TORSION POINTS AND GALOIS REPRESENTATIONS ON CM ELLIPTIC CURVES

ABBREY BOURDON AND PETE L. CLARK

Abstract. We prove three theorems on torsion points and Galois representations for complex multiplication (CM) elliptic curves over number fields. The first theorem is a sharp version of Serre’s Open Image Theorem in the CM case. The second theorem determines the degrees in which a CM elliptic curve has a rational point of order \( N \), provided the field of definition contains the CM field. The third theorem bounds the size of the torsion subgroup of an elliptic curve with CM by a nonmaximal order in terms of the torsion subgroup of an elliptic curve with CM by the maximal order. We give several applications.

Contents

1. Introduction 2
1.1. Related work 4
2. Preliminaries 4
2.1. Foundations 4
2.2. Torsion Kernels 6
2.3. On Weber Functions 8
3. The Isogeny Torsion Theorem 9
3.1. Proof of the Isogeny Torsion Theorem 9
4. The Uniform Open Image Theorem 10
4.1. The Projective Torsion Field 10
4.2. Proof of Theorem 1.1a) when \( F = K(j) \) 13
4.3. End of the Proof of Theorem 1.1a) 15
4.4. Proof of Theorem 1.1b) 15
4.5. Determination of the Weber Function Field 16
4.6. Curves with Surjective Mod \( N \) Galois Representations 17
5. Applications 18
5.1. A Theorem of Franz 18
5.2. SPY Divisibilities 18
5.3. Sharpness in the Isogeny Torsion Theorem 19
5.4. Minimal Cartan Orbits 21
5.5. Maximal Cartan Orbits 23
5.6. Torsion over \( K(j) \) 24
5.7. Isogenies over \( K(j) \) 27
6. The Torsion Degree Theorem 28
6.1. Statement and Preliminary Reduction 28
6.2. Generalities 29
6.3. The Case \( \ell \nmid f \) 31
6.4. The Case \( \ell \mid f \) 32
References 33
1. Introduction

Let $F$ be a field of characteristic 0, and let $E/F$ be an elliptic curve. We say $E$ has complex multiplication (CM) if the endomorphism algebra

$$\text{End}^0 E = \text{End}(E/F) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is strictly larger than $\mathbb{Q}$, in which case it is necessarily an imaginary quadratic field $K$ and $\mathcal{O} = \text{End}(E/F)$ is a $\mathbb{Z}$-order in $K$. This paper continues a program of study of torsion points and Galois representations on CM elliptic curves defined over number fields. Contributions have been made by Olson [Ol74], Silverberg [Si88], [Si92], Parish [Pa89], Aoki [Ao95], [Ao06], Ross [Ro94], Kwon [Kw99], Prasad-Yogananda [PY01], Breuer [Br10] and Lombardo [Lo15], and the present authors and our collaborators [CCRS13], [CCRS14], [BCS], [CP15], [BCP], [BP16].

Two long-term goals of this program are on the one hand to completely understand the adelic Galois representation on any CM elliptic curve defined over a number field and on the other hand to determine all degrees of CM points on modular curves associated to congruence subgroups of $\text{SL}_2(\mathbb{Z})$. These two problems are closely related. An archetypical example is the case of the First Main Theorem of Complex Multiplication (the full statement is reproduced as Theorem 2.9): if $K$ is an imaginary quadratic field $E/K(j(E))$ is an $\mathcal{O}_K$-CM elliptic curve, then for all $N \in \mathbb{Z}^+$ the field obtained by adjoining to $K(j(E))$ the Weber function of the $N$-torsion subgroup is $K^{(N)}$, the $N$-ray class field of $K$. For all $N \geq 3$, we have

$$[K^{(N)} : K(j(E))] = \#(\mathcal{O}_K/N\mathcal{O}_K)^\times \#\mathcal{O}_K^\times.$$

This implies that the mod $N$ Galois representation on an $\mathcal{O}_K$-CM elliptic curve $E/K(j(E))$ is as large as possible up to twisting, and we will show there is an $\mathcal{O}_K$-CM elliptic curve $E/K(j(E))$ such that the mod $N$ Galois representation surjects onto the mod $N$ Cartan subgroup $(\mathcal{O}/N\mathcal{O})^\times$ (see Theorem 4.9). This is a sharp version of Serre’s Open Image Theorem in the $\mathcal{O}_K$-CM case. The corresponding result on the modular curve side is: the field of moduli of an $\mathcal{O}_K$-CM point on $X(N)/K^{(N)}$ is $K^{(N)}$.

The above results restrict to the case of the maximal order $\mathcal{O}_K$, as does most of the classical theory. Here we work in the context of an arbitrary order $\mathcal{O}$, of conductor $\mathfrak{f}$, in an imaginary quadratic field $K$. Let $E/K(j(E))$ be an $\mathcal{O}$-CM elliptic curve. One of our main results (Theorem 4.8) determines the field obtained by adjoining to $K(j(E))$ the Weber function of $E[N]$: it is the compositum of the $N$-ray class field of $K$ and the $(N\mathfrak{f})$-ring class field of $K$. Moreover, as in the case of maximal orders, the image of Galois is as large as possible, up to twisting.

**Theorem 1.1. (Uniform Open Image Theorem)**

a) For all imaginary quadratic orders $\mathcal{O} \subset K$ and all $\mathcal{O}$-CM elliptic curves $E$ defined over a number field $F \supset K$, the index of the image of the adelic Galois representation on $E$ in the Cartan subgroup $\hat{\mathcal{C}} = (\mathcal{O} \otimes \hat{\mathbb{Z}})^\times$ divides $\#\mathcal{O}^\times[F : K(j(E))]$ and thus is at most $6[F : K(j(E))]$.

b) If $\mathcal{O} \subset K$ is an imaginary quadratic order of conductor $\mathfrak{f}$ and $N \geq 3$, there is a number field $F \supset K$ and an elliptic curve $E/F$ such that $[F : K(j(E))] = \#(\mathcal{O}/N\mathcal{O})^\times$ and $(\mathbb{Z}/N\mathbb{Z})^2 \rightarrow E(F)$.

If $F$ does not contain $K$, then it follows from Theorem 1.1 that the image of the adelic Galois representation has index dividing $[F : \mathbb{Q}(j(E))]/\#\mathcal{O}^\times$ in a subgroup of $\text{GL}_2(\hat{\mathbb{Z}})$ that contains the

\footnote{The adelic formalism incorporates arbitrary orders, but even so the explicit determination of the class field in the “First Main Theorem” has been given only for the maximal order.}
adelic Cartan $\mathcal{C}$ with index 2. This is close to being a complete description of the adelic Galois representation on any CM elliptic curve defined over a number field. It falls short in two aspects: first, for a fixed $N \geq 3$, to get a mod $N$ Galois representation with index $\#\mathcal{O}_L^\times$ in the mod $N$ Cartan, our construction takes $F$ to be a proper extension of the minimal possible ground field $K(j(E))$. Second, it shows that at any finite level $N$ the index of the mod $N$ representation in the Cartan can be any divisor of $\#\mathcal{O}_L^\times$ but does not address whether this can happen for the adelic Galois representation. These do not impact the second aspect of our program, which studies degrees of level $N$ – rather than adelic – structures of CM elliptic curves and fields of moduli of CM points on modular curves, and studies all pairs $(E, L_N)_{/F}$ for a level $N$ structure $L_N$ over a number field $F \supset K(j(E))$, not just pairs in which the underlying elliptic curve $E$ arises from base extension of an elliptic curve $E_{/F}$.

We propose to use Theorem 1.1 to completely determine degrees of CM points on modular curves. To carry this out requires some further work of a more algebraic nature: an analysis of orbits of the mod $N$ Cartan subgroup $(\mathcal{O}/\mathcal{N})^\times$ on level $N$ structures. To understand the relevance of this, let $E_{/K(j(E))}$ be an $O$-CM elliptic curve. It follows from Theorem 4.9 that the composite homomorphism

$$g_{K(j(E))}^{\rho_{EN}} : (\mathcal{O}/\mathcal{N})^\times \to (\mathcal{O}/\mathcal{N})^\times/q(\mathcal{O}^\times)$$

is surjective and model-independent, where $q : \mathcal{O} \to \mathcal{O}/\mathcal{N}$ is the natural map. If $P \in E[tors]$ is a point of order $N$, the field of moduli of the point $(E, P)$ on $X_1(N)$ depends only on the $\mathcal{O}^\times$ orbit $\mathcal{P}$ of $P$. Thus the degree of this field over $K(j(E))$ may be computed by determining the size of the orbit of $(\mathcal{O}/\mathcal{N})^\times/q(\mathcal{O}^\times)$ on $\mathcal{P}$.

We give an analysis of Cartan orbits on $\mathcal{O}/\mathcal{N}$ in $\S5$ and $\S6$. The algebra is much simpler when $\mathcal{O}$ is maximal, and in this case our analysis is complete. When $\mathcal{O}$ is nonmaximal we give substantial, but not full, information on the structure of the Cartan orbits, enough to yield the following result.

**Theorem 1.2.** Let $\mathcal{O}$ be an order in $K$ of conductor $f$, and let $N \in \mathbb{Z}^{\geq 2}$.

There is a positive integer $T(\mathcal{O}, N)$, explicitly computed in $\S6$, such that:

(i) If $F \supset K$ is a number field and $E_{/F}$ is an $O$-CM elliptic curve with an $F$-rational point of order $N$, then $T(\mathcal{O}, N) \mid |F : K(j(E))|$, and

(ii) there is a number field $F \supset K$ and an $O$-CM elliptic curve $E_{/F}$ such that $|F : K(j(E))| = T(\mathcal{O}, N)$ and $E(F)$ contains a point of order $N$.

Theorem 1.2 should be compared to Theorem 5.3, a refinement of bounds of Silverberg [Si88], [Si92] and Prasad-Yogananda [PY01]. Theorem 5.3 also gives a divisibility on $|F : K(j(E))|$ imposed by the existence of an $F$-rational point of order $N$: in the current notation, Theorem 5.3 asserts\(^2\)

$$\varphi(N) \mid T(\mathcal{O}, N).$$

This bound is “homogenous” in the sense that it is a single bound that holds in all cases. Theorem 1.2 gives the optimal divisibility in all cases.

We give two other applications of our Cartan orbit analysis: the determination of all possible torsion subgroups of a $K$-CM elliptic curve $E_{/K(j(E))}$ ($\S5.6$) and the set of $N \in \mathbb{Z}^+$ for which there is a $K(j(E))$-rational cyclic $N$-isogeny (Theorem 5.17).

Although we seek results which treat elliptic curves with CM by a nonmaximal order on an equal footing with the $\mathcal{O}_K$-CM case, in most cases (e.g. in Theorem 1.1) the proofs use “change of order”

\(^2\)Here we use the convention that for nonzero rational numbers $\alpha, \beta$, $\alpha \mid \beta$ means $\frac{\beta}{\alpha} \in \mathbb{Z}$.
functorialities. Let $F$ be a number field, let $E/F$ be an $O$-CM elliptic curve, and let $f$ be the conductor of $O$. Then there is a (well known) $F$-rational isogeny $\iota : E \to E'$ such that $\text{End} E' = \mathcal{O}_K$. The induced $g_F$-module map $E[N] \to E'[N]$ is an isomorphism iff $\gcd(f, N) = 1$; otherwise there is a nontrivial kernel. But nevertheless there are relations between the mod $N$ Galois representations on $E$ and $E'$. Here is the last main result of this paper:

**Theorem 1.3. (Isogeny Torsion Theorem)** Let $O$ be an order in an imaginary quadratic field $K$, $F \supset K$ be a number field, $E/F$ an $O$-CM elliptic curve, and $\iota : E \to E'$ the canonical isogeny, with $E'$ an $O_K$-CM elliptic curve. Then:

$$\#E(F)[\text{tors}] | \#E'(F)[\text{tors}].$$

We give examples where the exponent of $E'(F)[\text{tors}]$ is strictly smaller than that of $E(F)[\text{tors}]$, showing we cannot hope to view $E(F)[\text{tors}]$ as a subgroup of $E'(F)[\text{tors}]$, and we prove that $\frac{\#E'(F)[\text{tors}]}{\#E(F)[\text{tors}]}$ can be arbitrarily large (see Propositions 5.5 and 5.6). Moreover, the statement is false if we do not require $F \supset K$. Despite the fact that this relationship is not as strong as one might hope, Theorem 1.3 has applications to determining fields of moduli of partial level $N$ structures. We apply it in §5.1 to deduce an old result of Franz [Fr35], originally proven by very different means.

1.1. Related work.

Our proof of Theorem 1.1 builds crucially on work of J.L. Parish [Pa89]. Also the classification of torsion over $K(j(E))$ is one of the main results of [Pa89]. Parish’s work has minor flaws with regard to the imaginary quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ – leading in particular to some omitted groups in his classification of torsion over $K(j(E))$ – and at another key point is a bit laconic, so when we want to use results appearing in or motivated by [Pa89] we give complete proofs.

A paper of R. Ross [Ro94] contains a result related to Theorem 1.3: in the notation of Theorem 1.3, Ross’s assertion implies that the groups $E(F)[\text{tors}]$ and $E'(F)[\text{tors}]$ have the same exponent. This is false: Proposition 5.5 gives counterexamples. Nevertheless it was Ross’s work that led us to the statement of Theorem 1.3.

S. Kwon gave a classification of degrees of cyclic isogenies rational over $\mathbb{Q}(j(E))$ in the CM case [Kw99]. Our Theorem 5.17 is the analogue over $K(j(E))$.

D. Lombardo has recently shown that if $E/F$ is a CM elliptic curve defined over a number field $F$ containing the CM field $K$, then the index of the adelic Galois representation in the Cartan subgroup divides $\# \mathcal{O}_K^\times [F : K]$ [Lo15]. This is in general a weaker bound than that of Theorem 1.1; the two coincide when $j(E) \in \mathbb{Q}$. On the other hand, Lombardo establishes largeness of Galois results for all abelian varieties of CM type and then specializes to elliptic curves.

A. Lozano-Robledo has informed us that he has done work on the image of the adelic Galois representation in the CM case. His work is independent of ours and took place at roughly the same time. We have not yet seen his work nor he ours, and we have agreed not to claim priority in either direction.

2. Preliminaries

2.1. Foundations.

Let $K$ be an imaginary quadratic field and $\mathcal{O}$ a $\mathbb{Z}$-order in $K$. We put

$$f = [\mathcal{O}_K : \mathcal{O}],$$

**
the conductor of \( \mathcal{O} \). Then

\[ \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K, \quad \Delta(\mathcal{O}) = f^2\Delta_K. \]

Conversely, for fixed \( K \) and \( f \in \mathbb{Z}^+ \) there is a unique order \( \mathcal{O}(f) \) in \( K \) of conductor \( f \). Thus an imaginary quadratic order is determined by its discriminant \( \Delta \), a negative integer which is 0 or 1 modulo 4. In fact, for any negative integer \( \Delta \) which is 0 or 1 modulo 4, there is an imaginary quadratic order of discriminant \( \Delta \). Explicitly, if \( \tau_{\Delta} = \frac{\Delta + \sqrt{\Delta}}{2} \), then \( \mathbb{Z}[\tau_{\Delta}] \) has discriminant \( \Delta \).

For any \( \mathcal{O} \)-CM elliptic curve \( E \) we have \( K(j(E)) = K(f) \), the ring class field of \( K \) of conductor \( f \) ([Co89, Thm. 11.1]). We may thus determine \([K(j(E)) : K] \) via the following formula:

**Theorem 2.1.** For \( N \in \mathbb{Z}^+ \), let \( K(N) \) denote the \( N \)-ring class field of \( K \). Then \( K(1) = K^{(1)} \) is the Hilbert class field of \( K \), and for all \( N \geq 2 \) we have

\[ [K(N) : K^{(1)}] = \frac{2}{w_K} N \prod_{p|N} \left( 1 - \left( \frac{\Delta_K}{p} \right) \frac{1}{p} \right). \]

**Proof.** See e.g. [Co89, Cor. 7.24]. \( \square \)

For number field \( F \), a positive integer \( N \), and \( E/F \) an elliptic curve, we denote by \( \rho_N \) the homomorphism

\[ g_F \rightarrow \text{Aut} E[N] \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z}), \]

the \textbf{modulo} \( N \) Galois representation. If \( E/F \) has CM by the order \( \mathcal{O} \) in \( K \), then \( E[N] \cong \mathcal{O}/NO \) (see [Pa89, Lemma 1], generalized in Lemma 2.5 below), and provided \( F \supseteq K \) we have

\[ \rho_N : g_F \rightarrow \text{Aut}_\mathcal{O} E[N] \cong \text{GL}_1(\mathcal{O}/NO) = (\mathcal{O}/NO)^\times. \]

In other words, the image of the mod \( N \) Galois representation lands in the \textbf{mod \( N \) Cartan subgroup}

\[ C_N(\mathcal{O}) = (\mathcal{O}/NO)^\times. \]

**Lemma 2.2.** Let \( \mathcal{O} \) be an order of discriminant \( \Delta \), and let \( N = p_1^{e_1} \cdots p_r^{e_r} \in \mathbb{Z}^+ \).

1. We have \( C_N(\mathcal{O}) = \prod_{i=1}^r C_{p_i^{e_i}}(\mathcal{O}) \) (canonical isomorphism).
2. We have \( \#C_N(\mathcal{O}) = N^2 \prod_{p|N} \left( 1 - \left( \frac{\Delta}{p} \right) \frac{1}{p} \right) \left( 1 - \frac{1}{p} \right) \).

**Proof.** a) It suffices to tensor the Chinese Remainder Theorem isomorphism \( \mathbb{Z}/NZ = \prod_{i=1}^r \mathbb{Z}/p_i^{a_i} \mathbb{Z} \) with the \( \mathbb{Z} \)-module \( \mathcal{O} \) and pass to the unit groups.

b) By [CCRS13], for any prime number \( p \) we have

\[ \#C_p(\mathcal{O}) = p^2 \left( 1 - \left( \frac{\Delta}{p} \right) \frac{1}{p} \right) \left( 1 - \frac{1}{p} \right). \]

The natural map \( C_{p^n}(\mathcal{O}) \rightarrow C_p(\mathcal{O}) \) is surjective with kernel of size \( p^{2n-2} \) [CP15, p. 3]. Together with part a) this shows that if \( N = p_1^{a_1} \cdots p_r^{a_r} \) then

\[ \#C_N(\mathcal{O}) = \prod_{i=1}^r p_i^{2a_i-2} (p_i - 1) \left( p_i - \left( \frac{\Delta}{p_i} \right) \right) = N^2 \prod_{p|N} \left( 1 - \left( \frac{\Delta}{p} \right) \frac{1}{p} \right) \left( 1 - \frac{1}{p} \right). \] \( \square \)
Finally, we establish the following relationship between \([K(f) : K^{(1)}]\) and \(#C_N(O)\) which will be used in the proof of Theorem 1.1. Here, \(\varphi\) denotes Euler’s totient function and \(\varphi_K(I)\) the natural generalization for a nonzero ideal \(I\) of \(O_K\). That is,

\[
\varphi_K(I) = \#(O_K/I)^\times = |I| \prod_{p|I} \left(1 - \frac{1}{|p|}\right),
\]

where \(|I| = \#O_K/I\).

