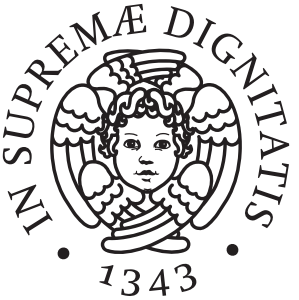
Università di Pisa



Dipartimento di Matematica

Galois Representations Attached to Elliptic Curves: around Serre's Uniformity Question

PhD Thesis
in Mathematics

Candidate
Lorenzo Furio

Advisor
Davide Lombardo
Università di Pisa

Academic Year 2023 - 2024

Acknowledgements

I am deeply grateful to my Ph.D. supervisor, Davide Lombardo, for his invaluable guidance, teaching, and patience. This work would not have been possible without him. He has been an excellent advisor, always providing thoughtful insights with remarkable dedication. If I had to choose a supervisor again, I would undoubtedly choose him. Beyond his expertise, he has always carried out his role in a spirit of friendship, making this journey even more enriching.

I sincerely thank Samuel Le Fourn for our helpful discussions and his valuable comments on this thesis as a referee. I am also grateful to René Schoof for his careful refereeing and insightful feedback.

I would also like to thank all the mathematicians with whom I had the opportunity to discuss my work for their comments and suggestions.

Finally, I am grateful to my university friends, Frenk, Luca, Giacomo, and Davide, with whom I grew both personally and as a mathematician, and to my office mates, Lorenzo, Alberto, Pietro, and Gallo, for the time shared, stimulating discussions, and valuable advice.

A special thank you to Cecilia, my family, and my friends for always being by my side, offering support and encouragement throughout this journey.

Contents

Introduction

Let K be a number field and let E be an elliptic curve defined over K. It is known that for a positive integer N, the set of N-torsion points of E is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2, i.e.

$$E[N] := \{P \in E(\overline{K}) \mid N \cdot P = O\} \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

with the isomorphism given by a choice of $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$. The action of the absolute Galois group of K on the N-torsion points of E defines a representation

$$\rho_{E,N} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right).$$

If p is a fixed prime, we can restrict to values of N of the form p^n and take the limit over n. We then obtain the representation

$$\rho_{E,p^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p),$$

where $T_pE = \varprojlim E[p^n]$ is the p-adic Tate module of E. If we take the product over all primes, we obtain the adelic representation

$$\rho_E = \prod_{p \text{ prime}} \rho_{E,p^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \prod_{p \text{ prime}} \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

which is the representation given by the action of the absolute Galois group of K on all the torsion points of E.

In 1972 Serre [Ser72] proved his celebrated open image theorem, stating that if the elliptic curve E does not have (potential) complex multiplication, then the representation ρ_{E,p^∞} is surjective for almost all primes. He actually proved a stronger statement [Ser72, Théorème 3]: if E does not have complex multiplication, then the image of the adelic representation ρ_E is open; equivalently, the image of ρ_E has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. From now on, we will say for simplicity that E does not have complex multiplication (CM) if it has no potential complex multiplication. In the same paper, Serre asked the following question.

Question 1 (Serre's uniformity question)**.** *Let K be a number field. Does there exist a constant N, depending only on K, such that for every non-CM elliptic curve E/K and for every prime $p > N$ the residual representation*

$$\rho_{E,p} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is surjective?

Although this problem has been widely studied, the question is still open, even in the case $K = \mathbb{Q}$. At least in this case, it is conjectured that it can be answered affirmatively (see for example [Zyw15a, Conjecture 1.12] or [Sut16, Conjecture 1.1]).

Conjecture 2. *For every elliptic curve $E/\mathbb{Q}$ without CM and for every prime $p > 37$, the representation $\rho_{E,p}$ is surjective.*

Over the years, many mathematicians provided various partial results towards an answer to Conjecture 2. Whenever the representation $\rho_{E,p}$ is not surjective, its image must be contained in a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Serre classified [Ser72, Section 2] all the maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ and proved that they can be of three types: some so-called 'exceptional' subgroups, the Borel subgroups, and the normalisers of (split or non-split) Cartan subgroups. He then showed [Ser81, §8.4, Lemma 18] that for $p > 13$ the exceptional subgroups cannot contain the image of $\rho_{E,p}$. Later, Mazur [Maz78] proved that there are no isogenies of prime degree p between non-CM elliptic curves over $\mathbb{Q}$ for $p > 37$: this is equivalent to the fact that for $p > 37$ the image of $\rho_{E,p}$ is not contained in a Borel subgroup. More precisely, he proved the following theorem.

Theorem 3 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that E admits a rational isogeny of degree p. One of the following holds:*

- $p \in \{2, 3, 5, 7, 13\}$*;*
- $p = 11$ *and* $j(E) \in \left\{-11^2,\ -11 \cdot 131^3\right\}$*;*
- $p = 17$ *and* $j(E) \in \left\{-2^{-1} \cdot 17^2 \cdot 101^3,\ -2^{-17} \cdot 17 \cdot 373^3\right\}$*;*
- $p = 37$ *and* $j(E) \in \left\{-7 \cdot 11^3,\ -7 \cdot 137^3 \cdot 2083^3\right\}$.

More recently, Bilu and Parent developed their version of Runge's method for modular curves [BP11a], which allowed them to prove [BP11b] that the image of $\rho_{E,p}$ is not contained in the normaliser of a split Cartan subgroup for sufficiently large p. The result was then sharpened by Bilu–Parent–Rebolledo

[BPR13], who showed that the same statement holds for every $p \geq 11$, with the possible exception of $p = 13$. Finally, it was extended to also cover the prime $p = 13$ by means of the so-called *quadratic Chabauty* method [BDM$^+$19]. These results together give the following theorem.

Theorem 4. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. For every prime $p > 7$ the image of the representation $\rho_{E,p}$ is not contained in the normaliser of a split Cartan subgroup.*

Thus, the only case that remains open is that of normalisers of non-split Cartan subgroups. In particular, Conjecture 2 can be reformulated in the following way.

Conjecture 5. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If p is a prime such that the image of $\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup, then $p \leq 11$.*

Actually, Conjecture 5 is a little bit stronger, because it also implies that there are no non-CM elliptic curves E for which $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup for $13 \leq p \leq 37$. Unfortunately, the techniques applied in the other cases, such as Runge's method, cannot be applied to the modular curves corresponding to normalisers of non-split Cartan subgroups. However, some partial results have been obtained even in this case. In particular, Zywina [Zyw15a] and Le Fourn–Lemos [LFL21] studied the possibility that the image of $\rho_{E,p}$ is *strictly* contained in the normaliser of a non-split Cartan subgroup. We now recall their results.

Assuming $p > 2$, we let ε be the reduction modulo p of the least positive integer which represents a quadratic non-residue in $\mathbb{F}_p^\times$. We denote by $C_{ns}(p)$ the non-split Cartan group

$$C_{ns}(p) := \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_p,\ (a,b) \neq (0,0) \right\} \tag{0.1}$$

and by $C_{ns}^+(p)$ its normaliser, obtained as $C_{ns}(p) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns}(p)$.

Theorem 6 (Zywina)**.** *Suppose that $\rho_{E,p}$ is not surjective for a non-CM elliptic curve $E/\mathbb{Q}$ and a prime $p > 37$.*

- *If $p \equiv 1 \pmod 3$, then $\operatorname{Im}\rho_{E,p}$ is conjugate to $C_{ns}^+(p)$ in $\mathrm{GL}_2(\mathbb{F}_p)$.*
- *If $p \equiv 2 \pmod 3$, then $\operatorname{Im}\rho_{E,p}$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ either to $C_{ns}^+(p)$ or to the group*

$$G(p) := \{a^3 \mid a \in C_{ns}(p)\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot a^3 \mid a \in C_{ns}(p) \right\} \subset C_{ns}^+(p).$$

This theorem follows from Proposition 1.13 of the unpublished preprint [Zyw15a]. A full proof is available in print as [LFL21, Proposition 1.4]. In their paper [LFL21], Le Fourn and Lemos studied the case where $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$, ruling out this possibility for all sufficiently large primes [LFL21, Theorem 1.2].

Theorem 7 (Le Fourn, Lemos)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If $p > 37$ is a prime number such that $\operatorname{Im}\rho_{E,p} \cong G(p)$, then $p < 1.4 \cdot 10^7$ and $j(E) \in \mathbb{Z}$.*

In the introduction to [LFL21], the authors describe the difficulties in extending their result to primes smaller than $1.4 \cdot 10^7$. In particular, they show that for any prime $p > 37$ and elliptic curve $E/\mathbb{Q}$ without CM for which $\operatorname{Im}\rho_{E,p} \cong G(p)$, we have $\log|j(E)| \leq \max\{12000, 7\sqrt{p}\} \leq 27000$, which together with the fact that $j(E) \in \mathbb{Z}$ shows that there are only finitely many ($\overline{\mathbb{Q}}$-isomorphism classes of) curves to check. However, as they point out, there seems to be no easy way to handle the remaining cases algorithmically.

In our first result, corresponding to the preprint [FL23b], we deal with the remaining primes to prove the following simple dichotomy in Serre's uniformity question.

Theorem 8. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let $p > 37$ be a prime number. The image of $\rho_{E,p}$ is either $\mathrm{GL}(E[p])$ or the normaliser of a non-split Cartan subgroup of $\mathrm{GL}(E[p])$.*

For $p \leq 37$, the images of the mod-p representations attached to elliptic curves over $\mathbb{Q}$ have been studied extensively (see [Zyw15a, RSZB22, BDM$^+$23] for the state of the art). Combined with Theorem 8, this allows us to show the following.

Theorem 9. *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let $p \geq 5$ be a prime such that the image of $\rho_{E,p}$ is contained in $C_{ns}^+(p)$. If $\operatorname{Im}\rho_{E,p} = G(p)$ then $p = 5$. In all the other cases, $\operatorname{Im}\rho_{E,p} = C_{ns}^+(p)$.*

Similar to the observation of Le Fourn and Lemos in [LFL21, Theorem 1.3], Theorems 8 and 9 also completely settle a question of Najman [Naj18], improving [LFL21, Theorem 1.3]. Let $d \geq 1$ be a positive integer and let $I_{\mathbb{Q}}(d)$ be the set of prime numbers p for which there exists a rational elliptic curve $E/\mathbb{Q}$ without complex multiplication and an isogeny $\varphi : E \to E'$ of degree p defined over a field K of degree $[K : \mathbb{Q}] \leq d$. From Mazur's work (Theorem 3) we know that $I_{\mathbb{Q}}(1) = \{2, 3, 5, 7, 11, 13, 17, 37\}$, and Najman's question concerns the sets $I_{\mathbb{Q}}(d)$ for $d \geq 2$. As a consequence of [LFL21, Proposition 1.4] and Theorem 9 we obtain:

Theorem 10. *For every positive integer d we have*

$$I_{\mathbb{Q}}(d) = I_{\mathbb{Q}}(1) \cup \{p \text{ prime} \mid p \leq d-1\}.$$

This is an unconditional version of [Naj18, Theorem 4.1], and the proof relies on the same arguments.

A more general goal is to classify all the possible images of ρ_E inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. This is known as Mazur's 'Program B' [Maz77]. In recent years, much progress has been made in the case of elliptic curves defined over $\mathbb{Q}$. Most of the results are given either in the 'vertical' or 'horizontal' direction, i.e. they either classify the possible images of the p-adic representations ρ_{E,p^∞}, or study the entanglement phenomenon at composite level.

A lemma of Serre [Ser98, IV-23, Lemma 3] implies that, for $p \geq 5$, the p-adic representation attached to $E/\mathbb{Q}$ is surjective if and only if the mod-p representation is surjective. In particular, to classify all the possible images of ρ_{E,p^∞}, it suffices to consider the case where $\rho_{E,p}$ is not surjective. Greenberg [Gre12] and Greenberg–Rubin–Silverberg–Stoll [GRSS14] classified the p-adic representations ρ_{E,p^∞} for $p \geq 5$ under the assumption that $\operatorname{Im}\rho_{E,p}$ is contained in a Borel subgroup. We present their result for non-CM elliptic curves.

Theorem 11. *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let $p \geq 5$ be a prime such that E admits a rational p-isogeny (i.e., such that $\operatorname{Im}\rho_{E,p}$ is contained in a Borel subgroup).*

- *If $p > 5$ then $\operatorname{Im}\rho_{E,p^\infty} \supseteq I + pM_{2\times 2}(\mathbb{Z}_p)$, and in particular $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] = [\mathrm{GL}_2(\mathbb{F}_p) : \operatorname{Im}\rho_{E,p}]$.*
- *If $p = 5$, then $[\mathrm{GL}_2(\mathbb{Z}_5) : \operatorname{Im}\rho_{E,5^\infty}]$ divides $5[\mathrm{GL}_2(\mathbb{F}_5) : \operatorname{Im}\rho_{E,5}]$.*

Proof. The statement follows combining [Gre12, Theorems 1 and 2], Theorem 3, [Gre12, Remark 4.2.1], and the main result of [GRSS14]. □

We remark that, by Theorem 3, the above result only applies to the primes $\{5, 7, 11, 13, 17, 37\}$.

Later, Rouse and Zureick-Brown [RZB15] completely classified all the possible 2-adic images. Then, Sutherland and Zywina [SZ17] described all the possible open subgroups $G < \mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which there are infinitely many isomorphism classes of elliptic curves $E/\mathbb{Q}$ with $\operatorname{Im}\rho_E = G$. Eventually, Rouse, Zureick-Brown and Sutherland [RSZB22] gave a detailed description of all the possible p-adic images for all primes p whenever the image of $\rho_{E,p}$ is not contained in the normaliser of a non-split Cartan. We will refer to the modular curves classified in [RSZB22] by the labels they were given there, which we

will call *RSZB labels*. We now give the precise statement of their theorem. Given an integer ε which is not a square modulo p, denote by

$$C_{ns}^{+}(p^n) := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \cdot \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z}/p^n\mathbb{Z},\ (a,b) \not\equiv (0,0) \mod p \right\}$$

the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$ (see Chapter 2 for definitions).

Theorem 12 ([RSZB22, Theorem 1.6])**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let p be a prime number and set $G := \operatorname{Im}\rho_{E,p^\infty}$. Exactly one of the following is true:*

- *the modular curve X_G has infinitely many rational points and $\pm G$ is listed in [SZ17, Tables 1–4];*
- *the modular curve X_G has an 'exceptional' rational point, and the pair $(G, j(E))$ appears in the finite list in [RSZB22, Table 1];*
- *$G \pmod{p^n}$ is contained in $C_{ns}^{+}(p^n)$ for $p^n \in \{3^3, 5^2, 7^2, 11^2\} \cup \{p \text{ prime} \mid p \geq 19\}$;*
- *G is a subgroup of one of the groups with RSZB label* `49.147.9.1` *or* `49.196.9.1`*.*

Building on the work of Zywina [Zyw15a], we give a restricted list of subgroups $G < \mathrm{GL}_2(\mathbb{Z}_p)$ such that $\operatorname{Im}\rho_{E,p^\infty}$ is possibly equal to G whenever $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a non-split Cartan, dealing with the cases not covered by Theorem 12. We will prove the following result as Theorem 6.1.5.

Theorem 13. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let p be an odd prime such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$ up to conjugation, and let $n \geq 1$ be the smallest integer such that $\operatorname{Im}\rho_{E,p^\infty} \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$. One of the following holds:*

- *$p = 3$ and $\pm\operatorname{Im}\rho_{E,3^\infty}$ is conjugate to one of the groups with RSZB labels* `3.6.0.1`*,* `3.12.0.1`*,* `9.18.0.1`*,* `9.18.0.2`*,* `9.36.0.1`*,* `9.36.0.2`*,* `9.36.0.3`*;*
- *$p = 5$ and the image of $\rho_{E,5^\infty}$ is the group with RSZB label* `5.30.0.2` *up to conjugation;*
- *The image of ρ_{E,p^n} is equal to $C_{ns}^{+}(p^n)$ up to conjugation;*

- $n = 2$ *and*

$$\operatorname{Im}\rho_{E,p^2} \cong C_{ns}^{+}(p) \ltimes \left\{ I + p \begin{pmatrix} a & \varepsilon b \\ -b & c \end{pmatrix} \right\},$$

with the semidirect product defined by the conjugation action.

While the eight groups with RSZB labels given in the first two cases of Theorem 13 actually occur for some elliptic curves E, the last two cases conjecturally never occur for large values of p. In particular, we know examples of elliptic curves E for which $\operatorname{Im}\rho_{E,p^n} \cong C_{ns}^{+}(p^n)$ only for $p^n \leq 11$, while the last case is only known to happen for $p = 3$.

On the other hand, many authors have studied the 'horizontal' entanglement classification problem, i.e. the classification of intersections of division fields at different primes, which we call entanglement fields. Serre [Ser72, Proposition 22] proved that for every non-CM elliptic curve E defined over $\mathbb{Q}$, the image of ρ_E lies in an index-2 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, even if the p-adic representation ρ_{E,p^∞} is surjective for every prime p. More recent results focus on the study of the intersection of $\mathbb{Q}(E[p])$ and $\mathbb{Q}(E[q])$ for two different primes p, q, usually small (see for example [BJ16, Mor19, DM22, JM22, DLR23]). In Section 6.3, we prove some general theorems to bound the degree of entanglement fields, especially in the case where one of the division fields has Galois group contained in the normaliser of a non-split Cartan. We then give a bound on the growth of the adelic index with respect to the product of the p-adic indices due to the entanglement phenomenon. In particular, in Lemma 6.4.10 (precisely, equation (6.4.5)) we show the following.

Proposition 14. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve that does not satisfy Conjecture 5 and let α be the number of primes $p > 5$ for which the image of $\rho_{E,p}$ is contained in $C_{ns}^{+}(p)$. We have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 1536 \cdot 6^{\alpha} \prod_{p \text{ prime}} [\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}].$$

A problem equivalent to Question 1 (uniformity question) is the following.

Question 15. *Let K be a number field. Does there exist a constant N, depending only on K, such that for every non-CM elliptic curve E/K we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] < N$?*

The equivalence between the two questions can be shown in the following way: if there exists an integer M such that for every prime p greater than M the mod-p representation is surjective, then by [Ser98, IV-23, Lemma 3] the same holds for p-adic representations. Consider now, for every prime p smaller than or equal to M, all the possible subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ and their

corresponding modular curves. Some of these curves will have finitely many K-rational points and we can ignore them. For the other modular curves, if we consider a rational point on one of them and the corresponding elliptic curve E, either the image of the p-adic representation ρ_{E,p^∞} contains the group $I + pM_{2\times 2}(\mathbb{Z}_p)$ (and hence the p-adic index is bounded), or E corresponds to a K-rational point on a level p^2 modular curve. We can then repeat the same argument for modular curves of level p^2, and go on with higher powers of p. Since the genus of the modular curves grows with the level, there exists an integer n such that all the modular curves of level p^n have genus greater than 1, and then they will have a finite number of K-rational points by Faltings theorem (see [Ara08, Theorem 1.3]). This gives a bound on the indices of the p-adic representations. Serre proved that the image of ρ_E has finite index in the product $\prod \operatorname{Im} \rho_{E,p^\infty}$ over the finite set of primes containing $2, 3, 5$ and those primes for which ρ_{E,p^∞} is not surjective [Ser98, IV-26, Lemma 5]. Since for every p the pro-p Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ has a finite index, it suffices to show that the intersection of the image of $\prod \rho_{E,p^\infty}$ with the product of the pro-p Sylow subgroups has finite index. However, a subgroup of a product of p-groups (for different primes p) is a product of subgroups, and since the projections on $\mathrm{GL}_2(\mathbb{Z}_p)$ have finite index, so have their product.

Recently, Zywina [Zyw11] provided a bound on the adelic index in the case where the elliptic curve E is defined over $\mathbb{Q}$, polynomial in terms of the height $\mathrm{h}(j(E))$. Moreover, he also gave a bound in terms of the conductor of E.

Theorem 16 (Zywina)**.** *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$.*

1. *There are absolute constants C and γ such that*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] \leq C(\max\{1, \mathrm{h}(j(E))\})^\gamma,$$

   where $\mathrm{h}(j(E))$ is the logarithmic Weil height of the j-invariant of E.

2. *Let N be the product of the primes of bad reduction of E. There is an absolute constant C such that*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] \leq C\left(68N(1 + \log\log N)^{\frac{1}{2}}\right)^{24\omega(N)},$$

   where $\omega(N)$ is the number of distinct prime divisors of N.

The bound in terms of the height of $j(E)$ relies on previous results of Masser and Wüstholz on isogenies [MW93b, MW93a]. Their results were made explicit by many authors, and optimised by Gaudron and Rémond. For example, in [GR14] they gave a bound on the minimal degree of an isogeny between two elliptic curves which is quadratic in the stable Faltings height of the curves (the stable Faltings height of an elliptic curve E is approximately $\frac{1}{12}\mathrm{h}(j(E))$ as shown in Theorem 1.2.6). Both of Zywina's bounds are ineffective. Later,

Lombardo gave a bound for the adelic index for elliptic curves defined over a generic number field [Lom15, Corollary 9.3 and Remark 1.1]. His proof exploits Gaudron–Rémond's improvements to the isogeny theorem. This bound is effective and polynomial in terms of the Faltings height of the curve.

Theorem 17 (Lombardo)**.** *Let E be a non-CM elliptic curve defined over a number field K and let $\mathrm{h}_{\mathcal{F}}(E)$ be the stable Faltings height of E. We have*

$$\left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E\left(\mathrm{Gal}(\overline{K}/K)\right)\right] < \gamma_1 \cdot [K:\mathbb{Q}]^{\gamma_2} \cdot \max\left\{1, \mathrm{h}_{\mathcal{F}}(E), \log[K:\mathbb{Q}]\right\}^{\gamma_2},$$

where $\gamma_1 = \exp(1.9 \cdot 10^{10})$ and $\gamma_2 = 12395$.

On the other hand, Zywina's bound in terms of the conductor is proved building on previous work of Serre and Kraus. In particular, given a non-CM elliptic curve E defined over $\mathbb{Q}$, under GRH Serre [Ser81, Theorem 22] obtained the following bound in terms of the conductor for the largest prime p for which $\rho_{E,p}$ is not surjective.

Theorem 18 (Serre)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let N be the product of the primes of bad reduction of E. Suppose that the generalised Riemann hypothesis is true. There exists a constant c such that for every prime number $p > c \log N (\log\log N)^3$ the representation $\rho_{E,p}$ is surjective.*

Later, Kraus [Kra95] proved a similar unconditional effective result for modular elliptic curves. Thanks to the modularity theorem [BCDT01], this is now known to be true for every elliptic curve.

Theorem 19 (Kraus)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let N be the product of the primes of bad reduction of E. For every prime number $p \geq 68N(1+\log\log N)^{\frac{1}{2}}$ the representation $\rho_{E,p}$ is surjective.*

Cojocaru [Coj05] extended Kraus's result to bound the product of the primes p for which the representation $\rho_{E,p}$ is not surjective. However, as Zywina notes in [Zyw11, Remark 3.4], there seems to be a mistake in her proof. Recently, Mayle and Wang [MW24] gave an effective sharp version of Serre's result assuming GRH.

One of the main aim of this thesis is to provide some bounds on the adelic index when E is an elliptic curve defined over $\mathbb{Q}$. In particular, in Theorem 6.4.1 we give a bound in terms of the stable Faltings height of the curve which is much better than that of Lombardo. Moreover, we give an effective and improved version of Zywina's bound in terms of the radical of the conductor.

Theorem 20. *Let $E/\mathbb{Q}$ be an elliptic curve without CM.*

1. *If $\mathrm{h}_{\mathcal{F}}(E)$ is the stable Faltings height of E, we have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 9.5 \cdot 10^{20} (\mathrm{h}_{\mathcal{F}}(E) + 40)^{4.42}.$$

2. *We have*
$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] < \mathrm{h}_{\mathcal{F}}(E)^{3+O\left(\frac{1}{\log\log \mathrm{h}_{\mathcal{F}}(E)}\right)}$$
as $\mathrm{h}_{\mathcal{F}}(E)$ *tends to* ∞*, where the constant is explicit.*

3. *If* N *is the product of the primes of bad reduction of* E *and* $\omega(N)$ *is the number of distinct prime factors of* N*, we have*
$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] < 2488320\left(51N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)}.$$

Description of contents

In this thesis, we present the proofs of Theorems 8, 9 and 20. We now briefly describe the strategy behind these proofs.

The proofs of Theorems 8 and 9 follow that of Theorem 7 by Le Fourn and Lemos. Their proof is based on two fundamental steps: first, they show that an elliptic curve satisfying the hypothesis of Theorem 7 has integral j-invariant (via the formal immersion method of Mazur). Second, they prove an upper bound on $|j(E)|$ by combining Runge's method with an effective surjectivity theorem, showing that $\operatorname{Im}\rho_{E,p} = \mathrm{GL}(E[p])$ for all p greater than an explicit bound depending on $j(E)$.

The first step works in complete generality: Theorem 7 gives the integrality of $j(E)$ as soon as $p > 37$, so – in order to prove Theorem 8 – we can assume $j(E) \in \mathbb{Z}$. Our main contribution lies in a much sharper upper bound on $|j(E)|$, which we achieve through three main innovations:

- We prove a sharp effective surjectivity theorem (in the spirit of [MW93a], [Lom15], and [LF16, Theorem 5.2]) by refining the proof of the effective isogeny theorem of Gaudron and Rémond [GR14]. The main results we show are Theorem 4.1.1 and Theorem 4.2.5. We obtain substantially improved constants by showing that certain auxiliary subvarieties considered in the proof are all trivial in our case (see Lemma 4.1.11).

- Second, we perform a detailed analysis of the local properties of the representations $\rho_{E,p}$. This analysis yields several improvements, such as ruling out all primes $p \equiv -1 \pmod 9$ (Theorem 3.1.4) and proving that p^4 divides $j(E)$ (Proposition 3.2.14). Furthermore, we show that $j(E)$ can be written as $p^k c^3$ for some integer c. When we eventually reduce the proof of Theorem 8 to an explicit calculation, this latter relation has the effect of dividing by three *on a logarithmic scale* the number of tests we have to perform, significantly reducing the computational component of our approach.

- Finally, the third and most significant innovation is our much more detailed study of the modular units on the curve $X_{G(p)}$. The main ingredients that lead to our improved bound on $\log|j(E)|$ are sharp bounds on character sums, which essentially draw on Weil's method to treat Kloosterman sums [Wei48], an idea based on Abel's summation to amplify certain cancellation phenomena among roots of unity, and direct computations to fully exploit the extent of these cancellations. All of these improvements are crucial to lowering the bound on $\log|j(E)|$ to values that are computationally tractable (see Theorem 5.4.16), and the result we obtain is sharp enough that the final computation takes less than two minutes of CPU time.

We now describe the strategy behind the proof of Theorem 20. It combines the different results described above about the growth of the adelic index in the 'vertical' and 'horizontal' directions. In particular, the proof consists of three main steps.

- For every odd prime p, we classify the possible images of ρ_{E,p^n} whenever the image of $\rho_{E,p}$ is contained in the normaliser of a non-split Cartan (Theorem 13). The main aim will be to show that if n is the smallest integer for which $\operatorname{Im}\rho_{E,p^\infty}$ contains $I + p^n M_{2\times 2}(\mathbb{Z}_p)$, then the image of ρ_{E,p^n} is exactly $C_{ns}^+(p^n)$. This will allow us to obtain a good bound on the p-adic index.

- We generalise the effective surjectivity theorem to show that the product of the prime powers p^n for which the image of ρ_{E,p^n} is contained in $C_{ns}^+(p^n)$ is bounded linearly in the stable Faltings height of E (Theorems 4.1.1 and 4.2.5). This is used to bound the product of the p-adic indices for all the primes p such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$. While in the proofs of Theorems 8 and 9 the most important improvement concerned the applicability of the theorem to curves with small height, in this case the main improvements are the generalisation of Le Fourn's theorem ([LF16, Theorem 5.2]) to product of prime powers and the elimination of the dependence on the cardinality of $\mathcal{C}$, where $\mathcal{C}$ is the set of primes p for which the mod-p representation is contained in the normaliser of Cartan subgroup.

- We give a bound on the entanglement phenomenon among all primes to obtain a bound on the adelic index from the bound on the product of the p-adic indices obtained via the surjectivity theorem. The main ingredient to obtain a good bound is the study of the ramification index of p in the field $\mathbb{Q}(E[p^n])$. Indeed, when the image of ρ_{E,p^n} is contained in the normaliser of a non-split Cartan subgroup, p is 'almost totally'

ramified in $\mathbb{Q}(E[p])$. On the other hand, by a variant of the Néron–Ogg–Shafarevich criterion (see Theorem 3.1.1) we know that the ramification index of p inside $\mathbb{Q}(E[N])$ for $p \nmid N$ is low. This shows that the intersection $\mathbb{Q}(E[p]) \cap \mathbb{Q}(E[N])$ is small. These ramification arguments rely on the work of Lozano-Robledo [LR16] and Smith [Smi23].

We now summarise the contents of each chapter and describe their main goal.

In Chapter 1, we give some preliminary results used throughout the thesis. We begin by giving some elementary lemmas. Then, we study in detail the stable Faltings height of elliptic curves defined over the rationals. We conclude the chapter with a profinite version of the Schur–Zassenhaus lemma and an application to groups of matrices in the p-adic numbers.

In Chapter 2, we study the subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$ that satisfy some restrictive conditions. In particular, we consider the subgroups that – modulo p – are contained in the normaliser of a non-split Cartan (but not in the Cartan) and that contain all the homotheties, i.e. the elements in $\mathbb{Z}_p^\times \cdot I$. We prove some theorems about the structure of these groups, which we call *N-Cartan lifts*. These results will play a crucial role in the classification of the possible images of the representations ρ_{E,p^∞}, because one can show that if p is a prime such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$, then $\operatorname{Im}\rho_{E,p^\infty}$ is an N-Cartan lift.

In Chapter 3, we investigate the local properties of the representations ρ_{E,p^n} when their image is contained in the normaliser of a non-split Cartan subgroup. We show that E has potentially good reduction at every prime $\ell \not\equiv \pm 1 \pmod{p^n}$ (Proposition 3.1.2). Then, given a prime ℓ, we describe the image of the ℓ-inertia group via $\rho_{E,p}$. This will allow us to show that if the image of $\rho_{E,p}$ is contained in the subgroup $G(p)$ defined in Theorem 6 then $p \not\equiv -1 \pmod 9$, and $j(E)$ can be written as $p^d \cdot c^3$. We then introduce the central topic of the chapter, the *canonical subgroup*. We show that if $\operatorname{Im}\rho_{E,p}$ is contained in $C_{ns}^+(p)$ then E does not have a canonical subgroup of order p (Theorem 3.2.9). This implies that the p-adic valuation of the Hasse invariant of E is quite large, a fact we will use to show that if $\operatorname{Im}\rho_{E,p} \subseteq G(p)$ then the p-adic valuation of $j(E)$ is at least 4.

In Chapter 4, precisely in Theorem 4.1.1, we provide our version of the effective surjectivity theorem. We modify and improve the proofs of Le Fourn's theorem ([LF16, Theorem 5.2]) and Gaudron–Rémond's theorem ([GR14, Theorem 1.4]). In particular, we obtain a better result via two main improvements: the first is to show that certain auxiliary abelian varieties called B_σ are all trivial (Lemma 4.1.11), making the bound efficacious for elliptic curves with small height. The second improvement consists in a generalisation of Le Fourn's theorem in order to consider the products of prime powers (instead of the product of primes). We then conclude the chapter by proving some bounds on the prime powers p^n for which $\operatorname{Im}\rho_{E,p^n}$ is contained in the nor-

maliser of a Cartan subgroup whenever $j(E) \notin \mathbb{Z}$. In fact, in this case one can obtain much better constants. The proofs of these last results only rely on local arguments, and hence have a completely different approach with respect to the periods theorem.

In Chapter 5, we study the existence of non-CM integral points on the modular curves $X_{ns}^+(N)$, i.e. rational points $P \in X_{ns}^+(N)(\mathbb{Q})$ such that $j(P) \in \mathbb{Z}$. We introduce the modular units, which are the main tool used to compute integral points. They will be exploited in two different ways: via Baker's bound for linear forms in logarithms and via Runge's method for modular curves. The first one is used in [BS14] to show that every elliptic curve such that $\operatorname{Im}\rho_{E,p}$ is contained in $C_{ns}^+(p)$ has j-invariant uniformly bounded in terms of p. The bound obtained is really large, but one can lower it using some techniques of diophantine approximation and then test the remaining cases. We will follow this strategy to show that the curve $X_{ns}^+(25)$ has no non-CM integral points (Proposition 5.3.9). The Runge method is used instead to find the integral points on the curve $X_{G(p)}$, where $G(p)$ is the group defined in Theorem 6. Indeed, this is the strategy followed by Le Fourn and Lemos to obtain their first bound on p in Theorem 7. However, we will conduct a deeper study of the modular units involved to obtain stronger bounds. To this end, we take into account the cancellation among roots of unity in their Fourier expansion. In particular, we follow Weil's strategy for bounding Kloosterman's sums. Using Abel's summation we then rewrite the sums of roots of unity we already estimated in a different form to amplify as much as possible the cancellation phenomena. We conclude the chapter by proving Theorems 8 and 9. Combining the bound obtained via Runge's method with the effective surjectivity theorem, we obtain an absolute bound on the j-invariant of elliptic curves E with $\operatorname{Im}\rho_{E,p} = G(p)$. Since by Theorem 7 these curves have integral j-invariant, we are left with a finite number of them. As proved in Chapter 3, the j-invariant of E must be of the form $p^d \cdot c^3$, with $d \geq 4$ and $p \equiv 2, 5 \pmod 9$. These restrictive properties reduce a lot the number of admissible j-invariants. We can then test the remaining curves by checking directly that none of them satisfies $\operatorname{Im}\rho_{E,p} \cong G(p)$.

In Chapter 6, we apply the classification results proved in Chapter 2 to describe the possible images of the representations ρ_{E,p^∞}: in Proposition 6.2.1 this allows us to explicitly compute the p-adic indices at every p in terms of the smallest power p^n for which $\operatorname{Im}\rho_{E,p^\infty} \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$. Then, we study the entanglement of division fields in the non-split Cartan case. Using a result by Lozano-Robledo [LR16] and Smith [Smi23], we show that if $\operatorname{Im}\rho_{E,p^n}$ is contained in $C_{ns}^+(p^n)$ then the ramification index of p in $\mathbb{Q}(E[p^n])$ is at least $\frac{p^{2n}-p^{2n-2}}{6}$, which is quite close to the degree $[\mathbb{Q}(E[p^n]) : \mathbb{Q}]$ (Theorem 6.3.1). In particular, p is almost totally ramified in $\mathbb{Q}(E[p^n])$. On the other hand, by Theorem 3.1.1 we know that for every other prime $q \neq p$, the ramifica-

tion index of p in $\mathbb{Q}(E[q^\infty])$ is at most 6. This implies that the intersection $\mathbb{Q}(E[q^\infty]) \cap \mathbb{Q}(E[p^n])$ has small, uniformly bounded degree. We use this fact to bound the adelic index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E]$ in terms of the product of the p-adic indices $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im} \rho_{E,p^\infty}]$ (equation (6.4.5)). Combining these results with the effective surjectivity theorem (Theorem 4.2.5), we obtain a bound on the adelic index in terms of the stable Faltings height of the curve. We conclude the chapter by using results in the previous sections to give another bound on $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E]$ in terms of the radical of the conductor of E. The proof of this result follows that of Zywina [Zyw11], which builds on previous work of Serre [Ser81] and Kraus [Kra95].

CHAPTER 1

Preliminaries

In this chapter we collect some auxiliary results that will be used in some proofs in the other chapters. In particular, we provide explicit comparisons between the stable Faltings height of an elliptic curve over the rationals and its modular height, i.e. the logarithmic Weil height of its j-invariant. Then, we give a variant of Schur–Zassenhaus lemma for p-adic matrices.

1.1 Elementary lemmas

We start by recalling the following lemma, which can be found in [BPR13, Lemma 3.5].

Lemma 1.1.1 (Bilu, Parent, Rebolledo)**.** *For every $x \in (0,1)$ we have*

$$-\sum_{k=1}^{\infty} \log(1-x^k) < -\frac{\pi^2}{6\log x}.$$

The next two lemmas will be useful for the proof of Theorem 8 and Theorem 9. In particular, we will use them in the parts of our argument that rely on the complex interpretation of modular curves.

Lemma 1.1.2. *Let p be a positive integer. Let $\tau \in \mathcal{H}$ be a point in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ (as defined in Definition 1.2.1), let $q = e^{2\pi i\tau}$, and let $q^{\frac{1}{p}}$ be the p-th root of q given by $(e^{2\pi i\tau})^{\frac{1}{p}} = e^{\frac{2\pi i\tau}{p}}$. We have*

$$|1-q^{\frac{1}{p}}| < 1 - |q|^{\frac{1}{p}} + |q|^{\frac{1}{2p}}\frac{\pi}{p}.$$

Proof. Since τ is in the standard fundamental domain, we have $|\Re\{\tau\}| \leq \frac{1}{2}$, hence we can write $q^{\frac{1}{p}} = |q|^{\frac{1}{p}} e^{i\theta}$ with $|\theta| \leq \frac{\pi}{p}$. By using that $\sqrt{a^2+b^2} \leq |a|+|b|$ for all real numbers a and b, and that $\cos\theta \geq 1 - \frac{\theta^2}{2}$, we obtain

$$\begin{aligned} |1 - q^{\frac{1}{p}}| &= \sqrt{(1 - |q|^{\frac{1}{p}}\cos\theta)^2 + |q|^{\frac{2}{p}}\sin^2\theta} \\ &= \sqrt{1 - 2|q|^{\frac{1}{p}}\cos\theta + |q|^{\frac{2}{p}}} \\ &= \sqrt{(1 - |q|^{\frac{1}{p}})^2 + 2|q|^{\frac{1}{p}}(1-\cos\theta)} \\ &\leq 1 - |q|^{\frac{1}{p}} + |q|^{\frac{1}{2p}}|\theta|, \end{aligned}$$

with equality holding only for $\theta = 0$, and the lemma follows. □

Lemma 1.1.3. *Let $p > 1$ be an integer and let $x \in (0,1)$. We have*

1. $1 - x^{\frac{1}{p}} < \frac{|\log x|}{p}$;
2. $\frac{x^{\frac{1}{p}}}{1-x^{\frac{1}{p}}} < \frac{p}{|\log x|}$.

Proof. Both results are obtained from the inequality $\log y < y - 1$, with $y = x^{\frac{1}{p}}$ and $y = x^{-\frac{1}{p}}$ respectively. □

The following Lemma will be used in the proof of Theorem 20 and consists in an effective variant of Merten's theorem. Given an integer $N > 2$, we want to bound the product $\prod_{p|N}\left(1 + \frac{1}{p}\right)$ over the prime divisors of N. A first result was given by Kraus in [Kra95], which bounds the product with $4(1+\log\log N)$. In the same article [Kra95], in a note at the end of the paper, he wrote that Serre remarked that one can improve the bound by replacing the constant 4 with 2.4. More recently, in [SP11, Corollary 2] the authors proved that the product above is bounded by $e^{\gamma}\log\log N$, where γ is the Euler–Mascheroni constant and $e^{\gamma} \approx 1.78$. Exploiting the results contained in [SP11], we show that we can actually replace the constant in Kraus's lemma with $\frac{6e^{\gamma}}{\pi^2} \approx 1.081$, which is asymptotically optimal (as shown in [SP11, Proposition 3]).

Lemma 1.1.4. *Let $N > 6$ be a positive integer. We have*

$$\prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right) < \frac{6e^{\gamma}}{\pi^2}(1 + \log\log N).$$

Proof. First of all, we notice that if the statement holds for a number N, then it holds for all the numbers $N' > N$ divisible by the same primes as N,

hence it suffices to verify the inequality for squarefree numbers. Moreover, if $N = \prod_{i=1}^{k} p_i$ and $N' = \prod_{i=1}^{k} q_i$ with $p_i \leq q_i$ for every i, then

$$\frac{\prod_{p|N}\left(1+\frac{1}{p}\right)}{1+\log\log N} \geq \frac{\prod_{q|N'}\left(1+\frac{1}{q}\right)}{1+\log\log N'}:$$

indeed, this is true if and only if

$$\prod_{i=1}^{k}\frac{1+1/p_i}{1+1/q_i} \geq \frac{1+\log\left(\sum_{i=1}^{k}\log p_i\right)}{1+\log\left(\sum_{i=1}^{k}\log q_i\right)},$$

which is true because $LHS \geq 1$ and $RHS \leq 1$. Therefore, it suffices to consider the primorials $N_k = \prod_{i=1}^{k} p_i$, where p_i is the i-th prime number and $k \geq 3$, and the numbers N whose radical is smaller than 7. In the latter case, it suffices to notice that either N is a power of a prime, and in this case we have

$$\frac{\prod_{p|N}\left(1+\frac{1}{p}\right)}{1+\log\log N} \leq \frac{3}{2(1+\log\log 7)} < 1 < \frac{6e^{\gamma}}{\pi^2},$$

or N has radical equal to 6, and so we have $N \geq 12$ and

$$\frac{\prod_{p|N}\left(1+\frac{1}{p}\right)}{1+\log\log N} \leq \frac{\frac{3}{2}\cdot\frac{4}{3}}{1+\log\log 12} < 1.05 < \frac{6e^{\gamma}}{\pi^2}.$$

If instead N is the primorial N_k, suppose first that $k \geq 2263$ (or equivalently $p_k > 20000$). By [SP11, Proposition 4] we have

$$\begin{aligned}\prod_{p|N_k}\left(1+\frac{1}{p}\right) = \prod_{i=1}^{k}\left(1+\frac{1}{p_i}\right) &\leq \frac{6\exp\left(\gamma+\frac{2}{p_k}\right)}{\pi^2}\left(\log\log N_k + \frac{1.125}{\log p_k}\right)\\ &< \frac{6e^{\gamma}}{\pi^2}\left(\log\log N_k + \frac{1.125}{\log p_k}\right) + \frac{6e^{\gamma}}{\pi^2}\cdot\frac{3}{p_k}\left(\log\log N_k + \frac{1.125}{\log p_k}\right),\end{aligned}$$

where the last inequality comes from the fact that $e^{\frac{2}{x}} < 1 + \frac{3}{x}$ for $x > 20000$. Using the trivial inequality

$$\log\log N_k < \log k + \log\log p_k < 2\log p_k$$

and the fact that $p_k > 20000$ we obtain

$$\begin{aligned}\prod_{p|N_k}\left(1+\frac{1}{p}\right) &< \frac{6e^{\gamma}}{\pi^2}\left(\log\log N_k + \frac{1.125}{\log p_k} + \frac{6\log p_k}{p_k} + \frac{4}{p_k\log p_k}\right)\\ &< \frac{6e^{\gamma}}{\pi^2}\left(\log\log N_k + 0.12\right),\end{aligned} \tag{1.1.1}$$

which is better than the statement of the lemma. We can then test the remaining cases with $2 < k < 2263$; the computation takes less than one second in MAGMA. □

The following lemma is not an elementary result. However, it easily follows from [LFL21, Theorem 1.2].

