An investigation into constants associated with Elliptic Curves over finite fields

Alexander Milner [1], supervised by Dr Jack Shotton [2]
University of Durham

Abstract

Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$, then we can define a constant $\mathcal{C}_{\mathcal{E},j}$ for positive integer j, which controls the density of rational primes p, such that the group of $\mathbb{F}_p$-rational points on $\mathcal{E}$ has full j-torsion ie. a subgroup of the form $(\mathbb{Z}/j\mathbb{Z})^2$. In this paper, we give a condition on when $\mathcal{C}_{\mathcal{E},j} = 0$, given by $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[2j])$ plus a small condition on the intersection of $\mathbb{Q}(\mathcal{E}[j])$ with a certain root of unity. This is proved using a re-framing of the definition of $\mathcal{C}_{\mathcal{E},j}$ using Galois representations to provide some new insight and results. We also provide a fix to a longstanding proof in [CoMu] as well as derive a formula for $\mathcal{C}_{\mathcal{E},j}$ depending just on the size of division fields that divide the adelic level.

1 Introduction to elliptic curves

An *elliptic curve* $\mathcal{E}$ defined over $\mathbb{Q}$, is a curve of the form

$$\mathcal{E} : y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{Z}$ are such that the discriminant $\Delta_{\mathcal{E}}$ is non-zero, together with an extra point at infinity, which we denote $\mathcal{O}$, given in projective coordinates as $[0 : 1 : 0]$. For a field K, we denote the set of K-rational points on $\mathcal{E}$ together with $\mathcal{O}$ by $\mathcal{E}(K)$.

Astoundingly, we can define a finitely-generated abelian group structure on $\mathcal{E}(K)$, simply by specifying the geometric condition that the sum of three points on the curve is $\mathcal{O}$ if and only if those three points lie on a straight line. In particular, if $\mathcal{E}$ is defined over $\mathbb{Q}$, then we can talk about the group $\mathcal{E}(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

Division fields of Elliptic Curves

Let $\mathcal{E}$ be an elliptic curve. For an arbitrary integer k, we denote the *group of k-torsion points* by $\mathcal{E}[k] \coloneqq \{P \in \mathcal{E}(\overline{\mathbb{Q}}) : kP = \mathcal{O}\}$. If we adjoin to $\mathbb{Q}$ the x and y coordinates of the k-torsion points, then we obtain a finite Galois extension of $\mathbb{Q}$. We denote this extension by $\mathbb{Q}(\mathcal{E}[k])$ and call it the *k-division field* of $\mathcal{E}$.

Below are some useful lemmas regarding division fields which we will use repeatedly later on.

Lemma 1.1. *For $a, b \in \mathbb{N}$, $\mathbb{Q}(\mathcal{E}[a]) \subseteq \mathbb{Q}(\mathcal{E}[ab])$.*

[1] alexander.milner@durham.ac.uk
[2] jack.g.shotton@durham.ac.uk

Lemma 1.2. *For* $a, b \in \mathbb{N}$, $\mathbb{Q}(\mathcal{E}[a])(\mathcal{E}[b]) = \mathbb{Q}(\mathcal{E}[lcm(a,b)])$.

Lemma 1.3. $\forall n \in \mathbb{N}$, $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\mathcal{E}[n])$.

Proof. See [Wash, Theorem 3.9]. □

Elliptic curves defined over Finite Fields $\mathbb{F}_p$

Following [Co2], we can now define the reduction of an elliptic curve $\mathcal{E}$ modulo p for $p > 3$,

$$\mathcal{E}_p : y^2 \equiv x^3 + ax + b \pmod{p}.$$

There is an integer associated with every elliptic curve $\mathcal{E}$ called the conductor of $\mathcal{E}$ and denoted N. One of the most useful properties of the conductor is that $\mathcal{E}_p$ is smooth if and only if $p \nmid N$ and we call primes p, satisfying this property, *primes of good reduction for* $\mathcal{E}$. Then, for p a prime of good reduction, $\mathcal{E}_p$ is an elliptic curve defined over $\overline{\mathbb{F}}_p$.

The classical theory of elliptic curves provides us with lots of information about $\mathcal{E}_p(\mathbb{F}_p)$ for p prime. For k a positive integer, we define the group of $\overline{\mathbb{F}}_p$-torsion points denoted $\mathcal{E}_p(\overline{\mathbb{F}}_p)[k] \coloneqq \{P \in \mathcal{E}_p(\overline{\mathbb{F}}_p) : kP = \mathcal{O}\}$ and then we have that:

- if p|k, $\mathcal{E}_p(\overline{\mathbb{F}}_p)[k] \cong \mathcal{O}$ or $\mathbb{Z}/k\mathbb{Z}$,
- else, $\mathcal{E}_p(\overline{\mathbb{F}}_p)[k] \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$.

Then $\mathcal{E}_p(\mathbb{F}_p)$ can be viewed as a subgroup of $\mathcal{E}_p(\overline{\mathbb{F}}_p)[k]$ for some k such that $\#\mathcal{E}_p(\mathbb{F}_p)|k$ meaning that we can write

$$\mathcal{E}_p(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \times \mathbb{Z}/e_p\mathbb{Z}$$

where d_p and e_p are uniquely determined positive integers with $d_p|e_p$.

Complex Multiplication

From now on, let $\mathcal{E}$ be a fixed elliptic curve over $\mathbb{Q}$. There are some natural maps we can define over $\mathcal{E}(\overline{\mathbb{Q}})$, which turn out to be group homomorphisms, called isogenies of $\mathcal{E}$ over $\mathbb{Q}$. Denote the ring of isogenies of $\mathcal{E}$ over $\mathbb{Q}$ by $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathcal{E})$. There are two possibilities for elliptic curves defined over $\mathbb{Q}$; for an elliptic curve $\mathcal{E}$, if:

- $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathcal{E}) \cong \mathbb{Z}$, we say $\mathcal{E}$ is *without Complex Multiplication*, often stated just as $\mathcal{E}$ is non-CM,
- $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathcal{E})$ is isomorphic to an order in a quadratic imaginary number field, we say $\mathcal{E}$ is *with Complex Multiplication*, stated as $\mathcal{E}$ has CM.

Serre's Open Image Theorem

We naturally have an injective representation called the *Galois representation* associated to $\mathcal{E}[k]$, given by

$$\rho_k : \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[k])/\mathbb{Q}) \to Aut(\mathcal{E}[k]) \cong \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}).$$

In 1972, J.P. Serre showed that for any non-CM elliptic curve $\mathcal{E}$, there exists a positive integer $A(\mathcal{E})$, depending on the elliptic curve $\mathcal{E}$, such that ρ_k is surjective for

any integer k coprime to $A(\mathcal{E})$ [Ser, Théorème 2]. Therefore, for such an $\mathcal{E}$ and k, we have $[\mathbb{Q}(\mathcal{E}[k])/\mathbb{Q}] = \#\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$.

Using the theory of Galois representations, we can get a more tangible constant associated to each elliptic curve $\mathcal{E}$, which we call the *adelic level* of $\mathcal{E}$, often just called the level of $\mathcal{E}$, and denote it by $m_{\mathcal{E}}$ where $m_{\mathcal{E}} \in \langle 2A(\mathcal{E})\rangle := \{k \in \mathbb{N} : p|k \Rightarrow p|2A(\mathcal{E}), p \text{ prime}\}$. Two useful properties of $m_{\mathcal{E}}$ are that, 2 always divides $m_{\mathcal{E}}$ and if k is coprime to $m_{\mathcal{E}}$ then ρ_k is surjective. The precise definition of the level $m_{\mathcal{E}}$ is given in Section 4.

Notation

We summarise some of the key notation used throughout this paper:

- For p prime and integer a, $p^{a_p}||a$ implies that a_p is the largest power of p that divides a. That is, if $p^{a_p}||a$, then $a_p = \max\{n \in \mathbb{Z}_{\geq 0} : p^n|a\}$.
- We denote the *Möbius function* by $\mu(n)$ which returns 0 if n is square-free otherwise it returns $(-1)^k$ where k is the number of prime factors of n.
- For a positive integer b with prime factors $p_i|b$ for $1 \leq i \leq n$, define $rad(b) := \prod_{i=1}^{n} p_i$.
- The degree of the k-th division field over $\mathbb{Q}$ is given by $L_k := [\mathbb{Q}(\mathcal{E}[k]) : \mathbb{Q}]$.
- Using angle bracket notation, we let $\langle c\rangle := \{k \in \mathbb{N} : p|k \Rightarrow p|c, p \text{ prime}\}$.
- We denote the commutator of the group G by $[G, G] := \{xyx^{-1}y^{-1} : x, y \in G\}$.
- For a positive integer k, we denote the general linear group over the k-th cyclic group by $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}) = \{M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/k\mathbb{Z}) : \det(M) \in (\mathbb{Z}/k\mathbb{Z})^\times\}$.
- The cardinality of the group $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ is given by

$$\psi(n) := \#\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}) = k^4 \prod_{\substack{q|k \\ q \text{ prime}}} \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right)$$