**Lemma 2.3.** Let \(K\) be an imaginary quadratic field with ring of integers \(O_K\), and let \(O\) be the order in \(K\) of conductor \(\mathfrak{f}\). Then for \(N \in \mathbb{Z}^+\) we have

\[
\frac{\varphi_K(N)}{[K(f) : K^{(1)}]} \varphi(N) = [O_K^\times : O^\times] \cdot #C_N(O).
\]

**Proof.** If \(\mathfrak{f} = 1\), then (1) reduces to \(\varphi_K(N) = #(O_K/NO_K)^\times\), which is true. Suppose \(\mathfrak{f} > 1\), so Theorem 2.1 can be applied. Then the left hand side of (1) is

\[
\frac{[O_K^\times : O^\times] N^2 \prod_{p|\mathfrak{f}} \left(1 - \frac{\Delta_K}{p}\right) \left(1 - \frac{1}{p}\right) \prod_{p|N} \left(1 - \frac{1}{p}\right)}{\prod_{p|\mathfrak{f}} \left(1 - \frac{\Delta_K}{p}\right) \prod_{p|\mathfrak{f}} \left(1 - \frac{1}{p}\right)}
\]

\[
=[O_K^\times : O^\times] N^2 \prod_{p|\mathfrak{f}} \left(1 - \frac{1}{p}\right) \prod_{p|N, p|\mathfrak{f}} \left(1 - \frac{\Delta_K}{p}\right) \frac{1}{p}
\]

\[
=[O_K^\times : O^\times] N^2 \prod_{p|\mathfrak{f}} \left(1 - \frac{\Delta_K}{p}\right) \frac{1}{p} = [O_K^\times : O^\times]\#C_N(O). \quad \square
\]

2.2. **Torsion Kernels.** Let \(E/C\) be an \(O\)-CM elliptic curve. For a nonzero ideal \(I\) of \(O\), we define the \(I\)-torsion kernel

\[
E[I] = \{P \in E \mid \forall \alpha \in I, \alpha P = 0\}.
\]

There is an invertible ideal \(\Lambda \subset O\) such that

\[
E \cong C/\Lambda.
\]

If we put

\[
(\Lambda : I) = \{x \in C \mid xI \subset \Lambda\} = \{x \in K \mid xI \subset \Lambda\}
\]

then we have (immediately) that

\[
E[I] = \{x \in C/\Lambda \mid xI \subset \Lambda\} = (\Lambda : I)/\Lambda.
\]

Let \(|I| = \#O/I\).

**Lemma 2.4.** Let \(I, J \subset O\) be nonzero ideals and \(E/C\) be an \(O\)-CM elliptic curve.

a) If \(I \subset J\), then \(E[J] \subset E[I]\).

b) We have \(E[I] \subset E[I^2]\). In particular

\[
\#E[I] \leq |I|^2.
\]

**Proof.** a) This is immediate from the definition. b) By Lagrange’s Theorem, every element of \(O/I\) is killed by \(|I|\), so \(|I| \subset |I|O \subset I\). Apply part a). \(\square\)

**Lemma 2.5.** If \(I\) is an invertible \(O\)-ideal, then

\[
E[I] = I^{-1}\Lambda/\Lambda \cong O/I.
\]

In particular \(#E[I] = |I| = \#O/I\).
Proof. Recall that $I$ is invertible if there is an $O$-submodule $I^{-1}$ of $K$ such that $II^{-1} = O$. If so, then for $x \in K$ we have

$$xI \subset \Lambda \iff xI^{-1} = xO \subset I^{-1}\Lambda \iff x \in I^{-1}\Lambda,$$

giving $E[I] = I^{-1}\Lambda/\Lambda$. Because $\Lambda$ is a locally free $O$-module, for all $p \in \text{Spec} O$ we have $\Lambda_p \cong O_p$ and thus $(I^{-1}\Lambda/\Lambda)_p \cong (I^{-1}/O)_p \cong (O/I)_p$. Thus $I^{-1}\Lambda/\Lambda$ is locally free of rank 1 as an $O/I$-module. But the ring $O/I$ is semilocal, hence has trivial Picard group: any locally free rank 1 $O/I$-module is isomorphic to $O/I$.

**Lemma 2.6.** Let $R$ be a Dedekind domain, and let $M$ be a cyclic torsion $R$-module, and let $N \subset M$ be an $R$-submodule. Then:

a) $N$ is also a cyclic $R$-module.

b) We have $N \cong R/\text{ann } N$.

*Proof.* Let $I = \text{ann } M$. Since $M$ is a finitely generated torsion module over a domain, we have $I \neq 0$ and $M \cong R/I$. Thus $N \cong I'/I$ for some ideal $I' \supset I$. The ring $R/I$ is principal Artinian [CA, Thm. 20.11], so the ideal $I'/I$ of $R/I$ is principal. Thus $N$ is a cyclic, torsion $R$-module, so $N \cong R/\text{ann } N$. $\square$

**Theorem 2.7.** Let $E/\mathbb{C}$ be an $O_K$-CM elliptic curve, and let $M \subset E(\mathbb{C})$ be a finite $O_K$-submodule. Then $M = E[\text{ann } M] \cong O/\text{ann } M$ and thus $\# M = |\text{ann } M|$.

*Proof.* That $M \subset E[\text{ann } M]$ is a tautology. Because $O = O_K$ every nonzero $O$-ideal is invertible, so by Lemma 2.5 we have $\# E[\text{ann } M] = |\text{ann } M|$. On the other hand, let $t = \# M$. Then $M \subset E[t] \cong O_K/O_K$, a finite cyclic $O_K$-module. By Lemma 2.6 we have $M \cong O_K/\text{ann } M$ so $\# M = |\text{ann } M|$. Thus $M = E[\text{ann } M]$, hence Lemma 2.5 gives $M \cong O/\text{ann } M$ and $\# M = |\text{ann } M|$. $\square$

**Remark 2.8.** Theorem 2.7 does not hold if $E$ has CM by a nonmaximal order. Let $O$ be a nonmaximal order in $K$. There is nonzero prime ideal $p$ of $O$ such that the local ring $O_p$ is not a DVR.

If $p \cap \mathbb{Z} = (\ell)$, then $O/p \cong \mathbb{Z}/\ell\mathbb{Z}$. Since every ideal of $O$ can be generated by two elements, we have $\dim O_p/p^2 = 2$. Thus $\# O/p^2 = \ell^2$ and $(\ell^2) \subset p^2$. It follows that in the quotient ring $O/\ell^2 O$ the maximal ideal $p + \ell^2 O$ is not principal. Let $E/\mathbb{C}$ be an $O$-CM elliptic curve, so $E[\ell^2] \cong O/\ell^2 O$. It follows that the $O$-submodule $M = pE[\ell^2]$ of $E[\ell^2]$ is not cyclic and thus not isomorphic to $O/\text{ann } M$.

Now we recall an important classical result.

**Theorem 2.9.** (First Main Theorem of Complex Multiplication) Let $E/\mathbb{C}$ be an $O_K$-CM elliptic curve, and let $I$ be a nonzero ideal of $O_K$. Let $\mathfrak{h} : E \to P^1$ be a Weber function. Then:

$$K^{(1)}(\mathfrak{h}(E[I])) = K^I.$$

*Proof.* See e.g. [Si94, Thm. II.5.6]. $\square$

By combining Theorems 2.7 and 2.9, we get the class-field theoretic containment corresponding to an arbitrary finite $O$-submodule of $E(\overline{K})$, for any $O_K$-CM elliptic curve $E$ defined over a number field $F \supset K$.

In particular, Theorem 2.9 implies that whenever $E$ is an $O_K$-CM elliptic curve, $K^{(1)}(\mathfrak{h}(E[N])) = K^{(N)}$. In the case of CM by an arbitrary order in $K$, we will show the Weber Function Field need not equal $K^{(N)}$ (see Theorem 4.8), but containment has previously been established:
Define "Theorem 2.12."

Let $E$ be a $K$-CM elliptic curve defined over a number field $F \supset K$. Then we have

$$F(h(E[N])) \supset K^{(N)}.$$ 

For convenience, we record here the formulas for $[K^I : K^{(1)}]$.

Lemma 2.11. Let $I$ be a nonzero ideal of $K$, and let $K^I$ be the $I$-ray class field. We put $U(K) = O_K$ and $U_I(K) = \{x \in U(K) \mid x - 1 \in I\}$.

a) We have

$$[K^I : K^{(1)}] = \frac{\varphi_K(I)}{|U(K) : U_I(K)|}.$$ 

b) If $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then

$$[K^I : K^{(1)}] = \left\{ \begin{array}{ll}
\varphi_K(I) & I \mid (1+i) \\
\varphi_K(I) & I \mid (1+1) \text{ and } I \nmid (2) \\
\varphi_K(I) & I \nmid (2).
\end{array} \right.$$ 

c) If $K = \mathbb{Q}(\sqrt{-1})$, then

$$[K^I : K^{(1)}] = \left\{ \begin{array}{ll}
1 & I = (1) \\
\frac{\varphi_K(I)}{2} & I \neq (1) \text{ and } I \mid (\zeta_3 - 1) \\
\frac{\varphi_K(I)}{3} & I = (2) \text{ and } I \nmid (\zeta_3 - 1) \\
\frac{\varphi_K(I)}{6} & \text{otherwise}
\end{array} \right.$$ 

d) If $K = \mathbb{Q}(\sqrt{-3})$, then

$$[K^I : K^{(1)}] = \left\{ \begin{array}{ll}
1 & I = (1) \\
\frac{\varphi_K(I)}{2} & I \neq (1) \text{ and } I \mid (\zeta_3 - 1) \\
\varphi_K(I) & I \nmid (2).
\end{array} \right.$$ 

Proof. Parts b)-d) can be deduced from a), which appears as [Co00, Cor. 3.2.4].

2.3. On Weber Functions.

Theorem 2.12. (Weber Function Principle) Let $N \in \mathbb{Z}^{\geq 3}$, $O$ the order of conductor $\frac{1}{2}$ in $K$, and $F = K(\xi)$. For an $O$-CM elliptic curve $E_{/F}$, fix an embedding $F \hookrightarrow \mathbb{C}$ such that $j(E) = j(\mathbb{C}/O)$.

Define

$$W(N, O) = K(\xi)(h(E[N])).$$ 

a) $W(N, O)$ is a subfield of $F(E[N])$ and $[F(E[N]) : W(N, O)] = \#O^\times$.

b) There is an elliptic curve $E_{/F}$ such that

$$[F(E[N]) : W(N, O)] = \#O^\times.$$ 

c) As we range over all elliptic curves $E_{/F}$ with $j(E) = j(\mathbb{C}/O)$, we have

$$\bigcap_{E} F(E[N]) = W(N, O).$$ 

Proof. a) Let $w = \#O^\times$. The field $F(E[N])/F$ is Galois with Galois group $\rho_N(g_F) \subset C_N(O)$. Because $N \geq 3$, the homomorphism $O^\times \to C_N(O)$ is injective. Since $h(P) = h(Q)$ for points $P, Q$ on $E$ if and only if there exists $\xi \in O^\times$ such that $\xi(P) = Q$ (e.g. [La87, Thm. 1.7]), it follows that

$$W(N, O) = F(E[N])^{\rho_N(g_F) \cap O^\times}.$$
Thus
\[ [F(E[N]) : W(N, \mathcal{O})] | w. \]

b), c) If \( E/F, E'/F \) with \( j(E) = j(E') \), then \( K(\{\mathfrak{b}(E[N])\}) = K(\{\mathfrak{b}(E'[N])\}) \) by the model independence of the Weber function. Thus \( W(N, \mathcal{O}) \subset \bigcap_E F(E[N]) \). To see that equality holds, let \( E/F \) have \( j(E) = j(\mathbb{C}/\mathcal{O}) \). Let \( \mathfrak{p} \) be a prime of \( \mathcal{O}_F \) which is unramified in \( F' = F(E[N]) \). By weak approximation, there is \( \pi \in \mathfrak{p} \setminus \mathfrak{p}^2 \). Put \( L = F(\pi^{\frac{1}{w}}) \), and let \( \chi : \mathfrak{g}_F \to \mu_w \) be a character with splitting field \( T \text{ker} \chi = L \). Then \( L/F \) is totally ramified over \( \mathfrak{p} \), so \( F' \) and \( L \) are linearly disjoint over \( F \). It follows that
\[
\rho_{N,E\chi}(\mathfrak{g}_F) = (\rho_{N,E\chi}, \otimes \chi)(\mathfrak{g}_F) = \chi(\mathfrak{g}_F) = \mu_w.
\]

Thus
\[
w = [F(E[N]) : F(E[N]) \cap F(E'[N])] | [F(E[N]) : W(N, \mathcal{O})] | w,
\]
so \( F(E[N]) \) has degree \( w \) over \( W(N, \mathcal{O}) = F(E[N]) \cap F(E'[N]) \).

\begin{remark}
In fact, the statement of Theorem 2.12 holds for \( N = 2 \) with \( \#\mathcal{O}^\times \) replaced by \( \#\mathcal{O}^\times \). See §4.5 and §4.6.
\end{remark}

3. The Isogeny Torsion Theorem

3.1. Proof of the Isogeny Torsion Theorem. Let \( \Delta_K \) be the discriminant of \( K \) and \( \Delta \) the discriminant of \( \mathcal{O} \), so
\[
\Delta = f^2\Delta_K,
\]
where \( f \) is the conductor of \( \mathcal{O} \). There is an \( F \)-rational isogeny \( \iota : E \to E' \) and a field embedding \( F \to \mathbb{C} \) such that after extending the base to \( \mathbb{C} \) we have \( E \cong_{\mathbb{C}} \mathcal{O}/\mathcal{O}_K, E' \cong_{\mathbb{C}} \mathcal{C}/\mathcal{O}_K, \) and after adjusting the source and target of \( \iota_{\mathbb{C}} \) by these isomorphisms it becomes the quotient map \( \mathcal{C}/\mathcal{O} \to \mathcal{C}/\mathcal{O}_K \). The kernel of \( \iota \) is cyclic of order \( f \). Let \( \tau_K = \frac{\Delta_K + \sqrt{\Delta_K}}{2} \) so \( \mathcal{O}_K = \mathbb{Z}[\tau_K] \) and \( \mathfrak{O} = \mathbb{Z}[f\tau_K] \).

Moreover, identifying \( E[\text{tors}] \) as a subgroup of \( \mathfrak{C}/\mathcal{O}[\text{tors}] \) as above, for any \( N \in \mathbb{Z}^+ \) we have that \( e_1 = \frac{1}{N} + \mathcal{O}, e_2 = \frac{f\tau_K}{N} + \mathfrak{O} \) is a \( \mathbb{Z}/N\mathbb{Z} \)-basis for \( E[N] \), and similarly \( e'_1 = \frac{1}{N} + \mathcal{O}_K, e'_2 = \frac{f\tau_K}{N} + \mathfrak{O}_K \) is a \( \mathbb{Z}/N\mathbb{Z} \)-basis for \( E'[N] \). With respect to this basis the image of the mod \( N \) Galois representation consists of matrices of the form
\[
\begin{bmatrix}
a & b f^2 \frac{\Delta_K - \Delta_K^2}{4} \\
b & a + bf \Delta_K
\end{bmatrix}
\]
\( a, b \in \mathbb{Z}/N\mathbb{Z} \).

For finite commutative groups \( T \) and \( T' \), we have \( \#T \mid \#T' \) if and only if \( \#T[\ell^\infty] \mid \#T'[\ell^\infty] \) for all prime numbers \( \ell \). So we fix \( \ell \) and show \( \#E(F)[\ell^\infty] \mid \#E'(F)[\ell^\infty] \). If \( \ell \nmid f \) then \( \iota \) induces an isomorphism \( E(F)[\ell^\infty] \to E'(F)[\ell^\infty] \), so we may assume that \( \text{ord}_f \nmid 1 \). By (e.g.) the Mordell-Weil Theorem there is \( 0 \leq m \leq n \) such that
\[
E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^m \mathbb{Z} \oplus \mathbb{Z}/\ell^n \mathbb{Z}.
\]

There is nothing to show unless \( n \geq 1 \), so we assume so. Put \( N = \ell^n, \) so \( E(F)[\ell^\infty] \subset E[N], \) and let \( \{e_1, e_2\} \) be the basis for \( E[\ell^n] \) and \( \{e'_1, e'_2\} \) be the basis for \( E'[\ell^m] \) as above. Put \( k = \min(\text{ord}_f, n) \).

By assumption, there exists a point \( P \in E(F) \) of order \( \ell^n \). Then \( P' = \iota(P) \) has order \( \ell^d \) for some \( n - k \leq d \leq n \). If \( d = n \), then \( E'(F)[\ell^m] \) has exponent \( \ell^n \) and full \( \ell^m \)-torsion since \( \iota(\ell^{n-m}e_1) = \ell^{n-m}e'_1 \in E'(F) \) generates \( E'[\ell^m] \) as an \( \mathcal{O}_K \)-module. Thus \( E'(F)[\ell^m] \) has size at least
\(\ell^{m+n}\) and we are done. So we may assume \(d < n\). There are \(\alpha, \beta \in \mathbb{Z}/\ell^n\mathbb{Z}\) such that \(P = \alpha e_1 + \beta e_2\), so we have
\[0 = \ell^d \iota(P) = \iota(\ell^d P) = \iota(\ell^d \alpha e_1) + \iota(\ell^d \beta e_2) = \ell^d \alpha e_1 + \ell^d \beta e_2 = \ell^d \alpha e_1'\]
since \(\ell^k \mid f\). This implies \(\ell^{n-d} \mid \alpha\), so we may write \(\alpha = \ell^{n-d} \alpha'\). In addition, we conclude \(\ell \nmid \beta\) since \(\ell^d P = \ell^d \beta e_2\) has order \(\ell^{n-d}\).