Lemma 1.1.5. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If $p > 5$ is a prime number such that $\operatorname{Im}\rho_{E,p} \cong G(p)$, where $G(p)$ is the group defined in Theorem 6, then $p \geq 19$ and $j(E) \in \mathbb{Z}$.*

Proof. Suppose by contradiction that $j(E)$ is not an integer. By [LFL21, Theorem 1.2] we have $p \in \{7, 11, 13, 17, 37\}$. However, by Theorem 6 we know that $p \equiv 2 \pmod 3$, and so $p \in \{11, 17\}$. The case $p = 11$ cannot occur by [Zyw15a, Theorem 1.6(i)], while the case $p = 17$ cannot occur by [BDM$^+$23, Theorem 1.2]. □

1.2 Faltings height of elliptic curves

We now give an upper bound on the stable Faltings height of an elliptic curve over $\mathbb{Q}$ in terms of its j-invariant. Any elliptic curve $E/\mathbb{Q}$ can also be considered as an elliptic curve over $\mathbb{C}$, so there exists a complex number $\tau \in \mathcal{H}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}$. We fix such a τ and set $q = e^{2\pi i\tau}$. Our results in this section refine the properties of heights explained in [Sil86].

Definition 1.2.1. We will consider the *standard fundamental domain for the action of* $\mathrm{SL}_2(\mathbb{Z})$ as

$$\mathcal{F} := \left\{ z \in \mathcal{H} : \Re\{z\} \in \left(-\frac{1}{2}, \frac{1}{2}\right], |z| > 1 \right\} \cup \left\{ e^{i\theta} : \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2} \right\}.$$

We begin with the following theorem, which combines [BP11a, Corollary 2.2] with [Paz19, Lemma 2.5].

Theorem 1.2.2. *Let $\tau \in \mathcal{H}$ be in the standard fundamental domain $\mathcal{F}$ and let $E/\mathbb{C}$ be the corresponding elliptic curve. Set $q = e^{2\pi i\tau}$. We have*

$$\log|j(E)| \leq \max\{\log 3500, |\log|q|| + \log 2\}$$

and

$$|\log|q|| \leq \log(|j(E)| + 970.8) < \log|j(E)| + \frac{970.8}{|j(E)|}.$$

Proof. The first inequality follows from [BP11a, Corollary 2.2], while the second one is obtained from [Paz19, Lemma 2.5] using the fact that $\log(x+a) - \log x = \log\left(1 + \frac{a}{x}\right) < \frac{a}{x}$. □

Corollary 1.2.3. *In the setting of Theorem 1.2.2, if* $|j(E)| \geq 3500$*, then*

$$\log|j(E)| - \log 2 \leq |\log|q|| \leq \log|j(E)| + 0.245.$$

Proof. We only need to notice that $|\log|q|| < \log|j(E)| + \log\left(1 + \frac{970.8}{3500}\right) < \log|j(E)| + 0.245$. □

Before stating the precise comparisons between heights that we need, we record the following fact that we will use often.

Theorem 1.2.4. *Let* ${}^{E}\!/_{\mathbb{R}}$ *be an elliptic curve isomorphic to* ${}^{\mathbb{C}}\!/_{\mathbb{Z} \oplus \tau\mathbb{Z}}$ *and let* $q = e^{2\pi i\tau}$*. If* τ *is in the standard fundamental domain* $\mathcal{F}$ *for the action of* $\mathrm{SL}_2(\mathbb{Z})$*, then either* $q \in \mathbb{R}$ *(i.e.* $\Re\{\tau\} \in \{0, \frac{1}{2}\}$*), or* $j(E) \in (0, 1728)$ *(equivalently,* $|\tau| = 1$*).*

Proof. By [Sil94, Proposition V.2.1] we know that the j-function gives a bijection between $\mathbb{R}$ and the set $\mathcal{C} = C_1 \cup C_2 \cup C_3$, where $C_1 = \{it \mid t \geq 1\}$, $C_2 = \left\{e^{i\theta} \mid \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}\right\}$ and $C_3 = \left\{\frac{1}{2} + it \mid t \geq \frac{\sqrt{3}}{2}\right\}$. Moreover, by continuity, it is easy to notice that $j(C_1) = [1728, +\infty)$, $j(C_2) = [0, 1728]$ and $j(C_3) = (-\infty, 0]$. Hence, if $j(E) \notin (0, 1728)$, then $\Re\tau \in \left\{0, \frac{1}{2}\right\}$, which concludes the proof. □

Notation 1.2.5. *Given* $x \in \mathbb{R}$*, we will write* $\log^+ x$ *to mean* $\log\max\{1, x\}$*.*

In the next result, as in the rest of the paper, we denote by $\mathrm{h}_{\mathcal{F}}(E)$ the stable Faltings height of an elliptic curve E, with the normalisation of [Del85a, Section 1.2].

Theorem 1.2.6. *Let* ${}^{E}\!/_{\mathbb{Q}}$ *be an elliptic curve with stable Faltings height* $\mathrm{h}_{\mathcal{F}}(E)$*. Let* $\tau \in \mathcal{H}$ *be the point in the standard fundamental domain* $\mathcal{F}$ *such that* $E(\mathbb{C}) \cong {}^{\mathbb{C}}\!/_{\mathbb{Z} \oplus \tau\mathbb{Z}}$*, and set* $q = e^{2\pi i\tau}$*.*

1. *If* $|j(E)| > 3500$*, then*

$$\mathrm{h}_{\mathcal{F}}(E) > \frac{\mathrm{h}(j(E))}{12} - \frac{1}{2}\log\log|j(E)| - 0.406 \qquad \textit{and} \tag{1.2.1}$$

$$\mathrm{h}_{\mathcal{F}}(E) < \frac{\mathrm{h}(j(E))}{12} - \frac{1}{2}\log\log|j(E)| + 0.159, \tag{1.2.2}$$

   where $\mathrm{h}(x)$ *is the logarithmic Weil height of* x *(i.e., if* $x = \frac{a}{b}$ *with* $(a, b) = 1$*, we set* $\mathrm{h}(x) = \log\max\{|a|, |b|\}$*).*

2. *If* $|j(E)| \leq 3500$*, then*

$$\frac{1}{12}\mathrm{h}(j(E)) - 1.429 < \mathrm{h}_{\mathcal{F}}(E) < \frac{1}{12}\mathrm{h}(j(E)) - 0.135. \tag{1.2.3}$$

3. If $j \in \mathbb{Z}$, then

$$\mathrm{h}_{\mathcal{F}}(E) < -\frac{1}{12}\log|q| - \frac{1}{2}\log|\log|q|| - \frac{1}{2}\log 2 - \frac{\pi^2}{3\log|q|}. \tag{1.2.4}$$

4. We always have

$$\mathrm{h}_{\mathcal{F}}(E) > -\frac{1}{12}\log|q| - \frac{1}{2}\log|\log|q|| - \frac{1}{2}\log 2 - \frac{2|q|}{1-|q|}. \tag{1.2.5}$$

Remark 1.2.7. It is well known that $|\,\mathrm{h}_{\mathcal{F}}(E) - \frac{\mathrm{h}(j)}{12}| < \log(\mathrm{h}(j)+1) + O(1)$ (see [Sil86, Proposition 2.1]), but the above theorem also gives a bound in the opposite direction, namely, $|\,\mathrm{h}_{\mathcal{F}}(E) - \frac{\mathrm{h}(j)}{12}| > \frac{1}{2}\log\log|j| + O(1)$.

Proof. By [Sil86, Proposition 1.1] we have that $\mathrm{h}_{\mathcal{F}}(E)$ equals

$$\frac{1}{12[K:\mathbb{Q}]}\left(\log|N_{K/\mathbb{Q}}(\Delta_{E/K})| - \sum_{v\in M_K^\infty} n_v \log\left(|\Delta(\tau_v)|(\pi^{-1}\Im\{\tau_v\})^6\right)\right), \tag{1.2.6}$$

where $K/\mathbb{Q}$ is a finite Galois extension over which E has semistable reduction everywhere, $\Delta_{E/K}$ is the minimal discriminant of E over K, M_K^∞ is the set of the Archimedean places of K, τ_v is an element of $\mathcal{H}$ such that $E(\overline{K}_v) \cong \mathbb{C}/\mathbb{Z} + \tau_v\mathbb{Z}$, and $\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}$, with $q = e^{2\pi i\tau}$. Note that [Sil86, Proposition 1.1] is formulated with a different normalisation of the Faltings height, but it is easy to convert from Silverman's convention to Deligne's: specifically, the height h in [Sil86, Proposition 1.1] satisfies $h(E) = \mathrm{h}_{\mathcal{F}}(E) - \frac{1}{2}\log\pi$. This difference is reflected in the factor π^{-1} in equation (1.2.6).

Let e_p, f_p be respectively the ramification index and inertia degree in K of the rational prime p, and let r_p be the number of distinct primes of $\mathcal{O}_K$ dividing p (the numbers e_p, f_p only depend on p since $K/\mathbb{Q}$ is a Galois extension). Given that $j = j(E)$ is a rational number, we have

$$\begin{aligned} N_{K/\mathbb{Q}}(\Delta_{E/K}) &= \prod_{\substack{Q\subset\mathcal{O}_K \\ \text{prime}}} \left|\frac{\mathcal{O}_K}{Q^{\max\{0,-v_Q(j)\}}}\right| = \prod_{p \text{ prime}} \left(p^{f_p \max\{0,-e_p v_p(j)\}}\right)^{r_p} \\ &= \prod_{p \text{ prime}} \left(p^{\max\{0,-v_p(j)\}}\right)^{[K:\mathbb{Q}]} = \prod_{p \text{ prime}} \left(\max\{1,\|j\|_p\}\right)^{[K:\mathbb{Q}]}, \end{aligned}$$

where the first equality holds by [Sil09, Table 15.1] and the fact that E has semistable, hence in particular multiplicative, reduction at primes dividing the discriminant. For every $v \in M_K^\infty$ we can assume that τ_v belongs to the

standard fundamental domain $\mathcal{F}$, so, since E is defined over $\mathbb{Q}$, we may use the same $\tau_v = \tau$ for every v. Writing $\Im\{\tau\} = -\frac{\log|q|}{2\pi} = \frac{|\log|q||}{2\pi}$, we have

$$\begin{aligned}|\Delta(\tau)|(\pi^{-1}\Im\{\tau\})^6 &= (2\pi)^{12}|q|\prod_{n=1}^{\infty}|1-q^n|^{24}\cdot 2^{-6}\pi^{12}|\log|q||^6\\ &= 2^6\,|q|\cdot|\log|q||^6\prod_{n=1}^{\infty}|1-q^n|^{24},\end{aligned}$$

and so $12\,\mathrm{h}_{\mathcal{F}}(E)$ equals

$$\sum_{p\text{ prime}}\log^+\|j\|_p - \log|q| - 6\log 2 - 6\log|\log|q|| - 24\sum_{n=1}^{\infty}\log|1-q^n|. \quad (1.2.7)$$

Using the fact that, for every $z\in\mathbb{C}$ such that $|z|<1$, by triangular inequality we have $|\log|1-z||\le -\log|1-|z||$, from Lemma 1.1.1 we obtain

$$-24\sum_{n=1}^{\infty}\log|1-q^n| < -24\sum_{n=1}^{\infty}\log(1-|q|^n) < -\frac{4\pi^2}{\log|q|}. \quad (1.2.8)$$

Replacing in equation (1.2.7), we get

$$\mathrm{h}_{\mathcal{F}}(E) < \frac{1}{12}\left(\sum_{p\text{ prime}}\log^+\|j\|_p - \log|q| - 6\log 2 - \frac{4\pi^2}{\log|q|} - 6\log|\log|q||\right).$$

We note that for $j\in\mathbb{Z}$ we have $\|j\|_p\le 1$ for every prime p, and (1.2.4) follows.

To prove the upper bound in part 1, we note that $\log|j| = \log\max\{1,|j|\}$, and using Corollary 1.2.3 together with the assumption $|j(E)|\ge 3500$ we obtain

$$\begin{aligned}\mathrm{h}_{\mathcal{F}}(E) &< \frac{1}{12}\left(\sum_{p\text{ prime}}\log^+\|j\|_p + \log^+|j| + 0.245\right.\\ &\qquad\left. -6\log 2 - \frac{4\pi^2}{\log|q|} - 6\log|\log|q||\right)\\ &= \frac{\mathrm{h}(j)}{12} + \frac{0.245}{12} - \frac{1}{2}\log 2 - \frac{\pi^2}{3\log|q|} - \frac{1}{2}\log|\log|q||\\ &< \frac{\mathrm{h}(j)}{12} - 0.326 + \frac{\pi^2}{3(\log|j| - \log 2)} - \frac{1}{2}\log(\log|j| - \log 2)\\ &< \frac{\mathrm{h}(j)}{12} - \frac{1}{2}\log\log|j| + 0.159.\end{aligned}$$

On the other hand, using that $\log(1+x) < x$ for every $x > 0$, we have

$$-2\sum_{n=1}^{\infty} \log|1-q^n| \geq -2\sum_{n=1}^{\infty} \log(1+|q|^n) > -2\sum_{n=1}^{\infty} |q|^n = -\frac{2|q|}{1-|q|}. \quad (1.2.9)$$

Noting that $\log\max\{1, \|j\|_p\} \geq 0$ for every p, we see from equation (1.2.7) that the inequality in (1.2.5) holds. To prove the lower bound in part 1, we use $\log|j| > -\log|q| > \log|j| - \log 2$ (Theorem 1.2.2) in equation (1.2.7) to obtain

$$\begin{aligned} \mathrm{h}_{\mathcal{F}}(E) &> \frac{1}{12}\sum_{p \text{ prime}} \log^+ \|j\|_p + \frac{1}{12}\log|j| - \frac{7}{12}\log 2 - \frac{1}{2}\log\log|j| - \frac{4}{|j|-2} \\ &> \frac{\mathrm{h}(j)}{12} - \frac{1}{2}\log\log|j| - \frac{7}{12}\log 2 - \frac{2}{1749}. \end{aligned}$$

It remains to show part 2. Assume that $|j(E)| \leq 3500$. Combining equations (1.2.8) and (1.2.9) we have

$$-\frac{24|q|}{1-|q|} < -24\sum_{n=1}^{\infty} \log|1-q^n| < -\frac{4\pi^2}{\log|q|}.$$

By Theorem 1.2.2 we know that $\pi\sqrt{3} \leq 2\pi\Im\{\tau\} = |\log|q|| < \log(3500 + 970.8) < 8.41$, and so we have

$$\begin{aligned} -\log|q| - 6\log|\log|q|| + \frac{4\pi^2}{|\log|q||} &< 2.533, \\ -\log|q| - 6\log|\log|q|| - \frac{24|q|}{1-|q|} &> -4.828. \end{aligned}$$

Using the inequality $0 \leq \log^+|j|$, we can then write

$$12\,\mathrm{h}_{\mathcal{F}}(E) < \sum_{p \text{ prime}} \log^+ \|j\|_p + \log^+|j| - 6\log 2 + 2.533,$$

which gives the desired upper bound. For the lower bound, we have that $\log^+|j| \leq \log 3500$, and then we conclude by writing

$$12\,\mathrm{h}_{\mathcal{F}}(E) > \sum_{p \text{ prime}} \log^+ \|j\|_p + \log^+|j| - \log 3500 - 6\log 2 - 4.828. \qquad \square$$

Remark 1.2.8. The above argument even gives

$$\mathrm{h}_{\mathcal{F}}(E) \leq \frac{\mathrm{h}(j)}{12} - \frac{1}{2}\log\log|j| - \frac{1}{2}\log 2 + o(1) \ \text{ as } |j| \to \infty,$$

yielding a better constant term as j grows. Explicitly, one has

$$\mathrm{h}_{\mathcal{F}}(E) < \frac{\mathrm{h}(j)}{12} - \frac{1}{2}\log\log|j| - \frac{1}{2}\log 2 + \left(\frac{\log 2}{2} + \frac{\pi^2}{3}\right)\frac{1}{\log|j| - \log 2} + \frac{970.8}{|j|},$$

where we have used $\log(x - \log 2) - \log x = -\sum_n \frac{(\log 2)^n}{nx^n} > -\sum_n \frac{(\log 2)^n}{x^n} = -\frac{\log 2}{x - \log 2}$, with $x = \log|j|$.

Remark 1.2.9. Minimising the function

$$-\frac{1}{12}\log x - \frac{1}{2}\log|\log x| - \frac{1}{2}\log 2 - \frac{2x}{1-x}$$

over the interval $(0, e^{-\pi\sqrt{3}}]$, we obtain that for every elliptic curve $E/\bar{\mathbb{Q}}$ we have $\mathrm{h}_{\mathcal{F}}(E) > -0.74885$. This fits well with the computation by Deligne of the absolute minimum of the height [Del85a, pag. 29]. With our normalisation, Deligne has shown that the minimum of $\mathrm{h}_{\mathcal{F}}(E)$ is approximately -0.74875, attained for the elliptic curve with $j = 0$, for which $|q| = e^{-\pi\sqrt{3}}$. Moreover, this is the minimum height for elliptic curves over every number field.

Remark 1.2.10. For $j \in \mathbb{Z}$, Theorem 1.2.6 implies that

$$\mathrm{h}_{\mathcal{F}}(E) = -\frac{1}{12}\log|q| - \frac{1}{2}\log|\log|q|| - \frac{1}{2}\log 2 + O\left(\frac{1}{\log|q|}\right)$$

as $|q| \to 0$.

1.3 Schur–Zassenhaus for p-adic matrices

Let p be an odd prime and let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$, uniformiser π_K and residue field $\mathbb{F}_q = \mathbb{F}_{p^k}$.

The following proposition is a profinite version of the Schur-Zassenhaus theorem, and can be found in [Wil98, Proposition 2.3.3].

Proposition 1.3.1. *Let G be a profinite group and let N be a normal subgroup such that $|N|$ and $\left|G/N\right|$ are coprime (where the cardinalities are supernatural numbers defined as in [Wil98, Definition 2.1.1]). Then G has subgroups H such that $G = NH$ and $H \cap N = 1$; moreover, all such subgroups H are conjugate in G. In particular, for any such H we have an isomorphism $G \cong H \ltimes N$, with the action given by conjugation.*

Proposition 1.3.2. *Let $\mathcal{G}' < \mathrm{GL}_n(\mathcal{O}_K)$ be a subgroup and let $\pi : \mathrm{GL}_n(\mathcal{O}_K) \to \mathrm{GL}_n\left(\mathcal{O}_K/\pi_K\right) = \mathrm{GL}_n(\mathbb{F}_q)$ be the canonical projection. Let $G < G' := \pi(\mathcal{G}')$ be a subgroup of order prime to p.*

- *There exists a subgroup $\mathcal{G} < \mathcal{G}'$ such that π induces an isomorphism $\mathcal{G} \cong G$. Moreover, $\mathcal{G}$ is unique up to conjugation in $\mathcal{G}'$.*
- *Suppose $G = G'$, let $\mathcal{G}$ be as above, and let $\mathcal{N} := \ker \pi \cap \mathcal{G}'$. We have*

$$\mathcal{G}' = \mathcal{G}\mathcal{N} \cong \mathcal{G} \ltimes \mathcal{N} \cong G \ltimes \mathcal{N},$$

where the action is given by conjugation of $\mathcal{G}$ on $\mathcal{N}$.

Proof. Consider the groups

$$\mathcal{G}'' := \{A \in \mathcal{G}' \mid \pi(A) \in G\} \qquad \text{and} \qquad \mathcal{N} := \{A \in \mathcal{G}' \mid A \equiv I \pmod{\pi_K}\}.$$

It is not difficult to notice that $\mathcal{N}$ is a pro p-group, $\mathcal{N} \lhd \mathcal{G}''$ and $\mathcal{G}''/\mathcal{N} = G$. By Proposition 1.3.1 there exists $\mathcal{G} < \mathcal{G}''$ such that $\mathcal{G}\mathcal{N} = \mathcal{G}''$ and $\mathcal{G} \cap \mathcal{N} = 1$, hence

$$G = \frac{\mathcal{G}''}{\mathcal{N}} = \frac{\mathcal{G}\mathcal{N}}{\mathcal{N}} \cong \frac{\mathcal{G}}{\mathcal{G} \cap \mathcal{N}} = \mathcal{G}.$$

This implies that $|\mathcal{G}| = |G|$, and since π surjects $\mathcal{G}$ onto G, as $\pi(\mathcal{G}'') = \pi(\mathcal{G}\mathcal{N}) = \pi(\mathcal{G})$, it is an isomorphism. Suppose now that $\widehat{\mathcal{G}} < \mathcal{G}'$ is another group with the same property. Since $\pi(\widehat{\mathcal{G}}) = G$, we have $\widehat{\mathcal{G}} < \mathcal{G}''$ and $\widehat{\mathcal{G}}\mathcal{N} = \mathcal{G}'' = \mathcal{G}\mathcal{N}$. Moreover, the homomorphism $\pi|_{\widehat{\mathcal{G}}}$ is injective, so $\widehat{\mathcal{G}} \cap \mathcal{N} = 1$. By Proposition 1.3.1 we conclude that $\mathcal{G}$ and $\widehat{\mathcal{G}}$ are conjugate in $\mathcal{G}''$ (and hence in $\mathcal{G}'$). The second part follows immediately from Proposition 1.3.1. □

We finish this section with the following lemma, which is an adapted version of Hensel's lemma to matrices.

Lemma 1.3.3. *Let m, n be positive integers. Fix $A \in M_{n\times n}\left(\mathcal{O}_K/\pi_K^m\right)$ and let $\overline{A}$ be its reduction modulo π_K. Suppose that $\overline{A}$ has n distinct eigenvalues in $\overline{\mathbb{F}}_p$. There exists an unramified extension L/K (hence such that $\mathcal{O}_K/\pi_K^m \subseteq \mathcal{O}_L/\pi_L^m$) for which the characteristic polynomial of A has exactly n distinct roots in $\mathcal{O}_L/\pi_L^m$, which are invariant under conjugation of A.*

Proof. Consider a lift $\widetilde{A}$ of A in $\mathcal{O}_K$. Since $\overline{A}$ has distinct eigenvalues, the splitting field L of the characteristic polynomial of $\widetilde{A}$ is unramified. In particular, we have that $\pi_L = \pi_K$ and $\mathcal{O}_K/\pi_K^m \subseteq \mathcal{O}_L/\pi_L^m$. Consider the characteristic polynomial $f_{\widetilde{A}}$ of $\widetilde{A}$ and its roots $\widetilde{\lambda}_1, \ldots, \widetilde{\lambda}_n$. We know that $\widetilde{\lambda}_1, \ldots, \widetilde{\lambda}_n \in \mathcal{O}_L$ and we consider their reductions $\lambda_1, \ldots, \lambda_n$ and $\overline{\lambda}_1, \ldots, \overline{\lambda}_n$ modulo π_L^m and π_L respectively. By Hensel's lemma, we know that $\lambda_1, \ldots, \lambda_n$ are the unique lifts of $\overline{\lambda}_1, \ldots, \overline{\lambda}_n$, which are the roots of $f_{\widetilde{A}} \pmod{\pi_L}$. In particular, $\lambda_1, \ldots, \lambda_n$ are the unique roots of the characteristic polynomial of A, which is $f_A = f_{\widetilde{A}} \pmod{\pi_L^m}$. Moreover, they are invariant under conjugation, as f_A is. □

CHAPTER 2

p-adic Cartan groups

The aim of this chapter is to improve some of the results of [Zyw11]. In particular, we study some subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$ with the main property of being contained in $C_{ns}^+(p)$ once we consider their projection modulo p. We define these subgroups *N-Cartan lifts*. We give a classification of all the possible N-Cartan lifts satisfying some restrictive properties. This classification will be used to prove that, given an elliptic curve $E/\mathbb{Q}$ without CM and a prime p such that $\mathrm{Im}\,\rho_{E,p} \subseteq C_{ns}^+(p)$, in most cases, there exists $n \geq 1$ such that $\mathrm{Im}\,\rho_{E,p^n} = C_{ns}^+(p^n)$ and $\mathrm{Im}\,\rho_{E,p^\infty} \supset I + p^n M_{2\times 2}(\mathbb{Z}_p)$. This will allow us to compute the index $[\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{Im}\,\rho_{E,p^\infty}]$ with quite good precision.

2.1 Cartan lifts

To study the possible images of a p-adic Galois representation attached to an elliptic curve, we start by considering a generic subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ satisfying some of the usual properties of these images. In particular, we will focus on the Cartan case.

Definition 2.1.1. Given a prime p and a subgroup $G < \mathrm{GL}_2(\mathbb{Z}_p)$, for every $n \geq 1$ we define:

- $G(p^n) := G \pmod{p^n} \subseteq \mathrm{GL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$;
- $G_n := \{A \in G \mid A \equiv I \pmod{p^n}\}$

Remark 2.1.2. It is not difficult to notice that $G(p^n) = G/G_n$.

Let $\mathfrak{gl}_2(\mathbb{F}_p)$ be the additive group of 2×2 matrices with coefficients in $\mathbb{F}_p$ and let $\mathfrak{sl}_2(\mathbb{F}_p)$ be the subgroup of trace 0 matrices. They are Lie algebras over $\mathbb{F}_p$ when equipped with the usual bracket $[A, B] = AB - BA$.

Definition 2.1.3. For every $n \geq 1$, we have an injective group homomorphism ${}^{G_n}\!/_{G_{n+1}} \hookrightarrow \mathfrak{gl}_2(\mathbb{F}_p)$, sending $I + p^n A$ to the class of A modulo p. We call $\mathfrak{g}_n$ the image of this homomorphism, and $\mathfrak{s}_n := \mathfrak{g}_n \cap \mathfrak{sl}_2(\mathbb{F}_p)$.

Given a group $G < \mathrm{GL}_2(\mathbb{Z}_p)$, throughout this section, we will call $S := G \cap \mathrm{SL}_2(\mathbb{Z}_p)$. Recall that $\det(I + xA) \equiv 1 + x \operatorname{tr} A \pmod{x^2}$ as polynomials in x. We notice that if $\det(G_n) \subseteq 1 + p^{n+1}\mathbb{Z}_p$, then $\mathfrak{g}_n \subseteq \mathfrak{sl}_2(\mathbb{F}_p)$. In particular, if $G = S$, then $\mathfrak{g}_n \subseteq \mathfrak{sl}_2(\mathbb{F}_p)$ for all $n \geq 1$, and so $\mathfrak{s}_n$ is the image of ${}^{S_n}\!/_{S_{n+1}}$ in $\mathfrak{gl}_2(\mathbb{F}_p)$.

As shown in [Zyw11, Lemma 2.2(i)], the groups $\mathfrak{g}_n$ have the following property.

Lemma 2.1.4 (Zywina)**.** *If p is an odd prime, for every $n \geq 1$ we have $\mathfrak{g}_n \subseteq \mathfrak{g}_{n+1}$. If $p = 2$, the same statement holds for $n \geq 2$.*

Definition 2.1.5. Let p be an odd prime and let ε be the reduction modulo p of the least positive integer which represents a quadratic non-residue in $\mathbb{F}_p^\times$. We define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$:

$$\text{Borel:} \qquad B := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Z}_p,\ a, c \in \mathbb{Z}_p^\times \right\},$$

$$\text{split Cartan:} \qquad C_{sp} := \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z}_p^\times \right\},$$

$$\text{non-split Cartan:} \qquad C_{ns} := \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z}_p,\ (a, b) \not\equiv (0, 0) \mod p \right\}.$$

Define also $C_{sp}^+ := C_{sp} \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C_{sp}$ and $C_{ns}^+ := C_{ns} \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns}$. These are the normalisers of C_{sp} and C_{ns} respectively.

Throughout this section, we will indicate with C a generic Cartan subgroup, which is either C_{sp} or C_{ns}. Moreover, we will assume that p is an odd prime.

Definition 2.1.6. Let p be an odd prime and let $G < \mathrm{GL}_2(\mathbb{Z}_p)$ be a subgroup. We will say that G is an *N-Cartan lift* if it satisfies the following properties:

- G is closed;
- $\det(G) = \mathbb{Z}_p^\times$;
- $G(p)$ is contained in the normaliser of a Cartan subgroup, but is not contained in the Cartan subgroup;

- $G(p)$ contains an element of the Cartan subgroup which is not a multiple of the identity.

We will say that G is a *split N-Cartan lift* or a *non-split N-Cartan lift* if $G(p)$ is contained in the normaliser of a split or non-split Cartan respectively.

Let $G < \mathrm{GL}_2(\mathbb{Z}_p)$ be a subgroup such that $p \nmid |G(p)|$. We notice that for every $n \geq 1$, the group G acts on G_n by conjugation, and hence also on the quotient G_n/G_{n+1}. This action factors through the group $G(p)$. In particular, this implies that $\mathfrak{g}_n$ is an $\mathbb{F}_p[G(p)]$-module, with $G(p)$ acting by conjugation. We have the following result by Zywina ([Zyw11, Lemma 2.4]).

Lemma 2.1.7 (Zywina)**.** *Let $G < \mathrm{GL}_2(\mathbb{Z}_p)$ be an N-Cartan lift with respect to the Cartan group C. The groups $\mathfrak{g}_n$ are $\mathbb{F}_p[G(p)]$-submodules of $\mathfrak{gl}_2(\mathbb{F}_p)$. Suppose that there exists an element in $G(p) \cap C(p)$ whose image in $\mathrm{PGL}_2(\mathbb{F}_p)$ has order greater than 2. If G is a non-split N-Cartan lift, then we have a decomposition in irreducible submodules $\mathfrak{gl}_2(\mathbb{F}_p) = V_1 \oplus V_2 \oplus V_3$, where*

$$V_1 = \mathbb{F}_p \cdot \mathrm{Id}, \quad V_2 = \mathbb{F}_p \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}, \quad V_3 = \mathbb{F}_p \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus \mathbb{F}_p \begin{pmatrix} 0 & \varepsilon \\ -1 & 0 \end{pmatrix}.$$

If instead G is a split N-Cartan lift, then we have a decomposition in irreducible submodules $\mathfrak{gl}_2(\mathbb{F}_p) = V_1 \oplus V_2 \oplus V_3$, where

$$V_1 = \mathbb{F}_p \cdot \mathrm{Id}, \quad V_2 = \mathbb{F}_p \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad V_3 = \mathbb{F}_p \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \mathbb{F}_p \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Finally, in both cases V_3 is not a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_p)$.

In [Zyw11, Lemma 2.4] Zywina assumes that the image of $G(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order at least 5. However, in his proof, this assumption is only used to apply [Zyw11, Lemma 2.1(v)], and then an element of order greater than 2 is sufficient.

Remark 2.1.8. If $G = C$ is a Cartan subgroup, by a direct computation it is easy to check that for every $n \geq 1$ we have $\mathfrak{g}_n = V_1 \oplus V_2$. Similarly, if $G = C^+$, since $[C^+ : C] = 2$, we have $\mathfrak{g}_n = V_1 \oplus V_2$.

Remark 2.1.9. When every element in the image of $G(p) \cap C(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ has order 1 or 2, one can verify that V_3 decomposes into two irreducible submodules. In the split case, V_3 decomposes as $\mathbb{F}_p \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \mathbb{F}_p \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. In the non-split case, V_3 decomposes as $\mathbb{F}_p \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus \mathbb{F}_p \begin{pmatrix} 0 & \varepsilon \\ -1 & 0 \end{pmatrix}$.

Lemma 2.1.10 (Zywina)**.** *Suppose $G < \mathrm{GL}_2(\mathbb{Z}_p)$ is a closed subgroup such that $\det G \supseteq 1 + p\mathbb{Z}_p$ and $p \nmid |G(p)|$. For every $n \geq 1$ we have $\mathrm{tr}(\mathfrak{g}_n) = \mathbb{F}_p$ and $\mathfrak{s}_n = \mathfrak{g}_n \cap \mathfrak{sl}_2(\mathbb{F}_p)$.*

Proof. The proof is the same as that of [Zyw11, Lemma 2.5]. □

Corollary 2.1.11. *If $G < \mathrm{GL}_2(\mathbb{Z}_p)$ is an N-Cartan lift, then $V_1 \subseteq \mathfrak{g}_n$ for every $n \geq 1$.*

Proof. Using Lemma 2.1.7 we see that $\mathrm{tr}(V_2 \oplus V_3) = 0$, hence $V_1 \subseteq \mathfrak{g}_n$. □

Lemma 2.1.12. *Let G be an N-Cartan lift. Suppose that the image of $G(p) \cap C(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order greater than 2.*

1. *If $\dim \mathfrak{g}_1 = 2$, then for every $n > 1$ we have $\dim \mathfrak{g}_n \in \{2, 4\}$, and if $\dim \mathfrak{g}_n = 4$ for some n, then for every $m > n$ the equality $\dim \mathfrak{g}_m = 4$ holds.*

2. *If $\dim \mathfrak{g}_1 = 3$, then $\dim \mathfrak{g}_n = 4$ for every $n > 1$.*

Proof. To prove the first part, it suffices to notice that by Lemma 2.1.7 and Corollary 2.1.11 we have $\mathfrak{g}_1 = V_1 \oplus V_2$, where V_1, V_2 and V_3 are defined in Lemma 2.1.7. Using Lemma 2.1.4 we see that for every $n \geq 1$ we have either $\mathfrak{g}_n = V_1 \oplus V_2$ or $\mathfrak{g}_m = \mathfrak{gl}_2$ for every $m \geq n$, and hence the conclusion follows. To prove the second part, we notice that $\mathfrak{g}_1 = V_1 \oplus V_3$ and if $\dim \mathfrak{g}_2 < 4$, then $\mathfrak{g}_2 = \mathfrak{g}_1$ (by Lemma 2.1.4). By [Zyw11, Lemma 2.2(iv)], this implies that $\mathfrak{g}_1$ is a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_p)$, hence also $\mathfrak{s}_1 = \mathfrak{g}_1 \cap \mathfrak{sl}_2(\mathbb{F}_p) = V_3$ is a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_p)$, which contradicts Lemma 2.1.7. □

The following proposition is a stronger version of [Zyw11, Proposition 1.2].

Proposition 2.1.13. *Let $G < \mathrm{GL}_2(\mathbb{Z}_p)$ be an N-Cartan lift with respect to the Cartan group C such that $\dim \mathfrak{g}_1 > 1$, and suppose that there exists an element in $G(p) \cap C(p)$ whose image in $\mathrm{PGL}_2(\mathbb{F}_p)$ has order greater than 2. For every integer $n \geq 1$ we have the following.*

1. *If $\dim \mathfrak{g}_n = 2$, then $G(p^n) \subseteq C^+(p^n)$ and $[C^+(p^n) : G(p^n)] = [C^+(p) : G(p)]$;*

2. *If $\dim \mathfrak{g}_n = 3$, then $n = 1$ and $G \supset I + p^2 M_{2\times 2}(\mathbb{Z}_p)$;*

3. *If $\dim \mathfrak{g}_n = 4$, then $G \supset I + p^n M_{2\times 2}(\mathbb{Z}_p)$.*

Proof. Set $S = G \cap \mathrm{SL}_2(\mathbb{Z}_p)$. The proof of this proposition follows that of [Zyw11, Proposition 2.3]. If $\dim \mathfrak{g}_n = 3$, by Lemma 2.1.12 we know that $n = 1$ and $\dim \mathfrak{g}_2 = 4$, so by [Zyw11, Lemma 2.2(ii)] we have $G \supset I + p^2 M_{2\times 2}(\mathbb{Z}_p)$. If $\dim \mathfrak{g}_n = 4$, by [Zyw11, Lemma 2.2(ii)] we have $G \supset I + p^n M_{2\times 2}(\mathbb{Z}_p)$. We now

focus on the case $\dim \mathfrak{g}_n = 2$. By Corollary 2.1.11 we have that $\dim \mathfrak{s}_i = 1$, so by immediate induction, ${}^{S_1}\!/_{S_{i+1}}$ is of order p^i for every $i \in \{1, \dots, n\}$. In particular, lifting to S_1 a non-zero element of $\mathfrak{s}_1$ and projecting it to $S(p^{n+1})$, we find an element $h = I + pA \in S(p^{n+1})$ such that $A \not\equiv 0 \pmod p$. Since h has order p^n in $G(p^{n+1})$, by cardinality arguments the group $H := S_1 \pmod{p^{n+1}}$ is generated by h. As $\dim \mathfrak{s}_1 = 1$, by Lemma 2.1.7 the matrix $A \pmod p$ is a non-zero element of V_2, hence in particular $A \pmod p \in C(p)$. Since H is stable under conjugation by $G(p^{n+1})$ and $A \pmod p$ is an element of $C(p)$, by [Zyw11, Lemma 2.1(iv)] we know that $H \subset C(p^{n+1})$. We have

$$H = \left\{ g \in C(p^{n+1}) \cap \mathrm{SL}_2\left({}^{\mathbb{Z}}\!/_{p^{n+1}\mathbb{Z}}\right) : g \equiv I \pmod p \right\},$$

since the inclusion "$\subseteq$" is trivial and the equality follows by cardinality. Consider the group $C_1(p^{n+1}) := \{M \in C(p^{n+1}) \mid M \equiv I \pmod p\}$: this is generated by the subgroups H and $\{(1 + p\alpha)I\}$; indeed, they are disjoint and the product of their cardinalities equals $|C_1(p^{n+1})|$. As $G(p^{n+1})$ normalises H, it also normalises the group $C_1(p^{n+1})$, since every matrix in this group can be written as $M = (1 + p\alpha)h^k$, for some $k \in \mathbb{N}$ and $\alpha \in {}^{\mathbb{Z}}\!/_{p^{n+1}\mathbb{Z}}$. Consider an element $I + pA \in \mathrm{GL}_2\left({}^{\mathbb{Z}}\!/_{p^{n+1}\mathbb{Z}}\right)$: this is in $C_1(p^{n+1})$ if and only if $A \pmod{p^n} \in C(p^n) \cup \{0\}$. For every $g \in G$ and $A \in C(p^n) \cup \{0\}$ we have $g^{-1}(I+pA)g = I+pg^{-1}Ag \in C_1(p^{n+1})$, and so $g^{-1}Ag \pmod{p^n} \in C(p^n)\cup\{0\}$, and it is 0 if and only if $A = 0$. This implies that $G(p^n)$ normalises $C(p^n)$, and so $G(p^n) \subseteq C^+(p^n)$. However,

$$|G(p^n)| = |G(p)| \cdot \prod_{i=1}^{n-1} |\mathfrak{g}_i| = |G(p)| \cdot p^{2n-2} = |G(p)| \cdot \frac{|C^+(p^n)|}{|C^+(p)|},$$

and hence we have $[C^+(p^n) : G(p^n)] = [C^+(p) : G(p)]$. □

If G is an N-Cartan lift such that $\dim \mathfrak{g}_n = 4$ for sufficiently large n, a statement equivalent to the proposition above (if we are not in the case $\dim \mathfrak{g}_1 = 3$) is that if n is the largest positive integer such that $G(p^n) \subseteq C^+_{ns}(p^n)$, then $G \supset I + p^{n+1}M_{2\times 2}(\mathbb{Z}_p)$. However, if we add the hypothesis that G contains many scalar matrices, we can prove a stronger result.

Theorem 2.1.14. *Let $G < \mathrm{GL}_2(\mathbb{Z}_p)$ be an N-Cartan lift as in Proposition 2.1.13 and such that $G \supset (1 + p\mathbb{Z}_p)I$. One of the following holds:*

- *$G < C^+$ up to conjugation and $[C^+ : G] = [C^+(p) : G(p)]$;*
- *There exists $n \geq 1$ such that $G \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$ and $G(p^n) \subseteq C^+(p^n)$ up to conjugation, with $[C^+(p^n) : G(p^n)] = [C^+(p) : G(p)]$;*

- $G \supseteq I + p^2 M_{2\times 2}(\mathbb{Z}_p)$ *and*

$$G(p^2) \cong G(p) \ltimes (V_1 \oplus V_3),$$

with V_i defined as in Lemma 2.1.7 and the semidirect product defined by the conjugation action.