2 The constant $\mathcal{C}_{\mathcal{E}}$

Definition 2.1. *We define* $\mathcal{C}_{\mathcal{E}}$ *as*

$$\mathcal{C}_{\mathcal{E}} = \sum_{k=1}^{\infty} \frac{\mu(k)}{L_k}$$

Theorem 2.2 (Co2, Theorem 1). *Let* $\mathcal{E}$ *be a non-CM elliptic curve defined over* $\mathbb{Q}$ *with conductor* N. *Under the assumption of the generalised Riemann hypothesis (GRH) for the Dedekind zeta functions of the division fields* $\mathbb{Q}(\mathcal{E}[k])$ *of* $\mathcal{E}$

$$\#\{p \leq x : p \nmid N, \mathcal{E}_p(\mathbb{F}_p) \text{ cyclic}\} \sim \mathcal{C}_{\mathcal{E}}\, Li(x)$$

Proposition 2.3 (Kim, Prop. 3.1). *For* $\mathcal{E}$ *a non-CM curve, let* $k = hj$ *with* $h \in \langle m_{\mathcal{E}}\rangle$ *and* $(j, m_{\mathcal{E}}) = 1$. *Also for* p *prime, let* $p^{h_p}||h$ *and* $p^{m_p}||m_{\mathcal{E}}$. *Then* $L_k = L_h L_j = L_h\psi(j)$. *Furthermore, setting* $h_1 = (h, m_{\mathcal{E}})$, *we have*

$$L_h = L_{h_1} \prod_{p|h} p^{4(h_p - m_p)}$$

Corollary 2.4 (Kim, Cor. 3.1). *For $\mathcal{E}$ a non-CM curve, we have*

$$\mathcal{C}_{\mathcal{E}} = \left(\sum_{k | rad(m_{\mathcal{E}})} \frac{\mu(k)}{L_k} \right) \prod_{\substack{p \nmid m_{\mathcal{E}} \\ p \, prime}} \left(1 - \frac{1}{\psi(p)} \right)$$

Proof. We only have to worry about the square-free terms in the sequence, and if $k = hj$ where $h | rad(m_{\mathcal{E}})$ and $(j, m_{\mathcal{E}}) = 1$, then $L_k = L_h \psi(j)$. We then use that $\psi(x)$ is multiplicative. □

Lemma 2.5. *For $a, b, j \in \mathbb{N}$, if $(a, m_{\mathcal{E}}) = 1$, then $\mathbb{Q}(\mathcal{E}[aj]) \cap \mathbb{Q}(\mathcal{E}[bj]) = \mathbb{Q}(\mathcal{E}[j])$*

Proof. Since $\mathbb{Q}(\mathcal{E}[k])$ is Galois over $\mathbb{Q}$ for all k, then we have

$$[\mathbb{Q}(\mathcal{E}[aj]) \cap \mathbb{Q}(\mathcal{E}[bj]) : \mathbb{Q}] = \frac{L_{aj} L_{bj}}{L_{abj}} = \frac{L_a L_j L_{bj}}{L_a L_{bj}} = L_j$$

by Lemma 2.3. Then since $\mathbb{Q}(\mathcal{E}[j]) \subseteq \mathbb{Q}(\mathcal{E}[aj]) \cap \mathbb{Q}(\mathcal{E}[bj])$ by Lemma 1.1, the result follows. □

Lemma 2.6 (CoMu, Lemma 6.1). *Let $\mathcal{F} = (\mathcal{M}_q)_{q \in \mathcal{P}}$, $\mathcal{F}' = (\mathcal{M}'_q)_{q \in \mathcal{P}'}$ be two families of finite Galois extensions of a number field $\mathcal{M}$, indexed over sets of rational primes $\mathcal{P}' \subseteq \mathcal{P}$. For any square-free integer k composed of primes from $\mathcal{P}$ or $\mathcal{P}'$, define*

- $\mathcal{M}_k := \prod_{\substack{q | k \\ q \in \mathcal{P}}} \mathcal{M}_q$ *and* $\mathcal{M}'_k := \prod_{\substack{q | k \\ q \in \mathcal{P}'}} \mathcal{M}'_q$
- $N_k := [\mathcal{M}_k : \mathcal{M}]$ *and* $N'_k := [\mathcal{M}'_k : \mathcal{M}]$ *where* $N_1 = N'_1 = 1$
- $\delta(\mathcal{F}) := \sum_{\substack{k \\ q | k \Rightarrow q \in \mathcal{P}}} \frac{\mu(k)}{N_k}$ *and* $\delta(\mathcal{F}') := \sum_{\substack{k \\ q | k \Rightarrow q \in \mathcal{P}'}} \frac{\mu(k)}{N'_k}$.

In addition, we assume that,

- *$\mathcal{F}$ covers $\mathcal{F}'$, ie. $\forall q' \in \mathcal{P}'$, $\exists q \in \mathcal{P} : L'_{q'} \subseteq L_q$ and $\forall q \in \mathcal{P}$, $\exists q' \in \mathcal{P}' : L'_{q'} \subseteq L_q$*
- $\sum_{\substack{k \, sq.free \\ q | k \Rightarrow q \in \mathcal{P}}} \frac{1}{N_k} < \infty$ *and* $\sum_{\substack{k \, sq.free \\ q | k \Rightarrow q \in \mathcal{P}'}} \frac{1}{N'_k} < \infty$

Then $\delta(\mathcal{F}) \geq \delta(\mathcal{F}')$.

The corollary [CoMu, Corollary 6.2] given after [CoMu, Lemma 6.1] is not quite true. We actually need a slightly stronger condition than just the fields in $\mathcal{F}'$ being mutually independent[3], which we give below.

Corollary 2.7. *If the fields $\mathcal{M}'_k$ are mutually independent over $\mathcal{M}$ for all k square-free where $p | k \Rightarrow p \in \mathcal{P}'$ for all p prime, then*

$$\delta(\mathcal{F}) \geq \prod_{q \in \mathcal{P}'} \left(1 - \frac{1}{N'_q} \right)$$

Luckily, it is still possible to resurrect the resulting proof in [CoMu, Chapter 6] by considering an additional case.

Theorem 2.8. *Let $\mathcal{E}$ be a non-CM curve. Then $\mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q} \Rightarrow \mathcal{C}_{\mathcal{E}} > 0$.*

[3] Recall $\mathcal{F}'$ contains just the fields $\mathcal{M}'_q$ for primes $q \in \mathcal{P}'$, whereas in Corollary 2.7 we need mutual independence of $\mathcal{M}'_k$ where k can be a product of primes from $\mathcal{P}'$.

Proof. Let $\mathcal{P}$ be the rational primes and let $\mathcal{M}_q = \mathbb{Q}(\mathcal{E}[q])$ for $q \in \mathcal{P}$. We then note that $\mathcal{M}_k = \mathbb{Q}(\mathcal{E}[k])$ for all square-free integers k by Lemma 1.2. We now define K_2 as the unique abelian sub-extension contained in $\mathbb{Q}(\mathcal{E}[2])$ where by assumption, K_2 is not trivial. We now define

$$\mathcal{M}'_q := \begin{cases} \mathcal{M}_q \text{ if } q \nmid m_{\mathcal{E}}, \\ \mathbb{Q}(\zeta_q) \text{ if } q \mid m_{\mathcal{E}},\ q \neq 2,\ \mathbb{Q}(\zeta_q) \cap K_2 = \mathbb{Q}, \\ K_2 \text{ if } q = 2 \text{ or } q \mid m_{\mathcal{E}},\ q \neq 2,\ \mathbb{Q}(\zeta_q) \cap K_2 \neq \mathbb{Q}. \end{cases}$$

where $\mathcal{P}'$ is defined by removing all except one of the primes with the field K_2 from $\mathcal{P}'$. $2|m_{\mathcal{E}}$ for all elliptic curves $\mathcal{E}$ so we can always take $\mathcal{P}' = \{q \text{ prime} : \mathbb{Q}(\zeta_q) \cap K_2 = \mathbb{Q}\}$. We also note that using a combination of Lemma 1.3, the properties of cyclotomic fields and Lemma 2.5 where we set $j = 1$, all the fields in the first two cases given above are mutually independent over $\mathbb{Q}$. Finally, define two integers: R, as the product of all primes in the second case given above ie. primes $p|m_{\mathcal{E}}$ where $p \neq 2$ and $\mathbb{Q}(\zeta_p) \cap K_2 = \mathbb{Q}$ and S, as the minimal integer dividing R such that $K_2 \subseteq \mathbb{Q}(\zeta_S)$. If there is no such integer S, then the families $\mathcal{F}$ and $\mathcal{F}'$ as defined above fulfil the conditions of Corollary 2.7 and in this case, since $\mathcal{M}'_q \neq \mathbb{Q}\ \forall q \in \mathcal{P}'$, we have

$$\mathcal{C}_{\mathcal{E}} = \delta(\mathcal{F}) \geq \prod_{q \in \mathcal{P}'} \left(1 - \frac{1}{N'_q}\right) > 0.$$