Put \(\delta = \min(m+n-d, n)\). Since \(\delta \leq m+n-d \leq m+k\) and \(E\) has full \(\ell^m\)-torsion, the mod \(\ell^\delta\) Galois representation takes a restricted form:
\[
\rho_{\ell^\delta}(\mathbb{g}_F) \subset \left\{ \begin{bmatrix} 1 + \ell^m A & 0 \\ \ell^m B & 1 + \ell^m A \end{bmatrix} \mid A, B \in \mathbb{Z}/\ell^\delta\mathbb{Z} \right\}.
\]

Since \(\ell^{n-\delta} P = \alpha \ell^{n-\delta} e_1 + \beta \ell^{n-\delta} e_2\) is rational, all such matrices in the image of Galois satisfy
\[
\begin{bmatrix} 1 + \ell^m A & 0 \\ \ell^m B & 1 + \ell^m A \end{bmatrix} \begin{bmatrix} \ell^{n-\delta} \alpha' \\ \beta \end{bmatrix} = \begin{bmatrix} \ell^{n-\delta} \alpha' \\ \beta \end{bmatrix},
\]
which gives the condition
\[
\ell^{n+m-d} B \alpha' + \beta \ell^m A \equiv 0 \pmod{\ell^\delta}.
\]
But \(\delta \leq n+m-d\) and \(\ell \nmid \beta\), so this implies \(\ell^{\delta-m} \mid A\). Thus the image of the mod \(\ell^\delta\) Galois representation consists of matrices of the form
\[
\begin{bmatrix} 1 & 0 \\ \ell^m B & 1 \end{bmatrix}.
\]

It follows that \(\iota(\ell^{n-\delta} e_1) \in E'[\text{tors}]\) is \(F\)-rational. Indeed, for all \(\sigma \in \mathbb{g}_F\) we have
\[
\sigma(\iota(\ell^{n-\delta} e_1)) = \iota(\sigma(\ell^{n-\delta} e_1)) = \iota(\ell^{n-\delta} e_1 + \ell^m B \ell^{n-\delta} e_2) = \iota(\ell^{n-\delta} e_1 + \ell^{m+n-\delta} B' e_2) = \iota(\ell^{n-\delta} e_1),
\]
since \(\ell^k \mid f\) and \(m+n+k-\delta > n\). So \(\iota(\ell^{n-\delta} e_1) = \ell^{n-\delta} e_1'\) is an \(F\)-rational point of \(E'\) of order \(\ell^\delta\) which generates \(E'[\ell^\delta]\) as an \(O_K\)-module. If \(\delta = n\), then
\[
\#E'(F)[\ell^\infty] = \ell^{m+n} \leq \ell^{2n} = \#E'(F)[\ell^n] \leq \#E'(F)[\ell^\infty].
\]
Otherwise, \(\delta = m+n-d\) and \(E'\) has full \(\ell^\delta\)-torsion and a point of order \(\ell^d\). Thus \(E'(F)[\ell^n]\) has size at least \(\ell^{\delta+m+d} = \ell^{m+n}\).

4. The Uniform Open Image Theorem.

4.1. The Projective Torsion Field.

Let \(F\) be a field. For a positive integer \(N\) not divisible by the characteristic of \(F\) and \(E/F\) an elliptic curve, we define the \textbf{projective modulo N Galois representation} as the composite map
\[
\mathbb{P} \rho_N : \mathbb{g}_F \xrightarrow{\rho_N} \text{Aut} E[N] \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \rightarrow \text{PGL}_2(\mathbb{Z}/N\mathbb{Z}).
\]

The \textbf{projective torsion field} is
\[
F(\mathbb{P} E[N]) = \overline{F} \ker \rho_N.
\]
Thus $F(\mathbb{P}E[N])$ is the unique minimal field extension of $F$ on which the image of $\rho_N$ consists of scalar matrices. It follows that $F(E[N])/F(\mathbb{P}E[N])$ is a Galois extension with automorphism group a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Observe that the projective Galois representation and thus the projective torsion field are unchanged by quadratic twists. If $E$ has CM by an order of discriminant $\Delta = \overline{f}^2 \Delta_K \neq -3, -4$, then the projective $N$-torsion field is a well-defined abelian extension of $K(f)$. An important result of J.L. Parish identifies this projective torsion field with a suitable ring class field. When $\Delta = -4$ (resp. $\Delta = -3$) we have quartic twists (resp. sextic twists) which can change the projective Galois representation and the projective torsion field.

**Theorem 4.1.** Let $\mathcal{O}$ be an order of discriminant $\Delta = \overline{f}^2 \Delta_K$. Let $E$ be an $\mathcal{O}$-CM elliptic curve defined over $F = K(f)$. Let $N \geq 2$.

a) We have $F(\mathbb{P}E[N]) \supset K(N\overline{f})$. Thus we may put

$$d(E, N) = [F(\mathbb{P}E[N]) : K(N\overline{f})].$$

b) If $\Delta \notin \{-3, -4\}$, then $d(E, N) = 1$, i.e., $F(\mathbb{P}E[N]) = K(N\overline{f})$.

c) If $\Delta = -4$, then $d(E, N) | 2$.

d) If $\Delta = -3$, then $d(E, N) | 3$.

e) There is an $\mathcal{O}$-CM elliptic curve $E_{/F}$ for which $d(E, N) = 1$.

**Proof.** For $N \in \mathbb{Z}^+$, let $\mathcal{O}(N)$ be the order of conductor $N$ in $K$. Thus $\mathcal{O} = \mathcal{O}(1)$.

Step 1: We show that $F(\mathbb{P}E[N]) \supset K(N\overline{f})$ in all cases.

There is a field embedding $F \hookrightarrow \mathbb{C}$ such that $E_{/\mathbb{C}} \cong \mathbb{C}/\mathcal{O}$. The $\mathbb{C}$-linear map $z \mapsto Nz$ carries $\mathcal{O}(1)$ into $\mathcal{O}(N\overline{f})$ and induces a cyclic $N$-isogeny $\mathbb{C}/\mathcal{O}(1) \to \mathbb{C}/\mathcal{O}(N\overline{f})$. Let $C$ be the kernel of this isogeny, viewed as a finite étale subgroup scheme of $E_{/\mathbb{C}}$. Then $C$ has a (unique) minimal field of definition $F(C) \subset F(E[N])$, hence of finite degree over $F$. The field $F(\mathbb{P}E[N])$ is precisely the compositum of the minimal fields of definition of all order $N$ cyclic subgroup schemes $C \subset E_{/\mathbb{C}}$, so $F(C) \subset F(\mathbb{P}E[N])$. Since $C$ is $F(\mathbb{P}E[N])$-rational, the elliptic curve $E/C$ has a model over this field, and thus

$$F(\mathbb{P}E[N]) \supset K(j(E/C)) = K(N\overline{f}).$$

Step 2: In view of Step 1, we have $F(\mathbb{P}E[N]) \supset K(N\overline{f}) \supset K(f) = K(j(E))$, so we have $F(\mathbb{P}E[N]) = K(N\overline{f})$ iff $[F(\mathbb{P}E[N]) : K(f)] \leq [K(N\overline{f}) : K(f)]$. We have

$$[F(\mathbb{P}E[N]) : K(f)] = \# F(\mathbb{P}N(\mathfrak{f} \mathcal{O})) \leq \#(\mathcal{O}/N\mathcal{O})^\times/(\mathbb{Z}/N\mathbb{Z})^\times = N \prod_{p \mid N} \left(1 - \left(\frac{\Delta}{p}\right) \frac{1}{p}\right).$$

- Suppose $\mathfrak{f} > 1$. Using Theorem 2.1 to compute $[K(N\overline{f}) : K^{(1)}]$ and $[K(f) : K^{(1)}]$ gives

$$[K(N\overline{f}) : K(f)] = \frac{[K(N\overline{f}) : K^{(1)}]}{[K(f) : K^{(1)}]} = N \prod_{p \nmid N} \left(1 - \left(\frac{\Delta}{p}\right) \frac{1}{p}\right) = N \prod_{p \nmid N} \left(1 - \left(\frac{\Delta}{p}\right) \frac{1}{p}\right);$$

because $1 - \left(\frac{\Delta}{p}\right) \frac{1}{p} = 1$ for all $p \mid \mathfrak{f}$. Thus $d(E, N) = 1$ in this case.

- Suppose $\mathfrak{f} = 1$, so $\Delta = \Delta_K$. Then

$$[K(N\overline{f}) : K(f)] = [K(N) : K^{(1)}] = \frac{2^{w_K}}{N} \prod_{p \mid N} \left(1 - \left(\frac{\Delta}{p}\right) \frac{1}{p}\right).$$
If $\Delta \not\in \{ -3, -4 \}$ then $\frac{2}{w_K} = 1$, and again we get $d(E, N) = 1$. If $\Delta = -4$ then $\frac{2}{w_K} = \frac{1}{2}$, so the calculation shows $d(E, N) \in \{ 1, 2 \}$, and if $\Delta = -3$ then $\frac{2}{w_K} = \frac{1}{3}$, so the calculation shows $d(E, N) \in \{ 1, 3 \}$.

**Remark 4.2.** The following result is an analogue of [BCS, Thm. 5.6] for higher twists.

**Proposition 4.3.** *(Higher Twisting at the Bottom)*

For $M \in \mathbb{Z}^+$, we denote the mod $M$ cyclotomic character by $\chi_M$.

a) Let $K = \mathbb{Q}(\sqrt{-1})$ and let $\ell \equiv 5 \pmod{8}$ be a prime number. There is a character $\Psi : \mathfrak{g}_K \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ of order $\frac{\ell - 1}{4}$ and an $\mathcal{O}_K$-CM elliptic curve $E_{1/K}$ such that the mod $\ell$ Galois representation is

$$
\sigma \mapsto \rho_\ell(\sigma) = \begin{bmatrix}
\Psi(\sigma) & 0 \\
0 & \Psi^{-1}(\sigma)\chi_\ell(\sigma)
\end{bmatrix}.
$$

b) Let $K = \mathbb{Q}(\sqrt{-3})$ and let $\ell \equiv 7, 31 \pmod{36}$ be a prime number. There is a character $\Psi : \mathfrak{g}_K \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ of order $\frac{\ell - 1}{6}$ and an $\mathcal{O}_K$-CM elliptic curve $E_{1/K}$ such that the mod $\ell$ Galois representation is

$$
\sigma \mapsto \rho_\ell(\sigma) = \begin{bmatrix}
\Psi(\sigma) & 0 \\
0 & \Psi^{-1}(\sigma)\chi_\ell(\sigma)
\end{bmatrix}.
$$

**Proof.** a) Because $\ell \equiv 1 \pmod{4}$, the Cartan subgroup $C_\ell(\mathfrak{O})$ is split, and for an $\mathcal{O}_K$-CM elliptic curve $(E_1)_{/K}$, the mod $\ell$ Galois representation has the form

$$
\sigma \mapsto \rho_\ell(\sigma) = \begin{bmatrix} 
\Psi_1(\sigma) & 0 \\
0 & \Psi_1^{-1}(\sigma)\chi_\ell(\sigma)
\end{bmatrix}
$$

for a character $\Psi_1 : \mathfrak{g}_K \to (\mathbb{Z}/\ell\mathbb{Z})^\times$. Under this isomorphism, the matrix representation of $i \in \mathcal{O}_K$ is a diagonal matrix $\begin{bmatrix} z & 0 \\
0 & z^{-1} \end{bmatrix}$, where $z$ is a primitive 4th root of unity in $\mathbb{Z}/\ell\mathbb{Z}$. A general $\mathcal{O}_K$-CM elliptic curve over $K$ is of the form $E_1^\psi$ for a character $\psi : \mathfrak{g}_K \to \mu_4 \subset (\mathbb{Z}/\ell\mathbb{Z})^\times$. Let $Q_4(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^\times / (\mathbb{Z}/\ell\mathbb{Z})^{\times 4}$. Then the image of $z$ in $Q_4(\ell)$ has order 4: if not, there is $w \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ such that $z = w^{\frac{1}{4}}$, and then $w$ has order 8 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, contradicting the assumption that $\ell \equiv 5 \pmod{8}$. Thus the natural map $\mu_4 \to Q_4(\ell)$ given by $i \mapsto z$ (mod $(\mathbb{Z}/\ell\mathbb{Z})^{\times 4}$) is an isomorphism; we denote the inverse isomorphism $Q_4(\ell) \to \mu_4$ by $i$. Now take

$$
\psi : \mathfrak{g}_K \xrightarrow{\psi^{-1}} (\mathbb{Z}/\ell\mathbb{Z})^\times \xrightarrow{\otimes} Q_4(\ell) \xrightarrow{i} \mu_4.
$$

Let $\Psi_2 = \psi \Psi_1$. Then the twist $E_1^\psi$ has mod $\ell$ Galois representation

$$
\sigma \mapsto \rho_\ell(\sigma) = \begin{bmatrix}
\Psi_2(\sigma) & 0 \\
0 & \Psi_2^{-1}(\sigma)\chi_\ell(\sigma)
\end{bmatrix}.
$$

The composite $\Psi_2 : \mathfrak{g}_K \to (\mathbb{Z}/\ell\mathbb{Z})^\times \to Q_4(\ell)$ is trivial, so $\Psi_2(\mathfrak{g}_K)$ has order $c \mid \frac{\ell - 1}{4}$. Thus

$$
\#\rho_{\ell, E_1^\psi}(\mathfrak{g}_K) \mid c(\ell - 1) \mid \frac{(\ell - 1)^2}{4} = [K^{(\ell)} : K^{(1)}] = [K^{(\ell)} : K].
$$

Because $K(E_1^\psi[\ell]) \supset K^{(\ell)}$, we have $\#\rho_{\ell, E_1^\psi}(\mathfrak{g}_K) \leq \frac{(\ell - 1)^2}{4}$ and $c = \frac{\ell - 1}{2}$.

b) Since $\ell \equiv 1 \pmod{3}$, we have a primitive 6th root of unity $z$ in $\mathbb{Z}/\ell\mathbb{Z}$. Since $\ell \equiv 7, 31 \pmod{36}$, we have 4, 9 $\mid \ell - 1$, so $z$ has order 6 in $Q_6(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^\times / (\mathbb{Z}/\ell\mathbb{Z})^{\times 6}$. Also $\frac{(\ell - 1)^2}{6} = [K^{(\ell)} : K^{(1)}]$. The argument of part a) carries over. \[ \square \]
Example 4.4. a) Let $K = \mathbb{Q}(\sqrt{-1})$, and let $\ell \equiv 5 \pmod{8}$. Let $E_{/K}$ be an $O_K$-CM elliptic curve with mod $\ell$ Galois representation as in Proposition 4.3a). Then since $\chi_{\ell}(g_K) = (\mathbb{Z}/\ell \mathbb{Z})^\times$, $[K(\mathbb{F}_\ell(f)) : K] = \ell - 1$, whereas $[K(\ell) : K] = \frac{\ell+1}{2}$. So $d(E, \ell) = 2$.

b) Let $K = \mathbb{Q}(\sqrt{-3})$, and let $\ell \equiv 7, 31 \pmod{36}$. Let $E_{/K}$ be an $O$-CM elliptic curve with mod $\ell$ Galois representation as in Proposition 4.3b). As in part a), we have $[K(\mathbb{F}_\ell(f)) : K] = \ell - 1$ and $[K(\ell) : K] = \frac{\ell+1}{3}$. So $d(E, \ell) = 3$.

Remark 4.5. Parts a) and b) of Theorem 4.1 are due to J.L. Parish [Pa89, Prop. 3]. However, Parish’s treatment is rather laconic: he alludes to a calculation of the above sort rather than explicitly carrying it out. Theorem 4.1 plays an important role in the proof of Theorem 1.1, so the reader deserves a complete proof.

In his statement of [Pa89, Prop. 3], Parish assumes that $K \not= \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. In an “addendum” [Pa89, p. 263], he claims:

- If $\Delta = -4$ then $F(\mathbb{F}[N]) = K(N)$ for all $N \geq 3,$ and
- If $\Delta = -3$ then $F(\mathbb{F}[N]) = K(N)$ for all $N \geq 4$.

As Example 4.4 shows, both claims are false.

Proposition 4.6. Let $O$ be an order of discriminant $\Delta = n^2 \Delta_K$, and let $N \in \mathbb{Z}^+$. Then there is an $O$-CM elliptic curve $E_{/K(N)}$ such that the mod $N$ Galois representation consists of scalar matrices.

Proof. When $\Delta \not\in \{-3, -4\}$, this is immediate from Theorem 4.1b): in that case, the elliptic curve has a model defined over $K(f)$. Thus we may assume that $\Delta \in \{-3, -4\}$, so $f = 1$. Let $\zeta \in O_K^\times$ be a primitive $w_K$th root of unity. Let $\hat{E}_{/K(N)}$ be an $O(N)$-CM elliptic curve, let $\nu : \hat{E} \to E$ be the canonical $K(N)$-rational isogeny to an $O_K$-CM elliptic curve $E$, let $\nu^\vee : E \to \hat{E}$ be the dual isogeny, and let $C$ be the kernel of $\nu^\vee$. Identifying $E[N]$ with $N^{-1}O_K/O_K \subset \mathbb{C}/O_K$, $\nu^\vee : \mathbb{C}/O_K \to \mathbb{C}/O$ is the map $z + O_K \mapsto Nz + O$, so $C$ is the $\mathbb{Z}$-submodule of $C/O_K$ generated by $P_1 = \frac{1}{N} + O_K$.

Because $C$ is stable under the action of $g_K(N)$, this action is given by an isogeny character, say

$$\sigma(P_1) = \Psi(\sigma)P_1.$$ 

Let $P_2 = \zeta P_1$. Then $\{P_1, P_2\}$ is a $\mathbb{Z}/N\mathbb{Z}$-basis for $E[N]$. Moreover, for $\sigma \in g_K(N)$,

$$\sigma P_2 = \sigma \zeta P_1 = \zeta P_1 = \zeta (\Psi(\sigma)P_1) = \Psi(\sigma)P_1 = \Psi(\sigma)P_2.$$ 

It follows that $\sigma \in g_K(N)$ acts on $E[N]$ via the scalar matrix $\Psi(\sigma)$. \qed

4.2. Proof of Theorem 1.1a) when $F = K(f)$.

In this section we prove Theorem 1.1 a) in the case $F = K(f)$. The general case $F \supset K(f)$ is treated in the next section.

Step 1: Let $O$ be an order in $K$ of conductor $f$, let $F = K(f)$ and let $E_{/F}$ be an $O$-CM elliptic curve. Let $N \in \mathbb{Z}^+$. Identifying $\rho_N(g_F)$ with a subgroup of $C_N(O)$, put

$$\mathcal{I}_N = \mathcal{I}_N(E_{/K(f)}) = [C_N(O) : \rho_N(g_F)].$$

Our task is to show that as we vary over all imaginary quadratic fields $K$, all $f \in \mathbb{Z}^+$, and all elliptic curves $E$ defined over $F = K(f)$ with $\text{End} E \cong O(f)$ in $K$ and all $N \in \mathbb{Z}^+$, we have $\mathcal{I}_N | \#O^\times$, or equivalently, 

$$\frac{\#C_N(O)}{\#O^\times} \mid [F(E[N]) : F].$$
Because the \( \rho_N \) form an inverse system, we have \( N | N' \implies \mathcal{I}_N | \mathcal{I}_N' \). So we may assume \( 3 | N \) (for reasons that will become clear later) and thus

\[
[K^{(N)} : K^{(1)}] = \frac{\varphi_K(N)}{w_K}.
\]

Put \( L = K(Nf) \). By Theorems 2.10 and 4.1 we have

\[
F(E[N]) \supset K^{(N)}L,
\]

so it is enough to show that

\[
(4) \quad \frac{\#C_N(O)}{\#O^\times} | [K^{(N)}L : K(f)].
\]

Although (4) is purely class-field theoretic, we will show it using CM elliptic curves!