Proof. Suppose that $\dim \mathfrak{g}_1 = 3$. By Proposition 2.1.13(1) we know that $G \supset I+p^2 M_{2\times 2}(\mathbb{Z}_p)$. We can then apply Proposition 1.3.2 to obtain $G \cong G(p) \ltimes G_1$, and projecting modulo p^2 we have $G(p^2) \cong G(p) \ltimes \mathfrak{g}_1$, where by Lemma 2.1.7 we have $\mathfrak{g}_1 = V_1 \oplus V_3$. Suppose now $\dim \mathfrak{g}_1 \neq 3$. It is sufficient to prove that, given $n \geq 2$, if $\dim \mathfrak{g}_{n-1} < 4$ we have $G(p^n) \subseteq C^+(p^n)$ up to conjugation and $[C^+(p^n) : G(p^n)] = [C^+(p) : G(p)]$. We divide the proof in 4 steps.
1. By Proposition 2.1.13 we know that $\dim \mathfrak{g}_{n-1} = 2$ and $G(p^{n-1}) \subseteq C^+(p^{n-1})$, with $[C^+(p^{n-1}) : G(p^{n-1})] = [C^+(p) : G(p)]$.
2. We now prove that the subgroup $G_1(p^n) \subseteq G(p^n)$ coincides with the group $H = C_1(p^n) := \{g \in C(p^n) : g \equiv I \pmod p\}$. By the proof of Proposition 2.1.13 we know that

$$H_2 := \left\{ g \in C(p^n) \cap \mathrm{SL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right) : g \equiv I \pmod p \right\} \subset G(p^n),$$

moreover, by hypothesis we have that the group $H_1 = \{(1+pk)I \mod p^n\}$ is also contained in $G(p^n)$. We notice that $|H_1| = |H_2| = p^{n-1}$ and $|H| = p^{2n-2}$. Moreover, H_1 is normal in H, hence H_1H_2 is a subgroup of $H \cap G(p^n)$. It is easy to notice that $\det(1+kp)I \equiv 1 \pmod{p^n}$ if and only if $k \equiv 0 \pmod{p^{n-1}}$ and so if and only if $(1+kp)I \equiv I \pmod{p^n}$. This implies that $H_1 \cap H_2 = \{I\}$, and so $|H_1H_2| = |H_1| \cdot |H_2| = |H|$, in particular $H = H_1H_2 \subseteq G(p^n)$. As by Lemma 2.1.12 we know that $|G_1(p^n)| = \prod_{i=1}^{n-1} |\mathfrak{g}_i| = p^{2n-2}$ and $H \subseteq G_1(p^n)$, we have that $G_1(p^n) = H$.
3. Since $p \nmid |G(p)|$, by Proposition 1.3.2 there exists a subgroup $\widetilde{G(p)} < G$ such that the projection modulo p induces an isomorphism $\widetilde{G(p)} \cong G(p)$, and modulo p^n we have $G(p^n) = \widetilde{G(p)} \cdot G_1(p^n) = \widetilde{G(p)} \cdot H$, where we identified $\widetilde{G(p)}$ with its projection modulo p^n. Consider

$$\Gamma := \{A \in \mathrm{GL}_2(\mathbb{Z}_p) \mid A \pmod{p^{n-1}} \in C^+(p^{n-1})\} < \mathrm{GL}_2(\mathbb{Z}_p).$$

By Proposition 2.1.13 we know that $G < \Gamma$, and obviously $C^+ < \Gamma$. By Proposition 1.3.2, there is a group $\widetilde{C^+(p)} < C^+$ isomorphic to $C^+(p)$ via the projection modulo p such that $C^+ = \widetilde{C^+(p)} \cdot C_1^+ \cong \widetilde{C^+(p)} \ltimes C_1^+$. We can then consider the unique subgroup $G' < C^+$ such that $G'_1 = C_1^+$ and $G'(p) = G(p)$. By Proposition 1.3.2 we have $\widetilde{G'(p)} < \widetilde{C^+(p)}$, and since $G, G' < \Gamma$ we have $\widetilde{G(p)} \equiv \widetilde{G'(p)} \pmod{p^{n-1}}$. Moreover, $\widetilde{G(p)}$ and $\widetilde{G'(p)}$ are conjugate in Γ, i.e. there exists $\gamma \in \Gamma$ such that $\gamma^{-1}\widetilde{G(p)}\gamma = \widetilde{G'(p)}$.

4. We notice that $G_1(p^n) = G'_1(p^n) = C^+_1(p^n) = H$. If we identify $\widetilde{G(p)}$, $\widetilde{G'(p)}$ and $\widetilde{C^+(p)}$ with their projections modulo p^n, we have

$$G(p^n) = \widetilde{G(p)} \cdot H, \qquad G'(p^n) = \widetilde{G'(p)} \cdot H, \qquad C^+(p^n) = \widetilde{C^+(p)} \cdot H.$$

Notice that $\gamma^{-1} H \gamma = H$: indeed, given $I + pA \in H$ we have $\gamma^{-1}(I + pA)\gamma = I + p\gamma^{-1}A\gamma \in H$, as $\gamma \pmod{p^{n-1}} \in C^+(p^{n-1})$. Therefore, we have

$$\gamma^{-1} G(p^n) \gamma = \gamma^{-1} \widetilde{G(p)} \gamma \cdot \gamma^{-1} H \gamma = \widetilde{G'(p)} \cdot H = G'(p^n)$$

as desired. Finally, it is easy to check that

$$[C^+(p^n) : G(p^n)] = [C^+(p^n) : G'(p^n)] = [C^+(p) : G(p)]. \qquad \square$$

CHAPTER 3

Local properties

Let E/K be an elliptic curve without CM defined over a number field K, and suppose that for some prime p we have $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ up to conjugacy. In this chapter, we consider E as an elliptic curve over a completion K_λ for various primes λ (including λ above p), and study the representation ρ_{E,p^n} upon restriction to $\operatorname{Gal}\left(\overline{K}_\lambda/K_\lambda\right)$, considered as a decomposition subgroup of $\operatorname{Gal}\left(\overline{K}/K\right)$. In particular, we will show that these curves have potentially good reduction for primes λ such that $N_{K/\mathbb{Q}}(\lambda) \not\equiv \pm 1 \pmod{p^n}$. Moreover, we will show that for sufficiently large p^n the curve E has potentially good supersingular reduction at primes above p.

The main arguments of the chapter rely on the study of the so-called *canonical subgroup* of E and its connection with the Hasse invariant of E. These arguments will allow us to prove different properties of E. First, we will give some conditions on the j invariants of elliptic curves with mod-p representation strictly contained in the normaliser of a non-split Cartan subgroup. Then, in Chapter 6 we will prove that the division fields $K(E[p^n])$ have high ramification index at primes above p, and we will use it to study the entanglement phenomenon among primes p for which $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$.

3.1 The image of the inertia subgroups

Let K be a p-adic field with valuation v and let E be an elliptic curve defined over K with potentially good reduction. If we consider the maximal unramified extension K^{nr} of K, the subgroup $I_K := \operatorname{Gal}\left(\overline{K}/K^{nr}\right) < \operatorname{Gal}\left(\overline{K}/K\right)$ is the

inertia subgroup of $\mathrm{Gal}\left(\overline{K}/K\right)$. By the Néron–Ogg–Shafarevich criterion, the curve E has good reduction if and only if $\rho_{E,\ell^\infty}(I_K) = \{1\}$ for every prime $\ell \neq p$. Every elliptic curve with potentially good reduction acquires good reduction over a finite extension L of K^{nr}. This implies that the subgroup $I_L < I_K$ defined as $\mathrm{Gal}\left(\overline{K}/L\right)$ is contained in the kernel of ρ_{E,ℓ^∞} for every $\ell \neq p$. In particular, the representation ρ_{E,ℓ^∞} over K^{nr} factors through the quotient $\frac{I_L}{I_K}$, i.e.

$$\rho_{E,\ell^\infty}(I_K) \hookrightarrow \frac{I_K}{I_L} \cong \mathrm{Gal}\left(L/K^{nr}\right). \tag{3.1.1}$$

If L is the minimal extension of K^{nr} over which E acquires good reduction, then (3.1.1) is an isomorphism. In particular, we have the following theorem from [Kra90, Proposition 1, Théorèmes 1, 2, 3].

Theorem 3.1.1. *Let E be an elliptic curve with potentially good reduction over K and let L be the minimal extension of K^{nr} over which E acquires good reduction. Let Δ be the minimal discriminant of E over K^{nr} and let c_4 be the standard invariant associated with E. Let $\ell \neq p$ be a prime.*

1. *If $p \geq 5$, then L is the unique tamely ramified extension of K^{nr} of degree $e \in \{1, 2, 3, 4, 6\}$ equal to the denominator of the fraction $\frac{v(\Delta)}{12}$ reduced to lowest terms. In particular,*

$$\rho_{E,\ell^\infty}(I_K) = \mathrm{Gal}\left(L/K^{nr}\right) \cong \mathbb{Z}/e\mathbb{Z}.$$

2. *If $p = 3$, then*

$$|\rho_{E,\ell^\infty}(I_K)| = [L : K^{nr}] \in \{1, 2, 3, 4, 6, 12\}$$

   depending on the valuation of Δ.

3. *If $p = 2$, then*

$$|\rho_{E,\ell^\infty}(I_K)| = [L : K^{nr}] \in \{1, 2, 3, 4, 6, 8, 24\}$$

   depending on the valuation of Δ and c_4.

The first part of Theorem 3.1.1(1) had been already studied by Serre in [Ser72, Section 5.6].

In the case $\ell = p$, we have the opposite phenomenon: the image of the inertia via $\rho_{E,p}$ is large. We will discuss it in details in Theorem 3.1.4 and in the next section.

If we now consider an elliptic curve E defined over a number field K, and λ a prime of K that does not divide p, we can consider the completion K_λ and

Theorem 3.1.1 applies. We can then use it to prove some interesting properties in the case where $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup.

Proposition 3.1.2. *Let E be an elliptic curve defined over a number field K, n a positive integer, and p an odd prime such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ up to conjugation. For any prime $\lambda \subseteq \mathcal{O}_K$ that does not divide p and such that $N_{K/\mathbb{Q}}(\lambda) \not\equiv \pm 1 \pmod{p^n}$, the elliptic curve E has potentially good reduction at λ. Moreover, given $\mathfrak{p} \mid p$ in K, if $p^{n-1}(p-1) \nmid 2e(\mathfrak{p}|p)$, then the elliptic curve E has potentially good reduction at $\mathfrak{p}$.*

Proof. The proof follows and generalises those of [Lem19b, Proposition 3.3] and [Lem19a, Proposition 2.2]. We can assume that E does not have CM, as CM curves have potentially good reduction everywhere. Let $\lambda \mid \ell$ be a prime of potentially multiplicative reduction, let E_{K_λ} be the base change of E to K_λ, and let E_q be the Tate curve with parameter $q \in K_\lambda^\times$, isomorphic to E over a quadratic extension of K_λ. Rename $E = E_{K_\lambda}$. There is a quadratic character ψ such that $\rho_{E_q,p^n} \cong \rho_{E,p^n} \otimes \psi$, and we have

$$\rho_{E,p^n} \cong \psi \otimes \begin{pmatrix} \chi_{p^n} & * \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \psi\chi_{p^n} & * \\ 0 & \psi \end{pmatrix}, \tag{3.1.2}$$

where χ_{p^n} is the cyclotomic character modulo p^n. Consider an automorphism $\sigma \in \operatorname{Gal}\left(\overline{K}_\lambda / K_\lambda\right)$, and set $A := \rho_{E_q,p^n}(\sigma) = \begin{pmatrix} \chi_{p^n}(\sigma) & * \\ 0 & 1 \end{pmatrix}$. By our hypothesis on $\operatorname{Im}\rho_{E,p^n}$ there exists an element of $C_{ns}^+(p^n)$ conjugate to A (up to changing sign by multiplying by $-I$). We now divide cases according to whether $\chi_{p^n}(\sigma) \equiv 1 \pmod{p}$ or $\chi_{p^n}(\sigma) \not\equiv 1 \pmod{p}$.

(i) Suppose first that $\chi_{p^n}(\sigma) \not\equiv 1 \pmod{p}$. We know that the roots of the characteristic polynomial of A are 1 and $\chi_{p^n}(\sigma)$. In particular, there exists an element g in $C_{ns}^+(p^n)$ satisfying the polynomial equation $(g-1)(g-\chi_{p^n}(\sigma)) = 0$. If $g \in C_{ns}(p^n)$, then $\overline{g} = g \pmod{p}$ is either a scalar matrix or it has eigenvalues in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In the first case, as 1 is an eigenvalue of $\overline{g}$, the matrix $\overline{g}$ is equal to the identity, contradicting the fact that $\chi_{p^n}(\sigma) \not\equiv 1 \pmod{p}$; the second case never occurs, as $\overline{g}$ has a reducible characteristic polynomial. This implies that $g \in C_{ns}^+(p^n) \setminus C_{ns}(p^n)$, and in particular, $\operatorname{tr} g = 0$, which implies that $\chi_{p^n}(\sigma) = -1$.

(ii) If instead $\chi_{p^n}(\sigma) \equiv 1 \pmod{p}$, then we can write $A = I + p^r \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$, with $r \leq n$ as large as possible. As for matrices in $M_{2\times 2}(\mathbb{F}_p)$ the rank is invariant under conjugation, if $r < n$ there would be a matrix in $\mathfrak{g}_r$ of

rank 1 (with $\mathfrak{g}_r$ defined as in Definition 2.1.3 for the group $G = C_{ns}^+$), which is impossible by Remark 2.1.8. This implies that $A = I$, and so that $\chi_{p^n}(\sigma) \equiv 1 \pmod{p^n}$.

We have then proved that $\chi_{p^n}(\sigma) \in \{\pm 1\}$ for every σ. Suppose first that $p \neq \ell$. If Frob_λ is a Frobenius element in $\mathrm{Gal}\left(\overline{K}/K\right)$ with respect to λ, we have that $N_{K/\mathbb{Q}}(\lambda) = \chi_{p^n}(\mathrm{Frob}_\lambda) \equiv \pm 1 \pmod{p^n}$. If instead $\ell = p$, as the character χ_{p^n} is surjective from $\mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p\right)$, we must have $[K_\mathfrak{p}(\zeta_{p^n}) : K_\mathfrak{p}] \leq 2$. However, this implies that $e(\mathfrak{p}|p)$ is a multiple of $\frac{\varphi(p^n)}{2}$, because $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified. □

Corollary 3.1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$, n a positive integer, and p an odd prime such that $p^n \neq 3$ and $\mathrm{Im}\,\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ up to conjugation. For any prime $\ell \not\equiv \pm 1 \pmod{p^n}$ the elliptic curve E has potentially good reduction at ℓ.*

We now focus on the case where E is defined over $\mathbb{Q}$ and the image of $\rho_{E,p}$ is a proper subgroup of $C_{ns}^+(p)$. By Theorem 6 we know that in this case $\mathrm{Im}\,\rho_{E,p}$ is conjugate to the unique subgroup $G(p) < C_{ns}^+(p)$ of index 3, whenever $p > 37$. However, by the results contained in [Zyw15a] one can obtain the same conclusion for primes $p \geq 5$.

We start by considering the image via $\rho_{E,p}$ of the ℓ-inertia subgroup, for all primes ℓ. We will draw different conclusions in the cases $\ell \neq p$ and $\ell = p$. We first consider the case $\ell = p$, which allows us to show that, for $p \equiv -1 \pmod 9$, the image of the residual representation modulo p cannot be isomorphic to the subgroup $G(p)$, and hence $\mathrm{Im}\,\rho_{E,p} \supseteq C_{ns}^+(p)$ up to conjugacy. This is a refinement of [LFL21, Proposition 1.4] (Theorem 6), itself an exposition of results of Zywina [Zyw15a, Proposition 1.13], which states that if $\mathrm{Im}\,\rho_{E,p} \subseteq G(p)$, then $p \equiv 2 \pmod 3$.

Theorem 3.1.4. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If $p \neq 2, 3$ is a prime number such that $\mathrm{Im}\,\rho_{E,p}$ is conjugate to $G(p)$, then $p \equiv 2 \pmod 3$ and $p \not\equiv -1 \pmod 9$.*

Proof. Since $\det \circ \rho_{E,p}$ surjects onto $\mathbb{F}_p^\times$ and $\det(G(p)) = (\mathbb{F}_p^\times)^3$, we have $(\mathbb{F}_p^\times)^3 = \mathbb{F}_p^\times$ and hence $p \equiv 2 \pmod 3$. Since the smallest prime p congruent to -1 modulo 9 is 17, and since we already noticed that p must be equal to 2 modulo 3, it suffices to consider primes $p \geq 17$. Choosing a suitable basis of $E[p]$, we can suppose $\mathrm{Im}\,\rho_{E,p} = G(p)$. We note that $\mathrm{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p\right)$ can be identified with a p-decomposition group of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, and $I_p := \mathrm{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr}\right)$

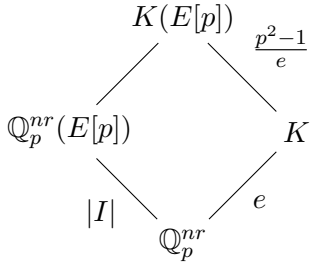
can be identified with the p-inertia, where $\mathbb{Q}_p^{nr}$ is the maximal unramified extension of $\mathbb{Q}_p$. We also let $\mathbb{Q}_p^{tame}$ be the maximal tamely ramified extension of $\mathbb{Q}_p^{nr}$. We have:

$$\begin{aligned}\operatorname{Im}\rho_{E,p} &= \rho_{E,p}\left(\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\right) > \rho_{E,p}\left(\operatorname{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p\right)\right)\\ &> \rho_{E,p}\left(\operatorname{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr}\right)\right) = \rho_{E,p}(I_p) =: I.\end{aligned}$$

Notice that the restriction of $\rho_{E,p}$ to $\operatorname{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{tame}\right)$ is trivial, because its image is a p-group contained in $G(p)$, which has $\frac{2(p^2-1)}{3}$ elements. Hence $\rho_{E,p}$ factors through the quotient, inducing a map from $\operatorname{Gal}\left(\mathbb{Q}_p^{tame}/\mathbb{Q}_p^{nr}\right)$ which we still denote by $\rho_{E,p}$. We have that

$$I = \rho_{E,p}(I_p) \cong \rho_{E,p}\left(\operatorname{Gal}\left(\mathbb{Q}_p^{tame}/\mathbb{Q}_p^{nr}\right)\right) \cong \operatorname{Gal}\left(\mathbb{Q}_p^{nr}(E[p])/\mathbb{Q}_p^{nr}\right).$$

Applying Corollary 3.1.3 we see that E has potentially good reduction at p. Let $K/\mathbb{Q}_p^{nr}$ be the minimal extension of $\mathbb{Q}_p^{nr}$ over which $E \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_p^{nr}$ acquires good reduction. Define the subgroup $I_K < I_p$ as $\operatorname{Gal}\left(\overline{\mathbb{Q}}_p/K\right)$. By Theorem 3.1.1 we know that $e := [K : \mathbb{Q}_p^{nr}] \in \{1,2,3,4,6\}$. By [Ser72, Section 1, Propositions 10, 11, 12] we know that either $\rho_{E,p}(I_K)$ contains an element of order $\frac{p^2-1}{e}$, or the image of $\rho_{E,p}(I_K)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order $\frac{p-1}{\gcd(e,p-1)}$. In the latter case, since the square of any element of $C_{ns}^+(p)\setminus C_{ns}(p)$ is a scalar matrix and hence has order 2 in $\mathrm{PGL}_2(\mathbb{F}_p)$, every element in $C_{ns}^+(p)$ has order dividing $p+1$ in $\mathrm{PGL}_2(\mathbb{F}_p)$. We then have that $\frac{p-1}{(e,p-1)} \mid p+1$, and so $p-1 \mid 2e \leq 12$. However, this is impossible for $p \geq 17$. This implies that $I_K \cong \operatorname{Gal}\left(K(E[p])/K\right)$ contains an element of order $\frac{p^2-1}{e}$. Actually, by [Ser72, Section 1, Propositions 10, 12], this element is a generator of the Galois group, and so $\left|\operatorname{Gal}\left(K(E[p])/K\right)\right| = [K(E[p]) : K] = \frac{p^2-1}{e}$.



Since $\mathrm{Gal}\left(\mathbb{Q}_p^{tame}/\mathbb{Q}_p^{nr}\right)$ is a procyclic group, $\mathrm{Gal}\left(K(E[p])/\mathbb{Q}_p^{nr}\right)$ is cyclic (of order $\frac{p^2-1}{e} \cdot e = p^2-1$). This implies that I is contained in C_{ns}, as every element of $C_{ns}^+ \setminus C_{ns}$ has order dividing $2(p-1)$, but a generator of I has order at least $\frac{p^2-1}{6}$ and $\frac{p^2-1}{6} > 2(p-1)$ for $p > 11$. As noticed in [LFL21, Appendix B], $\frac{p^2-1}{|I|}$ is necessarily odd, otherwise I would be contained in the subgroup of squares of C_{ns}, contradicting the fact that $\det \circ \rho_{E,p}|_{I_p}$ surjects onto $\mathbb{F}_p^\times$. Moreover, $\frac{p^2-1}{|I|}$ divides e, hence it is either 1 or 3. However, if we had $|I| = p^2-1$, the whole $I = C_{ns}$ would be contained in $G(p)$, contradiction, hence we must have $I = \frac{p^2-1}{3}$ and $e \in \{3, 6\}$. Given that $p \equiv 2 \pmod 3$, we have $e \mid \frac{p^2-1}{3} \iff 3e \mid p^2-1 \iff p \equiv -1 \pmod 9$. In particular, whenever $p \equiv -1 \pmod 9$, we have that e divides $|I|$, and so $\mathbb{Q}_p^{nr}(E[p])$ has a subextension of degree e. Since $K(E[p])/\mathbb{Q}_p^{nr}$ is cyclic, it has a unique subextension of degree e, hence $K \subset \mathbb{Q}_p^{nr}(E[p])$, and so $\mathbb{Q}_p^{nr}(E[p]) = K(E[p])$. This implies that $|I| = p^2-1$, and so $\mathrm{Im}\,\rho_{E,p}$ cannot be contained in $G(p)$. □

Remark 3.1.5. In the proof, we used the fact that when we are in the case of "good reduction of height 1" (i.e. [Ser72, Section 1.11, Proposition 11] applies), the image of the group I in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order $\frac{p-1}{(e,p-1)}$. This is the same argument used in [LFL21, Appendix B], however the authors write $p-1$ instead of $\frac{p-1}{e}$. Their argument works anyway, as they are assuming that $p \geq 19$.

Remark 3.1.6. Theorem 3.1.4 provides the best congruence condition on p that can be obtained by local arguments at p. Indeed, as shown in [Zyw15a, Proposition 1.16 (iv)], if $p \equiv 2, 5 \pmod 9$, the CM elliptic curve $E : y^2 = x^3 + 16p^k$, with $k \equiv -\frac{p+1}{3} \pmod 3$, is such that $\mathrm{Im}\,\rho_{E,p}$ is conjugate to $G(p)$. However, there exist elliptic curves E' without CM whose defining equations are arbitrarily close to that of E in the p-adic metric. By continuity of the local p-adic representation with respect to the coefficients of a defining equation (Krasner's lemma), taking E' sufficiently close to E gives examples of non-CM elliptic curves for which the image of $\rho_{E',p}$, restricted to the decomposition group at p, is contained in $G(p)$.

We now consider the action of the ℓ-inertia for $\ell \neq p$, which allows us to prove the following lemma.

Lemma 3.1.7. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If $p > 5$ is a prime number such that $\mathrm{Im}\,\rho_{E,p}$ is conjugate to $G(p)$, then $j(E) = p^d \cdot c^3$, with $d, c \in \mathbb{Z}$ and $d \geq 0$.*

Proof. By Lemma 1.1.5 we know that $j(E) \in \mathbb{Z}$. Let $\ell \neq p$ be a prime that divides $j(E)$, let $\mathbb{Q}_\ell^{nr}$ be the maximal unramified extension of $\mathbb{Q}_\ell$, and let

$K/\mathbb{Q}_\ell^{nr}$ be the minimal extension over which $E_\ell = E \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_\ell^{nr}$ acquires good reduction. Let $y^2 = x^3 + ax + b$ be a minimal model for E over $\mathbb{Q}$ with discriminant Δ. By the Néron-Ogg-Shafarevich criterion, we know that K is the minimal extension of $\mathbb{Q}_\ell^{nr}$ such that $\rho_{E_\ell,p}\left(\operatorname{Gal}\left(\overline{\mathbb{Q}}_\ell/K\right)\right)$ is trivial, hence $\operatorname{Gal}\left(\overline{\mathbb{Q}}_\ell/K\right) = \ker\rho_{E_\ell,p}$ and $\operatorname{Im}\rho_{E_\ell,p} \cong \operatorname{Gal}\left(K/\mathbb{Q}_\ell^{nr}\right)$. In particular, $\operatorname{Gal}\left(K/\mathbb{Q}_\ell^{nr}\right)$ embeds in $G(p)$. Since by Theorem 3.1.4 we know that $3 \nmid |G(p)|$, this implies that $3 \nmid [K : \mathbb{Q}_\ell^{nr}]$. However, by Theorem 3.1.1 we know that if $3 \nmid [K : \mathbb{Q}_\ell^{nr}]$, then $3 \mid v_\ell(\Delta)$, and hence $v_\ell(j(E)) = v_p\left(-12^3 \cdot \frac{(4a)^3}{\Delta}\right) = 3v_\ell(12) + 3v_\ell(4a) - v_\ell(\Delta)$ is divisible by 3. □

3.2 The canonical subgroup

In this section, we will study the canonical subgroup of order p of E and its connection with the ramification in the division field $K_{\mathfrak{p}}^{nr}(E[p])/K_{\mathfrak{p}}^{nr}$. As a consequence of these results, we will show some restrictive properties of the j-invariant of elliptic curves E for which $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$.

The canonical subgroup of $E[p]$ was first defined by Lubin and studied by Lubin and Katz (see [Lub79] and [Kat73]). Most of the properties that we will give below are due to them.

Let p be a prime and let K be a p-adic field. Denote by $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_K$. Let E be an elliptic curve defined over K with good reduction at $\mathfrak{p}$. Let $\hat{E}$ be the formal group associated with E and let $E_1(K)$ be the set of the points in $E(K)$ that reduce to the origin O modulo $\mathfrak{p}$. As explained in [Sil09, Chapter VII, Proposition 2.2], there is an isomorphism $\hat{E}(\mathfrak{p}) \cong E_1(K)$. In particular, if we consider the extension $L = K(E[p])$, with prime ideal $\mathfrak{P} \mid \mathfrak{p}$, we have $\hat{E}(\mathfrak{P})[p] \cong E_1(L)[p]$. Hence, when E has supersingular reduction modulo $\mathfrak{p}$, there is an isomorphism between the p-torsion subgroup of the formal group and the p-torsion subgroup of the elliptic curve, i.e., $\hat{E}(\mathfrak{P})[p] \cong E[p]$. The group $\hat{E}(\mathfrak{P})$ is by definition the set $\mathfrak{P}$ endowed with the group structure coming from the formal group $\hat{E}$. Considering the points $\hat{P}$ of $\hat{E}(\mathfrak{P})$ as elements of $\mathfrak{P}$, we can then refer to the *valuation* of $\hat{P} \in \hat{E}(\mathfrak{P})$: it is simply its valuation as an element of the field L.

Definition 3.2.1. If there exists $\lambda \in \mathbb{R}$ such that $\{\hat{P} \in \hat{E}(\mathfrak{P})[p] \mid v(\hat{P}) \geq \lambda\}$ is an order-p subgroup of $\hat{E}(\mathfrak{P})[p]$, then this is called the *canonical subgroup of order p* of E.

Remark 3.2.2. When E has ordinary reduction modulo $\mathfrak{p}$, there always exists a canonical subgroup, given by $\hat{E}(\mathfrak{P})[p] = E_1[p]$, i.e., the kernel of the reduction modulo $\mathfrak{p}$.

Remark 3.2.3. The isomorphism $E_1(L) \cong \hat{E}(\mathfrak{P})$ is given by the map $(x, y) \mapsto -\frac{x}{y}$, hence it is compatible with the action of the Galois group $\mathrm{Gal}\left(\overline{K}/K\right)$.

The notion of canonical subgroup can be extended to the case of elliptic curves defined over number fields.

Definition 3.2.4. Let K be a number field and let $\mathfrak{p} \mid p$ be a prime of K. Let E be an elliptic curve over K with potentially good reduction at $\mathfrak{p}$. Let L be an extension of $K_\mathfrak{p}$ such that E has good reduction over L. Given that $E(\overline{K})[p] = E(\overline{K}_\mathfrak{p})[p] = E[p]$, we define the *canonical subgroup of order p* of E as the canonical subgroup of order p of E over L, if this exists.

Definition 3.2.5. If E is given by the equation $y^2 = f(x)$, following [Deu41] we define the Hasse invariant A of E for a prime p as the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$.

Theorem 3.2.6. *Let $p \neq 2$ be a prime, let K be a number field and let $\mathfrak{p} \mid p$ be a prime of K. Let E/K be an elliptic curve with potentially good reduction at $\mathfrak{p}$ and let A be its Hasse invariant. The elliptic curve E has a canonical subgroup of order p if and only if $v(A) < \frac{p}{p+1}$.*

Proof. If E has ordinary reduction, it has a canonical subgroup and $v_p(A) = 0$, hence from now on we assume that E is supersingular. Let c be the coefficient of $x^{\frac{p^2-p}{2}}$ in the division polynomial $\psi_p(x)$. By [Smi23, Theorem 4.6] we know that E has a canonical subgroup of order p if and only if $v_p(c) < \frac{p}{p+1}$. However, by [Deb14, Theorem 1], we know that $c \equiv A \pmod{p}$. In particular, whenever $v_p(A) < 1$ we have that $v_p(c) = v_p(A)$, giving the statement of the theorem. If instead $v_p(A) \geq 1$, then $c \equiv A \equiv 0 \pmod{p}$, and therefore also $v_p(c) \geq 1$. □

The theory that leads to Theorem 3.2.6 is due to Lubin and Katz, but we have relied on [Smi23] because it formulates the results in a way that is closer to what we need.

The following lemma is a known fact which generalises [Ser72, Section 1, Proposition 1].

Lemma 3.2.7. *Let E be an elliptic curve over a p-adic field K and let $\mathfrak{p}$ be the prime of K above p. Suppose that E has good ordinary reduction at $\mathfrak{p}$. For every positive integer n, the inertia group I_K of K acts on $E[p^n]$ as $\begin{pmatrix} \chi_{p^n} & * \\ 0 & 1 \end{pmatrix}$, where χ_{p^n} is the cyclotomic character modulo p^n.*

Proof. Let μ be the p-adic cyclotomic character. Since E has ordinary reduction, we know that there is an exact sequence of $\mathbb{Z}[I_K]$-modules

$$0 \longrightarrow T_p(\mu) \longrightarrow T_pE \longrightarrow T_p\widetilde{E} \longrightarrow 0,$$

where $T_p\widetilde{E} \cong \mathbb{Z}_p$ has trivial action by I_K. Indeed, I_K acts trivially on $T_p\widetilde{E}$, and since the determinant is cyclotomic, the other character must be the cyclotomic character. In particular, modulo p^n we have

$$0 \longrightarrow \mu_{p^n} \longrightarrow E[p^n] \longrightarrow {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}} \longrightarrow 0,$$

and the group I_K acts on $E[p^n]$ as $\begin{pmatrix} \chi_{p^n} & * \\ 0 & 1 \end{pmatrix}$, where χ_{p^n} is the cyclotomic character modulo p^n. □

Lemma 3.2.8. *Let p be an odd prime and let E be an elliptic curve over a p-adic field K. Let $\mathfrak{p} \subseteq K$ be a prime above p with ramification index $e := e(\mathfrak{p}|p)$ and let I_K be the inertia group of K. Suppose that E has good reduction at $\mathfrak{p}$.*

1. *If E has ordinary reduction, E admits a canonical subgroup and for every positive integer n then the group $\rho_{E,p^n}(I_K)$ contains an element of order $\frac{p^n-p^{n-1}}{\gcd(p^n-p^{n-1},e)}$ when projected in $\mathrm{PGL}_2\left({}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}\right)$.*
2. *If E has supersingular reduction and does not have a canonical subgroup, then the group $\rho_{E,p^n}(I_K)$ contains an element of order $\frac{p^{n+1}-p^{n-1}}{\gcd(p^{n+1}-p^{n-1},e)}$.*

Proof. If E has potentially good ordinary reduction, by Lemma 3.2.7 the image of I_K in PGL_2 contains a subgroup isomorphic to $\chi_{p^n}(I_K)$. Since $[I_{\mathbb{Q}_p} : I_K] = e$ and $|\chi_{p^n}(I_{\mathbb{Q}_p})| = p^n - p^{n-1}$, the order of $\chi_{p^n}(I_K)$ must be divisible by $\frac{p^n-p^{n-1}}{\gcd(p^n-p^{n-1},e)}$, and noting that the image of χ_{p^n} is cyclic we obtain the desired property. Moreover, in this case E always has a canonical subgroup, which is the kernel of the reduction modulo $\mathfrak{p}$. Assume now that E has potentially good supersingular reduction and that E does not have a canonical subgroup. By [Smi23, Theorem 4.6] we know that $K(E[p]) \subseteq K(E[p^n])$ contains elements with valuation $\frac{1}{p^2-1}$, and hence the ramification degree of $K(E[p^n])$ over K is divisible by

$$\frac{p^2-1}{\gcd(p^2-1, [K :\ \mathbb{Q}_p^{nr} \cap K])} = \frac{p^2-1}{\gcd(p^2-1, e)}.$$

Moreover, since the tame extensions of K^{nr} are cyclic, there must be an element in the inertia subgroup $I(K(E[p^n])/K) \cong \rho_{E,p^n}(I_K)$ of order $\frac{p^2-1}{\gcd(e,p^2-1)}$. If $n > 1$, since $\det \circ \rho_{E_L,p^\infty}(I_K) = (\mathbb{Z}_p^\times)^e$, there is also an element of $\rho_{E,p^n}(I_K)$ with determinant of order $\frac{\varphi(p^n)}{(\varphi(p^n),e)}$, and so $\rho_{E,p^n}(I_K)$ contains an element of order $\frac{p^n-p^{n-1}}{(p^n-p^{n-1},e)}$. In particular, we have an element in $\rho_{E,p^n}(I_K)$ whose order is the less common multiple of $\frac{p^2-1}{\gcd(e,p^2-1)}$ and $\frac{p^n-p^{n-1}}{(p^n-p^{n-1},e)}$, and so with order $\frac{p^{n+1}-p^{n-1}}{\gcd(e,p^{n+1}-p^{n-1})}$. □

Theorem 3.2.9. *Let E be an elliptic curve over a number field K and let p be a prime. Let $\mathfrak{p} \subseteq K$ be a prime above p with ramification index $e := e(\mathfrak{p}|p)$. Suppose that E has potentially good reduction at $\mathfrak{p}$ and let L be the minimal extension of $K_{\mathfrak{p}}^{nr}$ over which E acquires good reduction, with degree $d = [L : K_{\mathfrak{p}}^{nr}]$. Suppose also that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$.*

1. *If $p > de+1$ and $p \neq 2de+1$, then E does not have a canonical subgroup of order p.*

2. *If E has potentially good supersingular reduction modulo $\mathfrak{p}$ and $p \geq \max\{de-1, 3\}$, then E does not have a canonical subgroup of order p.*

Proof. We start by proving part 1. Consider the subgroup $I < \operatorname{Im}\rho_{E,p}$ obtained as the image of the inertia group of L. If E has potentially good supersingular reduction, part 2 of the theorem supersedes part 1, hence we may assume that E has potentially good ordinary reduction. By Lemma 3.2.8 we know that the image of I in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order $\frac{p-1}{\gcd(de,p-1)}$. Since the square of any element of $C_{ns}^{+}(p) \setminus C_{ns}(p)$ is a scalar matrix and hence has order 2 in $\mathrm{PGL}_2(\mathbb{F}_p)$, we have that $\frac{p-1}{(de,p-1)} \mid p+1$, and so $p-1 \mid 2de$. However, this is impossible because $p-1 \neq 2de$ and $p-1 > de$.
Assume now that E has potentially good supersingular reduction and suppose that E/L admits a canonical subgroup. By Theorem 3.2.6 we know that its Hasse invariant A is a number in L with valuation $0 < v_p(A) < \frac{p}{p+1}$. However, $v_p(A)$ is a rational number with denominator dividing de. Suppose that $v_p(v_p(A)) > 0$: we can write $v_p(A) = \frac{\alpha p}{de}$, for some positive integer α. On the other hand, we have $\frac{\alpha p}{de} < \frac{p}{p+1}$, which gives $1 \leq \alpha < \frac{de}{p+1}$, contradicting the hypothesis that $p \geq de-1$. This implies that $v_p(v_p(A)) = 0$. Let c be the coefficient of $x^{\frac{p^2-p}{2}}$ in the division polynomial $\Psi_p(x)$ and let μ be its valuation. By [Deb14, Theorem 1] we know that $c \equiv A \pmod{p}$, and so $v_p(A) = \mu$. By [Smi23, Theorem 4.6] we know that $L(E[p])$ contains elements of valuation $\frac{\mu}{p^2-p}$. However, $v_p(\mu) = 0$, and so p must divide the degree $[L(E[p]) : L]$, which is a divisor of $2(p^2-1)$, giving a contradiction. □

Corollary 3.2.10. *Let E be an elliptic curve over a number field K and let p be a prime. Let $\mathfrak{p} \subseteq K$ be a prime above p with ramification index $e := e(\mathfrak{p}|p)$. Suppose that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$.*

1. *If $p > 6e+1$ and $p \neq 12e+1$, then E does not have a canonical subgroup of order p.*

2. *If E has potentially good supersingular reduction modulo $\mathfrak{p}$ and $p \geq 6e-1$, then E does not have a canonical subgroup of order p.*

Proof. We notice that $p \geq 6e-1$, and since $6e-1 > 2e+1$ we have $p-1 \nmid 2e$. By Proposition 3.1.2 this implies that E has potentially good reduction at $\mathfrak{p}$.

Moreover, using that $p \geq 6e-1 \geq 5$, by Theorem 3.1.1 we see that the degree $d = [L : K_{\mathfrak{p}}^{nr}]$ of the minimal extension of $K_{\mathfrak{p}}^{nr}$ over which E acquires good reduction is at most 6. We then conclude by applying Theorem 3.2.9. □

Corollary 3.2.11. *Let E be an elliptic curve over $\mathbb{Q}$. If p is a prime such that $p > 7$ and $p \neq 13$, and $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$, then E does not have a canonical subgroup of order p.*

Corollary 3.2.12. *Let E be an elliptic curve over a number field K and let p be a prime. Let $\mathfrak{p} \subseteq K$ be a prime above p with ramification index $e := e(\mathfrak{p}|p)$. Suppose that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. If $p > 6e+1$ and $p \neq 12e+1$, then E has potentially good supersingular reduction modulo $\mathfrak{p}$.*

Proof. We notice that by Proposition 3.1.2 the curve E has potentially good reduction at $\mathfrak{p}$. It then suffices to combine Corollary 3.2.10 and Theorem 3.2.6, using the fact that if A is the Hasse invariant of E, then $v_p(A)$ is equal to 0 if and only if E has ordinary reduction modulo p. □

The corollary above generalises [Ejd22, Proposition 3.1] written below to arbitrary number fields.

Corollary 3.2.13. *Let E be an elliptic curve over $\mathbb{Q}$. If p is a prime such that $p > 7$, $p \neq 13$ and $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$, then E has potentially good supersingular reduction modulo p.*

Consider again the unique subgroup $G(p) < C_{ns}^{+}(p)$ of index 3. The next proposition is one of the main goals of this section.

Proposition 3.2.14. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If $p > 5$ is a prime number such that $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$, then $p^4 \mid j(E)$.*

Before proving the proposition above, we prove a p-adic property of $j(E)$ that we establish in the next lemma.