In the other case where there exists a minimal integer S such that $K_2 \subseteq \mathbb{Q}(\zeta_S)$, let $\phi(x)$ be Euler's totient function and let $d = [K_2 : \mathbb{Q}]$, where we note $d \neq 1$. Then for $k|R$, we have, $N'_k = \phi(k)$, $N'_{2k} = d\phi(k)$ for $S \nmid k$ and $N'_{2k} = \phi(k)$ for $S|k$. Thus

$$\begin{aligned} \sum_{k|R} \mu(k) \left(\frac{1}{N'_k} - \frac{1}{N'_{2k}}\right) &= \sum_{k|R} \mu(k) \left(\frac{1}{\phi(k)} - \frac{1}{d\phi(k)}\right) + \sum_{k|\frac{R}{S}} \mu(Sk) \left(\frac{1}{d\phi(Sk)} - \frac{1}{\phi(Sk)}\right) \\ &= \left(1 - \frac{1}{d}\right) \prod_{\substack{p|R \\ p \text{ prime}}} \left(1 - \frac{1}{\phi(p)}\right) - \frac{\mu(S)}{\phi(S)} \left(1 - \frac{1}{d}\right) \sum_{k|\frac{R}{S}} \frac{\mu(k)}{\phi(k)} \\ &= \left(1 - \frac{1}{d}\right) \left(\prod_{\substack{p|R \\ p \text{ prime}}} \left(1 - \frac{1}{\phi(p)}\right) - \frac{\mu(S)}{\phi(S)} \prod_{\substack{p|\frac{R}{S} \\ p \text{ prime}}} \left(1 - \frac{1}{\phi(p)}\right) \right) \\ &\geq \frac{1}{\phi(S)} \left(1 - \frac{1}{d}\right) \prod_{\substack{p|\frac{R}{S} \\ p \text{ prime}}} \left(1 - \frac{1}{\phi(p)}\right) \left(\prod_{\substack{p|S \\ p \text{ prime}}} (\phi(p) - 1) - 1 \right) \\ &> 0 \end{aligned}$$

since $S \geq 3$. Finally, by Lemma 2.6, and since $\mathcal{M}'_q \neq \mathbb{Q}\ \forall q \in \mathcal{P}'$,

$$\mathcal{C}_{\mathcal{E}} = \delta(\mathcal{F}) \geq \delta(\mathcal{F}') = \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}'}} \frac{\mu(k)}{N'_k} = \sum_{k|R} \mu(k) \left(\frac{1}{N'_k} - \frac{1}{N'_{2k}}\right) \prod_{\substack{p \nmid m_{\mathcal{E}} \\ p \text{ prime}}} \left(1 - \frac{1}{N'_p}\right) > 0$$

□

3 The constant $\mathcal{C}_{\mathcal{E},j}$

Definition 3.1. *For j a positive integer, we define $\mathcal{C}_{\mathcal{E},j}$ as*

$$\mathcal{C}_{\mathcal{E},j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{L_{jk}}$$

Theorem 3.2 (Co2, Theorem 2). *Let $\mathcal{E}$ be a non-CM elliptic curve defined over $\mathbb{Q}$ with conductor N and let j be a postive integer. Under the assumption of the generalised Riemann hypothesis (GRH) for the Dedekind zeta functions of the division fields $\mathbb{Q}(\mathcal{E}[k])$ of $\mathcal{E}$*

$$\#\{p \leq x : p \nmid jN, d_p = j\} \sim \mathcal{C}_{\mathcal{E},j}\, Li(x)$$

Proposition 3.3. *For $\mathcal{E}$ a non-CM curve, let $m = jn$, where $j \in \langle m_{\mathcal{E}} \rangle$ and $(n, m_{\mathcal{E}}) = 1$. Then,*

$$\mathcal{C}_{\mathcal{E},m} = \frac{1}{\psi(n)} \left(\sum_{k | rad(m_{\mathcal{E}})} \frac{\mu(k)}{L_{jk}} \right) \prod_{\substack{p \nmid m_{\mathcal{E}} \\ p\ prime}} \left(1 - \frac{\psi(n)}{\psi(pn)} \right)$$

Proof. For k square-free, assume $k = rs$, where $r | rad(m_{\mathcal{E}})$ and $(s, m_{\mathcal{E}}) = 1$, then $L_{mk} = L_{jr}\psi(ns)$ by Proposition 2.3 since $(ns, m_{\mathcal{E}}) = 1$. We then use that $\psi(x)$ is multiplicative. □

Corollary 3.4. *For $\mathcal{E}$ a non-CM curve, let $m = jn$, where $j \in \langle m_{\mathcal{E}} \rangle$ and $(n, m_{\mathcal{E}}) = 1$. Then,*

$$\mathcal{C}_{\mathcal{E},m} = 0 \Leftrightarrow \mathcal{C}_{\mathcal{E},j} = 0 \Leftrightarrow \sum_{k | rad(m_{\mathcal{E}})} \frac{\mu(k)}{L_{jk}} = 0$$

Proof. For $a, b \in \mathbb{N}$, $b \geq 2$, we have $\psi(a) < \psi(ab)$. Thus $\frac{\psi(n)}{\psi(pn)} < 1\ \forall p$ prime. □

Lemma 3.5 (DL, Theorem 1.4). *For elliptic curve $\mathcal{E}$, prime p and positive integer n, if $\mathbb{Q}(\zeta_{p^{n+1}}) \subseteq \mathbb{Q}(\mathcal{E}[p^n])$, then $p = 2$.*

Theorem 3.6. *Let $\mathcal{E}$ be a non-CM elliptic curve, let $m = jn$, where $j \in \langle m_{\mathcal{E}} \rangle$ and $(n, m_{\mathcal{E}}) = 1$. Then, if $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[pj])$ for any prime p, then $\mathcal{C}_{\mathcal{E},m} = 0$.*

Proof. We know that $p | m_{\mathcal{E}}$ as otherwise we would have $L_{jp} = L_j L_p \neq L_j$ by Proposition 2.3, Lemma 1.3 and since $2 | m_{\mathcal{E}}$ for all elliptic curves $\mathcal{E}$. Letting $p^{m_p} || m_{\mathcal{E}}$, then

$$\sum_{k | rad(m_{\mathcal{E}})} \frac{\mu(k)}{L_{jk}} = \sum_{k | rad(\frac{m_{\mathcal{E}}}{p^{m_p}})} \mu(k) \left(\frac{1}{L_{jk}} - \frac{1}{L_{pjk}} \right) = 0$$

if $L_{jk} = L_{pjk}\ \forall k | rad(\frac{m_{\mathcal{E}}}{p^{m_p}})$. By Lemma 1.1, $\mathbb{Q}(\mathcal{E}[kj]) \subseteq \mathbb{Q}(\mathcal{E}[pkj])$. To see the other inclusion, we let $p^{j_p} || j$ and $j = p^{j_p} s$. Then by assumption and by Lemma 1.2, we have $\mathbb{Q}(\mathcal{E}[p^{j_p+1}])(\mathcal{E}[s]) = \mathbb{Q}(\mathcal{E}[pj]) = \mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[p^{j_p}])(\mathcal{E}[s])$. This means $\mathbb{Q}(\mathcal{E}[p^{j_p+1}]) \subseteq \mathbb{Q}(\mathcal{E}[p^{j_p}])(\mathcal{E}[s]) \subseteq \mathbb{Q}(\mathcal{E}[p^{j_p}])(\mathcal{E}[ks])$. Finally, since $p \nmid k$, we have $\mathbb{Q}(\mathcal{E}[pkj]) = \mathbb{Q}(\mathcal{E}[p^{j_p+1}])(\mathcal{E}[ks]) \subseteq \mathbb{Q}(\mathcal{E}[p^{j_p}])(\mathcal{E}[ks]) = \mathbb{Q}(\mathcal{E}[kj])$. Thus, we have $L_{kj} = L_{pkj}\ \forall k | rad(\frac{m_{\mathcal{E}}}{p^{m_p}})$, and the result follows by Corollary 3.4. □

In [CoMu, Chapter 6], a short proof is given that, for a non-CM elliptic curve $\mathcal{E}$ if $\mathcal{C}_{\mathcal{E}} \neq 0$ then $\mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q}$ which is dependent on GRH. However with Theorem 3.6, we can remove this constraint.

Corollary 3.7. *Let $\mathcal{E}$ be a non-CM curve. Then $\mathcal{C}_{\mathcal{E}} = 0 \Leftrightarrow \mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}$.*

Proof. The $\Rightarrow$ direction is given by Theorem 2.8. For $\Leftarrow$, take Theorem 3.6 with $m = 1$, and the result follows. □

Corollary 3.8. *Let $\mathcal{E}$ be a non-CM curve. For a positive integer n, if $(n, m_{\mathcal{E}}) = 1$, then $C_{E,n} = 0 \Leftrightarrow \mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}$.*

Proof. Using Corollary 3.4 together with Corollary 3.7, the result follows. □

In Theorem 3.2, we see that we must have $\mathcal{C}_{\mathcal{E},m} \geq 0$. However we can, in fact, give an unconditional proof of this using familiar techniques.