Step 2: Suppose first that \( f = 1 \), so \( O = O_K \). Then since \( 3 | N \) we have

\[
[K^{(N)}L : K(f)] = [K^{(N)} : K^{(1)}] = \frac{\varphi_K(N)}{w_K}.
\]

and we are done. Now suppose that \( f > 1 \). Then

\[
(5) \quad [K^{(N)}L : K(f)] = \frac{[K^{(Nf)} : K^{(1)}]}{[K(f) : K^{(1)}][K^{(N)} : K^{(Nf)}L]}.
\]

Combining equation (5) with Lemmas 2.11 and 2.3 we get

\[
[K^{(N)}L : K(f)] = \frac{\varphi_K(Nf)/w_K}{[K(f) : K^{(1)}][K^{(N)} : K^{(Nf)}L]}.
\]

It now suffices to show that

\[
[K^{(Nf)} : K^{(N)}L] | \frac{\varphi(Nf)}{\varphi(N)}.
\]

Step 3: By Proposition 4.6 there is an \( O_K \)-CM elliptic curve \( (E_0)/L \) for which the mod \( Nf \) Galois representation has scalar image. Since \( 3 | Nf \), there is a character \( \Psi : g_{L} \to (\mathbb{Z}/3\mathbb{Z})^\times = \{\pm 1\} \) such that

\[
\rho_3(\sigma) = \begin{bmatrix} \Psi(\sigma) & 0 \\ 0 & \Psi(\sigma) \end{bmatrix}.
\]

Thus the quadratic twist \( E_1 \) of \( E_0 \) by \( \Psi \) has trivial mod 3 Galois representation, so

\[
L(E_1[3]) = L = L(h(E_1[3])).
\]

We claim that this implies that for all \( 3 | M \in \mathbb{Z}^+ \), we have

\[
L(E_1[M]) = L(h(E_1[M])) = LK^{(M)}.
\]

Proof of claim: The Galois group \( \text{Aut}(L(E_1[M])/L) \) is naturally identified with a subgroup \( G(M) \) of \( C_M(O_K) \). Because \( M \geq 3 \), the composite homomorphism

\[
O_K^\times \to C_M(O_K) \to C_3(O_K)
\]

is injective. We have

\[
L(h(E_1[M])) = L(E_1[M])^{G(M) \cap O_K^\times}.
\]
Since 
\[ G(3) \cap O_K^\times = (G(M) \cap O_K^\times) \mod 3, \]
the injectivity of (6) means that if \( G(M) \cap O_K^\times \supseteq \{ e \} \), then \( G(3) \cap O_K^\times \supseteq \{ e \} \). But \( G(3) = \{ e \} \), so that \( G(M) \cap O_K^\times = \{ e \} \), establishing the claim.

Let \( G = \text{Aut}(K^{(N)})/L \), \( H = \text{Aut}(K^{(N)})/K^{(N)} L \). Since \( K^{(N)} = L(E_1[N]) \) and \( K^{(N)} L = L(E_1[N]) \), we may identify \( G \) with a subgroup of scalar matrices of \( C_{Nf}(O_K) \), and \( H \) is the subgroup of matrices which are 1 mod \( N \). So \( \#H \mid \frac{\#(N)}{\varphi(N)} \).

4.3. End of the Proof of Theorem 1.1a).

Let \( O \) be the order of conductor \( f \) in an imaginary quadratic field \( K \), let \( F \supseteq K(f) \) be a number field, and let \( E_{/F} \) be an \( O \)-CM elliptic curve: we may choose the embedding \( F \hookrightarrow \mathbb{C} \) such that \( j(E) = j(C/O) \). We want to show that the index of the image of the adelic Galois representation \( E_{/F} \) in the adelic Cartan \((O \otimes \mathbb{Z})^\times \) divides \( \#O^\times [F : K(f)] \). Equivalently, we want to establish this divisibility on the index of the mod \( N \) Galois representation for all sufficiently divisible \( N \in \mathbb{Z}^+ \), so we may (and shall) assume that \( 3 \mid N \). Let \( (E_1)_{/K(f)} \) be an elliptic curve with \( j(E_1) = j(E) \).

Put 
\[ W(N, O) = K(f)(h(E_1[N])). \]

We saw above that \( K^{(N)} K(Nf) \subset K(f)(E_1[N]) \). Since this holds for all \( E_1 \) with \( j(E_1) = j(C/O) \), the Weber Function Principle (Theorem 2.12) gives 
\[ K^{(N)} K(Nf) \subset W(N, O). \]

By part a) of the Weber Function Principle and (4) we have 
\[ [W(N, O) : K(f)] | \frac{\#C_{N}(O)}{\#O^\times} | [K^{(N)} K(Nf) : K(f)], \]
so we deduce

\[ W(N, O) = K^{(N)} K(Nf), \quad [W(N, O) : K(f)] = \frac{\#C_{N}(O)}{\#O^\times}. \]

It follows from (7) and the Weber Function Principle that we may choose \((E_1)_{/K(f)} \) so that 
\[ \rho_{E_1,N}(g_{K(f)}) = C_N(O). \]

By the standard theory of twists, there is an extension \( L/F \) of degree \( \#O^\times \) such that \( E_{/L} \cong (E_1)_{/L} \), and thus
\[ [C_N(O) : \rho_{E,N}(g_L)] | [C_N(O) : \rho_{E_1,N}(g_L)] | [L : K(f)] = \#O^\times [F : K(f)]. \]

4.4. Proof of Theorem 1.1b).

Let \( O \subset K \) be an imaginary quadratic order of conductor \( f \), let \( w = \#O^\times \), and let \( N \geq 3 \); the last assumption implies that \( \mu_w \hookrightarrow C_N(O) \). Let \( E_{/K(f)} \) be any \( O \)-CM elliptic curve. Again we may view \( G = \text{Aut}(K(f)[E[N]])/K(f) \) as a subgroup of \( C_N(O) \). Let \( H = G \cap \mu_w \) and \( L = (K(f)[E[N]])^H \). Then \([L : K(f)] | \frac{\#C_{N}(O)}{w} \) and \( \rho_{E,N}(g_L) \subset \mu_w \), so a suitable twist of \( E_{/L} \) has trivial mod \( N \) Galois representation. By Theorem 1.1a) we must in fact have
\[ [L : K(f)] = \frac{\#C_{N}(O)}{w}. \]

Remark 4.7. The excluded case \( N = 2 \) will be treated in \( \S 4.5 \).
4.5. Determination of the Weber Function Field.

Let $\mathcal{O} \subset K$ be an imaginary quadratic order of conductor $f$. For $N \in \mathbb{Z}^+$, put

$$W(N, \mathcal{O}) = K(f)(b(E[N])),$$

where $E_{/K(f)}$ is an elliptic curve with $j(E) = j(\mathbb{C}/\mathcal{O})$; the field is independent of the choice of $E$.

In the course of proving Theorem 1.1 we showed that

$$W(N, \mathcal{O}) \supseteq K^{(N)}K(N_f).$$

When $3 \mid N$, we showed that equality holds and that $[W(N, \mathcal{O}) : K(f)] = \frac{\#C_N(\mathcal{O})}{\#\mathcal{O}^\times}$. Conversely, these statements about $W(N, \mathcal{O})$ imply Theorem 1.1: immediately when $F = K(f)$, and by an easy twisting argument when $F \supset K(f)$, as in §4.3. This approach leaves open the question of whether (7) holds when $3 \nmid N$. The next result shows that it holds for all $N \geq 3$ and gives a suitable analogue when $N = 2$.

**Theorem 4.8.** Let $\mathcal{O}$ be an imaginary quadratic order of conductor $f$.

a) For all $N \geq 3$, we have

$$(8) \quad W(N, \mathcal{O}) = K^{(N)}K(N_f), \quad [W(N, \mathcal{O}) : K(f)] = \frac{\#C_N(\mathcal{O})}{\#\mathcal{O}^\times}.$$

b) We have

$$(9) \quad W(2, \mathcal{O}) = K^{(2)}K(2f), \quad [W(2, \mathcal{O}) : K(f)] = \frac{2\#C_2(\mathcal{O})}{\#\mathcal{O}^\times}.$$

**Proof.**

a) Step 0: When $f = 1$ this reduces to known results: $W_N = K^{(N)}$ and (since $N \geq 3$) $[K^{(N)} : K^{(1)}] = \frac{\#K^{(N)}}{\#K^{(1)}}$. Thus we may assume $f > 1$, so $\mathcal{O}^\times = \{\pm 1\}$.

Step 1: Let $M = K^{(N)}K(N_f)$. We already know

$$M \subset W(N, \mathcal{O})$$

and (by the Weber Function Principle)

$$[W(N, \mathcal{O}) : K(f)] \mid \frac{\#C_N(\mathcal{O})}{\#\mathcal{O}^\times}.$$

So it suffices to show

$$(10) \quad \frac{\#C_N(\mathcal{O})}{\#\mathcal{O}^\times} \mid [M : K(f)].$$

In turn, for this it is sufficient to construct an $\mathcal{O}$-CM elliptic curve $E_{/M}$ with trivial mod $N$ Galois representation, for then Theorem 1.1 gives (10).

Step 2: By Proposition 4.6, there is an $\mathcal{O}$-CM elliptic curve $E_{/K(N_f)}$ for which the mod $N$ Galois representation consists of scalar matrices. We extend the base to get $E_{/M}$. Let $\iota : E \to E'$ be the canonical isogeny to an $\mathcal{O}_K$-CM elliptic curve. Since $W(N, \mathcal{O}_K) = K^{(N)} \subset M$, we have $\rho_{E', N}(g_M) \subset \mu_K$. Let $\iota' : E' \to E$ be the dual isogeny. Since $\iota$ and $\iota'$ are cyclic isogenies, there is a point $P \in E'((\mathcal{M}))$ of order $N$ such that $Q = \iota'(P)$ has order $N$. If $K \neq \mathbb{Q}(\sqrt{-1}, \mathbb{Q}(\sqrt{-3})$ then $\mu_K = \{\pm 1\}$, so the $g_M$-orbit of $P$ is contained in $\{\pm P\}$, hence the $g_M$-orbit of $Q$ is contained in $\{\pm Q\}$. Thus $Q$ is an $M$-rational point on a suitable quadratic twist $E'_D$, and since quadratic twists do not change whether the Galois representation is given by scalar matrices, the mod $N$ Galois representation on $E_{/M}^D$ is trivial.
Now suppose \( K = \mathbb{Q}(\sqrt{-1}) \) or \( \mathbb{Q}(\sqrt{-3}) \) and let \( \zeta \) be a primitive \( w_K \)-th root of unity, so \( \mathcal{O} = \mathbb{Z}[\zeta] \).
Then we can take \( P = \frac{\zeta}{N} \). Explicitly, the dual isogeny is
\[
i^{\vee} : z + \mathcal{O}_K \mapsto f z + \mathcal{O},
\]
so \( Q = i^{\vee}(P) = \frac{w_K}{N} + \mathcal{O} \), which has order \( N \) in \( \mathbb{C}/\mathcal{O} \). However, for \( 1 \leq k < w_K \) the point \( i^{\vee}(\zeta^k P) = \frac{w_K^k}{N} + \mathcal{O} \) is only a scalar multiple of \( Q = \frac{w_K}{N} + \mathcal{O} \) if \( k = \frac{w_K}{w_K^k} \), and thus again the \( \mathfrak{g}_M \)-orbit of \( Q \) is contained in \( \{ \pm Q \} \) and we can make a quadratic twist as above. (In fact this argument shows that \( \rho_{N,E^{\vee}}(\mathfrak{g}_M) \subset \{ \pm 1 \}. \))

b) Step 0: Again, when \( f = 1 \), this reduces to known results: \( W(2,\mathcal{O}) = K^{(2)} \) and \( [K^{(2)} : K^{(1)}] = \frac{2p_K^{(2)}}{|\mathcal{O}^*|} \) (Lemma 2.11). So suppose \( f > 1 \).
Step 1: We show that for any \( \mathcal{O}\text{-CM elliptic curve} E_{/K(f)} \) (with \( f > 1 \)), we have
\[
\rho_{E,2}(\mathfrak{g}_{K(f)}) = C_2(\mathcal{O}).
\]
Theorem 1.1 implies that the index of \( \rho_{E,2}(\mathfrak{g}_{K(f)}) \) in \( C_2(\mathcal{O}) \) divides 2. This forces equality unless \( 2 \mid \#C_2(\mathcal{O}) \), which holds iff \( 2 \mid \Delta \). Failure of the result in this case means that there is an \( \mathcal{O}\text{-CM elliptic curve} E_{/K(f)} \) with trivial mod 2 Galois representation. But this would imply that any elliptic curve with \( j = j(\mathbb{C}/\mathcal{O}) \) defined over a number field \( F \supset K(f) \) has trivial mod 2 Galois representation. By Theorem 1.1 b), there is an odd prime \( \ell \) and a field extension \( F/K(f) \) of degree \( \frac{\#C_2(\mathcal{O})}{2} \) and an \( \mathcal{O}\text{-CM elliptic curve} (E_1)_{/F} \) with full \( \ell \)-torsion over \( F \). Then \( E_1 \) would have trivial mod 2 Galois representation, so the index of the mod 2 Galois representation in \( C_2(\mathcal{O}) \) would be
\[
\#C_2(\mathcal{O}) = 2 \cdot \#C_\ell(\mathcal{O}) > \#C_\ell(\mathcal{O}) = \#\mathcal{O}^*[F : K(f)],
\]
contradicting Theorem 1.1.

Step 2: Let \( E_{/K(f)} \) be an \( \mathcal{O}\text{-CM elliptic curve} \). Then the base extension \( E_{/K^{(2)}}(K^{(2)}) \) has trivial mod 2 Galois representation since the only scalar matrix in \( C_2(\mathcal{O}) \) is the identity. By Step 1 we get \( \#C_2(\mathcal{O}) \mid [K^{(2)}K^{(2)} : K^{(1)}] \), which implies the result.

\[\square\]

4.6. Curves with Surjective Mod \( N \) Galois Representations.

From Theorem 4.8 we deduce that the image of Galois is as large as possible, up to twisting.

**Theorem 4.9.** Let \( \mathcal{O} \) be an order of conductor \( f \) in an imaginary quadratic field \( K \), and let \( E_{/K(f)} \) be an \( \mathcal{O}\text{-CM elliptic curve} \). For any \( N \in \mathbb{Z}^+ \), there is a twist \( E' \) of \( E_{/K(f)} \) such that \( \rho_{E',N}(\mathfrak{g}_{K(f)}) = C_N(\mathcal{O}). \)

**Proof.** If \( N \geq 3 \), this follows from part b) of the Weber Function Principle and part a) of Theorem 4.8. If \( N = 2 \) and \( j \neq 0,1728 \), then this is part b) of Theorem 4.8. We now address the remaining cases.

Let \( K = \mathbb{Q}(\sqrt{-3}) \), and let \( E_{/K} \) be an \( \mathcal{O}_K\text{-CM elliptic curve} \). If \( [K(E[2]) : K] = 3 \), we are done, so suppose \( K(E[2]) = K \). As in the proof of the Weber Function Principle, let \( \pi \in \mathfrak{p} \backslash \mathfrak{p}^2 \) for some prime \( \mathfrak{p} \) of \( \mathcal{O}_K \). Then let \( L = K(\pi^{\frac{1}{3}}) \), and let \( \chi : \mathfrak{g}_K \to \mu_6 \) be a character with splitting field \( F_{\text{Ker}\chi} = L \). Then the twist \( E'_{/K} \) has \( [K(E'[2]) : K] = 3 \), as desired. The case where \( K = \mathbb{Q}(\sqrt{-1}) \) is similar: if \( K(E[2]) = K \), we take \( \chi : \mathfrak{g}_K \to \mu_4 \) to be a character corresponding to \( L = K(\pi^{\frac{1}{2}}) \). Then we will have \( E'_{/K} \) with \( [K(E'[2]) : K] = 2 \). \[\square\]
5. Applications

5.1. A Theorem of Franz.

Let $O$ be an order in $K$, of conductor $f$, and let $E_{/K(f)}$ be an $O$-CM elliptic curve. Choose a field embedding $K(f) \hookrightarrow \mathbb{C}$ such that $j(E) = j(\mathbb{C}/O)$ and an isomorphism $E/\mathbb{C} \cong \mathbb{C}/O$. This induces an isomorphism $E(\overline{K(f)})[\text{tors}] \cong \mathbb{C}/O[\text{tors}]$, which we use to view (the image in $\mathbb{C}/O$ of) $\tau_K = \frac{\Delta_K + \sqrt{\Delta_K}}{2}$ as a point of $E(\overline{K(f)})[\text{tors}]$ of order $f$.

**Theorem 5.1.** (Franz [Fr35]) With notation as above, we have $K(f)(b(\tau_K)) = K(f)$.

**Proof.** As in the proof of Theorem 1.3, over $\mathbb{C}$ we may view the canonical isogeny as $\iota : \mathbb{C}/O \to \mathbb{C}/O_K$. We take $e_1 = \frac{1}{f} + O$ and $e_2 = \tau_K + O$ as a basis for $E[f]$. Then $e_2$ generates $\ker(\iota)$, a $K(f)$-rational cyclic subgroup of order $f$, and there is a character $\Psi : g_F \to (\mathbb{Z}/f\mathbb{Z})^\times$ such that

$$
\rho_{E,f}(\sigma) = \begin{bmatrix}
\Psi(\sigma) & 0 \\
0 & \Psi(\sigma)
\end{bmatrix}.
$$

If $f \leq 2$, then $K(f) = K^{(f)}$ and the result holds. Thus we may assume $f \geq 3$. Let $L := K(f)(b(e_2))$. Since $j(E) \neq 0, 1728$, the restriction $\Psi_{|_{g_L}} : g_L \to \{\pm 1\}$ defines a quadratic character $\chi$, and on the twist $E^\chi$ of $E_{/L}$ the point $e_2$ becomes $L$-rational. As in the proof of Theorem 5.5 of [BCS], let $\Psi^\pm : g_K(f) \to (\mathbb{Z}/f\mathbb{Z}^\times)/\{\pm 1\}$ denote the composition of $\Psi$ with the natural map $(\mathbb{Z}/f\mathbb{Z})^\times \to (\mathbb{Z}/f\mathbb{Z})^\times/\{\pm 1\}$. Then $L \subset (K(f))^{\ker(\Psi^\pm)}$, so $[L : K(f)] \mid \varphi(f)$. If $\iota : E^\chi \to E'$ is the canonical isogeny, then the proof of Theorem 1.3 shows that $\iota(e_1)$ is an element of $E'(L)$ which generates $E'[f]$ as an $O_K$-module. Thus $E'$ has full $f$-torsion over $L$, so by Theorem 2.9, $K^{(f)} \subset L$. So

$$
[L : K(f)] \geq [K^{(f)} : K(f)] = \frac{\varphi(f)}{2} \geq [L : K(f)],
$$

and thus $K(f)(b(e_2)) = L = K^{(f)}$.