Lemma 3.2.15. *Under the assumptions of Proposition 3.2.14, we have $3 \nmid v_p(j(E))$. In particular, by Lemma 1.1.5 we have $v_p(j(E)) > 0$.*

Proof. By Lemma 1.1.5 the curve E has potentially good reduction at p. Let $y^2 = x^3 + ax + b$ be a minimal model for E over $\mathbb{Q}$ with discriminant Δ and let $K/\mathbb{Q}_p^{nr}$ be the minimal extension over which $E \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_p^{nr}$ acquires good reduction. As shown in the proof of Theorem 3.1.4, we have $3 \mid [K : \mathbb{Q}_p^{nr}]$, hence by Theorem 3.1.1(1) the denominator of $\frac{v_p(\Delta)}{12}$ is divisible by 3, and so $3 \nmid v_p(\Delta)$. Hence $v_p(j(E)) = v_p\left(-12^3 \cdot \frac{(4a)^3}{\Delta}\right) = 3v_p(a) - v_p(\Delta)$ is not divisible by 3. □

Proof of Proposition 3.2.14. By Lemma 1.1.5 we can assume that $p \geq 19$ and that E has potentially good reduction everywhere. Let ${}^{K}\!/_{\mathbb{Q}_p^{nr}}$ be the minimal extension over which $E \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_p^{nr}$ acquires good reduction, let $y^2 = x^3 + ax + b$ be a model of good reduction for E over $\mathcal{O}_K$ and let A_K and Δ_K be the Hasse invariant and the discriminant of this model respectively. By Corollary 3.2.11 and Theorem 3.2.6 we know that $v_p(A_K) \geq \frac{p}{p+1}$. As the ramification index of K over $\mathbb{Q}_p$ is $e \leq 6$, we have $v_p(A_K) \in \frac{1}{e}\mathbb{Z}$, and therefore $v_p(A_K) \geq 1$ since $p > 5$. The good reduction of E implies that $v_p(\Delta_K) = 0$, and by Lemma 3.2.15 we have $0 < v_p(j(E)) = 3v_p(a) - v_p(\Delta_K) = 3v_p(a)$. Using that $\Delta_K = -16(4a^3 + 27b^2)$, $v_p(a) > 0$ and $v_p(\Delta_K) = 0$, we also have that $v_p(b) = 0$. We now compute the Hasse invariant. We have

$$(x^3 + ax + b)^{\frac{p-1}{2}} = \sum_{i+j+k=\frac{p-1}{2}} \binom{(p-1)/2}{i,j} x^{3i} \cdot a^j x^j \cdot b^k,$$

hence in particular

$$A_K = \sum_{\substack{i+j+k=\frac{p-1}{2} \\ 3i+j=p-1}} \binom{(p-1)/2}{i,j} a^j b^k = \sum_{2j+3k=\frac{p-1}{2}} \binom{(p-1)/2}{j,k} a^j b^k.$$

Since by Theorem 6 we have $p \equiv 2 \pmod 3$, the minimum value of j among all the indices in the last sum is 1, hence it is not difficult to show that $v_p(a) = v_p(A_K) \geq 1$. This implies $v_p(j(E)) = 3v_p(a) \geq 3$. However, by Lemma 3.2.15, we know that $3 \nmid v_p(j(E))$, and so $v_p(j(E)) \geq 4$. □

For the proof of Proposition 3.2.14, the fact that $\operatorname{Im}\rho_{E,p} \subseteq G(p)$ is only needed in the proof of Lemma 3.2.15 and to assume that $p \equiv 2 \pmod 3$, so we can repeat the whole argument without this assumption and obtain the following.

Corollary 3.2.16. *If ${}^{E}\!/_{\mathbb{Q}}$ is an elliptic curve without complex multiplication and $p > 37$ is a prime such that $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup, then either $v_p(j(E)) = 0$ or $v_p(j(E)) \geq 3$. Moreover, in the latter case we always have $p \equiv 2 \pmod 3$.*

Proof. If $p \equiv 2 \pmod 3$ the proof is exactly the same as that of Proposition 3.2.14, hence it suffices to show that if $p \equiv 1 \pmod 3$ then $v_p(j(E)) = 0$. Following the argument in the proof of Proposition 3.2.14, assume by contradiction that $p \equiv 1 \pmod 3$ and $v_p(j(E)) > 0$. Over a suitable extension K of $\mathbb{Q}_p^{nr}$, we can write E as $y^2 = x^3 + ax + b$ with $v_p(\Delta_K) = v_p(b) = 0$ and $3v_p(a) = v_p(j(E)) > 0$. We can then write the Hasse invariant as $A_K = c \cdot b^{\frac{p-1}{6}} + a \cdot d(a,b)$ for some constants $c, d(a,b) \in \mathcal{O}_K$ with $v_p(c) = 0$. It follows that $v_p(A_K) = 0$, which gives a contradiction with Theorem 3.2.6 and Corollary 3.2.11. □

CHAPTER 4

Effective surjectivity theorem

Let E be an elliptic curve without CM defined over a number field K, and let p^n be a prime power for which the image of ρ_{E,p^n} is contained in the normaliser of a non-split Cartan subgroup. The aim of this chapter is to give a good bound on p^n in terms of the stable Faltings height of E. Moreover, we also want to bound the product of all such prime powers. The main strategy to obtain this kind of bound relies on the techniques developed by Masser and Wüstholz [MW93b, MW93a] to bound the degree of a minimal isogeny between two abelian varieties. Their argument was sharpened by Gaudron and Rémond [GR14] in the case of elliptic curves. We will mainly follow the proof of Gaudron and Rémond, taking advantage of some extra hypotheses specific to our setting.

In Section 4.2, we will exploit the local properties studied in Chapter 3 to provide even stronger bounds in the case where the j-invariant of the curve E is not an algebraic integer.

4.1 Abelian periods and isogeny theorem

In this section, we give a generalised version of the effective surjectivity theorem of Le Fourn [LF16, Theorem 5.2], obtaining a bound on the product of the prime powers p^n for which the image of the representation ρ_{E,p^n} is contained either in a Borel subgroup or in the normaliser of a Cartan subgroup of $\mathrm{GL}(E[p^n])$. There are two main differences with respect to [LF16, Theorem 5.2]: the first is that we are able to bound the product of prime powers and not just the product of primes, the second is that in the non-split Cartan case our version also applies non-trivially to curves of small height.

Theorem 4.1.1. *Let E be an elliptic curve without CM defined over a number field K. We denote by $\mathrm{h}_{\mathcal{F}}(E)$ the stable Faltings height of E (with the normalisation of [Del85a, Section 1.2]). Let $\mathcal{B}, \mathcal{C}_{sp}, \mathcal{C}_{ns}$ be sets of odd primes p such that $\operatorname{Im}\rho_{E,p} \subseteq G(p)$ up to conjugacy for $G = B, C_{sp}^{+}, C_{ns}^{+}$ respectively. For every $p \in \mathcal{B} \cup \mathcal{C}_{sp} \cup \mathcal{C}_{ns}$, let n_p be the largest positive integer such that $\operatorname{Im}\rho_{E,p^{n_p}} \subseteq G(p^n)$, and let $\Lambda := \prod_{p\in\mathcal{B}} p^{\frac{n_p}{2}} \prod_{p\in\mathcal{C}} p^{n_p}$, where $\mathcal{C} := \mathcal{C}_{sp} \cup \mathcal{C}_{ns}$.*

1. *We have*

$$\Lambda < 1454 \cdot 2^{|\mathcal{C}|}[K:\mathbb{Q}] \left(\mathrm{h}_{\mathcal{F}}(E) + \frac{7}{2}\log(\mathrm{h}_{\mathcal{F}}(E) + 2.72) + 4\log\Lambda + 5 \right).$$

2. *If $\mathcal{B} = \mathcal{C}_{sp} = \emptyset$ we have*

$$\Lambda < 1454 \cdot 2^{|\mathcal{C}|}[K:\mathbb{Q}] \left(\mathrm{h}_{\mathcal{F}}(E) + \frac{3}{2}\log(\mathrm{h}_{\mathcal{F}}(E) + 2.72) + 2\log\Lambda + 2.6 \right).$$

3. *If $K = \mathbb{Q}$ and $\mathcal{B} = \mathcal{C}_{sp} = \emptyset$, we have*

$$\Lambda < 1454 \cdot 2^{|\mathcal{C}|} \left(\mathrm{h}_{\mathcal{F}}(E) + 2\log\Lambda + \frac{3}{2}\max\{0, \log(\Im\{\tau\})\} + 1.38 \right),$$

where τ is the point in the standard fundamental domain $\mathcal{F}$ of $\mathcal{H}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}$.

Furthermore, if $\tau_\sigma \in \mathcal{F}$ corresponds to the curve $\sigma(E)$, for some $\sigma : K \hookrightarrow \mathbb{C}$, and if we assume that $\Im\{\tau_\sigma\} \geq \frac{15}{\pi}$ for every σ, we can replace the number 1454 with 1266.4 in all the inequalities.

We follow closely the approach of [LF16, Theorem 5.2] and [GR14, Theorem 1.4], but in parts (2) and (3) we are able to obtain much-improved constants by noticing that certain auxiliary subvarieties considered in [GR14] are in fact all trivial (see Lemma 4.1.11). Moreover, we are able to remove the dependence on the number of primes in $\mathcal{C}$ in [LF16, Theorem 5.2]. Section 4.1 is entirely devoted to proving Theorem 4.1.1.

We begin by recalling some crucial definitions from [GR14].

Definition 4.1.2. Let A be a complex abelian variety, let $B \subset A$ be an abelian subvariety of codimension $t \geq 1$, and let L be a polarisation on A. We define

$$x(B) := \left(\frac{\deg_L B}{\deg_L A} \right)^{\frac{1}{t}} \qquad \text{and} \qquad x := \min_{B \subsetneq A} x(B),$$

where $\deg_L A$ is the top self-intersection number of the line bundle L on A, and similarly $\deg_L B$.

Let (A, L) be a polarised abelian variety defined over a number field K. Fix an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and let (A_σ, L_σ) be the base-change of (A, L) to $\mathbb{C}$ via σ. We will denote by $B[\sigma]$ a proper abelian subvariety of A_σ such that $x(B[\sigma]) = x$.

Definition 4.1.3. Let A be a complex abelian variety and let L be a polarisation on A. Let $\|\cdot\|_L$ be the norm induced by L on the tangent space t_A, and let Ω_A be the period lattice. We define

$$\rho(A, L) := \min\{\|\omega\|_L \mid \omega \in \Omega_A \setminus \{0\}\}.$$

Remark 4.1.4. Let E be an elliptic curve defined over a number field K and let L be its canonical principal polarisation. As explained in [GR14, Remark 3.3], given an embedding $\sigma : K \hookrightarrow \mathbb{C}$ we have $\rho(E_\sigma, L_\sigma)^{-2} = \Im\{\tau_\sigma\}$, where τ_σ is the element in the standard fundamental domain $\mathcal{F}$ that corresponds to E_σ and L_σ is the base-change of the polarisation L via σ.

Definition 4.1.5. Let A be an abelian variety defined over a number field K and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding. Let L be a polarisation on A and let d_σ be the distance induced by L_σ on t_{A_σ}. We define

$$\delta_\sigma = \min\{\mathrm{d}_\sigma(\omega, t_{B[\sigma]}) \mid \omega \in \Omega_{A_\sigma} \setminus t_{B[\sigma]}\},$$

where $B[\sigma]$ is as in Definition 4.1.2.

We now begin the proof of Theorem 4.1.1 introducing the general setting; then we will split the proof in different parts, distinguishing the case $\mathcal{B}, \mathcal{C}_{sp} \neq \emptyset$, the case $\mathcal{B}, \mathcal{C}_{sp} = \emptyset$ and $K = \mathbb{Q}$, and the case $\mathcal{B}, \mathcal{C}_{sp} = \emptyset$ and $K \neq \mathbb{Q}$. Similarly to [LF16], we start by giving the construction of a particular quotient of the abelian surface $E \times E$. However, we will use a slightly different quotient, which is more natural.

Choose an extension K'/K of degree $2^{|\mathcal{C}|}$ such that for every prime $p \in \mathcal{C}$ we have

$$\rho_{E,p}\left(\mathrm{Gal}\left(\overline{K}/K'\right)\right) \subseteq C(p) \tag{4.1.1}$$

up to conjugation, where $C(p)$ is either $C_{sp}(p)$ or $C_{ns}(p)$. Note that, if $\rho_{E,p}\left(\mathrm{Gal}\left(\overline{K}/K\right)\right)$ is already contained in $C(p)$, we choose K' to be an arbitrary complex quadratic extension of K. Since the image of the complex conjugation is not contained in $C(p)$ for every p, the field K' is always a complex field. We now construct a subgroup G_p of $E[p^{n_p}]^2$ for every $p \in \mathcal{B} \cup \mathcal{C}$.

- $\underline{\mathbf{p} \in \mathcal{B}}$: We define the group G_p as $\Gamma_{p^{n_p}} \times E[p^{n_p}] \subseteq E \times E$, where $\Gamma_{p^{n_p}}$ is a cyclic subgroup of order p^{n_p} fixed by $\rho_{E,p^{n_p}}$. We have $|G_p| = p^{3n_p}$.

- $\underline{\mathbf{p} \in \mathcal{C}_{\mathbf{sp}}}$: We define the group G_p as $\Gamma_1 \times \Gamma_2$, where $\Gamma_1, \Gamma_2 \subset E[p^{n_p}]$ are two independent cyclic subgroups of order p^{n_p} stabilised by $\rho_{E,p^{n_p}}$ over K'. We have $|G_p| = p^{2n_p}$.

- $\underline{\mathbf{p} \in \mathcal{C}_{\mathbf{ns}}}$: Choose an element $g_p \in C_{ns}(p^{n_p})$ such that $g_p \pmod p \notin \mathbb{F}_p^\times \cdot \mathrm{Id}$. We define the subgroup G_p as $\{(x, g_p \cdot x) \mid x \in E[p^{n_p}]\}$. We have $|G_p| = p^{2n_p}$.

It is not difficult to notice that all the groups G_p we defined are stable under the action of the absolute Galois group of K': indeed, this is clear by definition in the case of the Borel and split Cartan subgroups, and it is true in the case of the non-split Cartan as $C_{ns}(p^{n_p})$ is abelian and for every $\gamma \in C_{ns}(p^{n_p})$ we have $\gamma(x, g_p x) = (\gamma x, \gamma g_p x) = (\gamma x, g_p(\gamma x))$. We now consider the group

$$G := \bigoplus_{p \in \mathcal{B} \cup \mathcal{C}} G_p \subset E \times E.$$

Define

$$\Lambda_{\mathcal{B}} := \prod_{p \in \mathcal{B}} p^{n_p} \qquad \text{and} \qquad \Lambda_{\mathcal{C}} := \prod_{p \in \mathcal{C}} p^{n_p}.$$

By taking the quotient A of $E \times E$ by the subgroup G, we have an isogeny $\varphi : E \times E \to A$ defined over K' such that $\deg \varphi = \Lambda_{\mathcal{B}}^3 \Lambda_{\mathcal{C}}^2$. There exists $\psi : A \to E \times E$ such that $\psi \circ \varphi = [\Lambda_{\mathcal{B}} \Lambda_{\mathcal{C}}]_{E \times E}$, so $\deg \psi = \Lambda_{\mathcal{B}} \Lambda_{\mathcal{C}}^2 = \Lambda^2$. As explained in the proof of [LF16, Proposition 5.1], for every embedding $\sigma : K' \hookrightarrow \mathbb{C}$, there is a canonical norm $\|\cdot\|_\sigma$ on the tangent space of E_σ, which contains the period lattice $\Omega_{E,\sigma}$. As in [GR14, Part 7.3] and in the proof of [LF16, Proposition 5.1], we choose an embedding σ_0 such that there exists a basis $(\omega_0, \tau_{\sigma_0}\omega_0)$ of Ω_{E,σ_0} for which τ_{σ_0} is as in Remark 4.1.4 and

$$\|\omega_0\|_{\sigma_0} = \max_{\sigma} \min_{\omega \in \Omega_{E,\sigma} \setminus \{0\}} \|\omega\|_\sigma.$$

By Remark 4.1.4, this choice of σ_0 minimizes $\Im\{\tau_\sigma\}$ among all σ, as in [GR14, Part 7.3]. Let Ω_{A,σ_0} be the period lattice of A_{σ_0}. We want to show that there exists an element $\chi \in \Omega_{A,\sigma_0}$ such that $\mathrm{d}\psi(\chi) = (\omega_0, \tau_{\sigma_0}\omega_0)$. To do this, we prove the following lemma.

Lemma 4.1.6. *For every embedding $\sigma : K' \to \mathbb{C}$, if $\Omega_{E,\sigma}$ and $\Omega_{A,\sigma}$ are the period lattices of E and A with respect to σ, then $\mathrm{d}\,\psi(\Omega_{A,\sigma}) \subseteq \Omega_{E,\sigma}^2$ contains an element (ω_1, ω_2) such that $\langle \omega_1, \omega_2 \rangle_{\mathbb{Z}} = \Omega_{E,\sigma}$.*

Proof. The proof is similar to the second part of the proof of [LF16, Theorem 5.2], however [LF16, Lemma 5.3] can no longer be applied. Let $t_E \times t_E$ be the tangent space of $E \times E$ with respect to the embedding σ, and let $\pi : t_E \times t_E \to$

$E \times E$ be the projection. The lattice $\Omega := \pi^{-1}(G) \subset t_E \times t_E$ defines a quotient abelian variety ${}^{t_E \times t_E}\!/_{\Omega}$ isomorphic to A.

$$\begin{array}{ccccc} t_E \times t_E & \xrightarrow{\mathrm{id}} & t_E \times t_E & \xrightarrow{\Lambda_{\mathcal{B}}\Lambda_{\mathcal{C}}} & t_E \times t_E \\ \pi\downarrow & & \downarrow & & \downarrow\pi \\ E \times E & \xrightarrow[\varphi]{} & A & \xrightarrow[\psi]{} & E \times E \end{array}$$

Let $\Omega' := \Lambda_{\mathcal{B}}\Lambda_{\mathcal{C}}\Omega \subseteq \Omega_E \times \Omega_E$ be the image of the lattice Ω under the homothety $\Lambda_{\mathcal{B}}\Lambda_{\mathcal{C}}$. This is equal to the image of Ω_A via $\mathrm{d}\,\psi$, i.e. $\Omega' = \mathrm{d}\,\psi(\Omega_A)$. We want to show that Ω' contains a basis of Ω_E. Fix a basis $(\widetilde{e_1}, \widetilde{e_2})$ of Ω_E. Let p be a prime in $\mathcal{B} \cup \mathcal{C}$ and consider the image of Ω' in $\left({}^{\Omega_E}\!/_{p^{n_p}\Omega_E}\right)^2$. Multiplying it by $\frac{1}{p^{n_p}}$ we can identify it with a subgroup of $\left({}^{\Omega_E/p^{n_p}}\!/_{\Omega_E}\right)^2 = E[p^{n_p}]^2$. By definition of Ω', the image of $\frac{1}{p^{n_p}}\Omega'$ in $E[p^{n_p}]^2$ is exactly $\frac{\Lambda_{\mathcal{B}}\Lambda_{\mathcal{C}}}{p^{n_p}}G_p = G_p$. Identify $E[p^{n_p}]$ with $\mathbb{F}_p^2$ choosing the basis $\pi\left(\frac{\widetilde{e_1}}{p^{n_p}}, \frac{\widetilde{e_2}}{p^{n_p}}\right) = (e_1, e_2)$. We now prove that for every G_p there is an element $(x, y) \in G_p$ such that $\det_{e_1,e_2}(x, y) = 1$. If $p \in \mathcal{B}$, let $(a, b) \in \Gamma_{p^{n_p}}$ be an element of order p^{n_p}. We can choose (c, d) such that $ad - bc = 1 \pmod{p^{n_p}}$, and hence the element $((a, b), (c, d)) \in G_p$ has determinant 1.
If $p \in \mathcal{C}_{sp}$, similarly to the Borel case, given two elements $(a, b) \in \Gamma_1$ and $(c, d) \in \Gamma_2$ of order p^{n_p}, we have $ad - bc = k \not\equiv 0 \pmod{p}$, because $\Gamma_1 \pmod{p} \neq \Gamma_2 \pmod{p}$. We can then take $(a', b') = (k^{-1}a, k^{-1}b) \in \Gamma_1$ such that $a'd - b'c = 1$.
If $p \in \mathcal{C}_{ns}$, let e_1', e_2' be another basis of $E[p^n]$. We have

$$\det_{e_1,e_2}(x, y) = \det_{e_1,e_2}(e_1', e_2') \cdot \det_{e_1',e_2'}(x, y),$$

hence it suffices to show that for a particular choice of a basis e_1', e_2', the group $\det_{e_1',e_2'} G_p$ contains the whole $\left({}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}\right)^{\times}$. Fix e_1', e_2' such that $g_p = \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}$ with $p \nmid b$. We have

$$\det(x, g_p \cdot x) = \det \begin{pmatrix} x_1 & ax_1 + \varepsilon b x_2 \\ x_2 & bx_1 + ax_2 \end{pmatrix} = b(x_1^2 - \varepsilon x_2^2) = b \cdot \det \begin{pmatrix} x_1 & \varepsilon x_2 \\ x_2 & x_1 \end{pmatrix}.$$

As $\det C_{ns}(p^n) = \left({}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}\right)^{\times}$, the proof of the claim is obtained by varying x. We showed that for every $p \in \mathcal{B} \cup \mathcal{C}$ there exists $\gamma_p \in \mathrm{SL}_2\left({}^{\mathbb{Z}}\!/_{p^{n_p}}\right)$ such that $\gamma_p \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \in {}^{\Omega'}\!/_{p^{n_p}\Omega_E^2}$. Since the projection $\mathrm{SL}_2(\mathbb{Z}) \to \prod_{p \in \mathcal{B}\cup\mathcal{C}} \mathrm{SL}_2\left({}^{\mathbb{Z}}\!/_{p^{n_p}\mathbb{Z}}\right)$

is surjective, there exists an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\gamma \begin{pmatrix} \widetilde{e_1} \\ \widetilde{e_2} \end{pmatrix} \in \Omega' + \Lambda_{\mathcal{B}} \Lambda_{\mathcal{C}} \Omega_E^2 \subseteq \Omega'.$$

Since $(\widetilde{e_1}, \widetilde{e_2})$ is a basis of Ω_E, also $\gamma(\widetilde{e_1}, \widetilde{e_2})$ is a basis, and it is contained in Ω' as desired. □

Using Lemma 4.1.6, composing ψ with an isomorphism of $E \times E$, we can assume that there exists an element $\chi \in \Omega_{A,\sigma_0}$ such that $\mathrm{d}\psi(\chi) = (\omega_0, \tau_{\sigma_0}\omega_0)$. Setting $\omega = (\omega_0, \tau_{\sigma_0}\omega_0, \chi) \in \Omega_{E\times E\times A,\sigma_0}$, we define A_ω as the minimal abelian subvariety of $(E \times E \times A)_{\sigma_0}$ containing $\omega = (\omega_0, \tau_{\sigma_0}\omega_0, \chi)$ in its tangent space. As in the proof of [LF16, Proposition 5.1], one shows that

$$A_\omega := \{(\psi(z), z) \mid z \in A_{\sigma_0}\} \subset (E \times E \times A)_{\sigma_0}.$$

Indeed, the inclusion $A_\omega \subseteq \{(\psi(z), z) \mid z \in A_{\sigma_0}\}$ is clear, and the projection from A_ω to $E \times E$ is a subvariety of $(E \times E)_{\sigma_0}$ containing $(\omega_0, \tau_{\sigma_0}\omega_0)$ in its period lattice. As E is an elliptic curve without complex multiplication, the endomorphism ring of $E \times E$ is $M_{2\times 2}(\mathbb{Z})$, therefore no strict abelian subvariety of $(E \times E)_{\sigma_0}$ contains $(\omega_0, \tau_{\sigma_0}\omega_0)$ in its tangent space. This proves that the dimension of A_ω is at least 2, hence the equality above. We then see that the complex abelian variety A_ω can be defined over K'. When we consider A_ω as being defined over K', we will write $(A_\omega)_\sigma$ for its base-change to $\mathbb{C}$ along a given embedding $\sigma : K' \hookrightarrow \mathbb{C}$. The abelian variety A_ω falls within the context of [GR14, Part 7.3].

As explained in [LF16, Proposition 5.1], one can repeat the proof of Gaudron and Rémond to obtain a bound on Λ similar to that of [LF16, Theorem 5.2]. However, we will change some details to improve the final result.

We choose a polarisation on A_ω as in [GR14, Part 7.3], namely, in the following way. Set $n = \lfloor |\tau_{\sigma_0}|^2 \rfloor$, let L_E be the canonical principal polarisation on E_{σ_0} and let π_1, π_2 be the projections from $(E \times E)_{\sigma_0}$ on the two copies of E_{σ_0}. We consider the polarisation $L' = \pi_1^* L_E^{\otimes n} \otimes \pi_2^* L_E$ on $(E \times E)_{\sigma_0}$ and the isogeny f defined as the composition $A_\omega \xrightarrow{\sim} A_{\sigma_0} \xrightarrow{\psi} (E \times E)_{\sigma_0}$, where the first isomorphism is given by the projection $(\psi(z), z) \mapsto z$. We define the polarisation $L := f^* L'$ on A_ω, and as in [GR14, Part 7.3] we compute

$$\deg_L A_\omega = (\deg f) \deg_{L'} E^2 = 2n\Lambda^2. \tag{4.1.2}$$

Lemma 4.1.7. *Let $\hat{\mu}_{max}(\overline{t^\vee_{A_\omega}})$ be the quantity defined in [GR14, Part 6.8]. The inequality*

$$\hat{\mu}_{max}(\overline{t^\vee_{A_\omega}}) \leq \mathrm{h}_{\mathcal{F}}(E) + 2\log\Lambda + \frac{1}{2}\log\frac{n}{\pi}$$

holds.

Proof. It suffices to combine the proof of [GR14, Lemma 7.6] with the remark at the end of the proof of [LF16, Proposition 5.1], which gives $\mathrm{h}_{\mathcal{F}}(A_\omega) \leq 2\,\mathrm{h}_{\mathcal{F}}(E) + \log\Lambda$. □

The following definition collects the notations that will be needed in the rest of the proof.

Definition 4.1.8. Following [GR14, Parts 6.2 and 6.3], we set $\varepsilon = \frac{3\sqrt{2}-4}{2}$, $\theta = \frac{\log 2}{\pi}$ and $S_\sigma := \left\lfloor \frac{\theta\varepsilon}{x\delta_\sigma^2} \right\rfloor$, where x is as in Definition 4.1.2 and δ_σ is as in Definition 4.1.5. We further define $\mathcal{V} = \{\sigma : K' \hookrightarrow \mathbb{C} \mid S_\sigma \geq 1\}$. For every $\sigma : K' \hookrightarrow \mathbb{C}$ choose $B[\sigma] \subset (A_\omega)_\sigma$ as in Definition 4.1.2. We introduce the following quantities.

$$\begin{aligned}\aleph_1 :=& 2\max\{0, \hat{\mu}_{max}(\overline{t^\vee_{A_\omega}})\} + 5\log 2 + \frac{2}{[K':\mathbb{Q}]}\sum_{\sigma\in\mathcal{V}} \log\max\left\{1, \frac{1}{\rho((A_\omega)_\sigma, L_\sigma)}\right\} \\ &+ \frac{4}{[K':\mathbb{Q}]}\sum_{\sigma\in\mathcal{V}} \log\deg_{L_\sigma} B[\sigma] + \varepsilon\log 12; \\ m :=& \frac{1}{[K':\mathbb{Q}]}\sum_{\sigma\in\mathcal{V}} \frac{1}{\delta_\sigma^2}.\end{aligned}$$

By [GR14, Part 6], and in particular [GR14, Part 6.8], we have

$$\varepsilon\log 2\left(\frac{\varepsilon\theta}{x}m - 1\right) < \frac{\varepsilon\log 2}{[K':\mathbb{Q}]}\sum_{\sigma\in\mathcal{V}} S_\sigma \leq \aleph_1 + \frac{\pi x}{2}\left(\frac{3}{2} + \frac{3\theta\varepsilon}{x}\sqrt{m} + \left(\frac{\theta\varepsilon}{x}\right)^2 m\right),$$

where the inequality on the left is obtained by the definition of S_σ together with the inequality $\lfloor x\rfloor > x - 1$, while the inequality on the right is that of [GR14, Part 6.8, equation (14)] together with the estimate on $\aleph_2$ obtained by the Cauchy-Schwarz inequality on the same page of [GR14]. Solving the inequality in $\sqrt{m}$, using that $\theta = \frac{\log 2}{\pi}$, we obtain

$$\sqrt{m} < \frac{3\pi x}{2\varepsilon\log 2}\left(1 + \sqrt{1 + \frac{8}{9\pi x}\left(\aleph_1 + \frac{3\pi}{4}x + \varepsilon\log 2\right)}\right). \tag{4.1.3}$$

We now want to find a bound on x in terms of n. Recall that $\omega = (\omega_0, \tau_{\sigma_0}\omega_0, \chi)$. We have

$$\|\omega\|^2_{L,\sigma_0} = \|(\omega_0, \tau_{\sigma_0}\omega_0)\|^2_{L',\sigma_0} = n\|\omega_0\|^2_{L_E,\sigma_0} + \|\tau_{\sigma_0}\omega_0\|^2_{L_E,\sigma_0}.$$

Using Remark 4.1.4 we obtain

$$\begin{aligned}\|\omega\|^2_{L,\sigma_0} &= (n + |\tau_{\sigma_0}|^2)\|\omega_0\|^2_{L_E,\sigma_0} = (n + |\tau_{\sigma_0}|^2)\rho(E_{\sigma_0}, (L_E)_{\sigma_0})^2 \\ &= \frac{n + |\tau_{\sigma_0}|^2}{\Im\{\tau_{\sigma_0}\}} \leq \frac{n + |\tau_{\sigma_0}|^2}{\sqrt{|\tau_{\sigma_0}|^2 - \frac{1}{4}}} \leq \frac{2n}{\sqrt{n - \frac{1}{4}}},\end{aligned}$$

where the last inequality follows from the fact that the function $\frac{n+t}{\sqrt{t-1/4}}$ for $t \in [n, n+1]$ attains its maximum at $t = n = \lfloor |\tau_{\sigma_0}| \rfloor$.

Suppose now that $\sigma_0 \notin \mathcal{V}$, and hence that $S_{\sigma_0} = 0$. We notice that $x \leq x(0) = \frac{1}{\sqrt{\deg_L A_\omega}} = \frac{1}{\Lambda\sqrt{2n}}$ by equation (4.1.2). By definition of S_{σ_0} we have

$$1 > \frac{\theta\varepsilon}{x\delta_{\sigma_0}^2} \geq \frac{\theta\varepsilon\Lambda\sqrt{2n}}{\|\omega\|_{L,\sigma_0}^2} \geq \left(\frac{1}{2} - \frac{1}{8n}\right)^{\frac{1}{2}} \theta\varepsilon\Lambda > \sqrt{\frac{3}{8}}\theta\varepsilon\Lambda,$$

that gives $\Lambda < \frac{\sqrt{8}}{\theta\varepsilon\sqrt{3}} < 62$, which is better than Theorem 4.1.1 (since $\mathrm{h}_{\mathcal{F}}(E) > -0.75$ by Remark 1.2.9). Thus, we can assume $S_{\sigma_0} \geq 1$, and in particular, we can assume that $\sigma_0 \in \mathcal{V}$.

Since K' is a complex field, there exists an embedding $\overline{\sigma_0}$ of K' different from σ_0, which is its complex conjugate, inducing the same norm $\|\cdot\|_{L_{\overline{\sigma_0}}} = \|\cdot\|_{L_{\sigma_0}}$ and such that $\delta_{\overline{\sigma_0}} = \delta_{\sigma_0}$. Combining the fact that $\delta_{\sigma_0}^2 \leq \frac{2n}{\sqrt{n-\frac{1}{4}}}$ and that $\sigma_0, \overline{\sigma_0} \in \mathcal{V}$ we obtain

$$m = \frac{1}{[K' : \mathbb{Q}]} \sum_{\sigma \in \mathcal{V}} \frac{1}{\delta_\sigma^2} \geq \frac{1}{[K' : \mathbb{Q}]} \cdot \frac{2}{\delta_{\sigma_0}^2} \geq \frac{2}{[K' : \mathbb{Q}]} \cdot \frac{\sqrt{n - 1/4}}{2n}. \tag{4.1.4}$$

We now notice that for every embedding σ we have

$$\rho((A_\omega)_\sigma, L_\sigma) \geq \rho(E_\sigma, (L_E)_\sigma). \tag{4.1.5}$$

Indeed, for every period $\overline{\omega} = (\overline{\omega}_1, \overline{\omega}_2, \overline{\chi}) \in \Omega_{A_\omega,\sigma} \subseteq \Omega_{E,\sigma}^2 \times \Omega_{A,\sigma}$ we have

$$\|\overline{\omega}\|_{L,\sigma}^2 = n\|\overline{\omega}_1\|_{L_E,\sigma}^2 + \|\overline{\omega}_2\|_{L_E,\sigma}^2 \geq \max\{\|\overline{\omega}_1\|_{L_E,\sigma}^2, \|\overline{\omega}_2\|_{L_E,\sigma}^2\}.$$

We then have $\log\max\left\{1, \frac{1}{\rho((A_\omega)_\sigma, L_\sigma)}\right\} \leq \log\max\left\{1, \frac{1}{\rho(E_\sigma, (L_E)_\sigma)}\right\}$. If we define

$$\begin{aligned}\overline{\aleph}_1 := {} & 2\,\mathrm{h}_{\mathcal{F}}(E) + 4\log\Lambda + \log\frac{n}{\pi} + 5\log 2 + \frac{4}{[K' : \mathbb{Q}]} \sum_{\sigma \in \mathcal{V}} \log\deg_{L_\sigma} B[\sigma] \\ & + \frac{2}{[K' : \mathbb{Q}]} \sum_{\sigma} \log\max\left\{1, \frac{1}{\rho(E_\sigma, (L_E)_\sigma)}\right\} + \varepsilon\log 12,\end{aligned} \tag{4.1.6}$$

by Lemma 4.1.7 we have $\aleph_1 \leq \overline{\aleph}_1$. We can then replace $\aleph_1$ by $\overline{\aleph}_1$ in equation (4.1.3), and by inequality (4.1.4) we obtain

$$\frac{(n - 1/4)^{\frac{1}{4}}}{\sqrt{n[K' : \mathbb{Q}]}} < \frac{3\pi x}{2\varepsilon\log 2}\left(1 + \sqrt{1 + \frac{8}{9\pi x}\left(\overline{\aleph}_1 + \frac{3\pi}{4}x + \varepsilon\log 2\right)}\right). \tag{4.1.7}$$

By Remark 1.2.9, we have $\mathrm{h}_{\mathcal{F}}(E) \geq -0.75$ for every elliptic curve E. Since $\Lambda - 4 \cdot 1266.4 \log \Lambda < 2 \cdot 1266.4(-0.75 + 1.38)$ holds for every $\Lambda \leq 57000$, we can assume $\Lambda > 57000$, otherwise Theorem 4.1.1 would trivially hold. Then we have

$$\overline{\aleph}_1 > -1.5 + 4 \log 57000 + 5 \log 2 + \varepsilon \log 12 > 44.$$

Using that $x \leq x(0) = \frac{1}{\Lambda\sqrt{2n}} \leq \frac{1}{\Lambda\sqrt{2}}$ (Lemma 4.1.11), this gives

$$\frac{8}{9\pi x}\left(\overline{\aleph}_1 + \frac{3\pi}{4}x + \varepsilon \log 2\right) > \frac{8\sqrt{2} \cdot 57000}{9\pi} \cdot 44 > 10^6.$$

Since the function $\frac{1+\sqrt{z}}{\sqrt{1+z}}$ is decreasing for $z > 1$, in equation (4.1.7) we obtain

$$\frac{(n-1/4)^{\frac{1}{4}}}{\sqrt{n[K':\mathbb{Q}]}} < \frac{3\pi x}{2\varepsilon \log 2} \cdot \frac{1+1000}{\sqrt{10^6+1}} \sqrt{2 + \frac{8}{9\pi x}\left(\overline{\aleph}_1 + \frac{3\pi}{4}x + \varepsilon \log 2\right)}.$$

Squaring both sides and bounding x with $x(0) = \frac{1}{\sqrt{2n}\,\Lambda}$ we have

$$\begin{aligned}\frac{\sqrt{n-1/4}}{n[K':\mathbb{Q}]} &< \frac{9\pi^2 x^2}{4\varepsilon^2(\log 2)^2} \cdot 1.002 \cdot \left(2 + \frac{8}{9\pi x}\left(\overline{\aleph}_1 + \frac{3\pi}{4}x + \varepsilon \log 2\right)\right) \\ &= \frac{2\pi x}{\varepsilon^2(\log 2)^2} \cdot 1.002 \left(\overline{\aleph}_1 + 3\pi x + \varepsilon \log 2\right) \\ &< \frac{2.004\pi}{\varepsilon^2(\log 2)^2 \Lambda\sqrt{2n}} \left(\overline{\aleph}_1 + 0.085\right),\end{aligned}$$

where in the last inequality we bounded x with $\frac{1}{57000\sqrt{2}}$, since we are assuming that $\Lambda > 57000$. We then obtained that

$$\Lambda < [K':\mathbb{Q}]\left(2 - \frac{1}{2n}\right)^{-\frac{1}{2}} \frac{2.004\pi}{\varepsilon^2(\log 2)^2}\ (\overline{\aleph}_1 + 0.085), \tag{4.1.8}$$

and writing $(2 - \frac{1}{2n})^{-\frac{1}{2}} \leq \sqrt{\frac{2}{3}}$, we have

$$\Lambda < 727\,[K':\mathbb{Q}]\left(\overline{\aleph}_1 + 0.085\right). \tag{4.1.9}$$

We now want to bound $\overline{\aleph}_1$. We will first do it in general, and then specialise to the case $\mathcal{B} = \mathcal{C}_{sp} = \emptyset$. We will use the following lemma.

Lemma 4.1.9. *Let E be an elliptic curve defined over a number field K. We have*

$$\frac{1}{[K:\mathbb{Q}]} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \frac{1}{\rho(E_\sigma, (L_E)_\sigma)^2} < 2.29\,\mathrm{h}_{\mathcal{F}}(E) + 6.21.$$

Proof. If we call $T := \frac{1}{[K:\mathbb{Q}]} \sum_\sigma \frac{1}{\rho(E_\sigma,(L_E)_\sigma)^2}$, by [GR14, Proposition 3.2] we have that either $T < \frac{3}{\pi}$, which is better than the statement of the lemma by Remark 1.2.9, or $\pi T \leq 3 \log T + 6\, \mathrm{h}_{\mathcal{F}}(E) + 8.66$. In the latter case, we can apply [Sma98, Lemma B.1] and obtain

$$T < \frac{3}{\pi} \log\left(\frac{12}{\pi}\, \mathrm{h}_{\mathcal{F}}(E) + 5.52 + 4e^2\right) + \frac{6}{\pi}\, \mathrm{h}_{\mathcal{F}}(E) + 2.76 < 2.29\, \mathrm{h}_{\mathcal{F}}(E) + 6.21,$$

where in the last inequality we used that $\frac{12}{\pi}\, \mathrm{h}_{\mathcal{F}}(E) + 5.52 + 4e^2 > 32.2$ for $\mathrm{h}_{\mathcal{F}}(E) > -0.75$, and that $\frac{\log x}{x} \leq \frac{\log 32.2}{32.2}$ for $x \geq 32.2$. □

We can apply Lemma 4.1.9 and use the concavity of the logarithm to obtain

$$\begin{aligned}
&\frac{2}{[K':\mathbb{Q}]} \sum_{\sigma: K' \hookrightarrow \mathbb{C}} \log \max\left\{1, \frac{1}{\rho(E_\sigma,(L_E)_\sigma)}\right\} \\
=&\frac{1}{[K':\mathbb{Q}]} \sum_{\sigma: K' \hookrightarrow \mathbb{C}} \log \max\left\{1, \frac{1}{\rho(E_\sigma,(L_E)_\sigma)^2}\right\} \\
\leq& \max\left\{0, \log\left(\frac{1}{[K':\mathbb{Q}]} \sum_{\sigma: K' \hookrightarrow \mathbb{C}} \frac{1}{\rho(E_\sigma,(L_E)_\sigma)^2}\right)\right\} \\
<& \log(2.29\, \mathrm{h}_{\mathcal{F}}(E) + 6.21) < \log(\mathrm{h}_{\mathcal{F}}(E) + 2.72) + 0.829.
\end{aligned} \tag{4.1.10}$$

By the definition of $B[\sigma]$ we have $x = x(B[\sigma]) \leq x(0)$, and so either $B[\sigma] = 0$, which gives $\deg_{L_\sigma} B[\sigma] = 1$, or $\frac{\deg_{L_\sigma} B[\sigma]}{\deg_{L_\sigma} A_\omega} \leq \frac{1}{\sqrt{\deg_{L_\sigma} A_\omega}}$, which gives $\deg_{L_\sigma} B[\sigma] \leq \sqrt{\deg_{L_\sigma} A_\omega}$. In particular, using equation (4.1.2) we have the bound

$$\begin{aligned}
\frac{4}{[K':\mathbb{Q}]} \sum_{\sigma \in \mathcal{V}} \log \deg_{L_\sigma} B[\sigma] &\leq 2 \log \deg_{L_\sigma} A_\omega \\
&\leq 4 \log \Lambda + 2 \log n + 2 \log 2.
\end{aligned} \tag{4.1.11}$$

If we use inequalities (4.1.10) and (4.1.11) to bound $\overline{\aleph}_1$ and we replace it in equation (4.1.9) we obtain

$$\begin{aligned}
\Lambda < 727[K':\mathbb{Q}]\big(&2\, \mathrm{h}_{\mathcal{F}}(E) + \log(\mathrm{h}_{\mathcal{F}}(E) + 2.72) + 8 \log \Lambda \\
&+ 3 \log n - \log \pi + 7 \log 2 + 0.914 + \varepsilon \log 12\big).
\end{aligned}$$

By our choice of σ_0, we know that $\frac{1}{\rho(E_{\sigma_0},(L_E)_{\sigma_0})^2} = \Im\{\tau_{\sigma_0}\}$ is smaller than or equal to the mean of the values $\Im\{\tau_\sigma\}$. Using Lemma 4.1.9 we then have

$$n \leq |\tau_{\sigma_0}|^2 \leq \Im\{\tau_{\sigma_0}\}^2 + \frac{1}{4} \leq (2.29\, \mathrm{h}_{\mathcal{F}}(E) + 6.21)^2 + \frac{1}{4},$$

and so

$$\log n \leq 2 \log(\mathrm{h}_{\mathcal{F}}(E) + 2.72) + 1.662. \tag{4.1.12}$$

We then obtain

$$\begin{aligned}\Lambda &< 1454\,[K':\mathbb{Q}]\left(\mathrm{h}_{\mathcal{F}}(E)+\frac{7}{2}\log(\mathrm{h}_{\mathcal{F}}(E)+2.72)+4\log\Lambda+5\right)\\ &= 1454\cdot 2^{|\mathcal{C}|}[K:\mathbb{Q}]\left(\mathrm{h}_{\mathcal{F}}(E)+\frac{7}{2}\log(\mathrm{h}_{\mathcal{F}}(E)+2.72)+4\log\Lambda+5\right),\end{aligned}$$

concluding the proof of the first part of Theorem 4.1.1.