Proposition 3.9. *Let $\mathcal{E}$ be a non-CM curve. Then, for all positive integers m, $\mathcal{C}_{\mathcal{E},m} \geq 0$.*

Proof. By Proposition 3.3, if $m = jn$ where $j \in \langle m_{\mathcal{E}} \rangle$ and $(n, m_{\mathcal{E}}) = 1$ then $\mathcal{C}_{\mathcal{E},m} \geq 0 \Leftrightarrow \mathcal{C}_{\mathcal{E},j} \geq 0$ so we only have to consider $\mathcal{C}_{\mathcal{E},j}$. We can now use Corollary 2.7, by defining two new families of fields $\mathcal{F}$ and $\mathcal{F}'$. Firstly, let $\mathcal{P}$ be the set of rational primes, then, for any positive integer j, let $\mathcal{M} = \mathbb{Q}(\mathcal{E}[j])$ and let $\mathcal{M}_q = \mathbb{Q}(\mathcal{E}[jq])$ for $q \in \mathcal{P}$. Similarly to before we note that $M_k = \mathbb{Q}(\mathcal{E}[kj])$ for all square-free integers k by Lemma 1.2. We now define

$$\mathcal{M}'_q := \begin{cases} \mathcal{M}_q \text{ if } q \nmid m_{\mathcal{E}}, \\ \mathcal{M} \text{ if } q | m_{\mathcal{E}}. \end{cases}$$

where as before, we can remove all $q | m_{\mathcal{E}}$ from $\mathcal{P}'$ except one. $2 | m_{\mathcal{E}}$ for all elliptic curves $\mathcal{E}$ so we can always take $\mathcal{P}' = \{q \text{ prime} : q \nmid m_{\mathcal{E}}\} \cup \{2\}$. $\mathcal{F}$ and $\mathcal{F}'$ now satisfy the requirements of Lemma 2.6. Also, since $\mathcal{M}_q \cap \mathcal{M}_p = \mathcal{M}$ for all primes $p, q \nmid m_{\mathcal{E}}$ by Lemma 2.5, the conditions of Corollary 2.7 are satisfied and thus

$$\mathcal{C}_{\mathcal{E},j} \geq \prod_{q \in \mathcal{P}'} \left(1 - \frac{1}{N'_q}\right) = 0.$$

□

We can now use the level of an elliptic curve $\mathcal{E}$ to reduce the amount of work we need to do to in order to calculate $\mathcal{C}_{\mathcal{E},j}$ depending on how nice a given j's properties are.

Lemma 3.10. *If $j \in \langle m_{\mathcal{E}} \rangle$, then*

$$L_j = L_{(m_{\mathcal{E}}, j)} \left(\frac{j}{(m_{\mathcal{E}}, j)}\right)^4$$

Proof. Let $f = (m_{\mathcal{E}}, j)$ and for p prime, $p^{j_p}||j$, $p^{m_p}||m_{\mathcal{E}}$ and $p^{f_p}||f$. Then using Proposition 2.3,

$$\frac{L_j}{L_f} = \prod_{\substack{p|j \\ j_p > m_p}} p^{4(j_p - m_p)} = \prod_{p|j} p^{4(j_p - f_p)} = \left(\frac{j}{f}\right)^4,$$

since $j_p \leq m_p \Leftrightarrow j_p - f_p = 0$. □

Corollary 3.11. *If $m_{\mathcal{E}}|j$, then*

$$\frac{L_j}{L_{m_{\mathcal{E}}}} = \left(\frac{j}{m_{\mathcal{E}}}\right)^4$$

Proposition 3.12. *For $j \in \langle m_{\mathcal{E}} \rangle$,*

$$\mathcal{C}_{\mathcal{E},j} = 0 \Leftrightarrow \sum_{k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}},j)}} = 0$$

Proof. Let $j = gh$ where g is maximal such that $\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},g)}, g\right) = 1$ and let $d = (m_{\mathcal{E}}, g)$, then

$$\sum_{k|rad(m_{\mathcal{E}})} \frac{\mu(k)}{L_{jk}} = \sum_{k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \sum_{l|rad(d)} \frac{\mu(kl)}{L_{jkl}}.$$

Now, we use that for $k|rad(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)})$ and $l|rad(d)$, $(k,l) = 1$ with the multiplicativity of $\mu(x)$ and also that $(jkl, m_{\mathcal{E}}) = (\frac{j}{g}k, m_{\mathcal{E}})(gl, m_{\mathcal{E}}) = (hk, m_{\mathcal{E}})(gl, m_{\mathcal{E}}) = hkd = k(m_{\mathcal{E}}, j)$ since $(\frac{j}{g}k, gl) = 1$, $hk|m_{\mathcal{E}}$ and $l|g$. Thus, using Lemma 3.10 replacing j with jkl, we have

$$\begin{aligned}
&= \sum_{k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \sum_{l|rad(d)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}},j)}} \frac{\mu(l)}{\left(\frac{jl}{(m_{\mathcal{E}},j)}\right)^4} \\
&= \left(\sum_{k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}},j)}}\right) \left(\sum_{l|rad(d)} \frac{\mu(l)}{l^4}\right) \left(\frac{(m_{\mathcal{E}},j)}{j}\right)^4 \\
&= \left(\frac{(m_{\mathcal{E}},j)}{j}\right)^4 \prod_{\substack{p|d \\ p\ prime}} \left(1 - \frac{1}{p^4}\right) \left(\sum_{k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}},j)}}\right).
\end{aligned}$$

Thus combining with Corollary 3.4, the result follows. □

Corollary 3.13. *If $m_{\mathcal{E}}|j$, then $\mathcal{C}_{\mathcal{E},j} > 0$.*

Proof. Assuming $m_{\mathcal{E}}|j$, we have $(m_{\mathcal{E}}, j) = m_{\mathcal{E}}$ meaning that $\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}, j\right) = (1, g) = 1$ so in the notation of Proposition 3.12, $j = g$ and $h = 1$. But,

$$\sum_{k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}},j)}} = \frac{1}{L_{m_{\mathcal{E}}}} > 0$$

so by Proposition 3.12, $\mathcal{C}_{\mathcal{E},j} > 0$. □

Remark 3.14. *It is interesting to note that to compute $\mathcal{C}_{\mathcal{E},m}$ for any m a positive integer, we only need to calculate the size of division fields L_k for $k|m_{\mathcal{E}}$.*

Proof. With notation as in Proposition 3.3 and Proposition 3.12, we can write

$$\mathcal{C}_{\mathcal{E},m} = \frac{1}{\psi(n)} \left(\frac{(m_{\mathcal{E}}, j)}{j} \right)^4 \prod_{\substack{q \nmid m_{\mathcal{E}} \\ q \text{ prime}}} \left(1 - \frac{\psi(n)}{\psi(qn)} \right) \prod_{\substack{p|d \\ p \text{ prime}}} \left(1 - \frac{1}{p^4} \right) \left(\sum_{k | rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}}, j)} \right)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}}, j)}} \right).$$

In addition, for $k|rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)$, we have that $(hk, d) = 1$ and $hk|m_{\mathcal{E}}$ by the maximality of g meaning $hkd|m_{\mathcal{E}}$ thus $k(m_{\mathcal{E}}, j)|m_{\mathcal{E}}$. □

4 Re-framing the problem using Galois representations

Precise definition of the level

As always, let $\mathcal{E}$ be a non-CM elliptic curve. To obtain a precise definition for the level $m_{\mathcal{E}}$, following [FK], we let the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on the k-torsion group $\mathcal{E}[k]$ of $\mathcal{E}$, inducing an injective representation $\rho_k : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(\mathcal{E}[k]) \cong GL_2(\mathbb{Z}/k\mathbb{Z})$.

With $T_\ell(E)$ denoting the ℓ-adic Tate module of $\mathcal{E}$, the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\prod_\ell \mathrm{Aut}\left(T_\ell(\mathcal{E})\right) \cong \prod_\ell \mathrm{GL}_2\left(\mathbb{Z}_\ell\right)$ induces a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_\ell \mathrm{GL}_2\left(\mathbb{Z}_\ell\right)$. By Serre's open image theorem [Ser, Théorème 3], the image of ρ is open, and, since $\prod_\ell \mathrm{GL}_2\left(\mathbb{Z}_\ell\right)$ is compact, the image is of finite index.

We now let

$$G := \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_\ell \mathrm{GL}_2\left(\mathbb{Z}_\ell\right) = \mathrm{GL}_2(\hat{\mathbb{Z}})$$

be the inverse limit over all n, and let H be the image under ρ in G ie. $H := \rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq G$. For all integers $n \geq 1$, there is thus a natural projection map from G to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which we denote $\mathrm{mod}_n : G \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let $\Gamma_n := \ker(\mathrm{mod}_n)$. Then by Serre's open image theorem [Ser, Théorème 3], since $|G : H| < \infty$, $\Gamma_n < H$ for some n, and we let the level $m_{\mathcal{E}}$ be the smallest such n.