5.2. SPY Divisibilities.

**Lemma 5.2.** Let $H, K$ be subgroups of a group $G$. If $H$ is normal and $H \cap K = \{1\}$, then $\#K \mid [G : H]$.

**Proof.** The composite homomorphism $K \hookrightarrow G \twoheadrightarrow G/H$ is an injection. $\square$

**Theorem 5.3.** Let $O$ be an order in an imaginary quadratic field $K$, and let $E$ be an $O$-CM elliptic curve defined over a number field $F \supseteq K$. If $E(F)$ has a point of order $N \in \mathbb{Z}^+$, then

$$
\varphi(N) \mid \begin{bmatrix}
\#O^\times & \#F^\times \\
\#O^\times & \#\text{Pic } O
\end{bmatrix}.
$$

**Proof.** Let $I_N = [C_N(O) : \rho_N(g_F)]$ be the index of the mod $N$ Galois representation in the Cartan subgroup. By Theorem 1.1 we have

$$
I_N \mid \begin{bmatrix}
\#O^\times & \#F / K(j(E)) \\
\#O^\times & \#\text{Pic } O
\end{bmatrix} = \begin{bmatrix}
\#O^\times & \#F / \mathbb{Q} \\
\#O^\times & \#\text{Pic } O
\end{bmatrix}.
$$

Since there is a rational point of order $N$, $\rho_N(g_F)$ contains no scalar matrices other than the identity, so by Lemma 5.2 we have $\varphi(N) \mid I_N$, and we're done. $\square$
5.3. Sharpness in the Isogeny Torsion Theorem.

**Lemma 5.4.** Let $E$ be an $\mathcal{O}$-CM elliptic curve defined over a number field $F$ containing the CM field $K$, and let $\iota : E \to E'$ be the canonical $F$-rational isogeny to an $\mathcal{O}_K$-CM elliptic curve $E'_F$. Write

$$E(F)[\text{tors}] = \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}, \quad E'(F)[\text{tors}] = \mathbb{Z}/s'\mathbb{Z} \times \mathbb{Z}/e'\mathbb{Z},$$

where $s \mid e$ and $s' \mid e'$. Then $s \mid s'$.

**Proof.** There is an $\mathcal{O}_K$-CM elliptic curve $E'_F$ and a canonical $F$-rational isogeny $\iota : E \to E'$. Moreover, there is a field embedding $F \hookrightarrow \mathbb{C}$ such that the base change of $\iota$ to $\mathbb{C}$ is, up to isomorphisms on the source and target, given by the canonical map $\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{O}_K$. There are positive integers $s \mid e$ and $s' \mid e'$ such that

$$E(F)[\text{tors}] \cong \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}, \quad E'(F)[\text{tors}] \cong \mathbb{Z}/s'\mathbb{Z} \times \mathbb{Z}/e'\mathbb{Z}.$$

Our $\mathbb{C}$-analytic description of $\iota$ shows that if

$$P = \frac{1}{s} + \mathcal{O} \in E[s], \quad P' = \frac{1}{s} + \mathcal{O}_K \in E'[s],$$

then $\iota(P) = P'$ and $\langle P' \rangle_{\mathcal{O}_K} = E'[s]$. As $P \in E(F)$, we have $P' = \iota(P) \in E'(F)$. \hfill $\Box$

In [Ro94, §4], Ross claims that a CM elliptic curve $E$ defined over a number field $F$ containing the CM field, then the exponent of the finite group $E(F)[\text{tors}]$ is an invariant of the $F$-rational isogeny class. In the setting of Lemma 5.4, this would give $e = e'$ and thus there is an injective group homomorphism $E(F)[\text{tors}] \hookrightarrow E'(F)[\text{tors}]$ (though this homomorphism need not be the one induced by $\iota$). This conclusion is stronger than that of Theorem 1.3. Moreover, in the first version of [CP15] it was used to reduce the general case to the $\mathcal{O}_K$-CM case.

Unfortunately Ross’s claim is false: in the setup of Lemma 5.4 one can have $e' < e$ (in which case there is no injective group homomorphism $E(F)[\text{tors}] \hookrightarrow E'(F)[\text{tors}]$), as the following result shows.

**Proposition 5.5.** Let $\ell > 3$ be a prime number, let $K = \mathbb{Q}(\sqrt{-\ell})$, let $n \in \mathbb{Z}^{\geq 3}$, let $\mathcal{O}$ be the order in $K$ of conductor $\mathfrak{f} = \ell^{\lfloor \frac{n}{2} \rfloor}$, and let $F = K(\mathfrak{f})$. For any $\mathcal{O}$-CM elliptic curve $E_F$, there is an extension $L/F$ of degree $\varphi(\ell^n)$ such that $E(L)$ has a point of order $\ell^n$, and no $\mathcal{O}_K$-CM elliptic curve has an $L$-rational point of order $\ell^k$ for $k > \frac{1}{2} (n + 1 + \lceil \frac{n}{2} \rceil)$ (hence no $L$-rational point of order $\ell^n$).

**Proof.** Let $E_F$ be an $\mathcal{O}$-CM elliptic curve. As in (3) we may choose a basis $\{e_1, e_2\}$ for $E[\ell^n]$ so that the image of the mod $\ell^n$ Galois representation consists of matrices

$$\begin{bmatrix} a & b\ell^2 \Delta_k - \Delta_k^2 \mathfrak{f} \\ b & a + b\ell \Delta_K \end{bmatrix}, \quad a, b \in \mathbb{Z}/\ell^n\mathbb{Z}.$$

Since $\ell$ ramifies in $K$ and $\mathfrak{f} = \ell^{\lfloor \frac{n}{2} \rfloor}$, we have $\text{ord}_\ell(b\ell^2 \Delta_k - \Delta_k^2 \mathfrak{f}) = 1 + 2\lceil \frac{n}{2} \rceil \geq n$, so the matrices have the form

$$\begin{bmatrix} a & 0 \\ b & a + b\ell \Delta_K \end{bmatrix}, \quad a, b \in \mathbb{Z}/\ell^n\mathbb{Z}.$$

The action of $g_F$ on $\langle e_2 \rangle$ gives a character $\Phi : g_F \to (\mathbb{Z}/\ell^n\mathbb{Z})^\times$. Take $M = (\mathfrak{F})^{\text{ker} \Phi}$. Then $[M : F] = \varphi(\ell^n)$ and $\Phi|_{\mathfrak{g}_M}$ is trivial. Thus there exists an extension $L/F$ with $[L : F] = \varphi(\ell^n)$ such that $E(L)$ contains $e_2$. 
Let $E'_L$ be an $O_K$-CM elliptic curve, and suppose $E'(L)$ contains a point $P$ of order $\ell^k$. Let $p$ be the prime ideal of $O_K$ such that $\ell pO_K = p^2$. We claim that the $O_K$-submodule $M = \langle p \rangle_{O_K}$ of $E'(L)$ generated by $P$ contains $E[p^{2k-1}]$ and thus, by Theorem 2.9, that $K^{p^{2k-1}} \subset L$. Indeed, by Theorem 2.7, we have $M = E[I]$ for some ideal $I$ of $O_K$ such that $(O_K/I, +)$ has $\ell$-power order and exponent $\ell^k$. Since $\ell$ ramifies in $O_K$, this forces $I$ to be of the form $p^a$ for some $a \in \mathbb{Z}^+$, and the smallest $a$ such that $(O_K/p^a, +)$ has exponent $\ell^k$ is $a = 2k - 1$, establishing the claim. Thus

$$\text{ord}_L([K^{p^{2k-1}} : K^{(1)}]) = 2k - 2 \leq \text{ord}_L([L : K^{(1)}]) = \left\lfloor \frac{n}{2} \right\rfloor + n - 1,$$

so $k \leq \frac{1}{2}(n + 1 + \lfloor \frac{n}{2} \rfloor)$.

In the setting of Theorem 1.3, one wonders whether $\# E(F)[\text{tors}] = \# E'(F)[\text{tors}]$. In fact $\# E'(F)[\text{tors}]$ can be arbitrarily large:

**Proposition 5.6.** Let $\ell$ be an odd prime, let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field, let $O$ be the order in $K$ of conductor $\ell$, and let $F = K(\ell)$. For any $O$-CM elliptic curve $E/F$ there is an extension $L/F$ such that if $\iota : E \to E'$ is the canonical isogeny to an $O_K$-CM elliptic curve $E$, then

$$\ell \mid \frac{\# E'(L)[\text{tors}]}{\# E(L)[\text{tors}]}.$$

**Proof.** Let $E/F$ be an $O$-CM elliptic curve. As above, there is a basis $\{e_1, e_2\}$ for $E[F]$ such that

$$\rho_F(\mathfrak{g}_F) \subset \left\{ \begin{bmatrix} a & 0 \\ b & a \end{bmatrix} : a, b \in \mathbb{Z}/\ell \mathbb{Z} \right\}$$

and there is an extension $L/F$ with $[L : F] = \ell - 1$ such that $E(L)$ contains $e_2$. In fact, $E(L)[\ell^\infty] \cong \mathbb{Z}/\ell \mathbb{Z}$. Indeed, $E$ does not have full $\ell$-torsion over $L$ since Theorem 4.8 would imply $K^{(\ell)}(K^{(\ell^2)} \subset L$ and $\frac{1}{2}(\ell - 1) = [K^{(\ell)}(K^{(\ell^2)} : K(\ell)]$. In addition, $E$ has no point of order $\ell^3$ by Theorem 5.3.

Let $\iota : E \to E'$ be the canonical $\ell$-rational isogeny from $E/L$ to $E'/L$, where $E'$ has $O_K$-CM. Since $e_2 \in E(L)$, the proof of Theorem 1.3 shows $\iota(e_1) \in E'(L)$, and $\iota(e_1)$ generates $E'[\ell]$ as an $O_K$-module. In other words, $\mathbb{Z}/\ell \mathbb{Z} \times \mathbb{Z}/\ell \mathbb{Z} \hookrightarrow E'(L)[\text{tors}]$. It follows that $\ell \mid \frac{\# E'(L)[\text{tors}]}{\# E(L)[\text{tors}]}$. \hfill \Box

Finally, Theorem 1.3 requires $K \subset F$. This hypothesis cannot be omitted:

**Proposition 5.7.** Let $\ell > 3$ be a prime with $\ell \equiv 3 \pmod{4}$ and let $n \in \mathbb{Z}\geq 3$. Let $K = \mathbb{Q}(\sqrt{-\ell})$, and let $O$ be the order in $K$ of conductor $\ell$, let $F = \mathbb{Q}(j(C/O))$. There is an elliptic curve $E_{L}$ and an extension $L/F$ of degree $\frac{\varphi(n)}{2}$ such that:

(i) $L \not\supset K$,

(ii) $E(L)$ has a point of order $\ell^n$, and

(iii) for every $O_K$-CM elliptic curve $E'/L$ we have $\ell^n \nmid \# E'(L)[\text{tors}]$.

**Proof.** Let $E/F$ be an $O$-CM elliptic curve. By [Kw99, Corollary 4.2], $E$ has an $F$-rational subgroup which is cyclic of order $\ell^n$. It follows from [BCS, Theorem 5.6] that there is a twist $E_1$ of $E/F$ and an extension $L/F$ of degree $\varphi(\ell^n)/2$ such that $E_1(L)$ has a point of order $\ell^n$. Note $[L : \mathbb{Q}] = h_K(\ell^n)(\varphi(\ell^n)/2)$ is odd (see [Go89, Proposition 3.11]) , so $K \not\subset L$.

Let $E'/L$ be an $O_K$-CM elliptic curve. Since $[L : \mathbb{Q}]$ is odd, $E'(L)[\ell^n]$ must be cyclic, as full $\ell^k$-torsion would imply $\mathbb{Q}((\zeta_{\ell^n}) \subset L$ by the Weil pairing. As in the proof of Proposition 5.5, $E'(LK)$ contains no point of order $\ell^n$. Hence $E'(L)$ contains no point of order $\ell^n$, and $\ell^n \nmid \# E'(L)[\text{tors}]$. \hfill \Box
5.4. Minimal Cartan Orbits.

Let \( \mathcal{O} \) be an imaginary quadratic order, and let \( N \in \mathbb{Z}^+ \). As above, since \( C_N(\mathcal{O}) \) contains all scalar matrices, if \( P \in \mathcal{O}/N\mathcal{O} \) has order \( N \), then the orbit of \( C_N(\mathcal{O}) \) on \( P \) has size at least \( \varphi(N) \). We will now determine when this bound is sharp.

We introduce the shorthand \( H(\mathcal{O}, N) \) to mean: There is a point \( P \) of order \( N \) in \( \mathcal{O}/N\mathcal{O} \) such that the \( C_N(\mathcal{O}) \)-orbit of \( P \) has size \( \varphi(N) \).

**Lemma 5.8.** Let \( \mathcal{O} \) be an imaginary quadratic order, and let \( N = \ell_1^{a_1} \cdots \ell_r^{a_r} \in \mathbb{Z}^+ \). Then \( H(\mathcal{O}, N) \) holds iff \( H(\mathcal{O}, \ell_i^{a_i}) \) holds for all \( 1 \leq i \leq r \).

*Proof.* This is an easy consequence of the Chinese Remainder Theorem. \( \Box \)

**Lemma 5.9.** Let \( \mathcal{O} \) be an imaginary quadratic order of discriminant \( \Delta \), \( \ell \) a prime number and \( a \in \mathbb{Z}^+ \).

a) If \( \left( \frac{a}{\ell} \right) = 1 \), there is an \( \mathcal{O} \)-submodule of \( \mathcal{O}/\ell^a\mathcal{O} \) with underlying \( \mathbb{Z} \)-module \( \mathbb{Z}/\ell^a\mathbb{Z} \).

b) If \( \left( \frac{a}{\ell} \right) = -1 \), then \( C_{\ell^a}(\mathcal{O}) \) acts transitively on the order \( \ell^a \) elements of \( \mathcal{O}/\ell^a\mathcal{O} \).

c) If \( \left( \frac{a}{\ell} \right) = 0 \), then there is an \( \mathcal{O} \)-submodule of \( \mathcal{O}/\ell\mathcal{O} \) of order \( \ell \).

*Proof.* See [CCRS13, §2.4]. \( \Box \)

**Lemma 5.10.** Let \( \mathcal{O} \) be a quadratic order of discriminant \( \Delta \), and let \( N \in \mathbb{Z}^+ \). The following are equivalent:

(i) If \( 2 \mid N \), then \( \left( \frac{a}{2} \right) \neq 1 \).

(ii) The \( \mathbb{Z}/N\mathbb{Z} \)-subalgebra of \( \mathcal{O}/N\mathcal{O} \) generated by \( C_N(\mathcal{O}) \) is \( \mathcal{O}/N\mathcal{O} \).

*Proof.* Using the Chinese Remainder Theorem we immediately reduce to the case in which \( N = \ell^a \) is a power of a prime number \( \ell \). Let \( B \) be the \( \mathbb{Z}/\ell^a\mathbb{Z} \)-subalgebra generated by \( C_{\ell^a}(\mathcal{O}) \), so \( \#B = \ell^b \) for some \( b \leq 2a \).

(i) \( \implies \) (ii): Since \( 0 \in B \setminus C_{\ell^a}(\mathcal{O}) \), we have

\[
\#B \geq \#C_{\ell^a}(\mathcal{O}) + 1
\]

\[
= \ell^{2a} \left( 1 - \frac{1}{\ell} \right) \left( 1 - \left( \frac{\Delta}{\ell} \right) \frac{1}{\ell} \right) + 1 \geq \begin{cases}
\frac{1}{3} \ell^{2a} + 1 & \text{if } \ell \geq 3 \\
\frac{1}{2} \ell^{2a} + 1 & \text{if } \ell = 2 \text{ and } \left( \frac{a}{2} \right) \neq 1.
\end{cases}
\]

Thus \( b = 2a \) and \( B = \mathcal{O}/\ell^a\mathcal{O} \).

\( \neg \) (i) \( \implies \neg \) (ii): If \( \ell = 2 \) and \( \left( \frac{a}{2} \right) = 1 \), then

\[
\mathcal{O}/2^a\mathcal{O} \cong \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}/2^a\mathbb{Z} \right\}
\]

and \( C_{2^a}(\mathcal{O}) \) consists of the set of such matrices with \( \alpha, \beta \in (\mathbb{Z}/2^a\mathbb{Z})^\times \). Thus \( C_{2^a}(\mathcal{O}) \) is contained in the subalgebra

\[
\mathcal{B} = \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}/2^a\mathbb{Z} \text{ and } \alpha \equiv \beta \pmod{2} \right\}
\]

of order \( 2^{2a-1} \), so \( B \subset \mathcal{B} \subset \mathcal{O}/2^a\mathcal{O} \).

\( \Box \)

---

\( ^3 \)Since \( \#B \geq \#C_{2^a}(\mathcal{O}) + 1 = 2^{2a-2} + 1 > 2^{2a-2} \), in fact we have \( B = \mathcal{B} \).
Lemma 5.11. For an order $\cal O$ and $N \in \mathbb{Z}^+$, the following are equivalent:

(i) There is an ideal $I$ of $\cal O$ with $\cal O/I \cong \mathbb{Z}/N\mathbb{Z}$.

(ii) There is an $\cal O$-submodule of $\cal O/N\cal O$ with underlying commutative group $\mathbb{Z}/N\mathbb{Z}$.

(iii) $H(\cal O, N)$ holds.

Proof. (i) $\iff$ (ii):

Step 1: Let $\Lambda$ be a free, rank 2 $\mathbb{Z}$-module, and let $\Lambda'$ be a $\mathbb{Z}$-submodule of $\Lambda$ containing $NA$. By the structure theory of modules over a PID, there is a $\mathbb{Z}$-basis $e_1, e_2$ for $\Lambda$ and positive integers $a \mid b$ such that $ae_1, be_2$ is a $\mathbb{Z}$-basis for $\Lambda'$. Thus

$$\Lambda/\Lambda' \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$$

$$\Lambda'/N\Lambda \cong \mathbb{Z}/(N/b)\mathbb{Z} \oplus \mathbb{Z}/(N/a)\mathbb{Z}.$$ 

It follows that $\Lambda/\Lambda' \cong \mathbb{Z}/N\mathbb{Z} \iff \Lambda'/N\Lambda \cong \mathbb{Z}/N\mathbb{Z}$.

Step 2: If $I$ is an ideal of $\cal O$ with $\cal O/I \cong \mathbb{Z}/N\mathbb{Z}$, then $I \supset N\cal O$, so $I/N\cal O \cong \mathbb{Z}/N\mathbb{Z}$ by Step 1. Let $M$ be an $\cal O$-submodule of $\cal O/N\cal O$ with underlying $\mathbb{Z}$-module $\mathbb{Z}/N\mathbb{Z}$. Then $M = I/N\cal O$ for an ideal $I$ of $\cal O$, and by Step 1 we have $\cal O/I \cong \mathbb{Z}/N\mathbb{Z}$.