The non-split Cartan case

When $\mathcal{B}=\mathcal{C}_{sp}=\emptyset$ we are able to obtain a better bound. To do this, we show that the subvarieties $B[\sigma]$ are equal to 0 for every embedding σ.

We distinguish cases according to whether $\Lambda\leq\sqrt{2n}$ or $\Lambda>\sqrt{2n}$.

Lemma 4.1.10. *If $\Lambda\leq\sqrt{2n}$, then Theorem 4.1.1 holds for E and Λ.*

Proof. If $\Lambda\leq\sqrt{2n}$, we can write

$$\Lambda\leq\sqrt{2\lfloor|\tau_{\sigma_0}|^2\rfloor}\leq\sqrt{2|\tau_{\sigma_0}|^2}\leq\sqrt{2\left((\Im\{\tau_{\sigma_0}\})^2+\frac{1}{4}\right)}\leq\sqrt{2}\,\Im\{\tau_{\sigma_0}\}+\frac{1}{\sqrt{2}}.$$

Remark 4.1.4 gives $\Im\{\tau_\sigma\}=\rho(E_\sigma,L_\sigma)^{-2}$, so by Lemma 4.1.9 we have

$$\Im\{\tau_{\sigma_0}\}\leq\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma}\Im\{\tau_\sigma\}\leq 3\,\mathrm{h}_{\mathcal{F}}(E)+6.5,$$

and therefore $\Lambda<5\,\mathrm{h}_{\mathcal{F}}(E)+10$, which is largely better than Theorem 4.1.1 (taking into account that $\mathrm{h}_{\mathcal{F}}(E)>-0.75$ by Remark 1.2.9). □

Lemma 4.1.11. *Assume $\Lambda>\sqrt{2n}$ and $\mathcal{B}=\mathcal{C}_{sp}=\emptyset$. Given A_ω considered as an abelian variety over K' as above, for every $\sigma:K'\hookrightarrow\mathbb{C}$ we have $B[\sigma]=0$, and hence $x=\frac{1}{\Lambda\sqrt{2n}}$.*

Proof. Since $A_\omega\cong A$, it is sufficient to prove the statement for A and $L=\psi^*L'$. First, we notice that $x(0)=\left(\frac{1}{2n\Lambda^2}\right)^{\frac{1}{2}}=\frac{1}{\Lambda\sqrt{2n}}$. Let us now consider an arbitrary proper abelian subvariety B such that $\dim B>0$. The subgroups of A correspond to those of $E\times E$ that contain the group

$$G=\prod_{p\in\mathcal{C}_{ns}}\{(x,g_p\cdot x)\mid x\in E[p^{n_p}]\}.$$

Since B is a proper subvariety of the abelian surface A, we have $\dim B=1$. Hence, given the isogeny $\varphi:E\times E\to A$, the group $\varphi^{-1}(B)\subset E\times E$ is an algebraic subgroup of dimension 1 containing G. In particular, there exists an elliptic curve $C\subset E\times E$ such that the algebraic group $\varphi^{-1}(B)$ is $\tilde{C}:=\langle C,G\rangle$,

and C is the connected component of $\tilde{C}$ that contains 0. Since $\ker\varphi = G$, we have $\varphi(C) = \varphi(\tilde{C}) = B$, and $C = [\Lambda](C) = \psi\circ\varphi(C) = \psi(B)$. By assumption, E does not have CM, hence there exist two relatively prime integers a, b such that

$$C = \{(P, Q) \in E \times E \mid aP = bQ\}.$$

Therefore, we have $\deg\varphi|_C = |\ker\varphi|_C| = |C \cap G|$. We now notice that $C \cap G = \prod_{p\in\mathcal{C}_{ns}}(C \cap G_p)$: indeed, the groups G_p are p-groups and hence have pairwise coprime orders. The same holds for the subgroups $C\cap G_p$. The group $C \cap G$ is generated by the groups $C \cap G_p$, and for every pair of primes p, q the groups $C \cap G_p$ and $C \cap G_q$ intersect trivially: this implies that $C \cap G$ is the direct product of the groups $C \cap G_p$. For every p we have

$$C \cap G_p = \{(x, g_p \cdot x) \mid x \in E[p^{n_p}] \text{ such that } (a - bg_p)x = 0\}.$$

However, given

$$g_p = \begin{pmatrix} \alpha & \varepsilon\beta \\ \beta & \alpha \end{pmatrix} \qquad \text{we have} \qquad a - bg_p = \begin{pmatrix} a - b\alpha & -\varepsilon b\beta \\ -b\beta & a - b\alpha \end{pmatrix}.$$

By assumption we have $p \nmid \beta$, hence if $p \nmid b$, we have that $a - bg_p$ is invertible (since it is an element of $C_{ns}(p^{n_p})$). If instead $p \mid b$, then $p \nmid a$ and so $p \nmid a-b\alpha$, and $a-bg_p$ is again invertible. This implies that $C\cap G_p = 0$, and so $C\cap G = 0$. This shows that $\deg\varphi|_C = 1$. We then have

$$\Lambda^2 = \deg[\Lambda]|_C = (\deg\psi|_B)(\deg\varphi|_C) = \deg\psi|_B,$$

and therefore $\deg_L B = \deg_{\psi^* L'} B = (\deg\psi|_B)\deg_{L'} C \geq \Lambda^2$. We can now estimate

$$x(B) = \frac{\deg_L B}{\deg_L A} \geq \frac{\Lambda^2}{2n\Lambda^2} = \frac{1}{2n},$$

and so $x(B) > x(0) = \frac{1}{\Lambda\sqrt{2n}}$ since $\Lambda > \sqrt{2n}$. □

Remark 4.1.12. As $B[\sigma] = 0$ for every σ, we have $\rho((A_\omega)_\sigma, L_\sigma) = \delta_\sigma$.

Given $\overline{\aleph}_1$ as in (4.1.6), we can use Lemma 4.1.11 and inequality (4.1.10) to obtain

$$\overline{\aleph}_1 < 2\,\mathrm{h}_{\mathcal{F}}(E) + \log(\mathrm{h}_{\mathcal{F}}(E)+2.72) + 4\log\Lambda + \log\frac{n}{\pi} + 5\log 2 + \varepsilon\log 12 + 0.829.$$

Combined with (4.1.12) and (4.1.9), this yields

$$\Lambda < 1454 \cdot 2^{|\mathcal{C}|}[K : \mathbb{Q}]\left(\mathrm{h}_{\mathcal{F}}(E) + \frac{3}{2}\log(\mathrm{h}_{\mathcal{F}}(E) + 2.72) + 2\log\Lambda + 2.6\right),$$

proving the second part of Theorem 4.1.1.

Suppose now that $K = \mathbb{Q}$. Since E is defined over $\mathbb{Q}$, we have that $\tau_\sigma = \tau_{\sigma_0} = \tau$ for every embedding σ. We then have

$$\frac{2}{[K' : \mathbb{Q}]} \sum_{\sigma \in \mathcal{V}} \log \max \left\{ 1, \frac{1}{\rho(E_\sigma, (L_E)_\sigma)} \right\} = \max\{0, \log \Im\{\tau\}\}$$

and $\log n \leq \log |\tau|^2 \leq \log \left(\Im\{\tau\}^2 + \frac{1}{4} \right)$. If $|\tau|^2 < 2$, we have $\log n = 0$, if instead $|\tau|^2 \geq 2$, then $\Im\{\tau\}^2 \geq \frac{7}{4}$ and so $\log \left(\Im\{\tau\}^2 + \frac{1}{4} \right) \leq \log \left(\frac{8}{7} \Im\{\tau\}^2 \right) = 2 \log(\Im\{\tau\}) + \log(8/7)$. We can combine the two cases by writing $\log n \leq \max\{0, 2 \log(\Im\{\tau\})\} + \log(8/7)$. Bounding $\overline{\aleph}_1$ with

$$2\, \mathrm{h}_{\mathcal{F}}(E) + 4 \log \Lambda - \log \pi + 5 \log 2 + \varepsilon \log 12 + 3 \max\{0, \log \Im\{\tau\}\} + \log \left(\frac{8}{7} \right),$$

by equation (4.1.9) we obtain

$$\Lambda < 1454 \cdot 2^{|\mathcal{C}|} \left(\mathrm{h}_{\mathcal{F}}(E) + 2 \log \Lambda + \frac{3}{2} \max\{0, \log(\Im\{\tau\})\} + 1.38 \right),$$

which proves part 3 of Theorem 4.1.1.

To conclude the proof of Theorem 4.1.1, we notice that for $\Im\{\tau_{\sigma_0}\} \geq \frac{15}{\pi}$, we can write $n \geq |\tau_{\sigma_0}|^2 - 1 \geq \Im\{\tau_{\sigma_0}\}^2 - 1 > 21.7$. We can then estimate $\left(2 - \frac{1}{2n}\right)^{-\frac{1}{2}} \leq \sqrt{\frac{44}{87}}$. Hence, in equation (4.1.8) we can use the estimate

$$\left(2 - \frac{1}{2n}\right)^{-\frac{1}{2}} \frac{2.004\pi}{\varepsilon^2 (\log 2)^2} \leq 633.2.$$

Repeating the rest of the proof in the same way we obtain the desired inequalities.

4.2 Bounds for non-integral j-invariants

In this section, we show that in the setting of Section 4.1, if we assume that $j(E) \notin \mathcal{O}_K$, we can obtain stronger bounds on Λ whenever $\mathcal{B} = \emptyset$. The approach here is completely different: instead of studying the complex structure of E and the periods of auxiliary complex abelian varieties, we rely on local arguments at primes $\mathfrak{p} \mid p$ for which $\rho_{E,p}$ is not surjective. Finally, we will use these results to simplify the inequalities in the statement of Theorem 4.1.1.

Proposition 4.2.1. *Let E be an elliptic curve defined over a number field K. Let $\mathcal{C}_{sp}, \mathcal{C}_{ns}$ be disjoint sets of odd primes p such that $\operatorname{Im} \rho_{E,p} \subseteq H(p)$ up to conjugacy for $H = C_{sp}^+, C_{ns}^+$ respectively. Let n_p be the largest positive integer such that $\operatorname{Im} \rho_{E,p^{n_p}} \subseteq H(p^n)$ up to conjugacy, and let $\Lambda := \prod_{p \in \mathcal{C}_{sp} \cup \mathcal{C}_{ns}} p^{n_p}$. Then Λ divides*

$$\gcd_{\lambda \subseteq \mathcal{O}_K \text{ prime}} (\max\{0, -v_\lambda(j(E))\}).$$

Proof. If $j(E) \in \mathcal{O}_K$ the statement is trivial. Let λ be a prime of K such that $e := -v_\lambda(j(E)) > 0$ and let p^n be a prime power such that $p^n \mid \Lambda$. We want to show that $p^n \mid e$. We can assume that $\zeta_p \in K$: indeed, p does not divide $[K(\zeta_p) : K]$ and so the power of p that divides the valuation of $j(E)$ at primes of $K(\zeta_p)$ above λ is the same as that of the λ-adic valuation of $j(E)$. Consider E to be defined over K_λ, and let E_q be the Tate curve with parameter $q \in K_\lambda^\times$, isomorphic to E over a quadratic extension of K_λ. We know that $v_\lambda(q) = e$. Suppose first that $p \in \mathcal{C}_{ns}$: if χ_{p^n} is the cyclotomic character modulo p^n, there is a quadratic character ψ such that $\rho_{E_q,p^n} \cong \rho_{E,p^n} \otimes \psi$, and we have

$$\rho_{E,p^n} \otimes \psi \cong \begin{pmatrix} \chi_{p^n} & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

where $k(\sigma)$ is such that $\sigma\left(q^{\frac{1}{p^n}}\right) = q^{\frac{1}{p^n}}\zeta_{p^n}^{k(\sigma)}$. Indeed, as shown in case (ii) of the proof of Proposition 3.1.2, the image of an automorphism σ via χ_{p^n} must be ± 1, however it cannot be -1 because $\chi_p = \chi_{p^n} \pmod p$ is trivial, as $\zeta_p \in K$. By the definition of $\mathcal{C}_{ns}$, for every $\sigma \in \mathrm{Gal}\left(\overline{K_\lambda}/K_\lambda\right)$ we know that $M_\sigma := (\rho_{E,p^n} \otimes \psi)(\sigma)$ is conjugate to an element of $C_{ns}^+(p^n)$. Following the definitions of Chapter 3, we call $G := \mathrm{Im}(\rho_{E,p^\infty} \otimes \psi)$ and $G(p^n) := \mathrm{Im}(\rho_{E,p^n} \otimes \psi)$. Let $0 \le i \le n$ be such that $M_\sigma = \begin{pmatrix} 1 & up^i \\ 0 & 1 \end{pmatrix}$, for $u \not\equiv 0 \pmod p$. If $i = 0$, then $M_\sigma \pmod p$ has non-diagonal Jordan form over $\overline{\mathbb{F}}_p$, and hence it cannot be an element of $C_{ns}^+(p)$. If instead $0 < i < n$, we can write $M_\sigma = I + p^i \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix}$, and so there is an element in $\mathfrak{g}_i$ of rank 1 (where $\mathfrak{g}_i$ is defined in Definition 2.1.3). However, since $G(p^n) \subseteq C_{ns}^+(p^n)$ up to conjugation, by Remark 2.1.8 the group $\mathfrak{g}_i$ is conjugate to a subgroup of $V_1 \oplus V_2$ defined as in Lemma 2.1.7, which contains no matrices of rank 1. Since the rank is invariant under conjugation, we have that $i = n$, and in particular $M_\sigma = I$. This implies that $k(\sigma) = 0$ for every σ, and in particular that $\sigma\left(q^{\frac{1}{p^n}}\right) = q^{\frac{1}{p^n}}$. Hence $q^{\frac{1}{p^n}} \in K_\lambda$, and so $p^n \mid e$.

If instead we have $p \in \mathcal{C}_{sp}$, there exists again a quadratic character ψ such that

$$\rho_{E,p^n} \otimes \psi \cong \begin{pmatrix} \chi_{p^n} & k \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \pmod p,$$

with $\sigma\left(q^{\frac{1}{p^n}}\right) = q^{\frac{1}{p^n}}\zeta_{p^n}^{k(\sigma)}$. In particular, every element in $\mathrm{Im}\,\rho_{E,p^n}$ can be written as $I + pA$, with A of the form $\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$. Since $C_{sp}^+(p)$ does not contain elements of order p, we must have $k \equiv 0 \pmod p$. If we call G a group

conjugate to $\operatorname{Im}\rho_{E_q,p^\infty}$ such that $\pm G(p^n) \subseteq C_{sp}^+(p^n)$, we must have that for every $1 \leq i < n$, every element in $\mathfrak{g}_i$ has rank at most 1. By Remark 2.1.8, these elements must lie in $V \oplus W$, with $V := \mathbb{F}_p \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $W := \mathbb{F}_p \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. However, we must have that either $\mathfrak{g}_i \subseteq V$ or $\mathfrak{g}_i \subseteq W$: indeed, if we had $0 \neq x \in \mathfrak{g}_i \cap V$ and $0 \neq y \in \mathfrak{g}_i \cap W$, then the matrix $x + y$ would lie in $\mathfrak{g}_i$, which is impossible as $x + y$ has rank 2. By Lemma 2.1.4, we have $\mathfrak{g}_1 \subseteq \ldots \subseteq \mathfrak{g}_{n-1}$, hence they are all contained in the same subspace V or W. Let i be the smallest integer for which $\mathfrak{g}_i \neq 0$. If we take a non-zero element of $\mathfrak{g}_i$, this is the image of an element in $G(p^n)$ of order p^{n-i}. On the other hand, as $G(p) = \{I\}$, we have

$$|G(p^n)| = \prod_{t=1}^{n-1} |\mathfrak{g}_t| = \prod_{t=i}^{n-1} |\mathfrak{g}_t| = p^{n-i}.$$

In particular, this implies that $G(p^n)$ is a cyclic p-group, as is $H(p^n) := \operatorname{Im}(\rho_{E,p^n} \otimes \psi)$. Let

$$M_\sigma := (\rho_{E,p^n} \otimes \psi)(\sigma) = I + p^i \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

be a generator of $H(p^n)$, where i is as large as possible (i.e. either a or b are coprime with p). If $i \geq n$ then $M_\sigma = I$, and so $H(p^n) = I$: we conclude as in the non-split case that $p^n \mid e$. If $i < n$, we can assume that $p \nmid a$: indeed, if we had $p \mid a$, modulo p^{i+1} we would have $M_\sigma \equiv I + p^i \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \pmod{p^{i+1}}$, where $b \not\equiv 0 \pmod{p^{i+1}}$. In particular, we would have a non-zero element $x \in \mathfrak{g}_i$ conjugate to $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, and so such that $\operatorname{tr} x = \det x = 0$. However, this is impossible because such an element cannot lie in $V \oplus W$. Consider the element $q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a}$: in the basis $(\zeta_{p^n}, q^{\frac{1}{p^n}})$ this is expressed as the vector $(-b/a, 1)$. We then have

$$\sigma(q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a}) \longleftrightarrow \begin{pmatrix} 1 + p^i a & p^i b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -b/a \\ 1 \end{pmatrix} = \begin{pmatrix} -b/a \\ 1 \end{pmatrix} \longleftrightarrow q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a},$$

and so $\sigma(q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a}) = q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a}$. Since M_σ generates $H(p^n)$, this implies that $q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a}$ is fixed by every automorphism, and so $q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a} \in K_\lambda$. We conclude as in the non-split case that $v_\lambda(q^{\frac{1}{p^n}} \zeta_{p^n}^{-b/a}) = \frac{e}{p^n} \in \mathbb{Z}$, and hence $p^n \mid e$. $\square$

Theorem 4.2.2. *Let E be an elliptic curve defined over a number field K of degree $d = [K : \mathbb{Q}]$, n a positive integer, and p an odd prime such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ up to conjugation. Suppose that $j = j(E) \notin \mathcal{O}_K$, then*

$$p^n \leq \frac{1.6dn\,\mathrm{h}(j)}{\log(1.6dn\,\mathrm{h}(j)) - \log\log(1.6dn\,\mathrm{h}(j))} < \frac{2.2dn\,\mathrm{h}(j)}{\log(dn\,\mathrm{h}(j))}.$$

Moreover, if $p^{n-1}(p-1) \nmid 2d$ we have

$$p^n < \frac{d\,\mathrm{h}(j) + 1.116}{\log(d\,\mathrm{h}(j) + 1.116) - \log\log(d\,\mathrm{h}(j) + 1.116)} < 1.68 \cdot \frac{d\,\mathrm{h}(j)}{\log(d\,\mathrm{h}(j))}.$$

Proof. Let M_K be the set of all places of K. We have

$$\mathrm{h}(j) = \frac{1}{d}\sum_{\nu \in M_K} n_\nu \log\max\{1, \|j\|_\nu\} \geq \frac{1}{d}\sum_{\substack{\lambda \subseteq \mathcal{O}_K \text{ prime} \\ v_\lambda(j) < 0}} n_\lambda \log\|j\|_\lambda, \tag{4.2.1}$$

where n_ν are the local degrees, and the inequality is obtained by taking the sum only over the finite places. We remark that, since $j \notin \mathcal{O}_K$, the sum on the RHS of equation (4.2.1) is non-zero. By Proposition 4.2.1 we know that for every prime $\lambda \subseteq \mathcal{O}_K$ such that $v_\lambda(j) < 0$, we have $p^n \leq -v_\lambda(j)$. Moreover, we have $\log\|j\|_\lambda = -v_\lambda(j)\log N_{K/\mathbb{Q}}(\lambda) \geq p^n \log N_{K/\mathbb{Q}}(\lambda)$. By Proposition 3.1.2 we know that either $\lambda \mid p$ or $N_{K/\mathbb{Q}}(\lambda) \equiv \pm 1 \pmod{p^n}$. This implies that either p divides $N_{K/\mathbb{Q}}(\lambda)$ or $N_{K/\mathbb{Q}}(\lambda) \geq p^n - 1 \geq p - 1$. In both cases, by equation (4.2.1) we have

$$d\,\mathrm{h}(j) \geq \sum_{\substack{\lambda \subseteq \mathcal{O}_K \text{ prime} \\ v_\lambda(j) < 0}} n_\lambda \log\|j\|_\lambda \geq p^n \log(p-1). \tag{4.2.2}$$

As $p \geq 3$, we have that $d\,\mathrm{h}(j) > 2$. Moreover, we have $\frac{\log p}{\log(p-1)} \leq 1.6$, hence we can write $1.6d\,\mathrm{h}(j) \geq p^n \log p$. The function $x^n \log x$ is strictly increasing, and its inverse function is $\sqrt[n]{\frac{nx}{W(nx)}}$, where $W(x)$ is the Lambert W function. This implies that $p^n \leq \frac{1.6dn\,\mathrm{h}(j)}{W(1.6dn\,\mathrm{h}(j))}$, and by [HH08, Theorem 2.1], using $d\,\mathrm{h}(j) > 2 > \frac{e}{1.6n}$, we have

$$p^n \leq \frac{1.6dn\,\mathrm{h}(j)}{\log(1.6dn\,\mathrm{h}(j)) - \log\log(1.6dn\,\mathrm{h}(j))}. \tag{4.2.3}$$

If we now assume that $p^{n-1}(p-1) \nmid 2d$ and take λ such that $v_\lambda(j) < 0$, by Proposition 3.1.2 we know that $\lambda \nmid p$, and so $N_{K/\mathbb{Q}}(\lambda) \equiv \pm 1 \pmod{p^n}$. Using $p^{n-1}(p-1) \nmid 2d$ we notice that $p^n \neq 3$, and hence $p^n \geq 5$. Similarly to above we obtain

$$d\,\mathrm{h}(j) \geq p^n \log(p^n - 1) = p^n \log(p^n) + p^n \log\left(1 - \frac{1}{p^n}\right) > p^n \log(p^n) - 1.116,$$

where we used that $\frac{\log(1-x)}{x} > -1.116$ for $x \in \left(0, \frac{1}{5}\right)$. As before, the function $x\log(x)$ has inverse $\frac{x}{W(x)}$, and using $d\,\mathrm{h}(j) + 1.116 \geq 2 + 1.116 > e$, we can apply again [HH08, Theorem 2.1], obtaining the desired inequality. To conclude the proof, it suffices to notice that the functions

$$\frac{1.6x}{\log(1.6x) - \log\log(1.6x)} \qquad \text{and} \qquad \frac{x + 1.116}{\log(x + 1.116) - \log\log(x + 1.116)}$$

are smaller than $\frac{cx}{\log x}$, for $c = 2.2$ and $c = 1.68$ respectively, whenever $x > 2$ (which is always the case for $d\,\mathrm{h}(j)$, as we proved above). □

Corollary 4.2.3. *Let E be an elliptic curve defined over $\mathbb{Q}$, n a positive integer, and p an odd prime such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ up to conjugation. Suppose that $j = j(E) \notin \mathbb{Z}$ and define $b(j) := \mathrm{h}(j) - \log\max\{1, |j|\}$. We have that either $p^n = 3$ or*

$$p^n < \frac{b(j) + 0.527}{\log(2b(j) + 1.054) - \log\log(2b(j) + 1.054)} < 1.3 \cdot \frac{b(j)}{\log b(j)}.$$

Proof. The proof is analogous to that of Theorem 4.2.2. First, we note that we can replace $\mathrm{h}(j)$ with $b(j)$ in equation (4.2.1), and that $b(j) \geq 2$, as $j \notin \mathbb{Z}$. We then note that by Corollary 3.1.3 we have $\ell \equiv \pm 1 \pmod{p^n}$, but for $p^n \neq 3$ the number $p^n \pm 1$ is even and greater than 2. In particular, it cannot be prime, and so $\ell \geq 2p^n - 1$. Since $p^n \neq 3$ we have $p^n \geq 5$ and $p^{n-1}(p-1) > 2$, so as in the proof of Theorem 4.2.2 we obtain

$$\begin{aligned} b(j) &\geq p^n \log(2p^n - 1) = p^n \log(2p^n) + p^n \log\left(1 - \frac{1}{2p^n}\right) \\ &> p^n \log(2p^n) - 0.527, \end{aligned} \tag{4.2.4}$$

where we used that $\frac{\log(1-x)}{x} > -1.054$ for $x \in \left(0, \frac{1}{10}\right)$. We notice that since $p^n \geq 5$ we have $b(j) \geq 5\log 9 > 10$. One can verify that the function $x\log(2x)$ has inverse $\frac{x}{W(2x)}$, and since $2(b(j)+0.527) > e$ we can apply [HH08, Theorem 2.1] to obtain the desired inequality. We conclude the proof by noting that the function $\frac{x+0.527}{\log(2x+1.054)-\log\log(2x+1.054)}$ is smaller than $\frac{1.3x}{\log x}$ for $x > 10$. □

Theorem 4.2.4. *Let E be an elliptic curve over a number field K of degree d over $\mathbb{Q}$. Let $\mathcal{C}_{sp}, \mathcal{C}_{ns}$ and Λ be as in Proposition 4.2.1 and suppose that $j(E) \notin \mathcal{O}_K$. We have*

$$\Lambda \leq \frac{d}{\log 2}\,\mathrm{h}(j(E)).$$

Moreover, if $K = \mathbb{Q}$ we have

$$\Lambda \leq \frac{1}{\log 2}\left(\mathrm{h}(j(E)) - \log\max\{1, |j(E)|\}\right) < \frac{12}{\log 2}\,\mathrm{h}_{\mathcal{F}}(E) + 25.$$

Proof. Set $j = j(E)$. As in equation (4.2.1) we have

$$[K : \mathbb{Q}]\, \mathrm{h}(j) \geq \sum_{\substack{\lambda \subseteq \mathcal{O}_K \text{ prime} \\ v_\lambda(j) < 0}} n_\lambda \log \|j\|_\lambda,$$

and by Proposition 4.2.1 we have that for every λ in the sum above, the inequality $\log \|j\|_\lambda \geq -v_\lambda(j) \log 2 \geq \Lambda \log 2$ holds, and the hypothesis $j(E) \notin \mathcal{O}_K$ ensures there is at least one such prime ideal λ. If $K = \mathbb{Q}$, as in Corollary 4.2.3, we can replace $\mathrm{h}(j)$ with $\mathrm{h}(j) - \log \max\{1, |j|\}$ to obtain the first inequality. By Theorem 1.2.6, for $|j| \leq 3500$ we have that

$$\frac{1}{\log 2}\, \mathrm{h}(j) < \frac{12}{\log 2}(\mathrm{h}_{\mathcal{F}}(E) + 1.429) < \frac{12}{\log 2}\, \mathrm{h}_{\mathcal{F}}(E) + 25.$$

If instead $|j| > 3500$, we have

$$\begin{aligned} \frac{1}{\log 2}(\mathrm{h}(j) - \log |j|) &< \frac{1}{\log 2}(12\, \mathrm{h}_{\mathcal{F}}(E) + 6 \log\log |j| - \log |j| + 12 \cdot 0.406) \\ &< \frac{12}{\log 2}\, \mathrm{h}_{\mathcal{F}}(E) + 14, \end{aligned}$$

which is even better. □

Theorem 4.2.5. *Let $E/\mathbb{Q}$ be an elliptic curve without CM, let $\mathcal{C}$ be the set of all primes $p > 2$ such that $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$ up to conjugation, and let Λ be as in Theorem 4.1.1. We have*

$$\Lambda < 21000\, (\mathrm{h}_{\mathcal{F}}(E) + 40)^{1.308}.$$

Moreover, if we define

$$\delta(x) := \frac{1}{\log(\log(x + 40) + 7.6) - 0.903}$$

for every $x > -0.75$, we have

$$\Lambda < 14400 \cdot (\mathrm{h}_{\mathcal{F}}(E) + 40)^{0.907 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))}\, (\mathrm{h}_{\mathcal{F}}(E) + 22.5).$$

Proof. By Theorem 4.2.4 we can assume that $j(E) \in \mathbb{Z}$, otherwise we would have a better bound. Let $\tau \in \mathcal{H}$ be the element in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ corresponding to E, and let $q = e^{2\pi i \tau}$. By Lemma 5.3.3, we can assume that $7 \nmid \Lambda$ and at most one among 3 and 5 divides Λ: indeed, if 7 divided Λ we would have $\Lambda \leq 504$, which is better than the statement of the theorem, while the case $15 \mid \Lambda$ never occurs. Since it is known that there are no non-CM elliptic curves E with $j(E) \in \mathbb{Z}$ and $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$ for $p \in \{11, 13, 17\}$ (see [ST12, Theorem 1.2], [BDM$^+$19,

Corollary 1.3] and [BDM$^+$23, Theorem 1.2]), we know that $|\mathcal{C}| \leq 1 + |\{p \geq 19 : p \mid \Lambda\}|$. This implies that

$$\begin{aligned} |\mathcal{C}| &\leq \max\left\{\log_{19}\Lambda,\ 1+\log_{19}\frac{\Lambda}{3},\ 1+\log_{19}\frac{\Lambda}{5}\right\} \\ &= \log_{19}\Lambda + 1 - \log_{19} 3 < \log_{19}\Lambda + 0.627. \end{aligned}$$

Suppose first that $|\log|q|| \leq 30$: by Theorem 1.2.6(3) we obtain that $\mathrm{h}_{\mathcal{F}}(E) < 0.6$. Using that $\Im\{\tau\} = \frac{|\log|q||}{2\pi}$ and writing $2^{|\mathcal{C}|} < 2^{0.627}\cdot\Lambda^{\log_{19}2}$, by Theorem 4.1.1(3) we have that

$$\Lambda^{1-\log_{19}2} < 1454\cdot 2^{0.627}\left(0.6 + 2\log\Lambda + \frac{3}{2}\log\left(\frac{15}{\pi}\right) + 1.38\right).$$

Solving the inequality numerically we obtain that $\Lambda < 2.41\cdot 10^6$, which satisfies the first statement of the theorem: indeed, by Remark 1.2.9 we have $\mathrm{h}_{\mathcal{F}}(E) > -0.75$, and so $20000\cdot 39.25^{1.308} > 2.41\cdot 10^6$. We can then assume that $|\log|q|| > 30$, and hence by Theorem 1.2.6(4) that $\mathrm{h}_{\mathcal{F}}(E) > 0.45$. By Theorem 4.1.1(2) we have

$$\Lambda < 1266.4\cdot 2^{|\mathcal{C}|}\left(\mathrm{h}_{\mathcal{F}}(E) + \frac{3}{2}\log(\mathrm{h}_{\mathcal{F}}(E)+2.72) + 2\log\Lambda + 2.6\right). \tag{4.2.5}$$

The function $(x + \frac{3}{2}\log(x+2.72)+2.6)/(x+8)$ is bounded by $\alpha := 1.0144$, so we have

$$\Lambda < 1266.4\alpha\cdot 2^{|\mathcal{C}|}\left(\mathrm{h}_{\mathcal{F}}(E) + \frac{2}{\alpha}\log\Lambda + 8\right). \tag{4.2.6}$$

Using again the inequality $2^{|\mathcal{C}|} < 2^{0.627}\cdot\Lambda^{\log_{19}2}$ we obtain

$$\begin{aligned} \Lambda^{1-\log_{19}2} &< 1266.4\alpha\cdot 2^{0.627}\left(\mathrm{h}_{\mathcal{F}}(E) + \frac{2}{\alpha}\log\Lambda + 8\right) \\ &< 1984\left(\mathrm{h}_{\mathcal{F}}(E) + \frac{2}{\alpha}\log\Lambda + 8\right). \end{aligned} \tag{4.2.7}$$

Since $\Lambda^{1-\log_{19}2} - \frac{2}{\alpha}\cdot 1984\log\Lambda > 0.225\,\Lambda^{1-\log_{19}2}$ for $\Lambda \geq 2.34\cdot 10^6$, we have

$$\Lambda < \left(\frac{1984}{0.225}\right)^{\frac{1}{1-\log_{19}2}}(\mathrm{h}_{\mathcal{F}}(E)+8)^{\frac{1}{1-\log_{19}2}} < 145000\,(\mathrm{h}_{\mathcal{F}}(E)+8)^{1.308}, \tag{4.2.8}$$

which holds also for $\Lambda < 2.34\cdot 10^6$ (indeed, since $\mathrm{h}_{\mathcal{F}}(E) > 0.45$, we have $145000\,(\mathrm{h}_{\mathcal{F}}(E)+8)^{1.308} \geq 145000\cdot 8.45^{1.308} > 2.34\cdot 10^6$), and hence for all values of Λ. Using inequality (4.2.8) to bound $\log\Lambda$ in (4.2.7), we obtain

$$\Lambda^{1-\log_{19}2} < 1984\left(\mathrm{h}_{\mathcal{F}}(E) + \frac{2.616}{\alpha}\log\left(\mathrm{h}_{\mathcal{F}}(E)+8\right) + 31.5\right). \tag{4.2.9}$$

The function $x + \frac{2.616}{\alpha}\log(x+8) + 31.5$ is smaller than $1.1 \cdot (x+35)$ for every $x > 0.45$, hence we have

$$\begin{aligned}\Lambda &< (1984 \cdot 1.1)^{1.308} \left(\mathrm{h}_{\mathcal{F}}(E) + 35\right)^{1.308} \\ &< 23300 \cdot \left(\mathrm{h}_{\mathcal{F}}(E) + 35\right)^{1.308}. \end{aligned} \tag{4.2.10}$$

Repeating this last step once more, using equation (4.2.10) in equation (4.2.7), we obtain

$$20900 \cdot \left(\mathrm{h}_{\mathcal{F}}(E) + 40\right)^{1.308}, \tag{4.2.11}$$

concluding the proof of the first part of the theorem. We now focus on the second part. We start by assuming again that $|\log|q|| > 30$. Using the bound on Λ given in equation (4.2.11) in equation (4.2.5), we obtain

$$\Lambda < 1266.4 \cdot 2^{\omega(\Lambda)}(\mathrm{h}_{\mathcal{F}}(E) + 2.616\log(\mathrm{h}_{\mathcal{F}}(E)+40) + 1.5\log(\mathrm{h}_{\mathcal{F}}(E)+2.72) + 22.5),$$

where $\omega(\Lambda)$ is the number of distinct prime factors of Λ, and applying the weighted AM-GM inequality we obtain

$$\Lambda < 1266.4 \cdot 2^{\omega(\Lambda)} \left(\mathrm{h}_{\mathcal{F}}(E) + 4.116\log(\mathrm{h}_{\mathcal{F}}(E) + 26.42) + 22.5\right). \tag{4.2.12}$$

As we can assume that $\Lambda \geq 26$, by [Rob83, Théorème 13] we have $\omega(\Lambda) \leq \frac{\log\Lambda}{\log\log\Lambda - 1.1714}$, and by equation (4.2.11) we have

$$\begin{aligned}\omega(\Lambda) &< \frac{1.308\log(\mathrm{h}_{\mathcal{F}}(E)+40) + \log 20900}{\log(1.308\log(\mathrm{h}_{\mathcal{F}}(E)+40) + \log 20900) - 1.1714} \\ &< \frac{1.308\log(\mathrm{h}_{\mathcal{F}}(E)+40) + \log 20900}{\log(\log(\mathrm{h}_{\mathcal{F}}(E)+40) + 7.6) - 0.903}.\end{aligned}$$

Suppose that $\mathrm{h}_{\mathcal{F}}(E) > 1.2 \cdot 10^{15}$. We have the bounds $\delta(\mathrm{h}_{\mathcal{F}}(E)) < 0.352$ and $\frac{4.116\log(\mathrm{h}_{\mathcal{F}}(E)+26.42)}{\mathrm{h}_{\mathcal{F}}(E)} < 10^{-10}$, so replacing in equation (4.2.12) and bounding $1.308 \cdot \log 2 < 0.907$, we obtain

$$\begin{aligned}\Lambda &< 1266.5 \cdot 20900^{\log 2 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E)+40)^{0.907\cdot\delta(\mathrm{h}_{\mathcal{F}}(E))} \left(\mathrm{h}_{\mathcal{F}}(E)+22.5\right) \\ &< 14400 \cdot (\mathrm{h}_{\mathcal{F}}(E)+40)^{0.907\cdot\delta(\mathrm{h}_{\mathcal{F}}(E))} \left(\mathrm{h}_{\mathcal{F}}(E)+22.5\right).\end{aligned}$$

To complete the proof, it suffices to notice that for $\mathrm{h}_{\mathcal{F}}(E) \leq 1.2 \cdot 10^{15}$ we have

$$21000\left(\mathrm{h}_{\mathcal{F}}(E)+40\right)^{1.308} < 14400\left(\mathrm{h}_{\mathcal{F}}(E)+40\right)^{0.907\cdot\delta(\mathrm{h}_{\mathcal{F}}(E))}\left(\mathrm{h}_{\mathcal{F}}(E)+22.5\right),$$

which also holds for $|\log|q|| \leq 30$, since in this case we have $\mathrm{h}_{\mathcal{F}}(E) < 0.6$ (as shown at the start of the proof). □

Remark 4.2.6. If we assume Claim 5.3.1, we can repeat the proof of Theorem 4.2.5 replacing $\log_{19} 2$ with $\log_{101} 2$ and obtain the following better inequalities:

$$\Lambda < 11500\left(\mathrm{h}_{\mathcal{F}}(E)+30\right)^{1.177}$$

and

$$\Lambda < 6200 \cdot (\mathrm{h}_{\mathcal{F}}(E) + 30)^{0.816 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} \left(\mathrm{h}_{\mathcal{F}}(E) + 21.5\right),$$

where

$$\delta(x) := \frac{1}{\log\left(\log(x+30) + 7.94\right) - 1.01}.$$

CHAPTER 5

Integral points on modular curves

In this chapter, we present some techniques to study integral points on modular curves. In particular, we will focus on the case of non-split Cartan modular curves.

Let X be a modular curve defined over $\mathbb{Q}$. As usual, we denote with $X(\mathbb{Q})$ the set of its rational points. We say that a point $P \in X(\mathbb{Q})$ is integral if $j(P) \in \mathbb{Z}$, where $j : X \to X(1)$ is the standard j-map. We denote with $X(\mathbb{Z})$ the set of the integral points of X.

Studying the integral points of the modular curve $X_{ns}^+(N)$ is easier than studying its rational points. In some cases, we are able to determine the set $X_{ns}^+(N)(\mathbb{Z})$ but not the set $X_{ns}^+(N)(\mathbb{Q})$. For modular curves such as $X_{sp}^+(N)$, the problem of studying the rational points can be reduced to that of studying integral points. This is done via the formal immersion argument introduced by Mazur [Maz78] to study the rational points of $X_0(N)$. Unfortunately, this method does not apply to the curves $X_{ns}^+(N)$. However, in the case of the subgroup $G(p) \subseteq C_{ns}^+(p)$ defined in Theorem 6, Le Fourn and Lemos proved that for every prime $p > 37$ we have $X_{G(p)}(\mathbb{Q}) = X_{G(p)}(\mathbb{Z})$ (see Theorem 7).

We will introduce modular units of X, which are elements of the function field of X with zeroes and poles only at the cusps. We can expand these functions in their Fourier series in the parameter $q = e^{\frac{2\pi i \tau}{p}}$. We will use them to give some bounds on $|q(E)|$ when E corresponds to a point in $X(\mathbb{Q})$, which gives in turn a bound on $\log |j(E)|$. This is possible because the modular units of a curve of level p are integral over the ring $\mathbb{Z}\left[\frac{1}{p}, j\right]$, and hence integral over the ring $\mathbb{Z}\left[\frac{1}{p}\right]$ when evaluated in an integral value of j. The bounds are then obtained via two different methods: Baker's bound for linear forms in

logarithms, as presented in [BS14, Sha14], and Runge's method for modular curves. The last one was developed by Bilu and Parent [BP11b] to determine the integral points on the modular curves $X_{sp}^{+}(p)$.

In the first part of the chapter we will focus on the integral points on $X_{ns}^{+}(N)$ for some small values of N. In the second part, we will study the integral points on the modular curve $X_{G(p)}$, where $G(p)$ is the group defined in Theorem 6. To conclude, we show that the curves $X_{G(p)}$ have no non-CM rational points.

5.1 Cusps of modular curves

We follow [LFL21] to deduce from [DR73] a parametrisation of the cusps of modular curves, with our focus on the curves $X_{ns}^{+}(p^n)$.

Lemma 5.1.1. *Given a positive integer N, there is a bijection between the cusps of $X(N)$ and the set $\mathcal{M}_N \times \left(\mathbb{Z}/N\mathbb{Z}\right)^{\times}$, where*

$$\mathcal{M}_N := \left\{(a,b) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \ : \ (N,a,b) = 1\right\}/\pm 1,$$

which is equivariant for the action of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$ (acting by its natural left action on $\mathcal{M}_N$ and by multiplication by the determinant on $\mathbb{Z}/N\mathbb{Z}$). Moreover, if $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ and c is a cusp of $X(N)$ corresponding to the pair $\left(\begin{pmatrix} a \\ b \end{pmatrix}, d\right)$, then $\sigma(c)$ corresponds to

$$\sigma \cdot \left(\begin{pmatrix} a \\ b \end{pmatrix}, d\right) := \left(\chi_N(\sigma)^{-1}\begin{pmatrix} a \\ b \end{pmatrix}, \chi_N(\sigma)^{-1} d\right),$$

where χ_N is the cyclotomic character.