To summarise, for any positive integer n, we have the commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\ \rho\ } & G \\ & \searrow^{\rho_n} & \downarrow \mathrm{mod}_n \\ & & \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \end{array}$$

and since $H \hookrightarrow G \twoheadrightarrow G/\Gamma_n \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, $L_n = |H/H \cap \Gamma_n|$.

We now present an equivalent definition of the level $m_{\mathcal{E}}$.

Lemma 4.1. *For any positive integer n, $\Gamma_n \leq H \Leftrightarrow H = \mathrm{mod}_n^{-1}(H \,\mathrm{mod}_n)$*

Proof. For the $\Rightarrow$ direction, let $g \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ such that $g \bmod_n = h \bmod_n$ for some $h \in H$, then $g^{-1}h \bmod_n = \mathbb{I} \bmod_n$. By assumption, $g^{-1}h \in H$ and thus $g \in H$. For the $\Leftarrow$ direction, since $\mathbb{I} \in H$, then $\Gamma_n = \bmod_n^{-1}(\mathbb{I}) \leq H$. □

Corollary 4.2. *Let $\mathcal{E}$ be a non-CM elliptic curve and k a positive integer where $k|m_E$, then*

$$L_k = |H/H \cap \Gamma_k| = \frac{|H \bmod_{m_\mathcal{E}}|}{|H \bmod_{m_\mathcal{E}} \cap \Gamma_k \bmod_{m_\mathcal{E}}|}.$$

Proof. By definition of the level $m_\mathcal{E}$ and the fact that $H \bmod_{m_\mathcal{E}}$ is a finite group, the result follows. □

Lemma 4.3. *Let $\mathcal{E}$ be a non-CM elliptic curve and $j \in \langle m_\mathcal{E} \rangle$. Let p_i be the prime factors of $\frac{m_\mathcal{E}}{(m_\mathcal{E}, j)}$ where $i \in \{1, ..., r\}$. Then, denoting $H' = H \bmod_{m_\mathcal{E}}$ and, for k a positive integer, $\Gamma'_k = \Gamma_k \bmod_{m_\mathcal{E}}$*

$$\left| \bigcup_{i=1}^{r} H' \cap \Gamma'_{jp_i} \right| = |H' \cap \Gamma'_j| - \sum_{k|p_1 ... p_r} \mu(k)|H' \cap \Gamma'_{kj}|.$$

Proof. We take as our induction hypothesis, that for distinct primes p_i where $p_i|\frac{m_\mathcal{E}}{(m_\mathcal{E}, j)}$, $i \in \{1, ..., n\}$,

$$\left| \bigcup_{i=1}^{n} H' \cap \Gamma'_{jp_i} \right| = |H' \cap \Gamma'_j| - \sum_{k|p_1 ... p_n} \mu(k)|H' \cap \Gamma'_{kj}|.$$

Suppose, for the base case that $p|\frac{m_\mathcal{E}}{(m_\mathcal{E}, j)}$. Then

$$|H' \cap \Gamma'_{jp}| = |H' \cap \Gamma'_j| - |H' \cap \Gamma'_j| + |H' \cap \Gamma'_{jp}| = |H' \cap \Gamma'_j| - \sum_{k|p} \mu(k)|H' \cap \Gamma'_{kj}|.$$

Now assume the hypothesis is true for n prime factors and let $p_{n+1}|\frac{m_\mathcal{E}}{(m_\mathcal{E}, j)}$ where $p_{n+1} \neq p_i \ \forall i \in \{1, ..., n\}$. Now,

$$\begin{aligned}
\left| \bigcup_{i=1}^{n+1} H' \cap \Gamma'_{jp_i} \right| &= \left| H' \cap \Gamma'_{jp_{n+1}} \cup \bigcup_{i=1}^{n} H' \cap \Gamma'_{jp_i} \right| \\
&= |H' \cup \Gamma'_{jp_{n+1}}| + \left| \bigcup_{i=1}^{n} H' \cap \Gamma'_{jp_i} \right| - \left| H' \cap \Gamma'_{jp_{n+1}} \cap \bigcup_{i=1}^{n} H' \cap \Gamma'_{jp_i} \right| \\
&= |H' \cup \Gamma'_{jp_{n+1}}| + |H' \cap \Gamma'_j| - \sum_{k|p_1 ... p_n} \mu(k)|H' \cap \Gamma'_{kj}| - \left| \bigcup_{i=1}^{n} H' \cap \Gamma'_{jp_{n+1}p_i} \right| \\
&= |H' \cup \Gamma'_{jp_{n+1}}| + |H' \cap \Gamma'_j| - \sum_{k|p_1 ... p_n} \mu(k)|H' \cap \Gamma'_{kj}| \\
&\quad - |H' \cap \Gamma'_{jp_{n+1}}| + \sum_{k|p_1 ... p_n} \mu(k)|H' \cap \Gamma'_{kp_{n+1}j}| \\
&= |H' \cap \Gamma'_j| - \sum_{k|p_1 ... p_{n+1}} \mu(k)|H' \cap \Gamma'_{kj}|
\end{aligned}$$

□

Corollary 4.4. *Let $\mathcal{E}$ be a non-CM elliptic curve and m a positive integer such that $m = jn$, where $j \in \langle m_{\mathcal{E}} \rangle$ and $(n, m_{\mathcal{E}}) = 1$. Then*

$$\mathcal{C}_{\mathcal{E},m} = 0 \Leftrightarrow H' \cap \Gamma'_j = \bigcup_{p \mid \frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}} H' \cap \Gamma'_{jp}.$$

Proof. Dividing by $|H' \cap \Gamma'_j|$, rearranging and using Corollary 4.2, we have that

$$1 - \frac{\left|\bigcup_{p \mid \frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}} H' \cap \Gamma'_{jp_i}\right|}{|H' \cap \Gamma'_j|} = \sum_{k \mid p_1 \dots p_r} \mu(k) \frac{|H' \cap \Gamma'_{kj}|}{|H' \cap \Gamma'_j|} = L_j \sum_{k \mid rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \frac{\mu(k)}{L_{kj}}$$

$$= L_j \sum_{k \mid rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}\right)} \frac{\mu(k)}{L_{k(m_{\mathcal{E}},j)}}$$

Then, using Proposition 3.12, the result follows from the fact that

$$\bigcup_{i=1}^{r} H' \cap \Gamma'_{jp_i} \subseteq H' \cap \Gamma'_j.$$

□

Definition 4.5. *Let $\mathcal{D}_k$ denote the determinant modulo k map*

$$\mathcal{D}_k : G \to (\mathbb{Z}/k\mathbb{Z})^\times,$$
$$g \mapsto \det g \bmod_k .$$

Lemma 4.6. *For positive integer k where $k | m_{\mathcal{E}}$, we have $\mathcal{D}_k = \rho_k \circ \Delta_k \circ \rho_{m_{\mathcal{E}}}^{-1}$ for maps*

$$\Delta_k : \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[m_{\mathcal{E}}])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}),$$

$$\mathcal{D}_k : H \bmod_{m_{\mathcal{E}}} \to (\mathbb{Z}/k\mathbb{Z})^\times.$$

Proof. The map Δ_k is induced by the inclusion $\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\mathcal{E}[m_{\mathcal{E}}])$ by Lemma 1.3. Then, by [Zy, Lemma 1.7], we have $H \bmod_{m_{\mathcal{E}}} \cap \mathrm{SL}_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z}) = [H \bmod_{m_{\mathcal{E}}}, H \bmod_{m_{\mathcal{E}}}] \leq \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[m_{\mathcal{E}}])/\mathbb{Q}(\zeta_k))$ meaning the only element in $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ with determinant 1 is the identity. Thus, if we take two distinct non-trivial elements $g, h \in \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$, we have $\det g \neq \det h$, since otherwise $\det gh^{-1} = 1$, so $gh^{-1} = \mathbb{I}$ which is a contradiction. Thus the result follows. □

Corollary 4.7. *For positive integer n, $\det(\rho_n(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proposition 4.8. *For positive integers j and k with $kj | m_{\mathcal{E}}$,*

$$\mathbb{Q}(\zeta_{jk}) \cap \mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\zeta_{jk})^{\mathcal{D}_{kj}(H \cap \Gamma_j)}.$$

Proof. Using Lemma 4.6 and the Galois correspondence,

$$\mathbb{Q}(\zeta_{jk})^{H \cap \Gamma_j} = \mathbb{Q}(\mathcal{E}[m_{\mathcal{E}}])^{H \cap \Gamma_j} \cap \mathbb{Q}(\zeta_{jk}) = \mathbb{Q}(\mathcal{E}[j]) \cap \mathbb{Q}(\zeta_{jk})$$
$$= \mathbb{Q}(\zeta_{jk})^{\mathcal{D}_{kj}(H \cap \Gamma_j)}.$$

□

Corollary 4.9. *For positive integers j and k with $kj|m_{\mathcal{E}}$,*

$$\mathbb{Q}(\mathcal{E}[j]) \cap \mathbb{Q}(\zeta_{jk}) = \mathbb{Q}(\zeta_j) \Leftrightarrow \mathcal{D}_{kj}(H \cap \Gamma_j) = (\mathbb{Z}/k\mathbb{Z})^{\times}.$$