(ii) $\implies$ (iii): Let $P \in \cal O/N\cal O$ have order $N$ such that the subgroup generated by $P$ is an $\cal O$-submodule. For all $g \in C_N(\cal O)$, $gP = a_gP$ for $a_g \in (\mathbb{Z}/N\mathbb{Z})^\times$. Conversely, since $C_N(\cal O)$ contains all scalar matrices, the orbit of $C_N(\cal O)$ on $P$ has size $\varphi(N)$.

(iii) $\implies$ (ii): Case 1: Suppose $2 \nmid N$ or $(\frac{\varphi(N)}{2}) \neq 1$. Let $P \in \cal O/N\cal O$ be a point of order $N$ with $C_N(\cal O)$-orbit of size $\varphi(N)$. There is a $\mathbb{Z}/N\mathbb{Z}$-basis $e_1, e_2$ of $\cal O/N\cal O$ with $e_1 = P$, and our hypothesis gives that with respect to this basis $C_N(\cal O)$ lies in the subalgebra $\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in \mathbb{Z}/N\mathbb{Z} \right\}$ of upper triangular matrices. By Lemma 5.10, $\cal O/N\cal O$ also lies in the subalgebra of upper triangular matrices, and thus $\langle P \rangle$ is an $\cal O$-stable submodule with underlying $\mathbb{Z}$-module $\mathbb{Z}/N\mathbb{Z}$.

Case 2: Suppose $2 \mid N$ and $(\frac{\varphi(N)}{2}) = 1$, and write $N = 2^e N'$ with $2 \nmid N'$. By Lemma 5.9 and the equivalence of (i) and (ii), there is an ideal $I_1$ in $\cal O$ with $\cal O/I_1 \cong \mathbb{Z}/2^e\mathbb{Z}$, and by Case 1 there is an ideal $I_2$ in $\cal O$ with $\cal O/I_2 \cong \mathbb{Z}/N'\mathbb{Z}$. By the Chinese Remainder Theorem, $\cal O/I_1 I_2 \cong \mathbb{Z}/N\mathbb{Z}$. Since (i) $\iff$ (ii), this suffices. \qed

Theorem 5.12. Let $\cal O$ be an order of discriminant $\Delta$ in the imaginary quadratic field $K$, and let $N \in \mathbb{Z}^+$. The following are equivalent:

(i) $H(\cal O, N)$ holds.

(ii) $\Delta$ is a square in $\mathbb{Z}/4N\mathbb{Z}$.

Proof. Using the Chinese Remainder Theorem and Lemma 5.8 we reduce to the case in which $N = \ell^a$ is a power of a prime number $\ell$. Since $\Delta$ is either prime to 4 or divisible by 4, we may put $D = \frac{\Delta}{4} \in \mathbb{Z}/\ell^a\mathbb{Z}$.

Case 1 ($\ell$ is odd): Then $\Delta$ is a square in $\mathbb{Z}/4\ell^a\mathbb{Z}$ iff $D$ is a square in $\mathbb{Z}/\ell^a\mathbb{Z}$, and

$$\cal O/\ell^a\cal O \cong \mathbb{Z}/\ell^a\mathbb{Z}[t]/(t^2 - D).$$

If there is $s \in \mathbb{Z}/\ell^a\mathbb{Z}$ such that $D = s^2$, then

$$\cal O/\ell^a\cal O \cong \mathbb{Z}/\ell^a\mathbb{Z}[t]/((t+s)(t-s)).$$

so if $I$ is the ideal $(t+s, \ell^a)$ of $\cal O$, then $\cal O/I \cong \mathbb{Z}/\ell^a\mathbb{Z}$. By Lemma 5.11, $H(\cal O, \ell^a)$ holds. Conversely, suppose $H(\cal O, \ell^a)$ holds, so by Lemma 5.11 there is an ideal $I$ of $\cal O$ with $\cal O/I \cong \mathbb{Z}/\ell^a\mathbb{Z}$. Since $\ell^a \in I$, we may regard $I$ as an ideal of $\cal O/\ell^a\cal O$ such that $\langle \cal O/\ell^a\cal O \rangle/I \cong \mathbb{Z}/\ell^a\mathbb{Z}$. In other words, we have a $\mathbb{Z}/\ell^a\mathbb{Z}$-algebra homomorphism

$$f : \mathbb{Z}/\ell^a\mathbb{Z}[t]/(t^2 - D) \to \mathbb{Z}/\ell^a\mathbb{Z}.$$
Then $f(t)^2 = D \in \mathbb{Z}/\ell^n\mathbb{Z}$, so $D$ is a square in $\mathbb{Z}/\ell^n\mathbb{Z}$.

Case 2 ($\ell = 2$, $\Delta$ is odd): Then $\left( \frac{\Delta}{2} \right) = \pm 1$.

- If $\left( \frac{\Delta}{2} \right) = 1$, then $\Delta \equiv 1 \pmod{8}$; by Hensel’s Lemma, $\Delta$ is a square in $\mathbb{Z}/\ell^n\mathbb{Z}$. On the other hand, by Lemmas 5.9a) and 5.11, $H(\mathcal{O}, \ell^n)$ holds.
- If $\left( \frac{\Delta}{2} \right) = -1$, then $\Delta \equiv 5 \pmod{8}$, so $\Delta$ is not a square modulo 8 and thus not a square modulo $4 \cdot 2^n$. On the other hand, by Lemma 5.9b) $H(\mathcal{O}, \ell^n)$ does not hold.

Case 3: ($\ell = 2$, $\Delta$ is even): Again (11) holds. The argument of Case 1 shows that $H(\mathcal{O}, \ell^n)$ holds iff $D$ is a square modulo $\mathbb{Z}/\ell^n\mathbb{Z}$ if $\Delta$ is a square modulo $\mathbb{Z}/4\ell^n\mathbb{Z}$. \hfill $\Box$

5.5. Maximal Cartan Orbits.

**Proposition 5.13.** Let $\mathcal{O}$ be an imaginary quadratic order, and let $N \in \mathbb{Z}^+$. The following are equivalent:

(i) $C_N(\mathcal{O})$ acts simply transitively on order $N$ elements of $\mathcal{O}/N\mathcal{O}$.

(ii) $C_N(\mathcal{O})$ acts transitively on order $N$ elements of $\mathcal{O}/N\mathcal{O}$.

(iii) For all primes $\ell$ such that $\ell$ divides $N$, we have $\left( \frac{\Delta}{\ell} \right) = -1$.

**Proof.** As usual, we may assume $N = \ell^n$ is a prime power. Certainly (i) $\implies$ (ii).

(ii) $\implies$ (iii): We have

$$\#C_{\ell^n}(\mathcal{O}) = \ell^{2^n-2}(\ell - 1)\left( \ell - \left( \frac{\Delta}{\ell} \right) \right),$$

whereas the number of elements of order $\ell^n$ in $\mathcal{O}/\ell^n\mathcal{O}$ is

$$N(\mathcal{O}, \ell^n) := \#\mathcal{O}/\ell^n\mathcal{O} - \#\mathcal{O}/\ell^n\mathcal{O} = \ell^{2^n-2}(\ell - 1)(\ell + 1).$$

Transitivity of the action implies $\#C_{\ell^n}(\mathcal{O}) \geq N(\mathcal{O}, \ell^n)$, which holds iff $\left( \frac{\Delta}{\ell} \right) = -1$.

(iii) $\implies$ (i): Since $\left( \frac{\Delta}{\ell} \right) \neq 0$, we have $\mathcal{O}/\ell^n\mathcal{O} \cong \mathcal{O}_K/\ell^n\mathcal{O}_K$, and thus also $C_{\ell^n}(\mathcal{O}) = (\mathcal{O}/\ell^n\mathcal{O})^\times \cong C_{\ell^n}(\mathcal{O}_K)$. Thus $\mathcal{O}/\ell^n\mathcal{O}$ is a finite local principal ring with maximal ideal $m = \ell$ and unit group $C_{\ell^n}(\mathcal{O}) = \mathcal{O}/\ell^n\mathcal{O} \setminus m$. The set of order $\ell^n$ elements of $\mathcal{O}/\ell^n\mathcal{O}$ is $\mathcal{O}/\ell^n\mathcal{O} \setminus m = C_{\ell^n}(\mathcal{O})$, and thus the action of the unit group $C_{\ell^n}(\mathcal{O})$ on this set is exactly the action of $C_{\ell^n}(\mathcal{O})$ on itself, which is simply transitive. \hfill $\Box$

**Theorem 5.14.** Let $\mathcal{O} \subset K$ be an imaginary quadratic order of conductor $\mathfrak{f}$. Let $N = \prod_{i=1}^r \ell_i^{e_i} \in \mathbb{Z}^+$ be such that $\left( \frac{\Delta}{\ell_i} \right) = -1$ for all $i$. Let $F$ be a number field, and let $E/F$ be an $\mathcal{O}$-CM elliptic curve such that $E(F)$ has a point of order $N$. Then

$$\#C_N(\mathcal{O}) = \prod_{i=1}^r \ell_i^{2e_i-2}(\ell_i^2 - 1) \mid \#\mathcal{O}^\times [FK : K(\mathfrak{f})].$$

**Proof.** Replace $F$ by $FK$; then $F \supset K(\mathfrak{f})$. By Proposition 5.13, $C_N(\mathcal{O})$ acts transitively on order $N$ points of $\mathcal{O}/N\mathcal{O}$, so the $\mathcal{O}$-submodule generated by any one such point is $\mathcal{O}/N\mathcal{O}$. Thus the existence of one $F$-rational point of order $N$ forces $\rho_{E,N}$ to be trivial. By Theorem 1.1, we have

$$\#C_N(\mathcal{O}) = [C_N(\mathcal{O}) : \rho_{E,N}(\mathfrak{g}_F)] \mid \#\mathcal{O}^\times [F : K(\mathfrak{f})].$$

**Remark 5.15.** By Theorem 1.1b), for all $\mathcal{O}$ and all $N \geq 3$ such that $\left( \frac{\Delta}{\ell} \right) = -1$ for all primes $\ell \mid \Delta$, equality can hold in (12). When $N = 2$ the sharp bound is

$$\#C_2(\mathcal{O}) = 3 \mid \frac{\#\mathcal{O}^\times}{2} [FK : K(\mathfrak{f})].$$
5.6. Torsion over $K(j)$.

Let $E$ be an $O$-CM elliptic curve defined over $F = K(O)$. We observe: if $E(F)$ has a point of order $N$, then since $[C_N(O) : \rho_N(g_F)] \mid O^\times$, there must be $P \in O/NO$ of order $N$ with a $C_N(O)$-orbit of order dividing $#O^\times$.

I. Suppose first that $\Delta \neq -3, -4$, so $#O^\times = 2$. Then:

- By Theorem 5.3, if $E(F)$ has a point of order $N$, then $\varphi(N) \mid 2$, so $N \in \{1, 2, 3, 4, 6\}$.
- Lemma 2.2b) implies that for all $N \geq 3$, we have $#C_N(O) \geq 4$ (equality holds if $N = 3$ and $\Delta \equiv 1 \pmod{3}$). By Theorem 1.1 we cannot have $E[N] = E[N](F)$.

Thus $E(F)[\text{tors}]$ is isomorphic to one of the groups in the following list:

$$\{e\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$  

We will show that all of these groups occur.

**Points of order 2:** By Theorem 4.8b), $E(F)[2]$ has order 4 if 2 splits in $O$, order 2 if 2 ramifies in $O$ and order 1 if 2 is inert in $O$. Thus:

$$E(F)[2] \cong \begin{cases} \{e\} & \Delta \equiv 5 \pmod{8} \\ \mathbb{Z}/2\mathbb{Z} & \Delta \equiv 0 \pmod{4} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \Delta \equiv 1 \pmod{8} \end{cases}.$$  

**Points of order 3, 4, or 6:** Let $E/F$ be any $O$-CM elliptic curve. We claim that for $N \in \{3, 4, 6\}$, there is a quadratic twist $E^D$ of $E$ such that $E^D(F)$ has a point of order in iff $H(O, N)$ holds. Indeed, as above, since the index of the mod $N$ Galois representation in $C_N(O)$ divides 2, if some $E^D(F)$ has a point of order $N$, then $O/NO$ has a point of order $N$ with a $C_N(O)$-orbit of size 2. Since $\varphi(N) = 2$, there is a Cartan orbit of size 2 iff $H(O, N)$ holds. Conversely, if $H(O, N)$ holds then there is a point of order $N$ with a $C_N(O)$-orbit of size 2, hence on some quadratic twist $E^D$ we have an $F$-rational point of order $N$. Applying Theorem 5.12, we get:

- Some $O$-CM $E/F$ has a point of order 3 iff $\Delta \equiv 0, 1 \pmod{3}$.
- Some $O$-CM $E/F$ has a point of order 4 iff $\Delta \equiv 0, 1, 4, 9 \pmod{16}$.
- Some $O$-CM $E/F$ has a point of order 6 iff $\Delta \equiv 0, 1, 2, 9, 12, 16 \pmod{24}$.

Because the only full $N$-torsion we can have is full 2-torsion, and 2-torsion is invariant under quadratic twists, we immediately deduce the complete answer in all cases.

- If $\Delta \equiv 0 \pmod{48}$, then there are twists $E_1, E_2, E_3$ of $E$ with
$$E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z}, \ E_2(F)[\text{tors}] \cong \mathbb{Z}/4\mathbb{Z}, \ E_3(F)[\text{tors}] \cong \mathbb{Z}/6\mathbb{Z}.$$  

- If $\Delta \equiv 1, 9, 25, 33 \pmod{48}$ then there are twists $E_1, E_2$ of $E$ with
$$E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \ E_2(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$
• If $\Delta \equiv 4, 16, 36 \pmod{48}$, then there are twists $E_1, E_2, E_3$ of $E$ with
  \[E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z}, \ E_2(F) \cong \mathbb{Z}/4\mathbb{Z}, \ E_3(F) \cong \mathbb{Z}/6\mathbb{Z}.\]

• If $\Delta \equiv 5, 29 \pmod{48}$, then $E(F)[\text{tors}] = \{e\}$.

• If $\Delta \equiv 8, 44 \pmod{48}$, then $E(F)[\text{tors}] = \mathbb{Z}/2\mathbb{Z}$.

• If $\Delta \equiv 12, 24, 28, 40 \pmod{48}$, then there are twists $E_1, E_2$ of $E$ with
  \[E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z}, \ E_2(F) \cong \mathbb{Z}/6\mathbb{Z}.\]

• If $\Delta \equiv 13, 21, 37, 45 \pmod{48}$, then there are twists $E_1, E_2$ of $E$ with
  \[E_1(F)[\text{tors}] = \{e\}, \ E_2(F)[\text{tors}] \cong \mathbb{Z}/3\mathbb{Z}.\]

• If $\Delta \equiv 16 \pmod{48}$, then there are twists $E_1, E_2, E_3$ of $E$ with
  \[E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z}, \ E_2(F) \cong \mathbb{Z}/4\mathbb{Z}, \ E_3(F) \cong \mathbb{Z}/6\mathbb{Z}.\]

• If $\Delta \equiv 17, 41 \pmod{48}$, then there are twists $E_1, E_2$ of $E$ with
  \[E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \ E_2(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.\]

• If $\Delta \equiv 20, 32 \pmod{48}$, then there are twists $E_1, E_2$ of $E$ with
  \[E_1(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z}, \ E_2(F) \cong \mathbb{Z}/4\mathbb{Z}.\]

II. Suppose $\Delta = -4$, so $j = 1728$ and $F = K(j) = \mathbb{Q}(\sqrt{-1})$.

• By Theorem 5.3, if $E(F)$ has a point of order $N$, then $\varphi(N) | 4$, so
  \[N \in \{1, 2, 3, 4, 5, 6, 8, 10\}.\]

**Points of order 2**: Since 2 ramifies in $\mathcal{O}$ and $\varphi(2) = 1$, there is a point of order 2 in $\mathcal{O}/2\mathcal{O}$ which is fixed under the action of $C_2(\mathcal{O})$. Thus every $\mathcal{O}$-CM $E/F$ has an $F$-rational point of order 2.

**Points of order 3**: Since $\left(\frac{2}{4}\right) = -1$, by Proposition 5.13 the group $C_3(\mathcal{O})$ acts transitively on all 8 points of $\mathcal{O}/3\mathcal{O}$ of order 3, so no $\mathcal{O}$-CM elliptic curve has an $F$-rational point of order 3.

**Points of order 4**: Because $\Delta = -4$ is not a square modulo 16, $H(\mathcal{O}, 4)$ does not hold, so there is no $C_4(\mathcal{O})$-orbit of size 2. However, since $\#\mathcal{O}^* = 4$, the existence of an $\mathcal{O}$-CM $E/F$ with an $F$-rational point of order 4 is not ruled out by this, and in fact there is such an elliptic curve, as we show now. Let $p_2 = (1+i)$ be the unique prime ideal of $\mathcal{O}$ of norm 2. Then $r = \mathcal{O}/4\mathcal{O} = \mathcal{O}/(1+i)^4\mathcal{O}$ is a finite, local principal ring with maximal ideal $m = (1+i)$. The unit group $C_4(\mathcal{O})$ has size 8 and is explicitly given as $\{a+bi+4\mathcal{O} \mid a \neq b \pmod{2}\}$. The $C_4(\mathcal{O})$-orbits on $r$ are $r \setminus m$, $m \setminus m^2$, $m^2 \setminus m^3$, $m^3 \setminus m^4$ and $m^4 = \{0\}$, of sizes 8, 4, 2, 1 and 1. Since $m^2 = 2r$, the orbits consisting of points of order 4 are $r \setminus m$ and $m \setminus m^2$. The second orbit consists of $\{1+i, i(1+i), -(1+i), -i(1+i)\}$. It follows that the action of $g_F$ on $P = 1+i+\mathcal{O}/4\mathcal{O}$ is given by a character with values in $\mu_4$; twisting by the inverse of this character we get a $\mathcal{O}$-CM $E/F$ with an $F$-rational point of order 4. Because Galois acts trivially on $P$ while the $C_4(\mathcal{O})$-orbit of $P$ has size 4, it follows that the index of the mod 4 Galois representation in $C_4(\mathcal{O})$ is divisible by 4; by Theorem 1.1 this index is exactly 4, and thus $\rho_{E,4}(g_F)$ has order 2. Taking $P$ as the first basis vector for $\mathcal{O}/4\mathcal{O}$ we find that the Galois representation

\[4^*\text{An alternate approach to the assertions of this paragraph is to note that the } \mathcal{O}\text{-CM elliptic curves defined over } F \text{ are precisely those given by Weierstrass equations of the form } y^2 = x^3 + Ax. \text{ Then } (0,0) \text{ is a point of order 2 independent of } A, \text{ and taking } A = -1 \text{ we get also } (\pm 1, 0).\]
consists of matrices \[
\begin{bmatrix}
1 & b(\sigma) \\
0 & d(\sigma)
\end{bmatrix}
\]. Moreover \(\sigma \mapsto d(\sigma)\) must be the mod 4 cyclotomic character, which is trivial since \(i \in F\). It follows that \(\rho_{E,4}(\mathcal{O}) = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \}\), and thus \(\rho_{E,2}\) is trivial. We conclude if \(\mathbb{Z}/4\mathbb{Z} \hookrightarrow E(F)\), then also \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \hookrightarrow E(F)\). The converse is not true: by [BCS, Thm. 2.1c], all but finitely many quadratic twists have \(E(D)(F) = E(D)(F)[2] = E(F)[2]\).