Proof. As in [LFL21, Lemma 2.1], by [DR73, 6, VI.5] we have a canonical Galois and $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$ equivariant bijection between the cusps of $X(N)$ and the set

$$S := \mathrm{Isom}\left(\mu_N \times \mathbb{Z}/N\mathbb{Z}, \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\right)/\pm U \ ,$$

where U is the set of matrices

$$U := \left\{\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \ : \ u \in \mathrm{Hom}\left(\mathbb{Z}/N\mathbb{Z}, \mu_N\right)\right\},$$

and the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ is induced by its natural action on μ_N and the trivial one on $\mathbb{Z}/N\mathbb{Z}$. The action of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$ corresponds to left matrix multiplication.
Given a class $\gamma \in S$ represented by

$$(\zeta_N, 0) \mapsto (a, b), \quad (1, 1) \mapsto (c, d),$$

we associate with it the element

$$\left(\begin{pmatrix} a \\ b \end{pmatrix}, \det \gamma\right) \in \mathcal{M}_N \times \left(\mathbb{Z}/N\mathbb{Z}\right)^\times,$$

where $\det \gamma := ad - bc$. The function is well defined, because since γ is an isomorphism we have $(N, a, b) = 1$, and every other representative of γ yields the same element. Moreover, it is easy to see that this function is equivariant with respect to the actions of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$ and of the Galois group.
We note that this function is surjective, as given $\left(\begin{pmatrix} a \\ b \end{pmatrix}, x\right)$ with $(N, a, b) = 1$, by Bezout's identity there exist c, d such that $ad - bc \equiv x \pmod N$, giving the matrix $\gamma = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in S$. We now prove that it is injective. Given $\gamma, \gamma' \in S$ with the same image in $\mathcal{M}_N \times \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$, we have $\begin{pmatrix} a_\gamma \\ b_\gamma \end{pmatrix} = \begin{pmatrix} a_{\gamma'} \\ b_{\gamma'} \end{pmatrix}$ and $x = a_\gamma d_\gamma - b_\gamma c_\gamma = a_\gamma d_{\gamma'} - b_\gamma c_{\gamma'}$. We can then notice that

$$\gamma^{-1}\gamma' = \frac{1}{x}\begin{pmatrix} d_\gamma & -c_\gamma \\ -b_\gamma & a_\gamma \end{pmatrix}\begin{pmatrix} a_\gamma & c_{\gamma'} \\ b_\gamma & d_{\gamma'} \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

for some $u \in \mathbb{Z}/N\mathbb{Z}$, concluding the proof. □

Corollary 5.1.2. *If H is a subgroup of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$, then there is a bijection between the set of cusps of X_H and the set ${}_H\backslash\mathcal{M}_N \times (\mathbb{Z}/N\mathbb{Z})^\times$. Moreover, if $\det H = \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$, this bijection induces a bijection between the set of cusps of X_H and ${}_{H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})}\backslash\mathcal{M}_N$.*

Proof. The proof is analogous to that of [LFL21, Corollary 2.2]. The first statement immediately follows from Lemma 5.1.1 and the definition of X_H. To prove the second statement, notice that, given a class in ${}_H\backslash\mathcal{M}_N \times (\mathbb{Z}/N\mathbb{Z})^\times$,

there is always a representative of this class of the form $(v,1)$, because $\det H = \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$. Therefore, the map

$$H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \backslash \mathcal{M}_N \longrightarrow H \backslash \mathcal{M}_N \times (\mathbb{Z}/N\mathbb{Z})^\times$$

given by $v \mapsto (v,1)$ is well-defined and bijective. □

Corollary 5.1.3. *Let H be a subgroup of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$ such that $\det H = \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$. Under the identification of Corollary 5.1.2, there is a one-to-one correspondence between the Galois orbits of cusps of X_H and the set $H \backslash \mathcal{M}_N$.*

Proof. The proof is analogous to that of [LFL21, Corollary 2.3]. One can also find it in [BBM21, Remark 2.2]. □

We now examine the case $N = p^n$. We notice that the set $\mathcal{M}_N$ becomes

$$\mathcal{M}_{p^n} = \left\{(a,b) \in \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \ : \ p \nmid (a,b)\right\}/\pm 1 \ .$$

We notice that there is a correspondence between the set $\mathcal{M}_{p^n}$ and the set $C_{ns}(p^n)/\pm 1$. Indeed, consider an integer ε such that $\varepsilon \in \mathbb{Z}_p^\times$ and $x^2 - \varepsilon \in \mathbb{Z}_p[x]$ is an irreducible polynomial. If $\sqrt{\varepsilon}$ is a root of that polynomial, modulo p^n we have

$$C_{ns}(p^n) \cong \left(\mathbb{Z}/p^n\mathbb{Z}[\sqrt{\varepsilon}]\right)^\times = \left\{a + b\sqrt{\varepsilon} \in \mathbb{Z}/p^n\mathbb{Z}[\sqrt{\varepsilon}] \ : \ p \nmid (a,b)\right\}.$$

It is not difficult to see that there is a one-to-one correspondence $\mathcal{M}_{p^n} \to C_{ns}(p^n)/\pm 1$ given by $(a,b) \mapsto a + b\sqrt{\varepsilon}$. Moreover, the action of the group $C_{ns}(p^n) = \left\{ \begin{pmatrix} a & b\varepsilon \\ b & a \end{pmatrix} \in \mathrm{GL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right) \right\}$ on $\mathcal{M}_{p^n}$ by left matrix multiplication is the same as the left multiplication on $C_{ns}(p^n) \cong \left(\mathbb{Z}/p^n\mathbb{Z}[\sqrt{\varepsilon}]\right)^\times$.

Corollary 5.1.4. *The Galois group $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ acts transitively on the cusps of the modular curve $X_{ns}(p^n)$ (and hence also on the cusps of the curve $X_{ns}^+(p^n)$).*

Proof. Since $\det C_{ns}(p^n) = \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$, by Corollary 5.1.3, the Galois orbits correspond to the elements of the set $\frac{C_{ns}(p^n)/\pm 1}{C_{ns}(p^n)} = \{1\}$. □

We now consider the case where $N = p \equiv 2 \pmod 3$ and H is the subgroup $G(p) < C_{ns}^+(p)$ defined in Theorem 6. We show that, unlike the case $H = C_{ns}^+(p)$, the cusps of $X_{G(p)}$ form two distinct Galois orbits. This fact will be crucial in the application of the Runge method in Section 5.4, as it gives the existence of a non-trivial modular unit defined over $\mathbb{Q}$.

We have the following lemma from [LFL21, Lemma 6.3].

Lemma 5.1.5. *The set of cusps of $X_{G(p)}$ consists of two Galois orbits. One of the orbits can be identified via Corollary 5.1.3 with the set ${\mathcal{O}_{\text{cubes}}}/{\pm 1} \subset \mathcal{M}_p$, where*

$$\mathcal{O}_{\text{cubes}} := \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{F}_p^2 \setminus \{0\} \;\middle|\; a + b\sqrt{\varepsilon} \in \mathbb{F}_{p^2}^{\times 3} \right\}.$$

Proof. As we noticed above, the action of $C_{ns}(p)$ on the set $\mathcal{M}_p$ corresponds to the multiplication of elements in ${\mathbb{F}_{p^2}^\times}/{\pm 1}$ by elements in $\mathbb{F}_{p^2}^\times$. Moreover, the action of the element $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ corresponds to the action of the Frobenius automorphism on $\mathbb{F}_{p^2}^\times$. We then see that the action of $G(p)$ corresponds to the multiplication by elements of $(\mathbb{F}_{p^2}^\times)^3$ and the action of the Frobenius automorphism of $\mathbb{F}_{p^2}$. It is not difficult to notice that ${\mathcal{O}_{\text{cubes}}}/{\pm 1}$ is an orbit. Indeed, the product of two cubes is a cube and the Frobenius automorphism of $\mathbb{F}_{p^2}$ preserves the cubes. Given an element $\gamma \in \mathbb{F}_{p^2}^\times \setminus (\mathbb{F}_{p^2}^\times)^3$, we see that $\mathbb{F}_{p^2}^\times = (\mathbb{F}_{p^2}^\times)^3 \sqcup \gamma(\mathbb{F}_{p^2}^\times)^3 \sqcup \gamma^2(\mathbb{F}_{p^2}^\times)^3$, and γ^2 is obtained from γ by applying the Frobenius automorphism. This implies that ${\gamma(\mathbb{F}_{p^2}^\times)^3 \sqcup \gamma^2(\mathbb{F}_{p^2}^\times)^3}/{\pm 1}$ is another orbit for the action of $G(p)$. □

5.2 Modular units

Let τ be an element in the upper half plane $\mathcal{H}$. Define $q^k := e^{2\pi i k\tau}$ and $e(k) := e^{2\pi i k}$ for every $k \in \mathbb{Q}$.

Definition 5.2.1. Let N be a positive integer. For all $(a, b) \in \frac{1}{N}\mathbb{Z}^2 \cap [0, 1)^2$, with a, b not both 0, we define

$$g_{a,b}(\tau) = q^{\frac{B_2(a)}{2}} e(b(a-1)/2) \prod_{n=0}^{\infty} (1 - q^{n+a}e(b))(1 - q^{n+1-a}e(-b)),$$

where $B_2(x) = x^2 - x + \frac{1}{6}$ is the second Bernoulli polynomial.

Consider the set

$$M_N := \left\{ (a, b) \in {\mathbb{Z}}/{N\mathbb{Z}} \times {\mathbb{Z}}/{N\mathbb{Z}} \;:\; (N, a, b) = 1 \right\},$$

where $M_N/\pm 1 = \mathcal{M}_N$ is the parametrising set from the previous section. Consider a group $G < \mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$, and a subset $\mathcal{O} \subset M_N$ stable by the action of G on M_N by left multiplication. We can identify (whenever it is not ambiguous) the elements in the set M_N with elements in $\frac{1}{N}\mathbb{Z}^2 \cap [0,1)^2$. If we consider the modular curve X_G of level N, this can be defined over a number field $K \subseteq \mathbb{Q}(\zeta_N)$.

Theorem 5.2.2. *Suppose $(N,6) = 1$. For every pair (a,b) in M_N consider an integer $m(a,b)$. If $12 \mid \sum_{(a,b)\in M_N} m(a,b)$ and $2 \mid m(a,b)$ for every (a,b), then the function*

$$U = \prod_{(a,b)\in M_N} g_{a,b}^{m(a,b)N}$$

is modular for $\Gamma(N)$. Moreover, U is integral over $\mathbb{Z}[j]$, where j is the standard j-function in $\mathbb{Q}(X(1))$.

Proof. See [KL81, §3 Theorem 5.2] and [BP11b, Proposition 2.2]. □

Given the modular curve $X(N)$, the set of modular units of $X(N)$ modulo constants form a free abelian multiplicative group of rank $C-1$, where C is the number of cusps of $X(N)$. The following lemma (which is a slightly improved version of [BBM21, Lemma 4.8]) gives a dependence relation between the generators $g_{a,b}$.

Lemma 5.2.3. *For every positive integer N, the set M_N has cardinality*

$$N^2 \prod_{\substack{p \text{ prime} \\ p\mid N}} \left(1 - \frac{1}{p^2}\right).$$

Proof. Suppose first that $N = p^n$ is a prime power. In this case, we can write

$$M_{p^n} = \{(a,b) : p \nmid ab\} \cup \{(a,b) : p \mid a,\, p \nmid b\} \cup \{(a,b) : p \nmid a,\, p \mid b\}.$$

Hence we have

$$|M_N| = \varphi(p^n)^2 + 2p^n\varphi(p^n) = p^{2n-2}(p^2-1)$$

as desired. Suppose now that N is the product of prime powers $N = \prod_{p\mid N} p^n$. By the Chinese remainder theorem, we know that $(a,b) \in M_N$ if and only if $(\overline{a},\overline{b}) \in M_{p^n}$ for every $p \mid N$, where $\overline{x}$ represents the projection from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$. Moreover, we have that $|M_N| = \prod_{p\mid N} |M_{p^n}|$, and the conclusion follows. □

Lemma 5.2.4. *For every $N > 2$, $N \neq 4$, set*

$$U = \prod_{(a,b)\in M_N} g_{a,b}.$$

We have $U = \Phi_N(1)$, where $\Phi_N(x)$ is the N-th cyclotomic polynomial.

Proof. By Theorem 5.2.2 we know that every $g_{a,b}^{12N}$ belongs to $\mathbb{Q}(\zeta_N)(X(N))$, so does U^{12N}. Since the set M_N is stable under the action of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$, the function U^{12N} is stable with respect to the Galois action over the field $\mathbb{Q}(X(1))$ (see [BBM21, Proposition 5.4]). In particular, U^{12N} is a unit in the function field $\mathbb{Q}(X(1))$. However, $X(1)$ has only one cusp, and hence there are no non-constant units for $X(1)$. In particular, U^{12N} must be an element of $\mathbb{Q}$, and so $U \in \overline{Q}$. By the expression of the functions $g_{a,b}$, evaluating in $q = 0$, this implies that

$$\begin{aligned} U &= \prod_{(a,b)\in M_N} e(b(a-1)/2) \cdot \prod_{\substack{0<k<N \\ (k,N)=1}} (1 - e^{\frac{2\pi i k}{N}}) \\ &= \prod_{(a,b)\in M_N} e(b(a-1)/2) \cdot \Phi_N(1) = \zeta \cdot \Phi_N(1) \end{aligned}$$

for some root of unity ζ. We now show that $\zeta = 1$. To do that, it suffices to show that

$$\sum_{(a,b)\in M_N} b'(a' - N) \equiv 0 \pmod{2N^2},$$

with $a' = Na$ and $b' = Nb$ (we recall that $a, b \in \frac{1}{N}\mathbb{Z}^2$). Consider now the permutation of M_N given by $(a', b') \mapsto (a', N - b')$: this gives

$$\sum_{(a,b)\in M_N} b'(a' - N) = \sum_{(a,b)\in M_N} (N - b')(a' - N),$$

and so

$$\sum_{(a,b)\in M_N} 2b'(a' - N) = \sum_{(a,b)\in M_N} N(a' - N).$$

Similarly we have

$$\sum_{(a,b)\in M_N} a' = \sum_{(a,b)\in M_N} N - a' \qquad \Longrightarrow \qquad \sum_{(a,b)\in M_N} 2a' = |M_N| \cdot N,$$

and so

$$\sum_{(a,b)\in M_N} b'(a' - N) = \frac{N}{2} \sum_{(a,b)\in M_N} (a' - N) = -\frac{N^2 \cdot |M_N|}{4}.$$

To conclude it suffices to notice that either 8 divides N, and so $|M_N| \equiv 0 \pmod 8$, or there exists an odd prime p such that $p \mid N$, and so $|M_N| \equiv 0 \pmod{p^2-1}$ and $8 \mid p^2-1$. □

Corollary 5.2.5. *Suppose $(N,6)=1$. Let $G < \mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$ and X_G the corresponding modular curve defined over the number field K. If $\mathcal{O} \subseteq M_N$ is stable under the action of G and $m \in \mathbb{Z}$ is such that $12 \mid m|\mathcal{O}|$ and $2 \mid m$, then*

$$U = \prod_{(a,b)\in\mathcal{O}} g_{a,b}^{mN}$$

belongs to $K(X_G)$. Moreover, U and $\frac{A^{mN}}{U}$ are integral over $\mathbb{Z}[j]$, where $A = p$ if $N = p^n$ is a prime power and $A = 1$ otherwise.

Proof. The function U is defined over K by Theorem 5.2.2 and by [BBM21, Proposition 5.4]. The fact that U is integral over $\mathbb{Z}[j]$ follows from Theorem 5.2.2, while the integrality of $\frac{A^{mN}}{U}$ is obtained applying Theorem 5.2.2 to the product $\prod_{(a,b)\notin\mathcal{O}} g_{a,b}^{mN} = \frac{A^{mN}}{U}$. □

When the level N is a prime p, one can prove the following better statement.

Theorem 5.2.6. *Suppose $p \geq 5$ is a prime. Let $G < \mathrm{GL}_2(\mathbb{F}_p)$ be a subgroup containing $-I$ such that $p \nmid |G|$, and let X_G be the corresponding modular curve defined over the number field K. Let $\mathcal{O} \subseteq M_p$ be a G-invariant subset such that the relations*

$$\sum_{(a,b)\in\mathcal{O}} a^2 \equiv \sum_{(a,b)\in\mathcal{O}} b^2 \equiv \sum_{(a,b)\in\mathcal{O}} ab \equiv 0 \pmod p, \tag{5.2.1}$$

$2 \mid m$ and $12 \mid m|\mathcal{O}|$ are satisfied. There exists $k \in \mathbb{Z}$ such that the function

$$U = \zeta_p^k \prod_{(a,b)\in\mathcal{O}} g_{a,b}^{m}$$

belongs to $K(X_G)$. Moreover, U and $\frac{p^m}{U}$ are integral over $\mathbb{Z}[j]$.

Proof. By [BBM21, Theorem 5.5] we know that U belongs to $K(X_G)$. The integrality of U and $\frac{p^m}{U}$ follows from Theorem 5.2.2 and Lemma 5.2.4. □

If we consider the modular curve $X(N)$, the function field $\mathbb{Q}(\zeta_N)(X(N))$ is a Galois extension of $\mathbb{Q}(X(1))$, with Galois group $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$. The functions $g_{a,b}^{12N}$ are generators of a finite index subgroup of the units of $\mathbb{Q}(\zeta_N)(X(N))$. The Galois group of $\mathbb{Q}(\zeta_N)(X(N))$ over $\mathbb{Q}(X(1))$ acts on the modular units of the curve $X(N)$, and the action is described (up to raising units to a suitable power) by the relations $(g_{a,b}^{12N})^\sigma = g_{(a,b)\sigma}^{12N}$ for every $\sigma \in \mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$

(see [BBM21, Proposition 5.4] for a general description). If G is a subgroup of $\mathrm{GL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)$, we can describe the conjugates of a modular unit $U \in \mathbb{Q}(\zeta_N)(X_G)$ in the field $\mathbb{Q}(\zeta_N)(X(N))$ in the same way.

We now study the modular units for the groups $C_{ns}^+(p^n)$ and $G(p) < C_{ns}^+(p)$. We start by giving the following result presented in [LFL21, Proposition 6.4].

Theorem 5.2.7 (Le Fourn, Lemos)**.** *Let $\mathcal{O}_{\text{cubes}}$ be as in Lemma 5.1.5 and define the function*

$$U(\tau) = \zeta \prod_{(a,b)\in\mathcal{O}_{\text{cubes}}} g_{a,b}^6,$$

where ζ is a root of unity such that the coefficient of the lowest power of q in U is 1. We have the following:

- *$U \in \mathbb{Q}(X_{G(p)})$.*
- *The zeroes of U are the cusps at infinity (that is, the Galois orbit of the cusp ∞ corresponding to $\mathcal{O}_{cubes}/\pm 1$ via Lemma 5.1.5), while its poles are the other cusps.*
- *Both U and $\frac{p^6}{U}$ are integral over $\mathbb{Z}[j]$.*

Proof. It immediately follows from Theorem 5.2.6 with $m = 6$, noting that $\mathcal{O}_{\text{cubes}}$ satisfies the relations 5.2.1, that $12 \mid 6|\mathcal{O}_{\text{cubes}}|$ and $2 \mid 6$. □

Remark 5.2.8. Le Fourn and Lemos in [LFL21, Proposition 6.4] choose $m = 3$. However, it seems that this choice of m shows that U is defined over $\mathbb{Q}(\zeta_p)(X_{G(p)})$, but does not ensure that there exists a root of unity ζ such that $\zeta \cdot U$ is defined over $\mathbb{Q}(X_{G(p)})$. In any case, they use this result to obtain an inequality which is homogeneous in m, and hence also $m = 12p$ would give the same results.

5.3 Small levels

The aim of this section is to study the integral points on some modular curves associated with normalisers of non-split Cartan subgroups. While the curves $X_{ns}^+(N)$ contain infinitely many integral points for $N = 1, 3, 4, 5$, many authors described the set of integral points on $X_{ns}^+(N)$ for small values of $N > 5$. For example, Kenku [Ken85] determined the integral points of $X_{ns}^+(7)$, Chen [Che99] proved that the integral points of $X_{ns}^+(15)$ are all CM, Schoof [ST12] dealt with the case $N = 11$ and Baran [Bar09, Bar10] with the cases $N = 9, 16, 20, 21$. Recently, Bajolet, Bilu and Matschke [BBM21] stated the following.

Claim 5.3.1. *Let $7 < p < 100$ be a prime and let $P \in X_{ns}^+(p)(\mathbb{Q})$. If $j(P) \in \mathbb{Z}$, then P is a CM point.*

Unfortunately, there seems to be a mistake in the article where they prove this statement, so it might not be true. However, there is evidence that it is very probably true. A detailed explanation of the mistake can be found in Remark 5.3.10.

Theorem 5.3.2. *Let N be a 100-smooth odd positive integer, i.e. an odd positive integer such that for every prime p dividing N we have $p \leq 100$. Suppose that Claim 5.3.1 is true. If $P \in X_{ns}^+(N)(\mathbb{Q})$ is such that $j(P) \in \mathbb{Z}$ and P is not CM, then either $N \in \{1, 3, 5\}$, or*

$$j(P) \in \{2^3 \cdot 5^3 \cdot 7^5, \quad 2^{15} \cdot 7^5, \quad 3^3 \cdot 41^3 \cdot 61^3 \cdot 149^3, \quad 2^9 \cdot 17^6 \cdot 19^3 \cdot 29^3 \cdot 149^3, \\ 2^6 \cdot 11^3 \cdot 23^3 \cdot 149^3 \cdot 269^3\}$$

We will prove this theorem in multiple steps.

Lemma 5.3.3. *Consider the modular curves $X_{ns}^+(7)$, $X_{ns}^+(9)$ and $X_{ns}^+(3) \times_{X(1)} X_{ns}^+(5)$.*

1. *If $P \in (X_{ns}^+(3) \times_{X(1)} X_{ns}^+(5))(\mathbb{Q})$ is such that $j(P) \in \mathbb{Z}$, then P is a CM point.*

2. *If $P \in X_{ns}^+(7)(\mathbb{Q})$ is such that $j(P) \in \mathbb{Z}$, then either P is a CM point or*

$$j(P) \in \{2^3 \cdot 5^3 \cdot 7^5, \quad 2^{15} \cdot 7^5, \quad 2^9 \cdot 17^6 \cdot 19^3 \cdot 29^3 \cdot 149^3, \\ 2^6 \cdot 11^3 \cdot 23^3 \cdot 149^3 \cdot 269^3\} \tag{5.3.1}$$

   and for the corresponding elliptic curves E_P we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_{E_P}] \in \{84, 504\}$.

3. *If $P \in X_{ns}^+(9)(\mathbb{Q})$ is such that $j(P) \in \mathbb{Z}$, then either P is a CM point or $j(P) = 3^3 \cdot 41^3 \cdot 61^3 \cdot 149^3$ and for the corresponding elliptic curve E_P we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_{E_P}] = 108$.*

Proof. The proof of part 1 can be found in [Che99, Corollary 6.5]. If $P \in X_{ns}^+(7)(\mathbb{Q})$ and $j(P) \in \mathbb{Z}$, by [Ken85] we know that either P is a CM point or $j(P)$ belongs to the list (5.3.1). Actually, Kenku's list in [Ken85] contains some typos: in the j-invariants column one finds $2^2 \cdot 5^3 \cdot 7^5$ and $7^5 \cdot 2^5$ instead of $2^3 \cdot 5^3 \cdot 7^5$ and $2^{15} \cdot 7^5$. The correct j-invariants are computed, for example, after equation (4.37) in [Elk99, p. 93]. By using the algorithm `FindOpenImage` developed by Zywina in [Zyw22] we can compute the index of the image of the adelic representations attached to elliptic curves with j-invariant in the list (5.3.1). Indeed, the index of $\operatorname{Im} \rho_E$ only depends on $j(E)$, as shown in

[Zyw15b, Corollary 2.3]. The first two j-invariants of the list give rise to elliptic curves with $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] = 84$, while for the last two j-invariants we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] = 504$. For the level 9 case, we know by [Bar09, Table 5.2] that P is either a CM point or $j(P) = 3^3 \cdot 41^3 \cdot 61^3 \cdot 149^3$. We can then compute the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_{E_P}]$ by using again the algorithm `FindOpenImage`. □

We now want to compute the integral points on the modular curve $X_{ns}^+(25)$. Before doing this, we need to define some modular units for the curve $X_{ns}^+(25)$ over a suitable number field. We follow the work of Bajolet, Bilu and Matschke [BBM21], generalising it to the case of non-split Cartan modular curves of prime power level.

Let N be an odd prime power, say $N = p^n$. Consider the normaliser of the non-split Cartan subgroup $C_{ns}^+(p^n) < \mathrm{GL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$. We know that $\det(C_{ns}^+(p^n)) = \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$. The group $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ is cyclic of order $\varphi(p^n)$. Let d be a divisor of $\frac{\varphi(p^n)}{2}$ and consider the unique subgroup H of $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ of index d. We define $G_H < C_{ns}^+(p^n)$ as $\det^{-1}(H)$. Clearly we have $[C_{ns}^+(p^n) : G_H] = d$.

The modular curves X_{G_H} and $X_{ns}^+(p^n)$ have the same geometrically integral model, however they are defined over different number fields. Let $K \subseteq \mathbb{Q}(\zeta_{p^n})^+$ be the unique subfield such that $[K : \mathbb{Q}] = d$. We have that X_{G_H} is defined over K and if we consider the function fields of X_{G_H} and $X_{ns}^+(p^n)$ we have

$$\mathrm{Gal}\left(K(X_{G_H})/\mathbb{Q}(X_{ns}^+(p^n))\right) \cong \mathrm{Gal}\left(K/\mathbb{Q}\right) \cong \mathbb{Z}/p^n\mathbb{Z}/H \cong C_{ns}^+(p^n)/G_H.$$

The curve X_{G_H} has the same cusps as the curve $X_{ns}^+(p^n)$, which are $\frac{\varphi(p^n)}{2}$ cusps defined over the field $\mathbb{Q}(\zeta_{p^n})^+$. However, while $X_{ns}^+(p^n)$ has a single Galois orbit of cusps (over $\mathbb{Q}$), the curve X_{G_H} has d different Galois orbits over the field K.

Fix a generator ε of $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$. We can assume that, up to conjugation, $C_{ns}^+(p^n) = \left\{ \begin{pmatrix} a & b \\ \varepsilon b & a \end{pmatrix} \right\}$. Consider the set

$$\mathcal{O} := \left\{ (a,b) \in M_{p^n} \;\middle|\; \begin{pmatrix} a & b \\ \varepsilon b & a \end{pmatrix} \in G_H \right\} = \left\{ (a,b) \in M_{p^n} \mid a^2 - \varepsilon b^2 \in H \right\}.$$

This has cardinality $\frac{p^{2n-2}(p^2-1)}{d}$ and is invariant under multiplication by G_H. By Corollary 5.2.5, if we have $m \in \{2,6\}$ such that $12 \mid m \cdot \frac{\varphi(p^n)}{d}$, then the

function

$$U := \prod_{(a,b)\in\mathcal{O}} g_{a,b}^{mp^n} \tag{5.3.2}$$

is an element of $K(X_G)$. Moreover, both U and $\frac{p^{mp^n}}{U}$ are integral over $\mathbb{Z}[j]$. We remark that by [BBM21, Proposition 5.4] the conjugates of U in the extension $K(X_{G_H})/\mathbb{Q}(j)$ are given by

$${}^{\sigma}U = \prod_{(a,b)\in\mathcal{O}} g_{(a,b)\sigma}^{mp^n} = \prod_{(a,b)\in\mathcal{O}\sigma} g_{a,b}^{mp^n}$$

for $\sigma \in G_H \cong \mathrm{Gal}\left(K(X_{G_H})/\mathbb{Q}(j)\right)$.

We recall that a point $P \in X_G(\mathbb{Q})$ is said to be integral if $j(P) \in \mathbb{Z}$. If we have an integral point P on X_G, we can evaluate U in P and obtain that $U(P) \in K$ is integral over $\mathbb{Z}$, hence $U(P) \in \mathcal{O}_K$. If we define $\eta_0 := N_{\mathbb{Q}(\zeta_{p^n})/K}(1-\zeta_{p^n})$, we know that there is a single ideal $\mathfrak{p} \subset \mathcal{O}_K$ dividing p, of norm p, which is generated by η_0. As also $\frac{p^{mp^n}}{U(P)}$ is integral over $\mathbb{Z}$, it follows that $U(P) \in \mathfrak{p} = (\eta_0)$. If we call $\eta_1, \dots, \eta_{d-1} \in \mathcal{O}_K$ a choice of generators of the free part of the group of units of $\mathcal{O}_K$ (we recall that K is contained in the totally real field $\mathbb{Q}(\zeta_{p^n})^+$), we have

$$U(P) = \pm\eta_0^{b_0} \cdot \eta_1^{b_1} \cdot \ldots \cdot \eta_{d-1}^{b_{d-1}}$$

for some $b_0, \dots, b_{d-1} \in \mathbb{Z}$ with $b_0 \geq 0$. Given $\phi \in \mathrm{Gal}\left(K(X_{G_H})/\mathbb{Q}(j)\right)$ we can consider the restriction of ϕ to K. As noticed in [BBM21, Propositions 6.4 and 6.5] we have $({}^{\phi}U)(P) = \phi(U(P))$, hence we can write

$${}^{\phi}U(P) = \pm\phi(\eta_0)^{b_0} \cdot \phi(\eta_1)^{b_1} \cdot \ldots \cdot \phi(\eta_{d-1})^{b_{d-1}}.$$

If we choose an order on the elements of $\mathrm{Gal}\left(K/\mathbb{Q}\right) = \{\phi_0, \dots, \phi_{d-1}\}$, we can define the $d \times d$ real matrix $\mathfrak{H} = (\log|\phi_k(\eta_i)|)_{0\leq k,i\leq d-1}$. This is non-singular, since $\eta_0, \eta_1, \dots, \eta_{d-1}$ are multiplicatively independent. Indeed, if the kernel of the matrix contains a line, there exist a d-tuple $r = (r_0, \dots, r_{d-1})$ of integers arbitrarily close to the line such that the $\mathfrak{H}r$ has arbitrarily small values. However, $\mathfrak{H}r$ represents (up to sign) an element in $\mathcal{O}_K \setminus \{0, 1\}$ and its conjugates, which cannot be all too close to 1 at the same time, giving a contradiction. Let $\mathfrak{A} = (\alpha_{k,i})_{0\leq k,i\leq d-1}$ be the inverse matrix of $\mathfrak{H}$. We have

$$b_k = \sum_{i=0}^{d-1} \alpha_{k,i} \log|{}^{\phi_i}U(P)|$$

for every $0 \leq k \leq d-1$.

Remark 5.3.4. By Lemma 5.2.4 we know that $\prod_{i=0}^{d-1}\phi_i(U(P)) = p^{mp^n}$, and so it is easy to notice that $b_0 = mp^n$.

Definition 5.3.5. Let $(a,b) \in M_N$. We define

$$\ell_{a,b} := \mathrm{Ord}_q(g_{a,b}) = B_2(a)/2 \quad \text{and} \quad \rho_{a,b} := \begin{cases} -e^{\pi i b(a-1)} & \text{if } a \neq 0 \\ -e^{\pi i b(a-1)}(1-e^{2\pi i b}) & \text{if } a = 0. \end{cases}$$

Given a subset $\mathcal{O} \subseteq M_N$ we define

$$\ell_{\mathcal{O}} := \sum_{(a,b)\in\mathcal{O}} \ell_{a,b} \qquad \text{and} \qquad \prod_{(a,b)\in\mathcal{O}} \rho_{a,b}.$$

The fundamental domain in the upper half plane $\mathcal{H}$ corresponding to the modular curve X_G is the union of fundamental domains of the curve $X(1)$, and every cusp of X_G represents the point at infinity of one of these domains. As P is a point on X_G, there exists a fundamental domain in which P is lying, and in particular, there exists a cusp c which is closer to P than all the other cusps (the cusp in the projective closure of the fundamental domain). There exists $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma(P)$ lies in the standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, and so such that $\sigma(c) = \infty$. We define the parameter $q_c = e^{2\pi i \sigma\tau}$, which is the q-expansion in the cusp c, i.e. such that $q_c(c) = 0$. With this choice of q we can write

$$\log|U(P)| = mp^n \ell_{\mathcal{O}\sigma} \log|q_c(P)| + mp^n \log|\rho_{\mathcal{O}\sigma}| + O_1(mp^{2n}|\mathcal{O}||q_c(P)|^{\frac{1}{p^n}}),$$

where $f(x) = O_1(x)$ means that $|f(x)| \leq x$, and hence

$$\log|U(P)| \leq mp^n \ell_{\mathcal{O}\sigma} \log|q_c(P)| + mp^n \log|\rho_{\mathcal{O}\sigma}| + mp^{2n}|\mathcal{O}|. \tag{5.3.3}$$

Indeed, this follows from the definition of U together with [BBM21, Corollary 4.6].

Notation 5.3.6. *Let c be a cusp of X_G and let $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\sigma(c) = \infty$ as above. For every $k = 0, \ldots, d-1$ consider the following quantities:*

$$\delta_{c,k} = -mp^n \sum_{i=0}^{d-1} \alpha_{k,i} \ell_{\mathcal{O}\phi_i\sigma}, \qquad \theta_{c,k} = mp^n \sum_{i=0}^{d-1} \alpha_{k,i} \log|\rho_{\mathcal{O}\phi_i\sigma}|,$$

$$\Theta = \frac{mp^{4n-2}(p^2-1)}{d} \max_k \sum_{i=0}^{d-1} |\alpha_{k,i}|.$$

As noticed in [BBM21, Remark 7.1], by the definitions above we have $\delta_{c,0} = 0$ for every cusp c, and at least one $\delta_{c,i}$ is non-zero (indeed, U is non-constant, as it is a non trivial product of multiplicatively independent functions).

Similarly to [BBM21, Section 6.1] we can notice that the curve X_G has $\frac{\varphi(p^n)}{2}$ cusps defined over $\mathbb{Q}(\zeta_{p^n})^+$, and that a good set of representatives in $\mathbb{P}^1(\mathbb{Q})$ for the cusps is $\left\{\widetilde{\sigma}_c(\infty) \mid c \in {(\mathbb{Z}/p^n\mathbb{Z})^\times}/{\pm 1}\right\}$, where $\widetilde{\sigma}_c$ is a lift to $\mathrm{SL}_2(\mathbb{Z})$ of the matrix $\sigma_c = \begin{pmatrix} a & cb \\ \varepsilon b & ca \end{pmatrix} \in \mathrm{SL}_2\left({\mathbb{Z}}/{p^n\mathbb{Z}}\right)$, for some a, b such that $a^2 - \varepsilon b^2 = c^{-1}$. Here, each $c \in {(\mathbb{Z}/p^n\mathbb{Z})^\times}/{\pm 1}$ corresponds to a different cusp.

Proposition 5.3.7. *If d is odd, we have that $\theta_{c,k} \in mp^n\mathbb{Z}$ for every c, k and $\theta_{c,0} = mp^n$. Moreover, up to changing the choice of η_0 by one of its conjugates, we can assume that $\theta_{c,1} = \ldots = \theta_{c,d-1} = 0$. If instead d is even, for every cusp c we have that $(\theta_{c,0}, \ldots, \theta_{c,d-1}) \notin \mathbb{Q}^d$.*

Proof. Since $\mathcal{O}$ is invariant under the action of G_H, there is an action of ${C_{ns}^+(p^n)}/{G_H} \cong {\mathbb{Z}/p^n\mathbb{Z}}/{H} \cong \mathrm{Gal}\left({K}/{\mathbb{Q}}\right)$ on the set $\{\mathcal{O}, \mathcal{O}\phi_1, \ldots, \mathcal{O}\phi_{d-1}\}$ of the cosets of $\mathcal{O}$ in M_{p^n}. Here, the automorphisms $id = \phi_0, \phi_1, \ldots, \phi_{d-1}$ can be taken to be representatives of ${C_{ns}^+(p^n)}/{G_H}$ such that $\phi_i \in C_{ns}(p^n)$ and $\det \phi_i = \varepsilon^i$. If we call $G'_H = G_H \cap C_{ns}(p^n)$, we can write

$$\mathcal{O} := \left\{ (a,b) \in M_{p^n} \;\middle|\; \begin{pmatrix} a & b \\ \varepsilon b & a \end{pmatrix} \in G_H \right\} = (1,0) \cdot G'_H,$$

and so $\mathcal{O}\phi_i = (1,0) \cdot G'_H\phi_i = \{(a,b) \in M_{p^n} \mid a^2 - \varepsilon b^2 \in \varepsilon^i H\}$. If we identify the cusp c with $c \in {\mathbb{Z}/p^n\mathbb{Z}}/{\pm 1}$, by the parametrisation above, we have $\sigma_c = \begin{pmatrix} a_c & b_c \\ \varepsilon b_c & a_c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$ for some a_c, b_c such that $a_c^2 - \varepsilon b_c^2 = c^{-1}$. As the group $C_{ns}(p^n)$ is abelian we have

$$\begin{aligned} \mathcal{O}\phi_i\sigma_c &= (1,0) \cdot G'_H\phi_i \begin{pmatrix} a_c & b_c \\ \varepsilon b_c & a_c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \\ &= \left\{(a, cb) \in M_{p^n} \mid a^2 - \varepsilon b^2 \in \varepsilon^i c^{-1} H\right\} \qquad (5.3.4) \\ &= \left\{(c^{-1}a, b) \in M_{p^n} \mid a^2 - \varepsilon b^2 \in \varepsilon^i c H\right\}. \qquad (5.3.5) \end{aligned}$$

We now want to compute the absolute value of the constants $\rho_{\mathcal{O}\phi_i\sigma_c}$. As the absolute value does not change under multiplication by roots of unity, by Definition 5.3.5 we see that

$$|\rho_{\mathcal{O}\phi_i\sigma_c}| = \prod_{(0,b) \in \mathcal{O}\phi_i\sigma_c} |1 - \zeta_{p^n}^b| = \prod_{\substack{b \in \mathbb{Z}/p^n\mathbb{Z} \\ -\varepsilon b^2 \in \varepsilon^i cH}} |1 - \zeta_{p^n}^b| = \prod_{b^2 \in -\varepsilon^{i-1}cH} |1 - \zeta_{p^n}^b|.$$

By definition of H, we know that $-1 \in H$, because $d \mid \frac{\varphi(p^n)}{2}$ (or equivalently H has even order), and so $-\varepsilon^{i-1}cH = \varepsilon^{i-1}cH$. We now treat separately the case when d is odd and the case when d is even.