Lemma 4.10 (Goursat's Lemma). *Let G_1 and G_2 be two groups and let K be a subgroup of $G_1 \times G_2$ so that the projection maps $p_1 : K \to G_1$ and $p_2 : K \to G_2$ are surjective. Let N_1 and N_2 be the normal subgroups of G_1 and G_2, respectively, for which $\ker(p_2) = N_1 \times \{1\}$ and $\ker(p_1) = \{1\} \times N_2$. Then the image of K in $(G_1 \times G_2)/(N_1 \times N_2) = G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $G_1/N_1 \xrightarrow{\sim} G_2/N_2$.*

Theorem 4.11. *Let $\mathcal{E}$ be a non-CM elliptic curve and $j \in \langle m_{\mathcal{E}} \rangle$. Then for $2^{m_2} || \frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}$ and $R := rad\left(\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)2^{m_2}}\right) j$, if $\mathbb{Q}(\mathcal{E}[j]) \cap \mathbb{Q}(\zeta_R) = \mathbb{Q}(\zeta_j)$ and $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j])$, then $\mathcal{C}_{\mathcal{E},j} > 0$.*

Proof. Define primes p_i, and integers a_i for $i \in \{1, .., r\}$ such that $\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)} = \prod_{i=1}^{r} p_i^{a_i}$. Also for p prime, let $p^{j_p} || j$, $p^{m_p} || m_{\mathcal{E}}$, and for k a positive integer, denote $H' = H \bmod_{m_{\mathcal{E}}}$ and $\Gamma'_k = \Gamma_k \bmod_{m_{\mathcal{E}}}$. Since $H' \cap \Gamma'_j \leq \mathrm{GL}_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z}) = \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}/p^{m_p}\mathbb{Z})$, we can construct a map $H' \cap \Gamma'_j \to \prod_{i=1}^{r} \mathrm{GL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$ where if $p|m_{\mathcal{E}}$ but $p \nmid \frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}$, $\mathrm{GL}_2(\mathbb{Z}/p^{m_p}\mathbb{Z}) \to \mathbb{I}$.

If $2 \notin \{p_i : 1 \leq i \leq r\}$, then, using Corollary 4.9, we can show that $\exists g \in H' \cap \Gamma'_j$ such that $\mathcal{D}_{pj}(g) \neq 1$ thus $g \notin H' \cap \Gamma'_{pj}$ for all primes $p|\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}$. Thus by Corollary 4.4, the result follows.

If $2 \in \{p_i : 1 \leq i \leq r\}$, without loss of generality let $p_1 = 2$. We can write $H' \cap \Gamma'_k \leq \mathrm{GL}_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/2^{a_1}\mathbb{Z}) \times \prod_{i=2}^{r} \mathrm{GL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$ where we denote $H_k^{im} = \mathrm{Im}(H' \cap \Gamma'_k \to \mathrm{GL}_2(\mathbb{Z}/2^{a_1}\mathbb{Z}))$ with the map induced by the inclusion above. Thus, using Corollary 4.2, $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j]) \Rightarrow L_{2j} \neq L_j \Rightarrow L_{2j_2+1} \neq L_{2j_2} \Rightarrow |H' \cap \Gamma'_{2j_2+1}| \neq |H' \cap \Gamma'_{2j_2}| \Rightarrow H_{2j}^{im} \neq H_j^{im} \Rightarrow \exists$ a group H_j^{ab} where $H_{2j}^{im} \leq H_j^{ab} \trianglelefteq H_j^{im}$ and H_j^{im}/H_j^{ab} is a non-trivial abelian group. We can now define the map $\pi : H' \cap \Gamma'_j \to H_j^{ab} \times \prod_{i=1}^{r} (\mathbb{Z}/p_i^{j_{p_i}+1}\mathbb{Z})^{\times}$, $g \mapsto (h, \prod_{i=1}^{r} \mathcal{D}_{p_i^{j_{p_i}+1}}(g))$ where $h \in H_j^{ab}$.

We now invoke Goursat's Lemma, where, in the notation of Lemma 4.10, $G_1 = H_j^{ab}$, $G_2 = \prod_{i=1}^{r} (\mathbb{Z}/p_i^{j_{p_i}+1}\mathbb{Z})^{\times} = \mathcal{D}_{Pj}(H \cap \Gamma_j)$ and $K = \pi(H' \cap \Gamma'_j) \leq G_1 \times G_2$. We then have projection maps p_1 and p_2 giving rise the normal subgroups N_1 and N_2.

By Goursat's Lemma, we have a surjective homomorphism $\Psi : G_2 \to H_j^{ab}/N_1$ restricted to elements of K. Let $x := (x_2, ..., x_r) \in G_2$. If $x_k = 1$ for some k, take $y_k \in \mathcal{D}_{p_k^{j_{p_k}+1}}(H \cap \Gamma_j)$ where $y_k \neq 1$, and $g_n, h_n \in \mathcal{D}_{p_n^{j_{p_n}+1}}(H \cap \Gamma_j)$ where $g_n h_n = x_n$ and $g_n, h_n \neq 1$ $\forall n \in \{2, ..., r\} \setminus \{k : x_k = 1\}$. Now, for $n \in \{2, ..., r\} \setminus \{k : x_k = 1\}$ and $i \in \{k : x_k = 1\}$, let $y := (..., g_n, ..., y_i, ...)$ and $z := (..., h_n, ..., {y_i}^{-1}, ...)$, where $y, z \in G_2$. If $\Psi(y) \neq \mathbb{I}$ or $\Psi(z) \neq \mathbb{I}$, $\pi^{-1}((\Psi(y), y))$ or $\pi^{-1}((\Psi(z), z)) \notin H' \cap \Gamma'_{pj}$ for all primes $p|\frac{m_{\mathcal{E}}}{(m_{\mathcal{E}},j)}$ and thus by Corollary 4.4, the result follows. Thus, in the other case, $\Psi(x) = \Psi(yz) = \Psi(y)\Psi(z) = \mathbb{I}$.

The only case that this argument fails for is if $j_3 = 0$ and, letting $p_2 = 3$, $x := (2, x_3, ..., x_r)$ since if k is odd, $|(\mathbb{Z}/k\mathbb{Z})^{\times}| \leq 2 \Rightarrow k = 3$. However, we can take $y := (2, ..., g_n, ...)$ and $z := (2, ..., h_n, ...)$ from before and multiply by $w := (2, ..., f_n, ...)$ where $f_n = x_n {g_n}^{-1} {h_n}^{-1}$ where we choose $g_n, h_n \neq 1$ such that $x_n \neq g_n h_n$. Then, assuming $\Psi(y) = \Psi(z) = \Psi(w) = \mathbb{I}$, otherwise the result follows as before, $\Psi(x) = \Psi(yzw) = \Psi(y)\Psi(z)\Psi(w) = \mathbb{I}$.

However, since x was arbitrary and Ψ was surjective, $H_j^{ab}/N_1 = \mathbb{I}$. Now $\exists g \in K$ such that $p_1(g) \neq \mathbb{I}$ but $p_2(g) = \mathbb{I}$. But, reasoning as before, we can also find an element $k \in G_2$ where k is not the identity in every component and thus $\pi^{-1}(gk) \notin H' \cap \Gamma'_{pj}$ for all primes $p|\frac{m_\mathcal{E}}{(m_\mathcal{E},j)}$ and thus by Corollary 4.4, the result follows. □

Corollary 4.12. *Let $\mathcal{E}$ be a non-CM elliptic curve and m a positive integer. Then, for $m = jn$ where $j \in \langle m_\mathcal{E} \rangle$, $(n, m_\mathcal{E}) = 1$ and for $2^{m_2}||\frac{m_\mathcal{E}}{(m_\mathcal{E},j)}$ and $R := rad\left(\frac{m_\mathcal{E}}{(m_\mathcal{E},j)2^{m_2}}\right) j$, if $\mathbb{Q}(\mathcal{E}[j]) \cap \mathbb{Q}(\zeta_R) = \mathbb{Q}(\zeta_j)$ then $\mathcal{C}_{\mathcal{E},m} = 0 \Leftrightarrow \mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[2j])$.*

5 Some mildly interesting elliptic curves

The data about the elliptic curves below was very kindly provided by the LMFDB and curve $\mathcal{E}_\mathcal{E}$ was given as an example in DL.

