_2) \cup \Sigma(L, K_3)$. Thus, from Theorem 3.4 part (3), we have that

$$\begin{aligned}
\#\Sigma(L) &= \#\Sigma(L, K_1) + \#\Sigma(L, K_2) + \#\Sigma(L, K_3) \\
&= (\sigma(2 \cdot 7^{m_1}) - J(K_1)) + \sigma_0(\mathfrak{f}_2) + \sigma_0(\mathfrak{f}_3) \\
&= (\sigma_0(2 \cdot 7^{m_1}) - 2) + \sigma_0(2 \cdot 31^{m_2}) + \sigma_0(2 \cdot 41^{m_3}) \\
&= (2(m_1 + 1) - 2) + 2(m_2 + 1) + 2(m_3 + 1) = 4 + 2m_1 + 2m_2 + 2m_3.
\end{aligned}$$

Next, Theorem 5.8 says that $\#\Sigma(L) \leq 2(1 + 1 + m_1 + m_2 + m_3) = 4 + 2m_1 + 2m_2 + 2m_3$. Therefore, the bound established in Theorem 5.8 is in fact sharp.

References

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[Cox12] David A. Cox. *Galois theory*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2012.

[CW77] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[Gol85] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[PR04] Robert Pollack and Karl Rubin. The main conjecture for CM elliptic curves at supersingular primes. *Ann. of Math. (2)*, 159(1):447–464, 2004.

[Rub99] Karl Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 167–234. Springer, Berlin, 1999.

[S+14] W. A. Stein et al. *Sage Mathematics Software (Version 6.2)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Wat04] Mark Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.*, 73(246):907–938 (electronic), 2004.

Department of Mathematics, Amherst College, Amherst, MA 01002
E-mail address: `hdaniels@amherst.edu`
URL: `www.amherst.edu/~hdaniels/`

Department of Mathematics, University of Connecticut, Storrs, CT 06269
E-mail address: `alvaro.lozano-robledo@uconn.edu`
URL: `www.alozano.clas.uconn.edu/`