- **d is odd**. In this case, either $\varepsilon^{i-1}c$ is a square or not. If it is a square, then

$$\{b \mid b^2 \in \varepsilon^{i-1}cH\} = \sqrt{\varepsilon^{i-1}c} \cdot \{b \mid b^2 \in H\} = \sqrt{\varepsilon^{i-1}c}H.$$

If instead $\varepsilon^{i-1}c$ is not a square, consider $h \in H$ a generator of H. Then h is not a square and we can write $\varepsilon^{i-1}cH = \varepsilon^{i-1}chH$. Repeating the same argument we obtain $\{b \mid b^2 \in \varepsilon^{i-1}cH\} = \sqrt{\varepsilon^{i-1}ch}H$. Define $\gamma := \sqrt{c}$ if c is a square and $\gamma := \sqrt{ch}$ if c is not a square. We notice that

$$\{b \mid b^2 \in \varepsilon^{i-1}cH\} = (\sqrt{\varepsilon h})^{i-1}\gamma H,$$

and in particular, that the set $\{(0,b) \in \mathcal{O}\sigma_c\}$ is equal to the coset $\frac{\gamma}{\sqrt{\varepsilon h}}H$ and that applying ϕ_i corresponds to multiplication by $(\varepsilon h)^{\frac{i}{2}}$. If we consider $i = 0$, there are integers $t_1, \ldots, t_{d-1}$ and an automorphism $\phi \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$ such that

$$|\rho_{\mathcal{O}\sigma_c}| = \prod_{b \in \frac{\gamma}{\sqrt{\varepsilon h}}H} |1-\zeta_{p^n}^{b}| = \prod_{b \in H} |1-\zeta_{p^n}^{\sqrt{\varepsilon h}\gamma^{-1}b}| = |\phi(\eta_0)| = |\eta_0 \cdot \eta_1^{t_1} \cdot \ldots \cdot \eta_{d-1}^{t_{d-1}}|,$$

and for every $i = 0, \ldots, d-1$ we have

$$\begin{aligned} |\rho_{\mathcal{O}\phi_i\sigma_c}| &= \prod_{b \in (\varepsilon h)^{\frac{i-1}{2}}\gamma H} |1 - \zeta_{p^n}^{b}| = \prod_{b \in H} |1 - \zeta_{p^n}^{(\varepsilon h)^{\frac{1-i}{2}}\gamma^{-1}b}| \\ &= |\phi_i\phi(\eta_0)| = |\phi_i(\eta_0) \cdot \phi_i(\eta_1)^{t_1} \cdot \ldots \cdot \phi_i(\eta_{d-1})^{t_{d-1}}|. \end{aligned}$$

Notice that up to changing the choice of η_0 by a conjugate, we can assume that $\phi = id$, and so $t_1 = \ldots = t_{d-1} = 0$. We can rewrite these relations as

$$\mathfrak{H} \begin{pmatrix} 1 \\ t_1 \\ \vdots \\ t_{d-1} \end{pmatrix} = \begin{pmatrix} \log|\rho_{\mathcal{O}\sigma_c}| \\ \log|\rho_{\mathcal{O}\phi_1\sigma_c}| \\ \vdots \\ \log|\rho_{\mathcal{O}\phi_{d-1}\sigma_c}| \end{pmatrix},$$

and so

$$\begin{pmatrix} 1 \\ t_1 \\ \vdots \\ t_{d-1} \end{pmatrix} = \mathfrak{A} \begin{pmatrix} \log|\rho_{\mathcal{O}\sigma_c}| \\ \log|\rho_{\mathcal{O}\phi_1\sigma_c}| \\ \vdots \\ \log|\rho_{\mathcal{O}\phi_{d-1}\sigma_c}| \end{pmatrix} = \frac{1}{mp^n} \begin{pmatrix} \theta_{c,0} \\ \theta_{c,1} \\ \vdots \\ \theta_{c,d-1} \end{pmatrix}.$$

- **d is even**. In this case, every element of H is a square. If $\varepsilon^{i-1}c$ is not a square we have $\{b \mid b^2 \in \varepsilon^{i-1}cH\} = \emptyset$, and so $|\rho_{\mathcal{O}\phi_i\sigma_c}| = 1$. Suppose

that $\theta_{c,0}, \dots, \theta_{c,d-1}$ are all rationals: up to raise to a power r, we can assume they are integers. We notice that they are not all zero: indeed, in that case we would have $\rho_{\mathcal{O}\phi_i\sigma_c} = 1$ for every i, but this is impossible as $\prod_{i=0}^{d-1} \rho_{\mathcal{O}\phi_i\sigma_c} = \prod_{(a,b)\in M_{p^n}} \rho_{a,b} = p$. Then, given i such that $\varepsilon^{i-1}c$ is not a square, we have

$$1 = |\rho_{\mathcal{O}\phi_i\sigma_c}|^{rmp^n} = |\phi_i(\eta_0)^{\theta_{c,0}}\phi_i(\eta_1)^{\theta_{c,1}} \dots \phi_i(\eta_{d-1})^{\theta_{c,d-1}}|.$$

The number $\phi_i(\eta_0)^{\theta_{c,0}}\phi_i(\eta_1)^{\theta_{c,1}} \dots \phi_i(\eta_{d-1})^{\theta_{c,d-1}}$ is real, and hence it must be ± 1. However, this is impossible since $\phi_i(\eta_0), \dots, \phi_i(\eta_{d-1})$ are multiplicatively independent. □

Lemma 5.3.8. *Let P be an integral point on X_G, c its nearest cusp and $q_c := q_c(P)$. For $k = 0, \dots d-1$ we have*

$$b_k = \delta_{c,k} \log |q_c|^{-1} + \theta_{c,k} + O_1\left(\Theta |q_c|^{\frac{1}{p^n}}\right).$$

Proof. The proof is analogous to that of [BBM21, Proposition 7.2]. It follows from equation (5.3.3) noting that the same relation holds when we substitute U with ${}^{\phi}U$ and $\mathcal{O}$ with $\mathcal{O}\phi$. □

Proposition 5.3.9. *If $P \in X_{ns}^{+}(25)(\mathbb{Q})$ is such that $j(P) \in \mathbb{Z}$, then P is a CM point.*

Proof. By [Sha14] and [Cai22] we obtain the bound $\log |j(P)|, |\log |q_c(P)|| \leq 10^{1000}$. We now follow [BBM21, Section 9] to reduce the bound via the Baker–Davenport method. Take $H \subseteq \left(\mathbb{Z}/25\mathbb{Z}\right)^{\times}$ as previously such that $d = [C_{ns}^{+}(25) : G_H] = 5$ and $K \subset \mathbb{Q}(\zeta_{25})$ the unique subfield such that $d = [K : \mathbb{Q}] = 5$: in this case it suffices to take $m = 2$ to define a modular unit U as above, indeed $|\mathcal{O}| = \frac{2 \cdot 25 \cdot 24}{5} = 240$ is divisible by 12. By Proposition 5.3.7 for every cusp c we can change the definition of η_0 so that $|\theta_0| = |\rho_{\mathcal{O}\sigma_c}|$, and this implies that $\theta_{c,1}, \dots, \theta_{c,d-1} = 0$. Set $\Omega_0 = 10^{1000}$ and initialise $\Omega = \Omega_0$. By Lemma 5.3.8 we have $b_k \leq B_k := |\delta_{c,k}|\Omega + \Theta$ for every $k = 1, \dots, d-1$. For every i, j such that $\delta_{c,i}, \delta_{c,j} \neq 0$, by Lemma 5.3.8 we can write

$$\delta_{c,j} b_i - \delta_{c,i} b_j = O_1\left(\Theta(|\delta_{c,i}| + |\delta_{c,j}|)|q_c|^{\frac{1}{25}}\right),$$

and in particular setting $\delta := \frac{\delta_{c,i}}{\delta_{c,j}}$ we have

$$b_i - \delta b_j = O_1\left(\Theta(1 + |\delta|)|q_c|^{\frac{1}{25}}\right).$$

We remark that after this step there is a mistake in [BBM21], as the authors assume that $\theta_{c,i}, \theta_{c,j}$ are not integers, but this is false every time that d is odd,

as shown in Proposition 5.3.7. We discuss this in detail in Remark 5.3.10. If $b_j = 0$, then we have $|\delta_{c,j} \log |q_c|| \leq \Theta |q_c|^{\frac{1}{25}}$. Taking the logarithm we obtain

$$\frac{1}{25} |\log |q_c|| \leq \log |\log |q_c|| + \frac{1}{25} |\log |q_c|| \leq \log \left| \frac{\Theta}{\delta_{c,j}} \right|. \tag{5.3.6}$$

We can then suppose that $b_j \neq 0$, and therefore we can write

$$\left| \frac{b_i}{b_j} - \delta \right| = \frac{\Theta(1 + |\delta|)|q_c|^{\frac{1}{25}}}{|b_j|} \leq \Theta(1 + |\delta|)|q_c|^{\frac{1}{25}}.$$

We can then compute the best rational approximation r of δ with denominator bounded by B_j and notice that $\left| \frac{b_i}{b_j} - \delta \right| \geq |r - \delta|$. We eventually obtain

$$|\log |q_c|| \leq 25 \log \left(\frac{\Theta(1 + |\delta|)}{|r - \delta|} \right), \tag{5.3.7}$$

which is usually a much better bound than Ω. Indeed, the expected value of $|r - \delta|$ is around B_j^{-2}, which has the size of Ω. We now proceed by substituting Ω with the maximum among $25 \log \left| \frac{\Theta}{\delta_{c,j}} \right|$ and $25 \log \left(\frac{\Theta(1+|\delta|)}{|r-\delta|} \right)$, and iterating the process while Ω keeps decreasing. This allows us to obtain the bound $|\log |q_c|| \leq 1063$.

We now test all possible j-invariants with absolute value smaller than e^{1100}. Our method is much more efficient than that of [BBM21] and only takes a few seconds. However, it is ad hoc for the modular curve $X_{ns}^+(25)$. Consider the map $X_{ns}^+(25) \to X_{ns}^+(5)$. An integral point on $X_{ns}^+(25)$ must give an integral point on the curve $X_{ns}^+(5)$. The modular curve $X_{ns}^+(5)$ has genus 0 and is isomorphic to $\mathbb{P}^1$, and the j-map $X_{ns}^+(5) \to X(1)$ is given by

$$j_5(t) = \frac{5^3(t+1)(2t+1)^3(2t^2 - 3t + 3)^3}{(t^2 + t - 1)^5} \tag{5.3.8}$$

(see for example [Zyw15a, Theorem 1.4]). This implies that there exists a rational number t such that $j(P) = j_5(t)$. The resultant between the polynomials $5^3(t+1)(2t+1)^3(2t^2-3t+3)^3$ and $(t^2+t-1)^5$ is 5^{75}. If we write $t = \frac{X}{Y}$, with X, Y coprime integers, and $F(X,Y) = 5^3(X+Y)(2X+Y)^3(2X^2-3XY+3Y^2)^3$, then

$$\gcd\left(F(X,Y), (X^2 + XY - Y^2)^5\right) \mid 5^{75} Y^{10}.$$

However, $j(P)$ is an integer, and so $(X^2 + XY - Y^2)^5$ also divides $5^{75}Y^{10}$. As X, Y are coprime, we obtain that $X^2 + XY - Y^2 = \pm 5^d$, with $0 \leq d \leq 15$. If $d > 0$, it is easy to notice that X and Y must be coprime with 5. Writing $X = \frac{1}{2}(-Y \pm \sqrt{5Y^2 \pm 4 \cdot 5^d})$ we see that $5Y^2 \pm 4 \cdot 5^d$ is a square, and so its

5-adic valuation must be even. This implies that $d \leq 1$. We then want to solve the following Pell equations:

$$5Y^2 - D^2 = \pm 4 \qquad 5Y^2 - D^2 = \pm 20,$$

which replacing $D = 5E$ reduce to

$$5Y^2 - D^2 = \pm 4 \qquad Y^2 - 5E^2 = \pm 4.$$

So we just need to solve the equations $u^2 - 5v^2 = \pm 4$. As $\mathbb{Q}(\sqrt{5})$ has class number 1, we have solutions

$$\begin{cases} u_k = \pm \left(\left(\frac{1+\sqrt{5}}{2} \right)^k + \left(\frac{1-\sqrt{5}}{2} \right)^k \right) \\ v_k = \pm \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right) \end{cases}$$

for $k \geq 0$, such that $u_k^2 - 5v_k^2 = (-1)^k \cdot 4$. All the possible solutions in X, Y are

$$\begin{cases} X = \frac{-v_k \pm u_k}{2} \\ Y = v_k \\ X^2 + XY - Y^2 = (-1)^k \end{cases} \qquad \begin{cases} X = \frac{-u_k \pm 5v_k}{2} \\ Y = u_k \\ X^2 + XY - Y^2 = (-1)^{k+1} \cdot 5 \end{cases}$$

and hence $j(P) \in \left\{ (-1)^k F(X,Y), \frac{(-1)^{k+1}}{5^5} F(X,Y) \right\}$. As the solutions of Pell's equation grow exponentially (and so does $F(X,Y)$), we have logarithmically fewer cases to test. To test the curves, we first compute the set of the j-invariants of points on $X_{ns}^+(5)$ with $j < e^{1100}$. Then for every j in the list we choose an elliptic curve E such that $j(E) = j$ and we search a small prime p of good reduction (it is sufficient to test a single curve by Lemma 5.4.27). We compute the characteristic polynomial of the Frobenius of the curve reduced modulo p and we check if this is the characteristic polynomial of an element of $C_{ns}^+(25)$ when reduced modulo 25. If it is, then we consider the next small prime p of good reduction, otherwise we remove j from the list. The algorithm takes a few seconds and it outputs a list of 9 CM j-invariants, which are the only integral points of $X_{ns}^+(25)$. □

Remark 5.3.10. We now give some more details on why there is a problem in [BBM21]. In [BBM21, Section 9] the authors define $\lambda = \frac{\delta_2\theta_1 - \delta_1\theta_2}{\delta_1}$ and assume that there exists an integer r such that the number $r\delta$ is close to an integer, while $r\lambda$ is not. However, by Proposition 5.3.7 we know that $\lambda \in \mathbb{Z}[\delta]$, and so $r\lambda$ will be close to an integer too. To see this easily notice that, similarly to the first part of the proof of Proposition 5.3.9, one can assume that $\theta_1 = \cdots = \theta_{d-1} = 0$, and so $\lambda = 0$.

We are now ready to prove Theorem 5.3.2.

Proof of Theorem 5.3.2. If we write $N = \prod p_i^{e_i}$, for every p_i the j map factors through a map $X_{ns}^+(N) \to X_{ns}^+(p^k)$ defined over $\mathbb{Q}$ for every $1 \leq k \leq e_i$. This implies that a rational point P on $X_{ns}^+(N)$ with $j(P) \in \mathbb{Z}$ maps to a rational point on $X_{ns}^+(p_i^{e_i})$ with the same j-invariant. Assuming Claim 5.3.1 this implies that $N = 3^a \cdot 5^b \cdot 7^c$. By Lemma 5.3.3(3) we have that either $j(P) = 3^3 \cdot 41^3 \cdot 61^3 \cdot 149^3$ or P does not map to $X_{ns}^+(9)(\mathbb{Q})$, so we can assume that $a \leq 1$. Similarly, by Proposition 5.3.9 and Lemma 5.3.3(2) we can assume that $b \leq 1$ and $c = 0$. To conclude, it suffices to notice that by Lemma 5.3.3(1) the exponents a and b cannot be both equal to 1. □

5.4 Proper subgroups of $C_{ns}^+(p)$

In this section, we give the proofs of Theorem 8 and Theorem 9. To do this, we will study the integral points of the modular curves $X_{G(p)}$, where $G(p)$ is defined as the unique subgroup of index 3 of $C_{ns}^+(p)$ (see Theorem 6). By Lemma 1.1.5, we know that for $p > 5$ the set of integral points of $X_{G(p)}$ coincides with the set of rational points. The main strategy involved in the proof is the Runge method for modular curves, developed by Bilu and Parent [BP11a]. This is the same strategy applied by Le Fourn and Lemos to prove that there are no non-CM elliptic curves E such that $\operatorname{Im}\rho_{E,p} \cong G(p)$ for $p > 1.4 \cdot 10^7$ (Theorem 7).

Le Fourn and Lemos's proof of Theorem 7 is based on two fundamental steps: first, they show that an elliptic curve satisfying the hypothesis of Theorem 7 has integral j-invariant (via the formal immersion method of Mazur). Second, they prove an upper bound on $|j(E)|$ by combining Runge's method with an effective surjectivity theorem showing that $\operatorname{Im}\rho_{E,p} = \mathrm{GL}(E[p])$ for all p greater than an explicit bound depending on $j(E)$.

The first step works in complete generality: Le Fourn and Lemos actually prove that $j(E)$ is integral for $p \notin \{2, 3, 5, 7, 11, 13, 17, 37\}$ and we can show that this is true for every $p > 5$, so, in order to prove Theorem 9, we can assume $j(E) \in \mathbb{Z}$. Our main contribution lies in a much sharper upper bound on $|j(E)|$, which we achieve through three main innovations: First, we apply the sharp effective surjectivity theorem proved in Chapter 4 (i.e. Theorem 4.1.1). Secondly, we exploit the local properties studied in Chapter 3, such as ruling out all primes $p \equiv -1 \pmod 9$ and proving that $j(E)$ can be written as $p^k c^3$ for some integers $c \geq 0$ and $k \geq 4$. When we eventually reduce the proof of Theorem 8 to an explicit calculation, this latter relation has the effect of dividing by three *on a logarithmic scale* the number of tests we have to perform, significantly reducing the computational component of our approach. Finally, the third and most significant innovation is our much more detailed study of the modular units on the curve $X_{G(p)}$. The main ingredients

that lead to our improved bound on $\log|j(E)|$ are sharp bounds on character sums, which essentially draw on Weil's method to treat Kloosterman sums [Wei48], an idea based on Abel's summation to amplify certain cancellation phenomena among roots of unity, and direct computations to fully exploit the extent of these cancellations. All of these improvements are crucial to lowering the bound on $\log|j(E)|$ to values that are computationally tractable, and the result we obtain is sharp enough that the final computation takes less than two minutes of CPU time.

The Runge method for modular curves

The aim of this section is to prove Proposition 5.4.16, which gives the absolute upper bound $\log|j(E)| \leq 39 + \log 2$ for all elliptic curves $E/\mathbb{Q}$ which satisfy $\operatorname{Im}\rho_{E,p} \cong G(p)$ for some prime number p. This should be contrasted with the estimate $\log|j(E)| \leq 27000$ given in [LFL21].

For technical reasons, in the whole section we work with the quantity $|\log|q||$ instead of $\log|j(E)|$, where $q = e^{2\pi i\tau}$ and τ is a point in the upper half plane $\mathcal{H}$ corresponding to $E(\mathbb{C})$. By Theorem 1.2.2, whenever τ is in the standard fundamental domain $\mathcal{F}$, estimates on $\log|j(E)|$ translate into estimates on $|\log|q||$ and vice versa.

The improved bound is obtained in two steps. In Proposition 5.4.5, we obtain a preliminary bound on $|\log|q||$ which is already sharper than [LFL21, Proposition 6.1] ($O(\sqrt[4]{p})$ instead of $O(\sqrt{p})$, with the key improvement given by Lemma 5.4.8). This allows us to prove that $p < 103000$: we then use this to re-estimate $|\log|q||$ and obtain the final bound $|\log|q|| < 39$.

From now on we will always assume that p is a prime greater than 5 for which $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$. This also implies by Theorem 6 that $p \equiv 2 \pmod 3$ and by Lemma 1.1.5 that $j(E) \in \mathbb{Z}$.

By Theorem 5.2.7, we can define the function

$$U := \zeta \prod_{(a,b)\in\mathcal{O}_{\text{cubes}}} g_{a,b}^6,$$

where ζ is a root of unity, such that $U \in \mathbb{Q}(X_{G(p)})$ and both U and $\frac{p^6}{U}$ are integral over $\mathbb{Z}[j]$. We then obtain the following result.

Corollary 5.4.1. *For every $P \in X_{G(p)}(\mathbb{Q})$ such that $j(P)$ is an integer, $U(P)$ is an integer dividing p^6. In particular, $0 \leq \log|U(P)| \leq 6\log p$.*

We now introduce the auxiliary quantities that we will have to bound in our proof.

Definition 5.4.2. Set $e(z) := e^{2\pi iz}$ for every $z \in \mathbb{C}$. We define functions $R_{a_1,a_2} = R_{a_1,a_2}(q)$ as follows. For all $(a_1,a_2) \in \frac{1}{p}\mathbb{Z}^2 \cap [0,1)^2$, with a_1, a_2 not

both 0, we define

$$R_{a_1,a_2} = \prod_{n=0}^{\infty}(1-q^{n+a_1}e(a_2))(1-q^{n+1-a_1}e(-a_2))$$

for $a_1 \neq 0$, and

$$R_{0,a_2} = \prod_{n=1}^{\infty}(1-q^{n}e(a_2))(1-q^{n}e(-a_2)).$$

We further set

$$R = \prod_{(pa_1,pa_2)\in\mathcal{O}_{\text{cubes}}} R_{a_1,a_2}^6,$$

where we identify $pa_1, pa_2 \in [0, p-1] \cap \mathbb{Z}$ with their residue classes modulo p.

Remark 5.4.3. We have $\prod_{a_2=1}^{p-1}(1-e(a_2)) = p$, because $\prod_{a_2=1}^{p-1}(x-e(a_2)) = 1+x+x^2+\ldots+x^{p-1}$.

Remark 5.4.4. Whenever $p \equiv 2 \pmod 3$, we have $\mathbb{F}_p^\times = \mathbb{F}_p^{\times 3}$, and so $\mathbb{F}_p^\times \subseteq \mathbb{F}_{p^2}^{\times 3}$. This implies that $(0,a_2) \in \mathcal{O}_{\text{cubes}}$ for every $a_2 \in \mathbb{F}_p^\times$, because $a_2\sqrt{\varepsilon} = \frac{a_2}{\varepsilon}\cdot\sqrt{\varepsilon}^3$ is a cube in $\mathbb{F}_{p^2}$, since it is the product of two cubes.

The last two remarks imply that when $p \equiv 2 \pmod 3$ we can write $U = \zeta \cdot q^{\mathrm{Ord}_q(U)} \cdot p^6 \cdot R$, hence

$$\log|U| = \mathrm{Ord}_q(U)\log|q| + 6\log p + \log|R|. \tag{5.4.1}$$

Comparing $\log|q|$ with p Our next goal is to establish the following bound on $\log|q|$ in terms of p.

Proposition 5.4.5. *Let $E/\mathbb{Q}$ be an elliptic curve and set $q = e^{2\pi i\tau}$, where $\tau \in \mathcal{H}$ corresponds to the complex elliptic curve $E(\mathbb{C})$. Suppose that $|\log|q|| \geq 30$. If $p > 5$ is a prime number such that $p \equiv 2 \pmod 3$ and $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$, then*

$$|\log|q|| \leq \frac{2\sqrt{2}\,\pi\cdot 101}{10\sqrt{102}}\cdot\sqrt[4]{p} + 1.65.$$

The proof of this result will occupy all of this section. The argument relies on estimating the various terms in equation (5.4.1). In particular, we need to compute the order at infinity of U and bound the contribution of $\log|R|$. The latter is the hard step; we take care of the former in the next lemma.

Lemma 5.4.6. *We have*

$$\mathrm{Ord}_q(U) = \frac{p^2-1}{3p}.$$

The calculation of $\mathrm{Ord}_q(U)$ already appears in [LFL21, Proposition 6.5], but unfortunately, due to an arithmetic error, the result is incorrect. For the sake of completeness, we repeat the calculation below. Note that the second half of [LFL21, Proposition 6.5], namely the statement that $|\rho_U| = (p-1)^3$, is also incorrect: by Remark 5.4.3 and Remark 5.2.8 we actually have $|\rho_U| = p^6$.

Proof. By Remark 5.4.4, we know that $(0, a_2) \in \mathcal{O}_{\mathrm{cubes}}$ for every $a_2 \in \mathbb{F}_p^\times$. On another hand, on $\mathbb{F}_p^\times \times \mathbb{F}_p$, the function $(a_1, a_2) \mapsto a_1$ has fibres with constant cardinality, because $\mathcal{O}_{\mathrm{cubes}}$ is stable under multiplication by $\mathbb{F}_p^\times$. In particular, the cardinality of each fibre is $\frac{(p^2-1)/3-(p-1)}{p-1} = \frac{p-2}{3}$. Hence

$$\mathrm{Ord}_q(U) = 6\left((p-1)\cdot\frac{1}{2}B_2(0) + \frac{p-2}{3}\sum_{a_1=1}^{p-1}\frac{1}{2}B_2\left(\frac{a_1}{p}\right)\right) = \frac{p^2-1}{3p}. \qquad \square$$

Our next objective is to estimate $\log|R|$.

Proposition 5.4.7. *We have*

$$|\log|R|| \leq -\frac{8\pi^2 p\sqrt{p}}{3\log|q|}.$$

Proof. The inequality $|\log|z|| \leq |\log z|$ holds for every $z \in \mathbb{C}^\times$ and every choice of a branch of the logarithm. Indeed, if $z = r\cdot e^{i\theta}$, we have $|\log|z|| = |\log r| \leq |\log r + i\theta + 2k\pi i| = |\log z|$. Thus, it suffices to bound $|\log R|$. As (a,b) is in $\mathcal{O}_{\mathrm{cubes}}$ if and only if $(-a,-b)$ is, we have

$$\begin{aligned} R &= \prod_{(pa_1,pa_2)\in\mathcal{O}_{\mathrm{cubes}}} R_{a_1,a_2}^6 \\ &= \left(\prod_{b=1}^{p-1}\prod_{n=1}^{\infty}(1-q^n e(b/p))^{12}\right)\cdot\left(\prod_{\substack{(pa_1,pa_2)\in\mathcal{O}_{\mathrm{cubes}}\\ a_1\neq 0}}\prod_{n=0}^{\infty}(1-q^{n+a_1}e(a_2))^{12}\right). \end{aligned}$$

We can further write

$$\begin{aligned}\log R &= 6 \sum_{(pa_1,pa_2)\in\mathcal{O}_{\text{cubes}}} \log R_{a_1,a_2} \\ &= 6\sum_{b=1}^{p-1} \log R_{0,\frac{b}{p}} + 6 \sum_{\substack{(pa_1,pa_2)\in\mathcal{O}_{\text{cubes}} \\ a_1\neq 0}} \log R_{a_1,a_2} \\ &= 12\sum_{b=1}^{p-1}\sum_{n=1}^{\infty} \log(1-q^n e(b/p)) + 12 \sum_{\substack{(pa_1,pa_2)\in\mathcal{O}_{\text{cubes}} \\ a_1\neq 0}} \sum_{n=0}^{\infty} \log(1-q^{n+a_1}e(a_2)) \\ &= -12\sum_{b=1}^{p-1}\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \frac{q^{kn}}{k}\cdot e(kb/p) - 12 \sum_{\substack{(pa_1,pa_2)\in\mathcal{O}_{\text{cubes}} \\ a_1\neq 0}} \sum_{n=0}^{\infty}\sum_{k=1}^{\infty} \frac{q^{k(n+a_1)}}{k}\cdot e(ka_2).\end{aligned}$$

Define now $c(a) := \sum_{b\in F(a)} e(b/p)$ with $F(a) := \{b \in \mathbb{F}_p \mid (a,b) \in \mathcal{O}_{\text{cubes}}\}$ for $a \not\equiv 0 \pmod p$. We extend the definition to $a \equiv 0 \pmod p$ by setting $c(a) = c(0) := \frac{p-2}{3}$.

The sum $\sum_{b=1}^{p-1} e(kb/p)$ equals either -1 or $p-1$ if respectively $k \not\equiv 0 \pmod p$ or $k \equiv 0 \pmod p$. Moreover, we also have $\sum_{b\in F(a)} e(kb/p) = c(ka)$: indeed, b is in $F(a)$ if and only if kb is in $F(ka)$, because k is an element of $\mathbb{F}_p^{\times}$ and therefore a cube in $\mathbb{F}_{p^2}^{\times}$. Hence we obtain

$$\begin{aligned}\log R &= 12\sum_{n=1}^{\infty}\sum_{k\not\equiv 0(p)} \frac{q^{kn}}{k} - 12(p-1)\sum_{n=1}^{\infty}\sum_{\substack{k\equiv 0(p)\\ k>0}} \frac{q^{kn}}{k} - 12\sum_{a=1}^{p-1}\sum_{n=0}^{\infty}\sum_{k=1}^{\infty} \frac{q^{k(n+\frac{a}{p})}}{k}\cdot c(ka) \\ &= 12\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{q^{kn}}{k} - 12p\sum_{n=1}^{\infty}\sum_{\substack{k\equiv 0(p)\\ k>0}} \frac{q^{kn}}{k} - 12\sum_{a=1}^{p-1}\sum_{n=0}^{\infty}\sum_{k=1}^{\infty} \frac{q^{k(n+\frac{a}{p})}}{k}\cdot c(ka).\end{aligned}$$

We notice that the definition we have given for $c(0)$ is compatible with this chain of equalities. Indeed, whenever $k \equiv 0 \pmod p$, for a fixed $a_1 \neq 0$ we have $\sum_{a_2\in F(a_1)} e(0\cdot a_2) = |F(a_1)| = \frac{p-2}{3} = c(0)$, as we noticed at the beginning of the proof of Lemma 5.4.6.

Lemma 5.4.8. *For every $s \in \mathbb{F}_p^{\times}$ we have $|c(s)| \leq \frac{4}{3}\sqrt{p}$.*

Proof. For $a + b\sqrt{\varepsilon} \in \mathbb{F}_{p^2}$ we have

$$(a+b\sqrt{\varepsilon})^3 = a^3 + 3\varepsilon ab^2 + (3a^2b + \varepsilon b^3)\sqrt{\varepsilon}.$$

To characterise the set $F(s)$ we write $a^3 + 3\varepsilon ab^2 = s$. Note that, since $s \neq 0$, we always have $a \neq 0$. Writing $e_p(x) := e(x/p)$ and $t = \frac{b}{a}$, this gives

$$\begin{aligned} c(s) = \sum_{x \in F(s)} e_p(x) &= \frac{1}{3} \sum_{\substack{a,b \in \mathbb{F}_p \\ a^3+3\varepsilon ab^2 = s}} e_p(3a^2b + \varepsilon b^3) \\ &= \frac{1}{3} \sum_{\substack{a,t \in \mathbb{F}_p \\ a^3(1+3\varepsilon t^2) = s}} e_p(a^3(3t + \varepsilon t^3)) = \frac{1}{3} \sum_{\substack{t \in \mathbb{F}_p \\ 1+3\varepsilon t^2 \neq 0}} e_p\left(\frac{s(3t+\varepsilon t^3)}{1+3\varepsilon t^2}\right), \end{aligned}$$

where the second and last equalities are due to the fact that, for $c \in \mathbb{F}_p^\times$, the equation $z^3 = c$ has 3 solutions in $\mathbb{F}_{p^2}$ and 1 solution in $\mathbb{F}_p$ (since $p \equiv 2 \pmod 3$). We now use the following result by Perel'muter [Per69, Theorem 1], obtained via a generalisation of Weil's strategy [Wei48] to bound Kloosterman sums.

Let $\varphi \in \mathbb{F}_p(t)$ be a rational function with poles $S = \{t_1, \dots, t_\ell\} \subseteq \overline{\mathbb{F}}_p \cup \{\infty\}$. We have

$$\left| \sum_{t \in \mathbb{F}_p \setminus S} e_p(\varphi(t)) \right| \leq (\ell + \deg(\varphi) - 2)\sqrt{p}.$$

In our case we have that $\varphi(t) = \frac{s(3t+\varepsilon t^3)}{1+3\varepsilon t^2}$ has 2 poles other than ∞, hence we get

$$|c(s)| \leq \frac{1}{3}(3 + 3 - 2)\sqrt{p} = \frac{4}{3}\sqrt{p},$$

as desired. □

Thanks to this lemma, we now have all the tools needed to complete the proof of Proposition 5.4.7. We notice that

$$\sum_{a=1}^{p-1} \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} \frac{q^{k(n+\frac{a}{p})}}{k} \cdot c(ka) = \sum_{n \not\equiv 0 (p)} \sum_{k=1}^{\infty} \frac{q^{\frac{nk}{p}}}{k} \cdot c(kn).$$

Isolating the terms involving $c(0)$ and using $c(0) = \frac{p-2}{3}$, we can rearrange the

sums as follows:

$$\begin{aligned}
\log R &= 12\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{q^{kn}}{k} - 12\sum_{n=1}^{\infty}\sum_{\substack{k\equiv 0(p)\\ k>0}}\frac{q^{\frac{k}{p}\cdot pn}}{k/p} - 12\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{q^{\frac{nk}{p}}}{k}\cdot c(kn)\\
&= 12\left(\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{q^{kn}}{k} - \sum_{\substack{n\equiv 0(p)\\ n>0}}\sum_{k=1}^{\infty}\frac{q^{kn}}{k}\right) - 12\left(\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{q^{\frac{nk}{p}}}{k}\cdot c(kn)\right)\\
&= 12\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{q^{kn}}{k} - 12\left(\sum_{n\not\equiv 0(p)}\sum_{k\not\equiv 0(p)}\frac{q^{\frac{nk}{p}}}{k}\cdot c(kn) + \frac{p-2}{3}\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{q^{nk}}{pk}\right)\\
&= \alpha\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{q^{kn}}{k} - 12\sum_{n\not\equiv 0(p)}\sum_{k\not\equiv 0(p)}\frac{q^{\frac{nk}{p}}}{k}\cdot c(kn) + 16\sqrt{p}\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{q^{nk}}{pk},
\end{aligned}$$

where $\alpha = 12 - \frac{4(p-2)}{p} - \frac{16\sqrt{p}}{p}$. We now notice that $\alpha \le 8$ for all p and apply Lemma 5.4.8 to estimate $\log R$:

$$\begin{aligned}
|\log R| &\le 8\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{|q|^{kn}}{k} + 12\sum_{n\not\equiv 0(p)}\sum_{k\not\equiv 0(p)}\frac{|q|^{\frac{nk}{p}}}{k}\cdot|c(kn)| + 16\sqrt{p}\sum_{n\not\equiv 0(p)}\sum_{\substack{k\equiv 0(p)\\ k>0}}\frac{|q|^{\frac{nk}{p}}}{k}\\
&\le 8\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{|q|^{kn}}{k} + 16\sqrt{p}\sum_{n\not\equiv 0(p)}\sum_{k\not\equiv 0(p)}\frac{|q|^{\frac{nk}{p}}}{k} + 16\sqrt{p}\sum_{n\not\equiv 0(p)}\sum_{\substack{k\equiv 0(p)\\ k>0}}\frac{|q|^{\frac{nk}{p}}}{k}\\
&= 8\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{|q|^{kn}}{k} + 16\sqrt{p}\sum_{n\not\equiv 0(p)}\sum_{k=1}^{\infty}\frac{|q|^{\frac{nk}{p}}}{k}\\
&= 8\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{|q|^{kn}}{k} - 16\sqrt{p}\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{|q|^{kn}}{k} + 16\sqrt{p}\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{|q|^{\frac{nk}{p}}}{k}\\
&= (16\sqrt{p}-8)\sum_{n=1}^{\infty}\log(1-|q|^{n}) - 16\sqrt{p}\sum_{n=1}^{\infty}\log(1-|q|^{\frac{n}{p}}).
\end{aligned}$$

To complete the proof, it suffices to notice that

$$\sum_{n=1}^{\infty}\log(1-|q|^{n}) < 0$$

and that

$$-16\sqrt{p}\sum_{n=1}^{\infty}\log(1-|q|^{\frac{n}{p}}) \le -\frac{16\pi^2\sqrt{p}}{6\log(|q|^{\frac{1}{p}})} = -\frac{8\pi^2 p\sqrt{p}}{3\log|q|}$$

by Lemma 1.1.1. □

Let now τ_P be a point in the fundamental domain of $X_{G(p)}$ that corresponds to a point $P \in X_{G(p)}(\mathbb{Q})$ with $j(P) \in \mathbb{Z}$. There exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau = \gamma^{-1}(\tau_P)$ is in the standard fundamental domain $\mathcal{F}$ of $X(1)$; in particular, it is in the domain corresponding to the cusp ∞ (i.e., ∞ is the cusp closest to τ). We remark that $(U \circ \gamma)(\tau) \in \mathbb{Z}$, since by Corollary 5.4.1 we have $U(P) \in \mathbb{Z}$.

Up to Galois conjugation (which fixes P but changes the cusps), we can choose an embedding $X_{G(p)}(\overline{\mathbb{Q}}) \hookrightarrow X_{G(p)}(\mathbb{C})$ such that either γ is the identity or $\gamma \pmod p$ is an element in $C_{ns}(p) \cap \mathrm{SL}_2(\mathbb{F}_p)$ that does not lie in $G(p)$. Indeed, this can be seen from the parametrisation of the cusps given in [LFL21, Section 2] and the fact that the cusps of $X_{G(p)}$ split into two Galois orbits, see [LFL21, Lemma 6.3]. From now on, whenever we write γ we will refer to the second case, in which $\gamma \pmod p$ is an element of $C_{ns}(p) \cap \mathrm{SL}_2(\mathbb{F}_p)$ not in $G(p)$, unless otherwise specified.

Remark 5.4.9. By Remark 5.4.4, we have that $(0, b) \in \mathcal{O}_{\text{cubes}}$ for every $b \in \mathbb{F}_p^\times$, hence every cusp in $\gamma^{-1}\mathcal{O}_{\text{cubes}}$ is parametrised by a pair (a, b) such that $a \neq 0$. The function $U \circ \gamma$ is a modular unit on $X_{G(p)}$ (though not necessarily defined over $\mathbb{Q}$), and the element γ acts by permutation on the set $\mathbb{F}_p^2 \setminus \{0\}$. From this, it is easy to see that we have

$$\log|U \circ \gamma| = \mathrm{Ord}_q(U \circ \gamma) \log|q| + \log|R_\gamma|,$$

where

$$R_\gamma = \prod_{(a,b) \in \gamma^{-1}\mathcal{O}_{\text{cubes}}} R^6_{\frac{a}{p}, \frac{b}{p}}. \tag{5.4.2}$$

Lemma 5.4.10. *We have*

$$\mathrm{Ord}_q(U \circ \gamma) = -\frac{p^2 - 1}{6p}.$$

This is proven by a calculation analogous to that of Lemma 5.4.6. The result also appears in [LFL21], where however it is affected by the same arithmetic error as [LFL21, Proposition 6.5]. The next proposition bounds $\log R_\gamma$ similarly to Proposition 5.4.7; we will not directly make use of this result, but some of the arguments in its proof will be useful later.

Proposition 5.4.11. *We have*

$$|\log|R_\gamma|| < -\frac{8\pi^2 p\sqrt{p}}{3\log|q|}.$$

Proof. The proof is analogous to that of Proposition 5.4.7. We notice that for every $(a_1, a_2) \in \gamma^{-1}\mathcal{O}_{\text{cubes}}$ we have $a_1 \neq 0$, hence

$$\log R_\gamma = -12 \sum_{n \not\equiv 0 (p)} \sum_{k=1}^{\infty} \frac{q^{\frac{nk}{p}}}{k} \cdot c_\gamma(kn),$$

where $c_\gamma(a) := \sum_{b\in F_\gamma(a)} e(b/p)$ and $F_\gamma(a) := \{b \in \mathbb{F}_p \mid (a,b) \in \gamma^{-1}\mathcal{O}_{\text{cubes}}\}$ for $a \neq 0$ and $c(0) = \frac{p+1}{3}$. To adapt Lemma 5.4.8 to the case of c_γ, we notice that if γ^{-1} acts as multiplication by $x+y\sqrt{\varepsilon}$ on $\mathbb{F}_{p^2}^\times$ for some $x, y \in \mathbb{F}_p$ (as explained in [LFL21, Lemma 6.3]), then the function $\varphi(t)$ of Lemma 5.4.8 becomes

$$\varphi(t) = s\ \frac{(3t+\varepsilon t^3)x + (1+3\varepsilon t^2)y}{(1+3\varepsilon t^2)x + (3t+\varepsilon t^3)\varepsilon y},$$

giving again $|c_\gamma(s)| \leq \frac{4}{3}\sqrt{p}$. The rest of the proof of Proposition 5.4.7 carries through. □

We remark that, even though the bound on $|\log|R_\gamma||$ is the same as that on $|\log|R||$, the order at infinity of the function U is halved in this case, that is, $|\operatorname{Ord}_q(U\circ\gamma)| = \frac{1}{2}|\operatorname{Ord}_q U|$. This leads to a weaker bound on $|\log|q||$ in terms of p, which is what we are really interested in for the proof of Proposition 5.4.5. To obtain a sharper bound on $|\log|R_\gamma||$, we consider a different p-th root of q.

Remark 5.4.12. We note that in order to prove Proposition 5.4.5, it suffices to consider $\tau \in \mathcal{H}$ lying in the standard fundamental domain $\mathcal{F}$ and such that $|\tau| > 1$. Indeed, $q(\tau) = q(\tau+n)$ for every $n \in \mathbb{Z}$, hence without loss of generality we can consider $\Re\tau \in \left(-\frac{1}{2}, \frac{1}{2}\right]$, and if $|\tau| \leq 1$ then $|\log|q|| \leq 2\pi < \frac{2\sqrt{2}\,\pi\cdot 101}{10\sqrt{102}} \cdot \sqrt[4]{p} + 1.65$.

From Theorem 1.2.4 we know that if E corresponds to $\tau \in \mathcal{H}$ in the standard fundamental domain $\mathcal{F}$ not lying on the lower boundary $\left\{e^{i\theta} \mid \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}\right\}$, then $q \in \mathbb{R}$. This is true for all the fundamental domains of the form $\mathcal{F}+n$ for $n \in \mathbb{Z}$. We notice that, for $\tau \in \mathcal{F}$ and $q > 0$, we have $\Re\tau = 0$ and therefore $q^{\frac{1}{p}} \in \mathbb{R}$. However, if $q < 0$, we have $\Re\tau = \frac{1}{2}$ and $q^{\frac{1}{p}} = e^{\frac{2\pi i\tau}{p}}$ is not real. However, we can consider $\tau' := \tau + \frac{p-1}{2} \in \mathcal{F} + \frac{p-1}{2}$, which gives the same value of q and is such that $e^{\frac{2\pi i\tau'}{p}} \in \mathbb{R}$ is the p-th real root of q.

We then repeat the previous construction changing the choice of τ. Let τ_P be a point in the fundamental domain of $X_{G(p)}$ that corresponds to a point $P \in X_{G(p)}(\mathbb{Q})$ with $j(P) \in \mathbb{Z}$. There exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau = \gamma^{-1}(\tau_P)$ is in the standard fundamental domain $\mathcal{F}$ if $q > 0$, and in the fundamental domain $\mathcal{F} + \frac{p-1}{2}$ if $q < 0$. As before, up to Galois conjugation, we can take γ to be either the identity or an element whose reduction modulo p lies in $C_{ns}(p) \cap \mathrm{SL}_2(\mathbb{F}_p)$ but not in $G(p)$ – this is again because the point P is defined over $\mathbb{Q}$ and therefore fixed by the Galois action, while there are two orbits of cusps.

All the previous estimates still hold for this new choice of τ and we can take advantage of the new choice of the p-th root of q to improve the bound on $\log|R_\gamma|$. To distinguish the two different p-th roots, we will write $q^{\left(\frac{1}{p}\right)}$ to denote the root that maps the real numbers to themselves.