- $\mathcal{E}_\mathcal{A} : y^2 = x^3 - 3x + 4$
  - The non-CM elliptic curve $\mathcal{E}_\mathcal{A}$ has the properties that $L_2 = 6$ and $m_\mathcal{E} = 4$. Thus by Corollary 3.13 and Corollary 3.4, $\mathcal{C}_{\mathcal{E}_\mathcal{A},m} > 0\ \forall m \in \mathbb{N}$.
- $\mathcal{E}_\mathcal{B} : y^2 = x^3 + 45x + 366$
  - The non-CM elliptic curve $\mathcal{E}_\mathcal{B}$ has the property that $\mathbb{Q}(\mathcal{E}_\mathcal{B}[2]) = \mathbb{Q}(\mathcal{E}_\mathcal{B}[3])$.
- $\mathcal{E}_\mathcal{C} : y^2 = x^3 - 7x + 6$
  - The non-CM elliptic curve $\mathcal{E}_\mathcal{C}$ has the property that $\mathbb{Q}(\mathcal{E}_\mathcal{C}[2]) = \mathbb{Q}$.
- $\mathcal{E}_\mathcal{D} : y^2 = x^3 - 2700x + 37125$
  - The non-CM elliptic curve $\mathcal{E}_\mathcal{D}$ has the property that $\mathbb{Q}(\mathcal{E}_\mathcal{D}[2]) = \mathbb{Q}(\sqrt{5})$, where $\mathbb{Q}(\mathcal{E}_\mathcal{D}[2]) \subseteq \mathbb{Q}(\mathcal{E}_\mathcal{D}[3])$ and $\mathbb{Q}(\mathcal{E}_\mathcal{D}[2]) \subseteq \mathbb{Q}(\mathcal{E}_\mathcal{D}[5])$. Thus, by Theorem 3.6, $\mathcal{C}_{\mathcal{E}_\mathcal{D},3} = \mathcal{C}_{\mathcal{E}_\mathcal{D},5} = 0$.
- $\mathcal{E}_\mathcal{E} : y^2 = x^3 - 27x - 1674$
  - The non-CM elliptic curve $\mathcal{E}_\mathcal{E}$ has the property that $\mathbb{Q}(\zeta_9) \subseteq \mathbb{Q}(\mathcal{E}_\mathcal{E}[7])$ and since $R = 45$ then $\mathbb{Q}(\mathcal{E}_\mathcal{E}[7]) \cap \mathbb{Q}(\zeta_{7R}) \neq \mathbb{Q}(\zeta_7)$ since $\mathbb{Q}(\zeta_{63}) \subset \mathbb{Q}(\mathcal{E}_\mathcal{E}[7])$ and $\mathbb{Q}(\zeta_{63}) \subset \mathbb{Q}(\zeta_{7R})$ which invalidates the necessary condition for the main theorem for $\mathcal{E}_\mathcal{E}$.

Non-theorems

Non-Theorem 5.1. *For all non-CM elliptic curves $\mathcal{E}$ and integers $a < b$, $\mathbb{Q}(\mathcal{E}[b]) \not\subseteq \mathbb{Q}(\mathcal{E}[a])$*

Counterexample: $\mathcal{E}_\mathcal{B}$

Non-Theorem 5.2. *For a non-CM elliptic curve $\mathcal{E}$ and primes p and q, $\mathbb{Q}(\mathcal{E}[p]) \cap \mathbb{Q}(\mathcal{E}[q]) \subseteq \mathbb{Q}(\zeta_{pq})$.*

Counterexample: $\mathcal{E}_\mathcal{D}$ taking $p = 2$, $q = 3$.

Non-Theorem 5.3. *Let $\mathcal{E}$ be a non-CM curve. Then for positive integers j and k, where k is odd, $\mathbb{Q}(\zeta_{kj}) \cap \mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\zeta_j)$.*

Counterexample: $\mathcal{E}_\mathcal{E}$ taking $j = 7$, $k = 9$.

6 What can we say about $\mathcal{C}_{\mathcal{E},j}$ generally?

Proposition 6.1. *Given a positive integer m where $6 \nmid m$, there exists a non-CM elliptic curve $\mathcal{E}$ such that $\mathcal{C}_{\mathcal{E},m} = 0$.*

Proof. If m is odd then take any elliptic curve $\mathcal{E}$ with $\mathbb{Q} = \mathbb{Q}(\mathcal{E}[2])$, for example, $\mathcal{E}_C$. Then using Lemma 1.2, $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[2m])$ and thus the result follows by Theorem 3.6. If j is even, by assumption $3 \nmid j$, so taking curve $\mathcal{E}_B$ which has the property that $\mathbb{Q}(\mathcal{E}_B[2]) = \mathbb{Q}(\mathcal{E}_B[3])$, again using Lemma 1.2, $\mathbb{Q}(\mathcal{E}_B[3j]) = \mathbb{Q}(\mathcal{E}_B[3]) \cup \mathbb{Q}(\mathcal{E}_B[j]) = \mathbb{Q}(\mathcal{E}_B[2]) \cup \mathbb{Q}(\mathcal{E}_B[j]) = \mathbb{Q}(\mathcal{E}_B[j])$ so the result follows by Theorem 3.6. □

Theorem 6.2 (Kronecker-Weber Theorem). *Every finite abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field.*

Proposition 6.3. *For non-CM elliptic curve $\mathcal{E}$, if $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) \in \{\mathbb{I}, \mathbb{Z}/3\mathbb{Z}\}$, then there are infinitely many positive integers m, where $\mathcal{C}_{\mathcal{E},m} = 0$.*

Proof. If $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) \cong \mathbb{I}$, then $\mathbb{Q} = \mathbb{Q}(\mathcal{E}[2])$. For any odd integer m, using Lemma 1.2, we have $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[2m])$ and thus the result follows by Theorem 3.6.

If $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, then by the Kronecker-Weber Theorem, Theorem 6.2, $\mathbb{Q}(\mathcal{E}[2]) \subseteq \mathbb{Q}(\zeta_R)$ for some odd positive integer R. We can require that R be odd as since L_2 is odd, $\mathbb{Q}(\mathcal{E}[2]) \cap \mathbb{Q}(\zeta_{2^r}) = \mathbb{Q}$ for positive integer r as $[\mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{r-1}$. Thus $\mathbb{Q}(\mathcal{E}[2]) \subseteq \mathbb{Q}(\zeta_R) \subseteq \mathbb{Q}(\mathcal{E}[R])$ by Lemma 1.3. Now, using Lemma 1.2, we have $\mathbb{Q}(\mathcal{E}[R]) = \mathbb{Q}(\mathcal{E}[2R])$ and thus by Theorem 3.6, $\mathcal{C}_{\mathcal{E},R} = 0$. Now for any positive integer n where $(n, m_{\mathcal{E}}) = 1$, let $m = Rn$, then the result follows by Corollary 3.4. □

Lemma 6.4. *For an odd integer k, $\mathbb{Q}(\sqrt{k}) \subseteq \mathbb{Q}(\zeta_k) \Leftrightarrow k \equiv 1 \pmod 4$.*

Proof. For integer n, let M be the maximal integer such that $n = M^2 k$ for integer k. Then define the square-free part of n, $(n)_{sf} \coloneqq k$.

We now only have to prove $\mathbb{Q}(\sqrt{(k)_{sf}}) \subseteq \mathbb{Q}(\zeta_k) \Leftrightarrow (k)_{sf} \equiv 1 \pmod 4$, as $\mathbb{Q}(\sqrt{k}) = \mathbb{Q}(\sqrt{(k)_{sf}})$ and $k \equiv 1 \pmod 4 \Leftrightarrow (k)_{sf} \equiv 1 \pmod 4$ since if an integer M is odd, then $M^2 \equiv 1 \pmod 4$. Let p_i be the prime factors of $(k)_{sf}$ then, for some i, if $p_i \equiv 1 \pmod 4$, then $\mathbb{Q}(\sqrt{p_i}) \subseteq \mathbb{Q}(\zeta_{p_i})$ and if $p_i \equiv 3 \pmod 4$, then $\mathbb{Q}(\sqrt{-p_i}) \subseteq \mathbb{Q}(\zeta_{p_i})$. Thus, letting $N = \#\{1 \leq i \leq r : p_i \equiv 3 \pmod 4\}$, $\mathbb{Q}(\sqrt{(-1)^N (k)_{sf}}) \subseteq \mathbb{Q}(\zeta_{(k)_{sf}}) \subseteq \mathbb{Q}(\zeta_k)$ and also $(k)_{sf} \equiv (-1)^N \pmod 4$. If N is even we have the $\Leftarrow$ direction. If N is odd, we have $\mathbb{Q}(\sqrt{(-1)^N (k)_{sf}}) = \mathbb{Q}(i\sqrt{(k)_{sf}}) \subseteq \mathbb{Q}(\zeta_k)$. Suppose $\mathbb{Q}(\sqrt{(k)_{sf}}) \subseteq \mathbb{Q}(\zeta_k)$, then $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_k)$, however this is a contradiction as $\mathbb{Q}(\zeta_4) \cap \mathbb{Q}(\zeta_k) = \mathbb{Q}$ since k is odd and thus $\mathbb{Q}(\sqrt{(k)_{sf}}) \not\subseteq \mathbb{Q}(\zeta_k)$ and the we get the $\Rightarrow$ direction. □

Proposition 6.5. *For a non-CM elliptic curve $\mathcal{E}$, if $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) \in \{\mathbb{Z}/2\mathbb{Z}, S_3\}$ and the discriminant $\Delta_{\mathcal{E}} \equiv 1 \pmod 4$, then there are infinitely many positive integers m, where $\mathcal{C}_{\mathcal{E},m} = 0$.*

Proof. If $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, then $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\sqrt{\Delta_\mathcal{E}}) \subseteq \mathbb{Q}(\zeta_{\Delta_\mathcal{E}}) \subseteq \mathbb{Q}(\mathcal{E}[\Delta_\mathcal{E}])$, by Lemma 6.4. Since $\Delta_\mathcal{E}$ is odd, using Lemma 1.2, we have $\mathbb{Q}(\mathcal{E}[\Delta_\mathcal{E}]) = \mathbb{Q}(\mathcal{E}[2\Delta_\mathcal{E}])$ and thus by Theorem 3.6, $\mathcal{C}_{\mathcal{E},\Delta_\mathcal{E}} = 0$. Now for any positive integer n where $(n, m_\mathcal{E}) = 1$, let $m = \Delta_\mathcal{E} n$, then the result follows by Corollary 3.4.