### Points of order 5 and 10

By Proposition 4.3, some \(\mathcal{O}\)-CM \(E/F\) has an \(F\)-rational point of order 5. Since every \(\mathcal{O}\)-CM \(E/F\) has a point of order 2, indeed some \(\mathcal{O}\)-CM \(E/F\) has an \(F\)-rational point of order 10.

#### Points of order 8

Because the index of the mod 8 Galois representation on \(E/F\) divides 4 = \#\(\mathcal{O}\) and \(\varphi(8) = 4\), if some \(\mathcal{O}\)-CM elliptic curve \(E/F\) has an \(F\)-rational point of order 8 then \(H(O, 8)\) holds. However, \(\Delta = -4\) is not a square in \(\mathbb{Z}/32\mathbb{Z}\), so by Theorem 5.12 no \(\mathcal{O}\)-CM \(E/F\) with a point of order 8.

#### Full \(N\)-torsion

If \(N \geq 3\) then \#\(C_N(\mathcal{O})\) > \#\(\mathcal{O}\), so we cannot have full \(N\)-torsion.

#### Subgroup \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}\)

We claim that for no \(\mathcal{O}\)-CM elliptic curve does \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}\) arise as a subgroup of \(E(F)/\text{tors}\). Above we saw that \(\mathcal{O}\)-CM elliptic curve \(E/F\) with an \(F\)-rational point of order 5 has \(\mathcal{I}(5) = 4\) and an \(\mathcal{O}\)-CM elliptic curve \(E/F\) with trivial mod 2 Galois representation has \(\mathcal{I}(2) = 2\). If we had both, then 8 \mid \mathcal{I}(10), contradicting Theorem 1.1.

Thus the groups which can occur as \(E(F)/\text{tors}\) are precisely

\[
\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}.
\]

III. Suppose \(\Delta = -3\), so \(j = 0\) and \(F = K(j) = \mathbb{Q}(\sqrt{-3})\).

- By Theorem 5.3, if \(E(F)\) has a point of order \(N\), then \(\varphi(N) \mid 6\), so

  \[
  N \in \{1, 2, 3, 4, 6, 7, 9, 14, 18\}.
  \]

#### Points of order 2

The group \(C_2(\mathcal{O})\) has order 3 and is generated by the class of \(\zeta = e^{2\pi i/6} \in \mathcal{O}\). Thus by a suitable sextic twist we may make the mod 2 Galois representation surjective onto \(C_2(\mathcal{O})\) – so there is no point of order 2 – or trivial – so \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset E(F)\). It is not possible to have exactly one point of order 2.

#### Points of order 3

The group \(C_3(\mathcal{O})\) has order 6 and is generated by the class of \(\zeta \in \mathcal{O}\). So by a suitable sextic twist we can make \(\mathcal{I}(3)\) take any value in \{1, 2, 3, 6\}. We have no \(F\)-rational points of order 3 iff \(\mathcal{I}(3) \in \{1, 3\}\), we have exactly one \(F\)-rational point of order 3 iff \(\mathcal{I}(3) = 2\) and we have full \(F\)-rational 3-torsion iff \(\mathcal{I}(3) = 6\). If we have full \(F\)-rational 3-torsion, we cannot have an \(F\)-rational point of order 2, for then \(18 \mid \mathcal{I}(6)\), contradicting Theorem 1.1.

#### Points of order 6

\(\varphi(6) = 2\) and \(H(O, 6)\) holds, there is an \(\mathcal{O}\)-CM \(E/F\) with an \(F\)-rational point of order 6, which as above forces \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \hookrightarrow E(F)\).

#### Points of order 7

By Proposition 4.3, there is an \(\mathcal{O}\)-CM \(E/F\) with an \(F\)-rational point of order 7. This forces \(\mathcal{I}(7) = 6\), and thus we cannot have a point of order 14, for that would imply \(\mathcal{I}(2) = 3\) and thus \(18 \mid \mathcal{I}(14)\), contradicting Theorem 1.1.

#### Points of order 9

Because \(\varphi(9) = 6 = \#\mathcal{O}\), if an \(\mathcal{O}\)-CM \(E/F\) had an \(F\)-rational point of order 9, then some order 9 point of \(O/9O\) has a \(C_9(\mathcal{O})\)-orbit of size 6. But \(\Delta = -3\) is not a square mod 36, so by Theorem 5.12 \(H(O, 9)\) does not hold, and there are no \(F\)-rational points of order 9, hence certainly none of order 18.

#### Full \(N\)-torsion

If \(N > 3\) then \#\(C_N(\mathcal{O}) < \#\mathcal{O}\): we cannot have full \(N\)-torsion.
Thus the groups which can occur as $E(F)[\text{tors}]$ are precisely
\[
\{e\}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.
\]

**Remark 5.16.** a) Case I. of the above calculation is a more detailed and explicit version of one of the main results of [Pa89]. Parish offers addenda on Cases II. and III., but without proof, and the possibilities $E(F)[\text{tors}] \cong \mathbb{Z}/10\mathbb{Z}$ in Case II. and $E(F)[\text{tors}] \cong \mathbb{Z}/7\mathbb{Z}$ and $E(F)[\text{tors}] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ in Case III are not mentioned. b) In Cases II. and III. a classification of the possibilities for $E(F)[\text{tors}]$ apart from the “Olson groups” $\{e\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is done in [BCS, Thm. 1.4]. We showed that in both Case II. and Case III. each occurring non-Olson group arises for a unique $E/F$ up to $F$-rational isomorphism. The older method of proof used computer calculations on degrees of preimages of $j = 0$ and $j = 1728$ on modular curves [BCS, Table 2]. The present method uses group- and ring-theoretic calculations in a way which should be much more amenable to generalization.

### 5.7. Isogenies over $K(j)$.

**Theorem 5.17.** Let $\mathcal{O}$ be an order of discriminant $\Delta = \ell^2 \Delta_K$, and let $N \in \mathbb{Z}^+$. a) If $\Delta \not\equiv -3, -4 \pmod{\mathbb{Z}}$, then there is an $\mathcal{O}$-CM elliptic curve $E_{/K(j)}$ with a $K(f)$-rational cyclic $N$-isogeny iff $\Delta$ is a square in $\mathbb{Z}/4NZ$. 

b) If $\Delta = -4$, then there is an $\mathcal{O}$-CM elliptic curve $E_{/K(j)}$ with a $K(f)$-rational cyclic $N$-isogeny iff $\Delta$ is a square in $\mathbb{Z}/4NZ$ or $N = 4$.

c) If $\Delta = -3$, then there is an $\mathcal{O}$-CM elliptic curve $E_{/K(j)}$ with a $K(f)$-rational cyclic $N$-isogeny iff $\Delta$ is a square in $\mathbb{Z}/4NZ$ or $N = 2$.

**Proof.** Step 1: Let $E_{/K(j)}$ be an $\mathcal{O}$-CM elliptic curve. If $\Delta$ is a square in $\mathbb{Z}/4NZ$, then by Theorem 5.12 there is a point $P$ of order $N$ in $\mathcal{O}/N\mathcal{O}$ such that $C = \langle P \rangle$ is invariant under $C_N(\mathcal{O})$, so $C$ is $\mathfrak{g}_{K(f)}$-stable and $E \to E/C$ is a cyclic $N$-isogeny.

If $\Delta \not\equiv -3, -4 \pmod{\mathbb{Z}}$, the projective Galois representation
\[
\mathbb{P}\rho_N : \mathfrak{g}_{K(j)} \to C_N(\mathcal{O})/(\mathbb{Z}/NZ)^\times
\]
is surjective, so $K(f)$-rational cyclic $N$-isogenies correspond to $C_N(\mathcal{O})$-orbits on $\mathcal{O}/N\mathcal{O}$ of size $\varphi(N)$, which by Theorem 5.12 exist iff $\Delta$ is a square in $\mathbb{Z}/4NZ$.

Step 2: Let $\Delta = -4$ and $K(f) = \mathbb{Q}(\sqrt{-1}) = K$. Suppose there is an $\mathcal{O}$-CM elliptic curve $E_{/K}$ with a cyclic rational $N$-isogeny. As usual we reduce immediately to the case in which $N = \ell^n$ is a prime power. If $\ell \equiv 1 \pmod{4}$, then $\Delta$ is a square in $\mathbb{Z}/4NZ$. If $\ell \equiv 3 \pmod{4}$ then $C_\ell(\mathcal{O})/(\mathbb{Z}/(\mathbb{Z})^\times$ acts transitively on the $\ell + 1 \geq 4$ order $\ell$ subgroups of $\mathcal{O}/\ell\mathcal{O}$, but index of the projective Galois representation is at most 2, so there is no rational $\ell$-isogeny. Finally suppose $\ell = 2$. We saw above that we can have a $K$-rational point of order 4 and also that there is no point of order 8 in $\mathcal{O}/8\mathcal{O}$ with a $C_8(\mathcal{O})$-orbit of size 4. Thus there is no rational 8-isogeny.

Step 3: Let $\Delta = -3$ and $K(f) = \mathbb{Q}(\sqrt{-3}) = K$. Suppose there is an $\mathcal{O}$-CM elliptic curve $E_{/K}$ with a cyclic rational $N$-isogeny where $N = \ell^n$ is a prime power. If $\ell \equiv 1 \pmod{3}$, then $\Delta$ is a square in $\mathbb{Z}/4NZ$. If $\ell \equiv 2 \pmod{3}$ then $C_\ell(\mathcal{O})/(\mathbb{Z}/(\mathbb{Z})^\times$ acts transitively on the $\ell + 1$ order $\ell$ subgroups of $\mathcal{O}/\ell\mathcal{O}$, but the index of the projective Galois representation is at most 3, so if $\ell \geq 5$ there is no rational $\ell$-isogeny. If $\ell = 2$ there is rational 2-torsion, hence a rational 2-isogeny. If there were a $K$-rational cyclic 4-isogeny, the isogeny character would have order 2 | $w_K$, and twisting by the inverse of this character would give a $K$-rational point of order 4, which was ruled out above. Similarly, there is no $K$-rational cyclic 9 isogeny: $\varphi(9) = 6 = w_K$, so this would yield a $K$-rational point of order 9, which was ruled out above. \qed

Throughout this section \( \mathcal{O} \) denotes an order in an imaginary quadratic field, of conductor \( \mathfrak{f} \) and discriminant \( \Delta = \mathfrak{f}^2 \Delta_K \). We put \( w = \# \mathcal{O}^\times \).

For \( N \in \mathbb{Z}^\geq 2 \), let \( \overline{T}(\mathcal{O}, N) \) be the least size of an orbit of \( C_N(\mathcal{O}) \) on an order \( N \) point of \( \mathcal{O}/\mathcal{O} \).

**Lemma 6.1.** We have \( \overline{T}(\mathcal{O}, 2) = \begin{cases} 1 & (\frac{\Delta}{2}) \neq -1 \\ 3 & (\frac{\Delta}{2}) = -1 \end{cases} \).

**Proof.** This is an immediate consequence of the results of §5.4 and §5.5. \( \square \)

**Theorem 6.2.** (Torsion Degree Theorem) Let \( \mathcal{O} \) be an order in \( K \) of conductor \( \mathfrak{f} \), and let \( N \in \mathbb{Z}^\geq 3 \).

a) There is a positive integer \( T(\mathcal{O}, N) \) such that:

(i) If \( F \supseteq K(\mathfrak{f}) \) is a number field and \( E_{/F} \) is an \( \mathcal{O} \)-CM elliptic curve with an \( F \)-rational point of order \( N \), then \( T(\mathcal{O}, N) \mid [F : K(\mathfrak{f})] \), and

(ii) There is a number field \( F \supseteq K(\mathfrak{f}) \) with \( [F : K(\mathfrak{f})] = T(\mathcal{O}, N) \) and an \( \mathcal{O} \)-CM elliptic curve \( E_{/F} \) with an \( F \)-rational point of order \( N \).

b) If \( (\Delta, N) = (-3, 3) \), then \( T(\mathcal{O}, N) = 1 \).

c) Suppose \( (\Delta, N) \neq (-3, 3) \). Let \( N = \ell_1^a \cdots \ell_r^a \) be the prime power decomposition of \( N \). Then

\[
T(\mathcal{O}, N) = \prod_{i=1}^r \overline{T}(\mathcal{O}, \ell_i^a)^w.
\]

d) For a prime power \( \ell^a \), the quantity \( \overline{T}(\mathcal{O}, \ell^a) \) is explicitly computed in Lemma 6.1 when \( \ell^a = 2 \), in §6.3 when \( \ell \nmid \mathfrak{f} \) and in §6.4 when \( \ell \mid \mathfrak{f} \).

**Remark 6.3.** The case \( N = 2 \) is excluded because of the somewhat anomalous behavior of \( 2 \)-torsion. But it is easy to see that Theorem 6.2a) remains true when \( N = 2 \), and moreover:

- If \( \Delta \in \{ -4, 3 \} \) then \( T(\mathcal{O}, 2) = 1 \).
- Otherwise, \( T(\mathcal{O}, 2) = \begin{cases} 1 & (\frac{\Delta}{2}) \neq -1 \\ 3 & (\frac{\Delta}{2}) = -1 \end{cases} \).

Let \( F \supseteq K(\mathfrak{f}) \) be a number field, and let \( E_{/F} \) be an \( \mathcal{O} \)-CM elliptic curve. As usual, we choose an embedding \( F \hookrightarrow \mathbb{C} \) such that \( j(E) = j(\mathbb{C}/\mathcal{O}) \). Let \( P \in E[\text{tors}] \) have order \( N \). We call the field \( K(\mathfrak{f})(h(P)) \) the **field of moduli** of \( P \). It is independent of the chosen model of \( E_{/F} \), and on some twist \( E^X \) of \( E_{/F} \) the point \( P \) is \( K(\mathfrak{f})(h(P))-\text{rational} \). Further, the pair \( (E, P) \) induces a closed point \( P \) on the modular curve \( X(X_N)_{/K} \), and \( K(\mathfrak{f})(h(P)) \) is the residue field \( K(P) \). Theorem 6.2 concerns the degree \( [K(\mathfrak{f})(h(P)) : K(\mathfrak{f})] \). Our setup shows that it is no loss of generality to assume \( F = K(\mathfrak{f}) \).

Let \( q : \mathcal{O} \to \mathcal{O}/\mathcal{O} \) be the natural map, and let \( q^\times : \mathcal{O}^\times \to C_N(\mathcal{O}) \) be the induced map on unit groups. We define the **reduced mod \( N \) Cartan subgroup**

\[
\overline{C}_N(\mathcal{O}) = C_N(\mathcal{O})/q(\mathcal{O}^\times).
\]

Let \( E[N] \) be the set of \( \mathcal{O}^\times \)-orbits on \( E[N] \). Then the action of \( C_N(\mathcal{O}) \) on \( E[N] \) induces an action of \( \overline{C}_N(\mathcal{O}) \) on \( E[N] \). The field of moduli \( K(\mathfrak{f})(h(P)) \) depends only on the image \( P \) of \( P \) in \( E[N] \).
By Theorem 1.1, the composite homomorphism
\[ g_P \xrightarrow{\rho \circ N} C_N(\mathcal{O}) \to \overline{C_N(\mathcal{O})} \]
is surjective (and model-independent). Let \( H_\mathcal{T} = \{ g \in \overline{C_N(\mathcal{O})} \mid gP = P \} \). It follows that
\[ \text{Aut}(K(\mathfrak{f})(\mathfrak{h}(P))/K(\mathfrak{f})) \cong \overline{C_N(\mathcal{O})}/H_\mathcal{T} \]
Thus \( [K(\mathfrak{f})(\mathfrak{h}(P)) : K(\mathfrak{f})] \) is the size of the orbit of the reduced Cartan subgroup \( \overline{C_N(\mathcal{O})} \) on \( \overline{P} \). (As we will see, in almost every case this is the size of the orbit of \( C_N(\mathcal{O}) \) on \( P \) divided by \( w \).) This reduces the proof of Theorem 6.2 to a purely algebraic problem.

6.2. Generalities.

For an order \( N \) point \( P \in \mathcal{O}/N\mathcal{O} \), let \( M_P = \{ xP \mid x \in \mathcal{O} \} \) be the cyclic \( \mathcal{O} \)-submodule of \( \mathcal{O}/N\mathcal{O} \) generated by \( P \). If we put \( I_P = \{ x \in \mathcal{O} \mid xP = 0 \} \), then we have
\[ M_P \cong \mathcal{O}/I_P \]
The isomorphism is canonical and determined by mapping \( P \in M_P \) to \( 1 + I_P \in \mathcal{O}/I_P \).

**Lemma 6.4.** a) With notation as above, let
\[ S(I_P) = \{ g \in C_N(\mathcal{O}) \mid g \equiv 1 \pmod{I_P} \} \]
Then with respect to the \( C_N(\mathcal{O}) \)-action, \( S(I_P) \) is the stabilizer of \( P \), so as a \( C_N(\mathcal{O}) \)-set the orbit \( C_N(\mathcal{O})/S(I_P) \) is isomorphic to \( C_N(\mathcal{O})/S(I_P) \).
b) Moreover, there is a canonical isomorphism of groups \( C_N(\mathcal{O})/S(I_P) \cong (\mathcal{O}/I_P)\times \).

**Proof.** a) For \( g \in C_N(\mathcal{O}) \), we have \( gP = P \iff (g-1)P = 0 \iff (g-1) \in I_P \), giving the first assertion. The Orbit Stabilizer Theorem gives the second assertion.
b) The ring homomorphism \( f : \mathcal{O}/N\mathcal{O} \to \mathcal{O}/I \) induces a homomorphism on unit groups \( f^\times : C_N(\mathcal{O}) \to (\mathcal{O}/I_P)^\times \), with kernel \( S(I_P) \). Since \( \mathcal{O}/N\mathcal{O} \) has finitely many maximal ideals, \( f^\times \) is surjective [CA, Thm. 4.32]. \( \square \)

**Lemma 6.5.** There is a positive integer \( M \mid N \) such that
\[ \mathcal{O}/I_P \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z} \]

**Proof.** As a \( \mathbb{Z} \)-module, \( \mathcal{O}/I_P \) is a quotient of \( \mathcal{O}/N\mathcal{O} \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \), so
\[ \mathcal{O}/I_P \cong \mathbb{Z}/N'\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z} \]
with \( M \mid M' \mid N \). Since \( P \) has order \( N \) in \( (\mathcal{O}/I_P,+), \) we have \( N' = N \). \( \square \)

The following result computes the size of the reduced Cartan orbit on an order \( N \) point of \( \mathcal{O}/N\mathcal{O} \) in terms of the size of the Cartan orbit. We recall that we have assumed \( N \geq 3 \).

**Lemma 6.6.** a) Suppose \( (\Delta,N) \not= (-3,3) \), and let \( P \in \mathcal{O}/N\mathcal{O} \) have order \( N \). Then the orbit of \( C_N(\mathcal{O}) \) on \( P \) has size \( w \) times the size of the orbit of \( \overline{C_N(\mathcal{O})} \) on \( \overline{P} \).
b) Suppose \( (\Delta,N) = (-3,3) \). Then the order 3 points of \( \mathcal{O}/N\mathcal{O} \) lie in two orbits under \( C_N(\mathcal{O}) \): one of size 2 and one of size 6. The corresponding reduced Cartan orbits each have size 1.
Proof. a) The Cartan orbit has size \( \#(O/IP)^x \), and the reduced Cartan orbit is smaller by a factor of the cardinality of the image of \( O^x \to (O/IP)^x \).

- Suppose \( \Delta \notin \{-4, -3\} \). Then \( O^x = \{\pm 1\} \), and since \( N \geq 3 \), we have \(-1 \not\equiv 1 \pmod{IP}\).
- Suppose \( \Delta = -4 \). Since \( IP \not\equiv (2) \), by Lemma 2.11 the group \( U_1(K) \) is trivial, and thus the map \( O^x \to (O/IP)^x \) is injective.
- Suppose \( \Delta = -3 \). By assumption \( N \geq 4 \), so \( IP \not\equiv (\zeta_4 - 1) \) and the map \( O^x \to (O/IP)^x \) is injective.

b) The assertion about Cartan orbits is a case of [CCRS13, Lemma 19]. (And another proof will be given in the next section.) The fact that both reduced Cartan orbits have size 1 follows from the already established fact that there is an \( O-CM \ E/\mathbb{Q}(-3) \) with full 3-torsion.


In view of Lemma 6.6, to prove Theorem 6.2 it suffices to compute the least size of an orbit of \( C_N(O) \) on an order \( N \) point of \( O/NO \) and show that this divides the size of every such orbit. The following results further reduce us to the case of \( N \) a prime power.

Lemma 6.7. a) With notation as above, let

\[
S(IP) = \{g \in C_N(O) \mid g \equiv 1 \pmod{IP}\}.
\]

Then with respect to the \( C_N(O) \)-action, \( S(IP) \) is the stabilizer of \( P \), so as a \( C_N(O) \)-set the orbit \( C_N(O)/S(IP) \) is isomorphic to \( C_N(O)/S(IP) \).

b) Moreover, there is a canonical isomorphism of groups \( C_N(O)/S(IP) \to (O/IP)^x \).

Proof. a) If \( g \in C_N(O) \) then \( gP = P \iff (g-1)P = 0 \iff (g-1) \in IP \), giving the first assertion. The Orbit Stabilizer Theorem gives the second assertion.

b) The homomorphism \( f : O/NO \to O/I \) induces a group homomorphism \( f^x : C_N(O) \to (O/IP)^x \), with kernel \( S(IP) \). Because \( O/NO \) is finite, it has finitely many maximal ideals, so \( f^x \) is surjective [CA, Thm. 4.32].

Proposition 6.8. Let \( N \geq 2 \) have prime power decomposition \( N = \ell_1^{a_1} \cdots \ell_r^{a_r} \). Let \( P \in O/NO \) have order \( N \), and let \( IP = \text{ann} \, P \). For \( 1 \leq i \leq r \), let \( P_i = \frac{N}{\ell_i} P \), and let \( I_{P_i} = \text{ann} \, P_i \). Then:

a) The ideals \( IP_1, \ldots, IP_r \) are pairwise comaximal: we have \( I_i + I_j = O \) for all \( i \neq j \).

b) We have \( IP = IP_1 \cdots IP_r \).

c) We have a canonical isomorphism of rings

\[
O/IP \cong \prod_{i=1}^r O/IP_i
\]

which induces a canonical isomorphism of unit groups

\[
(O/IP)^x \cong \prod_{i=1}^r (O/IP_i)^x.
\]

d) The Cartan orbit of \( P \) is isomorphic, as a \( C_N(O) \)-set, to the direct product of the \( C_{e_i}(O) \)-orbits of the \( P_i \)’s.

Proof. a) For \( 1 \leq i \leq r \), we have \( (O/IP_i, +) \cong \mathbb{Z}/\ell_i^{a_i} \mathbb{Z} \oplus \mathbb{Z}/\ell_i^{b_i} \mathbb{Z} \) with \( 0 \leq b_i \leq a_i \); in particular it is an \( \ell_i \)-group. Thus for \( i \neq j \), \( (O/(I_i + I_j), +) \) is a homomorphic image of an \( \ell_i \)-group and an \( \ell_j \)-group, so it is trivial. b) By the Chinese Remainder Theorem, we have \( IP_1 \cdots IP_r = \bigcap_{i=1}^r IP_i \).

Since \( P \) is a multiple of \( P_i \), we have \( IP \supset IP_i \) for all \( i \), and thus \( IP \supset \bigcap_{i=1}^r IP_i \). Conversely, choose \( y_1, \ldots, y_r \in \mathbb{Z} \) such that \( \sum_{i=1}^r y_i \ell_i^{a_i} = 1 \). If \( x \in \bigcap_{i=1}^r IP_i \) then \( x \ell_i^{a_i} P = 0 \) for all \( i \), hence

\[
0 = \sum_{i=1}^r y_i \ell_i^{a_i} xP = xP.
\]
Thus there are two Cartan orbits, one of size $\ell$ for $i = a$. The Chinese Remainder Theorem gives the first isomorphism; the second follows by passing to unit groups. d) Apply Lemma 6.7 and part c).

6.3. The Case $\ell \nmid f$.

**Theorem 6.9.** Let $E_{/K(f)}$ be an $O$-CM elliptic curve. Let $\ell^a > 2$ be a prime power such that $\ell \nmid f$. We will describe all orbits of $C_{\ell^a}(O)$ on order $\ell^a$ points of $O/\ell^a$: their sizes and their multiplicities.

a) If $(\frac{\Delta}{\ell}) = 1$, there are $2a + 1$ orbits: an orbit of size $\varphi(\ell^a)\varphi(\ell^a)$ and, for all $0 \leq i \leq a - 1$, two Cartan orbits of size $\varphi(\ell^a)\varphi(\ell)$.

b) If $(\frac{\Delta}{\ell}) = 0$, there are two orbits: an orbit of size $\varphi(\ell^a)\varphi(\ell^a - 1)$ and an orbit of size $\varphi(\ell^a)\varphi(\ell^a)$.

c) If $(\frac{\Delta}{\ell}) = -1$, there is one orbit, of size $\varphi(\ell^a)$.

**Proof.** Step 1: We suppose $O = O_K$. Then every $O$-submodule of $E[N]$ is of the form $E[I]$ for an ideal $I \supset NO$, and we have $E[I] \cong O/I$: thus every submodule is of the form $M_P = \langle P \rangle_O$ and is determined by its annihilator ideal $I_P$.

**Split Case** $(\frac{\Delta}{\ell}) = 1$: Then $\ell O = p_1 p_2$ for distinct prime ideals $p_1, p_2$ of norm $\ell$. The ideals containing $\ell^a O$ are precisely $p_1^a p_2$ with $\max(c, d) = a$. We have

$O/p_1^a p_2 \cong O/p_1^a \times O/p_2 \cong \mathbb{Z}/\ell^a \mathbb{Z} \times \mathbb{Z}/\ell^a \mathbb{Z}$,

$(O/p_1^a p_2)^\times \cong (O/p_1^a)^\times \times (O/p_2)^\times \cong (\mathbb{Z}/\ell^a \mathbb{Z})^\times \times (\mathbb{Z}/\ell^a \mathbb{Z})^\times$.

To get points of order $\ell^n$ we impose the condition $\max(c, d) = a$. Thus $O$-modules generated by the points of order $\ell^n$ are

$E[p_1^a], E[p_1^a p_2], \ldots, E[p_1^a p_2^b] = E[\ell^n], E[p_1^{-1} p_2], \ldots, E[p_1 p_2], E[p_2^2]$.

So there are $2a + 1$ Cartan orbits, one of size $\varphi(\ell^a)\varphi(\ell^a)$ and, for all $0 \leq i \leq a - 1$, two of size $\varphi(\ell^a)\varphi(\ell^a)$.

**Ramified Case** $(\frac{\Delta}{\ell}) = 0$: Then $\ell O = p^a$ for a prime ideal $p$ of norm $\ell$. The ideals containing $\ell^a O$ are $p^b$ for $b \leq a$. If $b = 2i$ is even, then

$O/p^b \cong O/\ell^b \mathbb{Z} \cong \mathbb{Z}/\ell^b \mathbb{Z} \times \mathbb{Z}/\ell^b \mathbb{Z}$,

$(O/p^b)^\times \cong (\mathbb{Z}/\ell^b \mathbb{Z})^\times \times (\mathbb{Z}/\ell^b \mathbb{Z})^\times$.

If $b = 2i - 1$ is odd, then

$O/p^b \cong \mathbb{Z}/\ell^b \mathbb{Z} \times \mathbb{Z}/\ell^b \mathbb{Z}$,

$(O/p^b)^\times \cong (\mathbb{Z}/\ell^b \mathbb{Z})^\times \times (\mathbb{Z}/\ell^b \mathbb{Z})^\times$.

To get points of order $\ell^n$ we take $b = 2a, b = 2a - 1$. The $O$-modules generated by the points of order $\ell^n$ are

$E[p_1^{2a-1}], E[p_2^{2a}] = E[\ell^n]$.

Thus there are two Cartan orbits, one of size $\varphi(\ell^a)\varphi(\ell^a - 1)$ and one of size $\varphi(\ell^a)\varphi(\ell^a)$. The smallest orbit size is $\varphi(\ell^a)\varphi(\ell^a - 1)$ and the other orbit size is a multiple of it.

**Inert Case** $(\frac{\Delta}{\ell}) = -1$: Then $\ell O$ is a prime ideal, so the ideals containing $\ell^a O$ are precisely $\ell O$ for $i \leq a$. Clearly $O/\ell^a O$ has exponent $\ell^a$ iff $i = a$, so the $O$-module generated by any point of order $\ell^a$ is $E[\ell^n]$. There is a single Cartan orbit, of size $\#(O/\ell^a O) = \varphi_K(\ell^a)$.

Step 2: Now let $O$ be an order with $\ell \nmid f$. The natural maps $O/\ell^a O \to O_K/\ell^a O_K$ and $C_{\ell^a}(O) \to C_{\ell^a}(O_K)$ are isomorphisms, so the sizes and multiplicities of orbits carry over from $O_K$ to $O$. □
6.4. The Case $\ell | f$.

Now suppose $\ell | f$. The ring $O/\ell O$ is isomorphic to $\mathbb{Z}/\ell \mathbb{Z}[t]/(t^2)$ – as one sees, e.g., using the explicit representation of (3) – and is thus a local Artinian ring with maximal ideal $p$, say, and residue field $\mathbb{Z}/\ell \mathbb{Z}$. Because $[p : \ell O] = \ell$, the only proper nonzero $O$-submodule of $O/\ell O$ is $p/\ell$.

Thus there are two Cartan orbits on the order $\ell$ elements of $O/\ell O$: one of order $\ell - 1$ and one of order $\ell^2 - \ell = \#(O/\ell O)^\times$.

For all $a \in \mathbb{Z}^+$, the ring $O/\ell^a O$ is local – for a maximal ideal $m$ of $O$, we have $\ell^a \in m \iff \ell \in m$ – with residue field $\mathbb{Z}/\ell \mathbb{Z}$. It turns out that for any order $\ell^a$ point $P \in O/\ell^a O$ and $I_P = \{x \in O \mid xP = 0\}$, the ring $O/I_P$ is local with residue field $\mathbb{Z}/\ell \mathbb{Z}$. By Lemma 6.5, we may write

$$M_P = O/I_P \cong \mathbb{Z}/\ell \mathbb{Z} \oplus \mathbb{Z}/\ell^b \mathbb{Z}$$

for some $0 \leq b \leq a$, and then

$$\#((O/I_P)^\times) = \#O/I_P - \frac{\#O/I_P}{\ell} = \varphi(\ell^{a+b}).$$

So the size of a Cartan orbit on an order $\ell^a$ element of $O/\ell^a O$ is of the form $(\ell - 1)\ell^c$ for some $a - 1 \leq c \leq 2a - 1$. So in this case it is a priori clear that the minimal size of a Cartan orbit divides the size of all the Cartan orbits. We want to understand how Cartan orbits grow when we lift a point of order $\ell^a$ to a point of order $\ell^{a+1}$. First observe that $x \mapsto \ell x$ gives an $O$-module isomorphism $O/\ell^a O \cong \ell O/\ell^{a+1} O$.

so we can view $O/\ell^a O$ as an $O$-submodule of $O/\ell^{a+1} O$. With $P$ as in (13), let $Q \in O/\ell^{a+1} O$ be such that $\ell Q = P$. Put $M_Q = \{xQ \mid x \in O\}$ and $I_Q = \{x \in O \mid xQ = 0\}$, and write

$$M_Q = O/I_Q \cong \mathbb{Z}/\ell^{a+1} \mathbb{Z} \oplus \mathbb{Z}/\ell^b \mathbb{Z}$$

for $0 \leq b' \leq a + 1$. Because $\ell Q = P$, we have $\ell M_Q = M_P$. Thus we find: if $b = 0$, then $b' \in \{0, 1\}$, whereas if $b \geq 1$ then necessarily $b' = b + 1$. So: if the $C_{\ell a}(O)$-orbit on $P$ has the smallest possible $\varphi(\ell^a)$, then the $C_{\ell a+1}(O)$-orbit on $Q$ either has size $\varphi(\ell^{a+1})$ or size $\varphi(\ell^{a+2})$ (as we will see shortly, both possibilities can occur), whereas if the $C_{\ell a}(O)$-orbit on $P$ has size $\varphi(\ell^a) > \varphi(\ell^a)$, then the $C_{\ell a+1}(O)$-orbit on $Q$ has size $\varphi(\ell^{a+b+2})$: i.e., upon lifting from $P$ to $Q$ the size grows by a factor of $\ell^2$.

Since $H(O, \ell^{a+1})$ implies $H(O, \ell^a)$, for each fixed $\ell$ and $O$ there are two possibilities.

**Type I:** $H(O, \ell^a)$ holds for all $a \in \mathbb{Z}^+$.

In Type I, for all $a \in \mathbb{Z}^+$ the least size of a $C_{\ell a}(O)$-orbit is $\varphi(\ell^a)$.

**Type II:** There is some $A \in \mathbb{Z}^+$ such that $H(O, \ell^a)$ holds iff $a < A$.

In Type II, for $1 \leq a \leq A$, the least size of a $C_{\ell a}(O)$-orbit is $\varphi(\ell^a)$, but for all $a > A$, whenever we lift a point of order $\ell^a$ to a point of order $\ell^{a+1}$ the size of the Cartan orbit grows by a factor of $\ell^2$, so for all $a > A$ the least size of a $C_{\ell a}(O)$-orbit is $\ell^{a-A} \varphi(\ell^a)$.

We now determine the smallest size of a $C_{\ell a}(O)$-orbit on an order $\ell^a$ point of $O/\ell^a O$ by using Theorem 5.12 to determine the type and compute the value of $A$ in Type II.

**Case 1:** Suppose $(\Delta_K) = 1$. Then for all $a \in \mathbb{Z}^+$ $H(O_K, \ell^a)$ holds, so $\Delta_K$ is a square modulo $4\ell^a$, hence $\Delta = \ell^2 \Delta_K$ is also a square modulo $4\ell^a$, so $H(O, \ell^a)$ holds, and we are in Type I.

**Case 2:** Suppose $(\Delta_K) = -1$, and put $k = \text{ord}_{\ell}(f)$.

• Let $\ell > 2$. If $a \leq 2k$, then $\ell^a | \Delta$, so $\Delta$ is a square mod $\ell^a$ and hence also mod $4\ell^a$: thus
$H(\mathcal{O}, \ell^a)$ holds. However, if $a = 2k + 1$ then we claim $H(\mathcal{O}, \ell^a)$ does not hold. Indeed, suppose there is $s \in \mathbb{Z}$ such that $\Delta = \ell^a \Delta_K \equiv s^2 \pmod{\ell^a}$. Then $\ell^k \mid s$; taking $S = \frac{s^2}{\ell^k}$ we have $\frac{s^2}{\ell^k} \Delta_K \equiv S^2 \pmod{\ell^{a-2k}}$, which implies that $\Delta_K$ is a square modulo $\ell$: contradiction. So we are in Type II with $A = 2k$.

- Let $\ell = 2$, and write $f = 2^k F$. Suppose $a \leq 2k$. Since $4 \mid \Delta_K - 1$, we have

$$2^{a+2} \mid (2^k F)^2 \Delta_K = \Delta - (2^k F)^2,$$

so $H(\mathcal{O}, 2^a)$ holds. Suppose $a \geq 2k + 1$. If $\Delta$ is a square modulo $2^a$, then we find that $\Delta_K \equiv 1 \pmod{8}$, so $(\frac{\Delta_K}{2}) = 1$: contradiction. So we are in Type II with $A = 2k$.

**Case 3:** Suppose $(\frac{\Delta_K}{2}) = 0$, and put $k = \text{ord}_\ell(f)$.

- Let $\ell > 2$. If $a \leq 2k + 1$, then $\ell^a \mid \Delta$, so $\Delta$ is a square mod $\ell^a$ and hence also mod $4\ell^a$: thus $H(\mathcal{O}, \ell^a)$ holds. However, if $a = 2k + 2$ then we claim $H(\mathcal{O}, \ell^a)$ does not hold. Indeed, $\text{ord}_\ell(\Delta) = 2k + 1 < a$, so if $\Delta \equiv s^2 \pmod{\ell^a}$, then $\text{ord}_\ell(s^2) = 2k + 1$: contradiction. So we are in Type II with $A = 2k + 1$.

- Let $\ell = 2$, and write $f = 2^k F$. Suppose $a \leq 2k + 1$. Since $4 \mid s^2$, there is $s \in \mathbb{Z}$ such that $8 \mid \Delta_K - s^2$, so

$$2^{a+2} \mid 2^{2k+3} \mid (2^k F)^2 (\Delta_K - s^2) = \Delta - (2^k F s)^2,$$

so $H(\mathcal{O}, 2^a)$ holds. Suppose $a \geq 2k + 2$. If $\Delta$ is a square modulo $2^{a+2}$, then $\Delta_K$ is a square modulo $2^{a+2-2k}$, hence modulo 16: contradiction. So we are in Type II with $A = 2k + 1$.

**References**