If $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) \cong S_3 \cong \langle r, s\rangle$, where $r^3 = e = s^2$ then we can find quotient group $S_3/\langle r\rangle \cong \mathbb{Z}/2\mathbb{Z}$ and corresponding field K over $\mathbb{Q}$. By the Kronecker-Weber Theorem, Theorem 6.2, $K \subseteq \mathbb{Q}(\zeta_R)$ for some odd positive integer R. We can require that R be odd as since $[K : \mathbb{Q}]$ is odd, $K \cap \mathbb{Q}(\zeta_{2^r}) = \mathbb{Q}$ for positive integer r as $[\mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{r-1}$. Thus $K \subseteq \mathbb{Q}(\zeta_R) \subseteq \mathbb{Q}(\mathcal{E}[R])$ by Lemma 1.3. Now, $\mathbb{Q}(\mathcal{E}[2]) = K(\sqrt{\Delta_\mathcal{E}}) \subseteq K(\zeta_{\Delta_\mathcal{E}}) \subseteq K(\mathcal{E}[\Delta_\mathcal{E}]) \subseteq \mathbb{Q}(\mathcal{E}[R\Delta_\mathcal{E}])$, by Lemma 6.4. Since $R\Delta_\mathcal{E}$ is odd, using Lemma 1.2, we have $\mathbb{Q}(\mathcal{E}[R\Delta_\mathcal{E}]) = \mathbb{Q}(\mathcal{E}[2R\Delta_\mathcal{E}])$ and thus by Theorem 3.6, $\mathcal{C}_{\mathcal{E},R\Delta_\mathcal{E}} = 0$. Now for any positive integer n where $(n, m_\mathcal{E}) = 1$, let $m = R\Delta_\mathcal{E} n$, then the result follows by Corollary 3.4. □

7 Commutator of $GL_2(\hat{\mathbb{Z}})$ and its implications

Proposition 7.1. *For k an odd integer,* $[\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$.

Proof. For $i \in \{1, ..., r\}$, we define primes p_i and integers n_i where $k = \prod_{i=1}^r p_i^{n_i}$ and then we can write $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}) = \prod_{i=1}^r \mathrm{GL}_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$. Thus, letting $G := \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for odd prime p and integer n, we only need to show that $[G, G] = \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

We have the $[G, G] \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ inclusion as for $A, B \in G$, $\det(ABA^{-1}B^{-1}) = 1$. To show the $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \subseteq [G, G]$ inclusion, we will first find some elements of $[G, G]$. Since $2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, for $x \in \mathbb{Z}/p^n\mathbb{Z}$,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} \in [G, G], \text{ and}$$

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}^{-1} \in [G, G].$$

Also, for $y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$,

$$\begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \in [G, G], \text{ and finally}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix}^{-1} \in [G, G].$$

Now, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. If $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ ca^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in [G, G].$$

If $a \notin (\mathbb{Z}/p^n\mathbb{Z})^\times$, then $b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ otherwise $p|ad - bc$ implying $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ which is a contradiction. Thus, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ db^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & -ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix} \in [G, G].$$

□

Definition 7.2. *For r a positive integer, define the surjective homomorphism*

$$\Psi_r : \mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \pmod 2 & b \pmod 2 \\ c \pmod 2 & d \pmod 2 \end{pmatrix}.$$

Lemma 7.3. $\Psi_r([\mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z})]) = [\Psi_r(\mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z})), \Psi_r(\mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z}))]$

Proof. Since Ψ_r is a homomorphism, for $x, y \in \mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z})$ we have $\Psi_r(xyx^{-1}y^{-1}) = \Psi_r(x)\Psi_r(y)(\Psi_r(x))^{-1}(\Psi_r(y))^{-1}$. □

Proposition 7.4. $[\mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z})] = \Psi_r^{-1}\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/2^r\mathbb{Z}) : b \equiv c \pmod 2 \right\}$$

In addition, $|\mathrm{SL}_2(\mathbb{Z}/2^r\mathbb{Z}) : [\mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z})]| = 2$.

Proof. By calculation,

$$[\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})] = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \ \mathrm{SL}_2(\mathbb{Z}/2^r\mathbb{Z}) / \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

Thus, by Lemma 7.3, the result follows. □

Theorem 7.5. *The commutator subgroup of* $\mathrm{GL}_2(\hat{\mathbb{Z}})$ *is an index 2 subgroup of* $\mathrm{SL}_2(\hat{\mathbb{Z}})$ *ie.* $|\mathrm{SL}_2(\hat{\mathbb{Z}}) : [\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{GL}_2(\hat{\mathbb{Z}})]| = 2$.

Proof. Combining Propositions 7.1 and 7.4, the result follows. □

Corollary 7.6. *For every non-CM elliptic curve, H has even index in G.*

Proof. $H \leq G$ implies $[H, H] \leq [G, G]$. Then, since $|G : H| = |\mathrm{SL}_2(\hat{\mathbb{Z}}) : [H, H]|$ by [Zy, Lemma 1.7], by Theorem 7.5, $|G : H|$ is even. □

Corollary 7.7. *Every non-CM elliptic curve has even level.*

Proof. $[G, G] \bmod_2 < \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is a strict inequality. □

Corollary 7.8. *There are no non-CM elliptic curves with level equal to* 1.

Proof. If $m_{\mathcal{E}} = 1$, then $\Gamma_1 = G \subseteq H$. However this is a contradiction as for every non-CM curve H has even index in G by Corollary 7.6. □

Definition 7.9. *For a non-CM elliptic curve $\mathcal{E}$, $\mathcal{E}$ is a Serre curve if $|G : H| = 2$, ie. $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ has maximal image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.*

Lemma 7.10. *If an elliptic curve $\mathcal{E}$ is a Serre curve and k and j are positive integers with k odd, then $\mathbb{Q}(\zeta_{kj}) \cap \mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\zeta_j)$.*

Proof. If an elliptic curve $\mathcal{E}$ is a Serre curve and k is an odd integer, then $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[k])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$. □

Theorem 7.11 (Jon, Theorem 4). *Almost all elliptic curves are Serre curves.*

8 Acknowledgements and citations

A big thank you goes to Dr Jack Shotton for his constant guidance and advice. This project would certainly not have been possible without him. Also to the London Mathematical Society and Durham University who very generously helped fund this research. Finally, a big thank you the LMFDB for providing invaluable data throughout this project.

References

[Co1] Cojocaru, A.C., (2016), *Primes, elliptic curves and cyclic group: A synopsis*, https://api.semanticscholar.org/CorpusID:17530256.

[Co2] Cojocaru, A.C., (2004), *Questions About the Reductions Modulo Primes of an Elliptic Curve*, CRM Proc, Lecture Notes, https://doi.org/10.1090/crmp/036/05

[CoMu] Cojocaru, A.C., Murty, M., (2004), *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. 330, 601–625, https://doi.org/10.1007/s00208-004-0562-x.

[FK] Freiberg, T., Kurlberg, P., (2014), *On the average exponent of elliptic curves modulo p*. International mathematics research notices, 2265-2293, https://doi.org/10.48550/arXiv.1203.4382.

[DL] Daniels, H.B., Lozano-Robledo, Á., (2019). *Coincidences of division fields*, https://doi.org/10.48550/arXiv.1912.05618.

[Jon] Jones, N., (2010), *Almost all elliptic curves are Serre curves. Transactions of the American Mathematical Society*, 362(3), 1547-1570, https://doi.org/10.48550/arXiv.math/0611096.

[Kim] Kim S., (2015), *Positivity of constants related to elliptic curves*, Journal of Number Theory, Volume 157, 54-63, https://doi.org/10.1016/j.jnt.2015.04.017.

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org,2023.

[Ser] Serre, J.P., (1971), *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15, 259-331, https://doi.org/10.1007/BF01405086.

[Wash] Washington, L., (2008), *Elliptic curves: number theory and cryptography*, CRC press, ISBN-13: 978-1420071467.

[Zy] Zywina, D., (2022), *Explicit open images for elliptic curves over* $\mathbb{Q}$, https://doi.org/10.48550/arXiv.2206.14959.