Proposition 5.4.13. *Let $\tau = \gamma^{-1}\tau_P \in \mathcal{H}$ be as above and such that $j(\tau) \notin (0, 1728)$. We have*

$$\log|R_\gamma(\tau)| = -\frac{1}{2}\log R(\tau).$$

Proof. As in Proposition 5.4.11 we have

$$\log R_\gamma(\tau) = -12 \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot c_\gamma(kn),$$

where $c_\gamma(a) := \sum_{b\in F_\gamma(a)} e(b/p)$ and $F_\gamma(a) := \{b \in \mathbb{F}_p \mid (a, b) \in \gamma^{-1}\mathcal{O}_{\text{cubes}}\}$ for $a \neq 0$ and $c(0) = \frac{p+1}{3}$.
As explained in [LFL21, Lemma 6.3], the action of γ^{-1} on the cusps of $X_{G(p)}$ corresponds to the multiplication by $(x + y\sqrt{\varepsilon})$ on $\mathbb{F}_{p^2}^\times/\pm 1$ for some $x, y \in \mathbb{F}_p$. It is then easy to see that $\mathcal{O}_{\text{cubes}} \sqcup \gamma^{-1}\mathcal{O}_{\text{cubes}} \sqcup \gamma^{-2}\mathcal{O}_{\text{cubes}} = \mathbb{F}_p^2 \setminus \{(0, 0)\}$, and that $(a, b) \in \gamma^{-1}\mathcal{O}_{\text{cubes}}$ if and only if $(a, -b) \in \gamma^{-2}\mathcal{O}_{\text{cubes}}$. Therefore, we obtain that $c_\gamma(k) = \overline{c_{\gamma^2}(k)}$ and $c(k) + c_\gamma(k) + c_{\gamma^2}(k) = 0$ for every $k \in \mathbb{F}_p^\times$. This implies that $c(k)$ is real (this can also be seen directly from the definition of $\mathcal{O}_{\text{cubes}}$) and that $\Re\{c_\gamma(k)\} = -\frac{1}{2}c(k)$ for every $k \not\equiv 0 \pmod p$.
Using that $q \in \mathbb{R}$ by Theorem 1.2.4 and that $\log|z| = \Re\{\log z\}$ for every $z \in \mathbb{C}^\times$, we have

$$\begin{aligned}
\log|R_\gamma(\tau)| = \Re\{\log R_\gamma(\tau)\} &= -12 \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot \Re\{c_\gamma(kn)\} \\
&= 6 \sum_{n,k\not\equiv 0(p)} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot c(kn) - 4(p+1) \sum_{n\not\equiv 0(p)} \sum_{k\equiv 0(p)} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \\
&= 6 \sum_{n,k\not\equiv 0(p)} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot c(kn) - \frac{4(p+1)}{p} \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{nk}}{k}.
\end{aligned}$$

On the other hand, similarly to the proof of Proposition 5.4.7 we have

$$\log R(\tau) = 12 \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{kn}}{k} - 12 \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot c(kn).$$

By isolating the terms containing $c(0)$, we obtain

$$\begin{aligned}
\log R(\tau) &= 12 \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{kn}}{k} - 12 \sum_{n,k\not\equiv 0(p)} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot c(kn) - \frac{4(p-2)}{p} \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{nk}}{k} \\
&= -12 \sum_{n,k\not\equiv 0(p)} \frac{q^{\left(\frac{nk}{p}\right)}}{k} \cdot c(kn) + \frac{8(p+1)}{p} \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{nk}}{k},
\end{aligned}$$

concluding the proof. □

We are now ready to prove Proposition 5.4.5.

Proof of Proposition 5.4.5. By Remark 5.4.12 it suffices to prove the statement for $\tau \in \mathcal{F} + n$, where $n \in \mathbb{Z}$ and $\mathcal{F}$ is the standard fundamental domain, and such that τ does not lie on the lower boundary. Suppose first that P is close to a cusp lying in the Galois orbit corresponding to $\mathcal{O}_{\text{cubes}}$ (i.e., the case in which $\gamma = \text{Id}$). Evaluating U in $\tau = \tau_P$ we obtain

$$\text{Ord}_q(U) \log |q| = -\log |R(\tau)| - 6 \log p + \log |U(\tau)|,$$

and the triangle inequality yields

$$|\,\text{Ord}_q(U) \log |q|| \leq |\log |R(\tau)|| + |-6 \log p + \log |U(\tau)||.$$

By Corollary 5.4.1 we have $0 \leq \log |U(\tau)| \leq 6 \log p$, and hence $|\log U(\tau) - 6 \log(p)| \leq 6 \log p$. Combining this with Proposition 5.4.7 and Lemma 5.4.6 we finally obtain

$$\frac{p^2-1}{3p} |\log |q|| \leq 6 \log p + \frac{8\pi^2 p \sqrt{p}}{3 |\log |q||}.$$

Suppose instead that P is close to a cusp lying in the other Galois orbit (i.e., the case in which $\gamma \neq \text{Id}$). Evaluating $U \circ \gamma$ in $\tau = \gamma^{-1} \tau_P$ (lying in $\mathcal{F}$ or in $\mathcal{F} + \frac{p-1}{2}$ depending on the sign of q, as above) and proceeding in the same way (using Lemma 5.4.10 and Proposition 5.4.13 instead of Lemma 5.4.6 and Proposition 5.4.7 respectively), we obtain the inequality

$$\frac{p^2-1}{6p} |\log |q|| \leq 6 \log p + \frac{4\pi^2 p \sqrt{p}}{3 |\log |q||}.$$

We now set $x = |\log |q||$. So far we have obtained, respectively for $\gamma = \text{Id}$ and $\gamma \neq \text{Id}$,

$$\frac{p^2-1}{3p} x^2 - 6x \log p - \frac{8\pi^2 p \sqrt{p}}{3} \leq 0 \tag{5.4.3}$$

$$\frac{p^2-1}{6p} x^2 - 6x \log p - \frac{4\pi^2 p \sqrt{p}}{3} \leq 0. \tag{5.4.4}$$

The first inequality implies the second, so (independently of whether $\gamma = \text{Id}$ or not) we get that x satisfies (5.4.4), and therefore

$$x \leq \frac{18 p \log p}{p^2-1} + \sqrt{\frac{18^2 p^2 (\log p)^2}{(p^2-1)^2} + \frac{8\pi^2 p^2 \sqrt{p}}{p^2-1}}.$$

Using that $\sqrt{a^2+b^2} \leq a+b$ we obtain

$$x \leq f(p) := \frac{36p\log p}{p^2-1} + \frac{2\sqrt{2}\,\pi p\sqrt[4]{p}}{\sqrt{p^2-1}}.$$

Since the function $f(t)$ is smaller than 30 for $t \in [2,100]$ we can assume that $p > 100$, and then we obtain

$$\begin{aligned} x &\leq \frac{36p\log p}{p^2-1} + \frac{2\sqrt{2}\,\pi p\sqrt[4]{p}}{\sqrt{p^2-1}} \leq \frac{36\cdot 101\cdot \log 101}{100\cdot 102} + \frac{2\sqrt{2}\,\pi\cdot 101}{10\sqrt{102}}\cdot \sqrt[4]{p} \\ &\leq \frac{2\sqrt{2}\,\pi\cdot 101}{10\sqrt{102}}\cdot \sqrt[4]{p} + 1.65, \end{aligned}$$

which concludes the proof. □

Remark 5.4.14. We notice that in the proof of Proposition 5.4.5 we showed that if E is a non-CM elliptic curve and $5 < p < 100$ is a prime such that $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$, then $|\log|q|| < 30$. In particular, this implies that every time that we assume $|\log|q|| \geq 30$ we are implicitly assuming that $p > 100$.

Corollary 5.4.15. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and set $q = e^{2\pi i\tau}$, where $\tau \in \mathcal{H}$ corresponds to the complex elliptic curve $E(\mathbb{C})$. Let $p > 5$ be a prime number such that $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$. If $|\log|q|| \geq 30$, then $p < 103000$.*

Proof. By Theorem 6 we can assume that $p \equiv 2 \pmod 3$. Writing $\log(\Im\{\tau\}) = \frac{1}{2\pi}|\log|q||$, by Theorem 4.1.1(3) we have

$$\Lambda < 2533\left(\mathrm{h}_{\mathcal{F}}(E) + 2\log\Lambda + \frac{3}{4\pi}\log|\log|q|| + 1.38\right).$$

We recall that by Theorem 7 we have that $j(E) \in \mathbb{Z}$, indeed we can assume that $p > 37$, as smaller primes satisfy the condition $p < 103000$. We can then apply Theorem 1.2.6(3) to bound $\mathrm{h}_{\mathcal{F}}(E)$ in the inequality above with

$$-\frac{1}{12}\log|q| - \frac{1}{2}\log|\log|q|| - \frac{1}{2}\log 2 - \frac{\pi^2}{3\log|q|},$$

obtaining a linear bound on p in terms of $|\log|q||$. On the other hand, by Proposition 5.4.5 we have

$$|\log|q|| \leq \frac{2\sqrt{2}\,\pi\cdot 101}{10\sqrt{102}}\cdot \sqrt[4]{p} + 1.65,$$

and we obtain an explicit inequality in p, which can be numerically solved. □

The upper bound on p given by Corollary 5.4.15 is sharper than the corresponding bound in Theorem 7, but it is still not good enough to test all the remaining primes by the direct computation we describe in Section 5.4. For this reason, in the next section we improve on Proposition 5.4.5. The intermediate result we just obtained will be an important ingredient in this improvement.

Abel summation and a sharper bound on $\log|q|$

Proposition 5.4.5 improves the bound on $\log R$ given in [LFL21] by considering cancellation among roots of unity. In particular, the argument in [LFL21] used the trivial estimate $|c(k)| \leq \frac{p-2}{3}$, which we replaced by $|c(k)| \leq \frac{4}{3}\sqrt{p}$ using Lemma 5.4.8. In this section, we show that by rearranging the sums in $\log R$ using partial summation, we obtain an expression for $\log R$ which gives even more cancellations. This leads to a further improvement of the bound of Proposition 5.4.7 and ultimately to the following result, which supersedes Proposition 5.4.5.

Proposition 5.4.16. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and set $q = e^{2\pi i\tau}$, where $\tau \in \mathcal{H}$ corresponds to the complex elliptic curve $E(\mathbb{C})$. If $p > 5$ is a prime number such that $\operatorname{Im}\rho_{E,p}$ is conjugate to $G(p)$, then $|\log|q|| < 39$.*

To prove this result, we can and do assume that $|\log|q|| \geq 30$. By Remark 5.4.14 this implies that $p > 100$. By Corollary 5.4.15 and Theorem 3.1.4 we can also assume that p is less than 103000 and that it satisfies $p \equiv 2, 5 \pmod 9$. We keep the notation from the previous section. Similarly to the proof of Proposition 5.4.13 we have

$$\log R = -12 \sum_{n,k\not\equiv 0(p)} \frac{q^{\frac{kn}{p}}}{k} \cdot c(kn) + \frac{8(p+1)}{p} \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{nk}}{k}.$$

Writing $m = kn$ we have

$$\log R = -12 \sum_{m\not\equiv 0(p)} \sum_{k|m} \frac{q^{\frac{m}{p}}}{k} \cdot c(m) + \frac{8(p+1)}{p} \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{kn}}{k}. \tag{5.4.5}$$

Using Lemma 1.1.1, we bound the second term as follows:

$$\left| \frac{8(p+1)}{p} \sum_{n\not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{kn}}{k} \right| < \frac{8(p+1)}{p} \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{|q|^{kn}}{k} < \frac{8(p+1)\pi^2}{6p|\log|q||}. \tag{5.4.6}$$

This quantity is bounded uniformly in p. We now focus on the first sum in equation (5.4.5), which we denote by S. By partial summation, we have

$$\begin{aligned} S &= -12 \sum_{m\not\equiv 0(p)} \sum_{k|m} \frac{q^{\frac{m}{p}}}{k} \cdot c(m) = -12 \sum_{m\not\equiv 0(p)} q^{\frac{m}{p}} \sum_{k|m} \frac{c(m)}{k} \\ &= -12 \sum_{s=1}^{\infty} (q^{\frac{s}{p}} - q^{\frac{s+1}{p}}) D(s), \end{aligned} \tag{5.4.7}$$

where

$$D(s) := \sum_{\substack{m\leq s \\ m\not\equiv 0(p)}} \sum_{k|m} \frac{c(m)}{k}. \tag{5.4.8}$$

The idea of using this rewriting of S is that, when p is large, the factor $q^{\frac{s}{p}} - q^{\frac{s+1}{p}} = q^{\frac{s}{p}}(1 - q^{\frac{1}{p}})$ becomes small, because $|q^{\frac{1}{p}} - 1| = |e^{\frac{\log q}{p}} - 1| \approx \frac{|\log |q||}{p}$. Provided that $D(s)$ does not grow too quickly, the factor of p in the denominator leads to a much better upper bound on S, hence on $\log R$, than that provided by Proposition 5.4.7. We now give two different estimates for $|D(s)|$, one for $s < p$ and one for $s \geq p$, in Lemmas 5.4.17 and 5.4.21 respectively.

Consider all the primes p smaller than a fixed bound M. For $s < p$ we have

$$D(s) = \sum_{m\leq s} \sum_{k|m} \frac{c(m)}{k},$$

and we can write $|D(s)| \leq C\sqrt{p}\sqrt{s}$ for some $C = C(M)$.

Lemma 5.4.17. *Let $M = 103000$ and $C = 4.25$. We have $|D(s)| \leq C\sqrt{p}\sqrt{s}$ for all $s < p < M$ with p prime, $p \equiv 2, 5 \pmod 9$.*

Proof. We get a suitable value of C by explicitly computing the values of $D(s)$ for all primes $p \equiv 2, 5 \pmod 9$ up to M and for $s = 1, \ldots, p-1$. More precisely, in order to quickly compute $D(s)$ we obtain the values of the coefficients $c(m)$ using Rader's FFT algorithm [Rad68] applied to the characteristic function of the set $F(m)$. Indeed, every $c(m)$ is defined as the (non-normalised) Fourier transform of the characteristic function $\mathbb{1}_{F(m)}$ of the set $F(m)$. Computing the fast Fourier transform is the most expensive step of the algorithm, taking time $O(p \log p)$. Since there are $O\left(\frac{M}{\log M}\right)$ primes up to M (this remains true also restricting to the congruence classes $2, 5 \bmod 9$), the asymptotic complexity of the algorithm is $O(M^2)$. For $M = 1.03 \cdot 10^5$, the run time of our implementation [FL23a] is of a few hours on modest hardware. □

Remark 5.4.18. It is important to notice that the value of $D(s)$ depends on the choice of ε (see equation (0.1)). All the calculations in this section, including

in particular that of Lemma 5.4.17, are performed by taking as ε the image in $\mathbb{F}_p$ of the least positive integer which is a quadratic non-residue modulo p.

Remark 5.4.19. For the computationally accessible values of M, one can check that the optimal $C(M)$ grows very slowly: for example, $C(10^4) \approx 3.789$, $C(10^5) \approx 4.246$ and $C(10^6) \approx 5.169$.

Remark 5.4.20. The choice of the form of the bound in Lemma 5.4.17 is supported by the following heuristics. We assume that the coefficients $c(m)$ are pseudo-random values in the interval $\left[-\frac{4}{3}\sqrt{p}, \frac{4}{3}\sqrt{p}\right]$. Since $\sigma_{-1}(m) = \sum_{k|m} \frac{1}{k} = O(\log\log m)$, the quantity $D(s)$ is the sum of s random values in the interval $\left[-\alpha\sqrt{p}\log\log s, \alpha\sqrt{p}\log\log s\right]$ for some constant α, so we expect it to be $O(\sqrt{ps}(\log\log s)^2)$. By taking small values of p (for example, $p < 103000$) and $s < p$, we can essentially treat $(\log\log s)^2$ as a constant.

In the regime $s \geq p$, it will be enough to use the following easier upper bound on $D(s)$:

Lemma 5.4.21. *Let p be a prime and let $s \geq p$ be an integer. We have $|D(s)| < \frac{2\pi^2}{9} s\sqrt{p}$.*

Proof. It suffices to note that by Lemma 5.4.8 we have

$$|D(s)| \leq \sum_{\substack{m \leq s \\ m \not\equiv 0 (p)}} \sum_{k|m} \frac{|c(m)|}{k} \leq \frac{4}{3}\sqrt{p} \sum_{k=1}^{s} \sum_{\ell=1}^{\lfloor \frac{s}{k} \rfloor} \frac{1}{k} \leq \frac{4}{3}\sqrt{p} \sum_{k=1}^{s} \frac{s}{k^2} < \frac{4\pi^2}{18} s\sqrt{p}.$$

□

We now combine these results to prove the following.

Proposition 5.4.22. *Let E, p, q be as in Proposition 5.4.5 and let R be as in Definition 5.4.2. Let $D(s)$ be as in equation* (5.4.8) *and let C be the minimum constant such that $|D(s)| \leq C\sqrt{ps}$ for $s < p$. If $x := |\log|q|| \geq 30$, then*

$$|\log|R|| \leq \frac{6Cp\sqrt{\pi}}{x^{\frac{1}{2}}} \cdot 1.28 + \frac{10}{3}\pi^2 e^{-x} p\sqrt{p} + \frac{4(p+1)\pi^2}{3px}.$$

Proof. Since $2\pi\Im\tau = |\log|q|| \geq 30$, we know that $\Im\tau > 1$, and hence we may also assume that τ is in the standard fundamental domain $\mathcal{F}$ for the action of $\mathrm{SL}_2(\mathbb{Z})$, since every fundamental domain containing such a τ is obtained as $\mathcal{F} + n$ for $n \in \mathbb{Z}$, but integer translations do not change the value of q. We start by estimating the sum S defined in equation (5.4.7), dividing it into two

parts. Using Lemmas 5.4.17 and 5.4.21 we obtain

$$\begin{aligned} |S| &\leq 12\,|1-q^{\frac{1}{p}}| \sum_{s=1}^{\infty} |q|^{\frac{s}{p}} |D(s)| \\ &\leq 12C\sqrt{p}\,|1-q^{\frac{1}{p}}| \sum_{s=1}^{p-1} |q|^{\frac{s}{p}}\sqrt{s} \;+\; \frac{8}{3}\pi^2\sqrt{p}\,|1-q^{\frac{1}{p}}| \sum_{s=p}^{\infty} |q|^{\frac{s}{p}} s. \end{aligned} \tag{5.4.9}$$

We now use the following elementary fact: if $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a differentiable function with a single local maximum in $x_0 \in \mathbb{R}_{\geq 0}$, then

$$\sum_{n=1}^{\infty} f(n) < \int_1^{\infty} f(x)dx + f(x_0).$$

Since $\frac{d}{ds}(|q|^{\frac{s}{p}}\sqrt{s}) = |q|^{\frac{s}{p}}\sqrt{s}\left(\log|q|^{\frac{1}{p}} + \frac{1}{2s}\right)$, the function $|q|^{\frac{s}{p}}\sqrt{s}$ is increasing for $s \leq -\frac{1}{2\log|q|^{1/p}} = \frac{p}{2|\log|q||}$ and decreasing for larger values of s. We then have the following estimate:

$$\begin{aligned} \sum_{s=1}^{p-1} |q|^{\frac{s}{p}}\sqrt{s} < \sum_{s=1}^{\infty} |q|^{\frac{s}{p}}\sqrt{s} &< \int_1^{\infty} |q|^{\frac{s}{p}}\sqrt{s}\,ds + |q|^{\frac{1}{2|\log|q||}}\sqrt{\frac{p}{2|\log|q||}} \\ &< \int_0^{\infty} e^{-\frac{|\log|q||}{p}s}\sqrt{s}\,ds + e^{-\frac{1}{2}}\sqrt{\frac{p}{2|\log|q||}} \\ &= \frac{p\sqrt{p}}{|\log|q||^{\frac{3}{2}}}\frac{\sqrt{\pi}}{2}\left(1 + \frac{\sqrt{2}|\log|q||}{p\sqrt{\pi e}}\right). \end{aligned}$$

Using Proposition 5.4.5, and using the fact that by Remark 5.4.14 we can assume $p > 100$, we have

$$\frac{|\log|q||}{p} < \frac{2\sqrt{2}\,\pi\cdot 101}{10\sqrt{102}\,p^{\frac{3}{4}}} + \frac{1.65}{p} \leq \frac{2\sqrt{2}\,\pi\cdot\sqrt[4]{101}}{10\sqrt{102}} + \frac{1.65}{101} < 0.3,$$

and so

$$\sum_{s=1}^{p-1} |q|^{\frac{s}{p}}\sqrt{s} < \frac{p\sqrt{p}}{|\log|q||^{\frac{3}{2}}}\frac{\sqrt{\pi}}{2}\cdot 1.15.$$

To estimate the sum of the terms with $s \geq p$, we use the following fact. If $x \in (0,1)$, then

$$\sum_{s=p}^{\infty} x^s s = x\frac{d}{dx}\sum_{s=p}^{\infty} x^s = x\frac{d}{dx}\frac{x^p}{1-x} = x^p\left(\frac{p}{1-x} + \frac{x}{(1-x)^2}\right).$$

Putting everything together, equation (5.4.9) yields

$$|S| \leq 6Cp\sqrt{p}\,|1-q^{\frac{1}{p}}|\frac{\sqrt{\pi p}}{|\log|q||^{\frac{3}{2}}}\cdot 1.15+\frac{8}{3}\pi^2|q|\sqrt{p}\,|1-q^{\frac{1}{p}}|\left(\frac{p}{1-|q|^{\frac{1}{p}}}+\frac{|q|^{\frac{1}{p}}}{(1-|q|^{\frac{1}{p}})^2}\right).$$

Applying Lemmas 1.1.2 and 1.1.3 we obtain

$$\begin{aligned}|S| &\leq 6Cp\sqrt{p}\left(\frac{|\log|q||}{p}+\frac{\pi}{p}\right)\frac{\sqrt{\pi p}}{|\log|q||^{\frac{3}{2}}}\cdot 1.15\\ &\quad+\frac{8}{3}\pi^2|q|\sqrt{p}\left(1-|q|^{\frac{1}{p}}+|q|^{\frac{1}{2p}}\frac{\pi}{p}\right)\left(\frac{p}{1-|q|^{\frac{1}{p}}}+\frac{|q|^{\frac{1}{p}}}{(1-|q|^{\frac{1}{p}})^2}\right),\end{aligned}$$

which we rewrite as

$$\begin{aligned}|S| &\leq \frac{6Cp\sqrt{\pi}}{|\log|q||^{\frac{1}{2}}}\cdot 1.15\left(1+\frac{\pi}{|\log|q||}\right)\\ &\quad+\frac{8}{3}\pi^2|q|\sqrt{p}\left(1+\frac{|q|^{\frac{1}{2p}}}{1-|q|^{\frac{1}{p}}}\cdot\frac{\pi}{p}\right)\left(p+\frac{|q|^{\frac{1}{p}}}{1-|q|^{\frac{1}{p}}}\right).\end{aligned}$$

Using Lemma 1.1.3 again we have

$$\frac{|q|^{\frac{1}{2p}}}{1-|q|^{\frac{1}{p}}}=\frac{|q|^{\frac{1}{2p}}}{(1-|q|^{\frac{1}{2p}})(1+|q|^{\frac{1}{2p}})}<\frac{1}{1+|q|^{\frac{1}{2p}}}\cdot\frac{2p}{|\log|q||}<\frac{2p}{|\log|q||},$$

and using the assumption $|\log|q|| \geq 30$ we obtain

$$\begin{aligned}|S| &< \frac{6Cp\sqrt{\pi}}{|\log|q||^{\frac{1}{2}}}\cdot 1.28+\frac{8}{3}\pi^2|q|\sqrt{p}\left(1+\frac{2\pi}{|\log|q||}\right)\left(p+\frac{p}{|\log|q||}\right)\\ &\leq \frac{6Cp\sqrt{\pi}}{|\log|q||^{\frac{1}{2}}}\cdot 1.28+\frac{8}{3}\pi^2|q|p\sqrt{p}\cdot 1.25.\end{aligned}$$

Bounding the sums in equation (5.4.5) and recalling equation (5.4.6), we have obtained

$$|\log|R|| \leq \frac{6Cp\sqrt{\pi}}{x^{\frac{1}{2}}}\cdot 1.28+\frac{10}{3}\pi^2|q|p\sqrt{p}+\frac{4(p+1)\pi^2}{3px},$$

which concludes the proof (recalling that $x=|\log|q||$). □

Corollary 5.4.23. *Let E, p, q be as in Corollary 5.4.15 and let R be as in Definition 5.4.2. If $|\log|q|| \geq 30$, then*

$$|\log|R|| \leq 58\cdot\frac{p}{|\log|q||^{\frac{1}{2}}}+0.45.$$

Proof. By Proposition 3.2.14 we have $p^4 \mid j(E)$, and Theorem 1.2.2 implies first $30 \leq x \leq \log(|j(E)| + 970.8)$, so $|j(E)| > 3500$, and then $|j(E)| \leq \frac{2}{|q|}$. Therefore, we have $p^4|q| \leq |j(E)| \cdot |q| \leq 2$. By Proposition 5.4.22 we obtain

$$|\log|R|| \leq \frac{6Cp\sqrt{\pi}}{x^{\frac{1}{2}}} \cdot 1.28 + \frac{20\pi^2}{3p^2\sqrt{p}} + \frac{4(p+1)\pi^2}{3px}.$$

The result follows by using $C \leq 4.25$ (Lemma 5.4.17, which we can use thanks to Corollary 5.4.15), $x \geq 30$ and $p > 100$ (which we can assume by Remark 5.4.14). □

We now notice that all the arguments we applied to $\log R$ are also valid for $\log R_\gamma$. We can then give an analogue of Corollary 5.4.23 for $\log R_\gamma$. As before, we have

$$\begin{aligned}\log R_\gamma &= -12 \sum_{n,k \not\equiv 0(p)} \frac{q^{\frac{nk}{p}}}{k} \cdot c_\gamma(kn) - \frac{4(p+1)}{p} \sum_{n \not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{nk}}{k} \\ &= -12 \sum_{s=1}^{\infty} (q^{\frac{s}{p}} - q^{\frac{s+1}{p}}) D_\gamma(s) - \frac{4(p+1)}{p} \sum_{n \not\equiv 0(p)} \sum_{k=1}^{\infty} \frac{q^{nk}}{k},\end{aligned}$$

where

$$D_\gamma(s) := \sum_{\substack{m \leq s \\ m \not\equiv 0(p)}} \sum_{k \mid m} \frac{c_\gamma(m)}{k}$$

is an analogue of $D(s)$ in this context.

Lemma 5.4.24. *For every prime $p < 103000$ with $p \equiv 2, 5 \pmod 9$, the following hold:*

1. *for $s < p$, we have $|D_\gamma(s)| < C_\gamma\sqrt{ps}$ with $C_\gamma = 2.81$.*
2. *for $s \geq p$, we have $|D_\gamma(s)| < \frac{2\pi^2}{9} s\sqrt{p}$.*

Proof. The proof is analogous to those of Lemmas 5.4.17 and 5.4.21. □

Reasoning as in the proof of Proposition 5.4.22 we obtain the following.

Proposition 5.4.25. *Let E, p, q be as in Proposition 5.4.5 and let R_γ be as in equation (5.4.2). Let C_γ be the minimum constant such that $|D_\gamma(s)| \leq C_\gamma\sqrt{ps}$ for $s < p$. If $x := |\log|q|| \geq 30$, then*

$$|\log|R_\gamma|| \leq \frac{6C_\gamma p\sqrt{\pi}}{x^{\frac{1}{2}}} \cdot 1.28 + \frac{10}{3}\pi^2 e^{-x} p\sqrt{p} + \frac{2(p+1)\pi^2}{3px}.$$

Since we know that it suffices to consider primes up to 103000 (Corollary 5.4.15), we can use the bound on the value of C_γ provided by Lemma 5.4.24 to obtain the following numerical estimate.

Corollary 5.4.26. *Let E, p, q be as in Corollary 5.4.15 and let R_γ be as in equation* (5.4.2)*. If $|\log|q|| \geq 30$, then*

$$|\log|R_\gamma|| \leq 38.26 \cdot \frac{p}{|\log|q||^{\frac{1}{2}}} + 0.23.$$

We can finally prove the main result of this section.

Proof of Proposition 5.4.16. Suppose $|\log|q|| \geq 30$. As in the previous section, from the two possible equations

$$\log|U| = \mathrm{Ord}_q(U)\log|q| + 6\log p + \log|R|$$
$$\log|U \circ \gamma| = \mathrm{Ord}_q(U \circ \gamma)\log|q| + \log|R_\gamma|$$

we obtain the inequalities

$$\frac{p^2-1}{3p}|\log|q|| \leq 6\log p + |\log|R||,$$
$$\frac{p^2-1}{6p}|\log|q|| \leq 6\log p + |\log|R_\gamma||.$$

Comparing Corollary 5.4.23 with Corollary 5.4.26 we notice that it suffices to consider the second inequality. Writing $x = |\log|q||$ we have

$$\frac{p^2-1}{6p}x \leq 6\log p + 38.26\frac{p}{\sqrt{x}} + 0.23.$$

By Remark 5.4.14 we can assume that $p > 100$, hence

$$x\sqrt{x} - 2\sqrt{x} - 230 \leq 0,$$

which implies $x < 39$. □

Conclusion of the proof of Theorems 8 and 9

We recall the statement of Theorem 9 (Theorem 8 follows): there exists no pair (E, p), where E is an elliptic curve over $\mathbb{Q}$ without CM and $p > 5$ is a prime for which the image of the representation $\rho_{E,p}$ is the group $G(p)$ (up to conjugacy). Suppose by contradiction that such a pair exists. We consider the base change of E to $\mathbb{C}$ (along the unique embedding $\mathbb{Q} \hookrightarrow \mathbb{C}$). There is a unique τ in the standard fundamental domain $\mathcal{F}$ of the upper half plane $\mathcal{H}$ that corresponds to $E(\mathbb{C})$; we set $q = e^{2\pi i\tau}$. In this setting, in the previous sections we have proved the following properties:

- $j(E)$ is an integer: follows from Lemma 1.1.5;
- $p \equiv 2, 5 \pmod 9$: follows from Theorem 3.1.4;
- $p^4 \mid j(E)$: follows from Proposition 3.2.14;
- $|j(E)| \leq 2 \cdot e^{39}$: follows from Proposition 5.4.16 and Theorem 1.2.2;
- $p < 20400$: we know that $p^4 \leq |j(E)| \leq 2 \cdot e^{39}$, hence $p \leq \sqrt[4]{2} \cdot e^{\frac{39}{4}} < 20400$;
- $j(E) = p^d \cdot c^3$ for $d \in \{4, 5\}$ and $c \in \mathbb{Z}$: by Lemma 3.1.7, we know that $j(E) = p^d \cdot c^3$, and by Proposition 3.2.14 we also know that $d \geq 4$. We can assume that $d \in \{4, 5, 6\}$, since higher exponents can be reduced modulo 3 by reabsorbing the factors of p in c^3. Moreover, by Lemma 3.2.15 the case $d = 6$ does not occur, hence we can assume that $d \in \{4, 5\}$.

To complete the proof of Theorem 8 and Theorem 9, we check directly, for all primes $p < 20400$, whether there exists any pair (E, p) as above. To be able to test a finite number of curves, we also need the following well-known lemma.

Lemma 5.4.27. *If E and E' are two non-CM elliptic curves over $\mathbb{Q}$ with $j(E) = j(E')$, $p > 2$ is a prime, and $H \subseteq \mathrm{GL}(E[p])$ is a subgroup that contains $-\mathrm{Id}$, then $\mathrm{Im}\,\rho_{E,p} \subseteq H$ if and only if $\mathrm{Im}\,\rho_{E',p} \subseteq H$.*

Proof. Since either $E' \cong E$ or E' is a quadratic twist of E, the statement follows from [Sut16, Corollary 5.25]. □

We now proceed as follows (see [FL23a]):

1. For every odd prime $p \equiv 2, 5 \pmod 9$ with $5 < p < 20400$, every $d \in \{4, 5\}$ and every integer $c \neq 0$ in the interval $\left[-\sqrt[3]{2} \cdot e^{13} p^{-\frac{d}{3}}, \sqrt[3]{2} \cdot e^{13} p^{-\frac{d}{3}}\right]$, we take an integral model $\mathcal{E}$ of a curve $E/\mathbb{Q}$ with j-invariant $j(E) = p^d \cdot c^3$.

2. We loop over primes ℓ distinct from p, in increasing order. For each such prime ℓ:

   a) We check if $\mathcal{E}$ has good reduction at ℓ. If it does, we continue with (b); otherwise, we move on to the next prime ℓ.

   b) We compute $a_\ell = \ell + 1 - |\widetilde{\mathcal{E}}(\mathbb{F}_\ell)|$ by counting the $\mathbb{F}_\ell$-rational points of $\mathcal{E}$ modulo ℓ.

c) We check whether the roots of the polynomial $t^2 - a_\ell t + \ell \in \mathbb{F}_p[t]$ are cubes in $\mathbb{F}_{p^2}^\times$ (note that $\lambda \in \mathbb{F}_{p^2}^\times$ is a cube if and only if $\lambda^{\frac{p^2-1}{3}} = 1$). If they are cubes, we continue with the next prime ℓ. If they are not, we mark $j(E) = p^d \cdot c^3$ as *ruled out* and continue with the next candidate (p, d, c).

The algorithm terminates, in the sense that every candidate j-invariant is marked as *ruled out*: the loop in step 2 is always broken by finding some prime ℓ (in fact, $\ell < 200$ in all cases) for which the roots of $t^2 - a_\ell t + \ell$ are not cubes in $\mathbb{F}_{p^2}^\times$. We claim that this proves Theorem 8. Indeed, suppose by contradiction that there exists a pair (E_1, p) such that E_1 is a non-CM elliptic curve over $\mathbb{Q}$ and p is a prime for which $\operatorname{Im}\rho_{E_1,p}$ is conjugate to $G(p)$. Then, by the discussion above we know that $j(E_1)$ is of the form $p^d \cdot c^3$ for some p, d, c satisfying the conditions in step 1 (note that $j = 0$ gives a CM elliptic curve), so the curve E we construct in this step is a quadratic twist of E_1. By Lemma 5.4.27, the image of $\rho_{E,p}$ is conjugate to a subgroup of $G(p)$ (note that $-\operatorname{Id} \in G(p)$), and by fixing a basis, we can assume that it is in fact contained in $G(p)$.

On the other hand, let ℓ be a prime for which the roots of $t^2 - a_\ell t + \ell$ are not cubes in $\mathbb{F}_{p^2}^\times$ (the output of the algorithm shows that such a prime exists), and let $F_\ell \in \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ be a Frobenius corresponding to ℓ. The element $\rho_{E,p}(F_\ell)$ has characteristic polynomial $t^2 - a_\ell t + \ell$. Since $\rho_{E,p}(F_\ell)$ is in $G(p)$, it satisfies at least one of the following: $a_\ell = 0$ (if $\rho_{E,p}(F_\ell)$ lies in the normaliser $C_{ns}^+(p)$, but not in the Cartan $C_{ns}(p)$ itself), or $\rho_{E,p}(F_\ell)$ is the cube of some element g_ℓ in $\mathrm{GL}_2(\mathbb{F}_p)$ (if it lies in the subgroup of cubes of $C_{ns}(p)$). In both cases, the eigenvalues of $\rho_{E,p}(F_\ell)$ are cubes in $\mathbb{F}_{p^2}^\times$: if $a_\ell = 0$, this follows from the fact that the roots of the characteristic polynomial are $\pm\sqrt{-\ell}$, and $-\ell$ is a cube in $\mathbb{F}_p^\times$ since $p \equiv 2 \pmod 3$; if $a_\ell \neq 0$, it follows from the fact that the eigenvalues of $\rho_{E,p}(F_\ell)$ are the cubes of the eigenvalues of g_ℓ. However, the choice of ℓ shows that the eigenvalues of $\rho_{E,p}(F_\ell)$ are *not* cubes in $\mathbb{F}_{p^2}^\times$: the contradiction shows that the pair (E_1, p) cannot exist, which concludes the proof of Theorem 8.

To conclude the proof of Theorem 9 it suffices to notice that for $p = 5$ there are many curves E for which $\operatorname{Im}\rho_{E,5}$ is conjugate to $G(5)$, as suggested by [Zyw15a, Theorem 1.4 (ii)] (for example the curve $y^2 = x^3 - 950x - 11480$, with LMFDB label 70400.bg1).

Remark 5.4.28. Our algorithm [FL23a] terminates in around 2 minutes. Since the running time is clearly exponential in the bound on $\log|j(E)|$, it would have been impossible to carry out this calculation without a sharp absolute bound on $\log|q|$, such as that given by Proposition 5.4.16. To showcase the sharpness of our bound, we point out that even just knowing $\log|j(E)| < 50$

would have led to a perfectly tractable computation: our algorithms test all j with $\log|j| < 50$ in about an hour and a half. On the other hand, it is clear that the bound $\log|j(E)| < 162$ which follows from Proposition 5.4.5 and Corollary 5.4.15 would have been too loose to carry out the final calculation as described in this section. Indeed, knowing $\log|j(E)| < 39$ we have to test 645552 pairs (j-invariant, prime); with only $\log|j(E)| < 50$ the number rises to $\approx 2.8 \cdot 10^7$, and with $\log|j(E)| < 162$ to $\approx 4.6 \cdot 10^{23}$.

CHAPTER 6

p-adic and adelic Galois representations

Given an elliptic curve $E/\mathbb{Q}$ without complex multiplication and a prime number p, the main aim of this chapter is to study the image of the p-adic Galois representations ρ_{E,p^∞} attached to E, as well as the adelic representation ρ_E. In particular, we will focus on the case where $\rho_{E,p}$ has image contained in the normaliser of a non-split Cartan subgroup. This is the only case not covered by Theorem 12 (apart from the curve `49.196.9.1`). We will show that, thanks to the classification given in Chapter 2, if n is the smallest integer for which $\operatorname{Im}\rho_{E,p^\infty} \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$, then the image of ρ_{E,p^n} is exactly $C_{ns}^+(p^n)$ in almost all cases. This allows us to obtain the precise value of the p-adic index $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}]$ depending on n. Using Theorem 4.2.5 we are then able to give a bound on the product of the p-adic indices in terms of the stable Faltings height of the curve E.

We also give a bound on the index of the adelic representation ρ_E. To do this, we study the entanglement of division fields at primes p for which the image of $\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup. This allows us to give a bound on the adelic index in terms of the product of the p-adic indices. The main ingredient to obtain a good bound is the study of the ramification index of p in $\mathbb{Q}(E[p^n])$. Indeed, when the image of ρ_{E,p^n} is contained in the normaliser of a non-split Cartan subgroup, p is 'almost totally' ramified in $\mathbb{Q}(E[p])$. On the other hand, by Theorem 3.1.1 we know that the ramification index of p in $\mathbb{Q}(E[N])$ for $p \nmid N$ is low. This shows that the intersection $\mathbb{Q}(E[p]) \cap \mathbb{Q}(E[N])$ is small. The ramification arguments rely on the work of Lozano-Robledo [LR16] and Smith [Smi23]. All these properties are proved in Section 6.3.

The entanglement properties of Section 6.3 are combined in Lemma 6.4.10, which together with the effective surjectivity Theorem 4.2.5, gives a bound on the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E]$ in terms of the Faltings height $\mathrm{h}_{\mathcal{F}}(E)$. We then conclude this chapter providing another bound on the adelic index in terms of the conductor of E.

6.1 Images of p-adic Galois representations

Fix an elliptic curve $E/\mathbb{Q}$ and an odd prime p, and write $G := \operatorname{Im}\rho_{E,p^\infty}$ and $S := G \cap \mathrm{SL}_2(\mathbb{Z}_p)$. The aim of this section is to show that G is often an N-Cartan lift (as defined in Chapter 2), and that in this case many of the propositions of Chapter 2 apply. We start by proving the following.

Proposition 6.1.1. *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let p be an odd prime such that $G(p) \subseteq C_{ns}^+(p)$. Then the group G is a non-split N-Cartan lift.*

Proof. Since $\det \circ \rho_{E,p^\infty}$ is the p-adic cyclotomic character, it follows that $\det(G) = \mathbb{Z}_p^\times$. By [Ser81, Lemme 17] we know that $G(p) \not\subset C_{ns}(p)$. By the open image theorem ([Ser72, Section 4.4, Théorème 3]) we know that G is open in $\mathrm{GL}_2(\mathbb{Z}_p)$, and hence it is closed. Finally, we need to show that $G(p) \cap C_{ns}(p)$ contains an element which is not a multiple of the identity. It is easy to notice that every element in $C_{ns}^+(p) \setminus C_{ns}(p)$ has order dividing $2(p-1)$, and the same holds for scalar matrices. Suppose by contradiction that $G(p) \cap C_{ns}(p)$ consists of multiples of the identity. In particular, every element of $G(p)$ has order dividing $2(p-1)$. Suppose now that $p > 11$. By Corollary 3.1.3 we know that E has potentially good reduction at p. If we consider the subgroup $I < \operatorname{Im}\rho_{E,p}$ obtained as the image of a pro-p inertia subgroup of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, by Theorem 3.1.1, Theorem 3.2.9 and Lemma 3.2.8 we know that there exists $e \in \{1,2,3,4,6\}$ such that either I contains an element of order $\frac{p^2-1}{e}$, or the image of I in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order $\frac{p-1}{e}$. In the former case, we get a contradiction, because $\frac{p^2-1}{e} \nmid 2(p-1)$ for $p > 11$. In the latter case, since the square of any element of $C_{ns}^+(p) \setminus C_{ns}(p)$ is a scalar matrix, we have that $\frac{p-1}{e} \mid 2$. However, this can happen only for $p = 13$, which does not occur by [BDM$^+$19, Corollary 1.3]. To conclude, it suffices to notice that for $p \in \{3,5,7,11\}$ the statement follows from [Zyw15a, Theorems 1.2, 1.4, 1.5, 1.6]. □

For $G = \operatorname{Im}\rho_{E,p^\infty}$ consider the Lie algebras $\mathfrak{g}_i$ as in Definition 2.1.3.

Lemma 6.1.2. *Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime such that $G(p) \subseteq C_{ns}^+(p)$. We have $\dim \mathfrak{g}_n \geq 2$ for every $n \geq 1$.*

Lemma 6.1.2 is the same as [Ejd22, Proposition 3.2], however, our version also holds for $p \in \{3, 5, 7, 13\}$. For every prime $p > 7$ and $p \neq 13$, this is a consequence of the fact that if $G(p) \subseteq C_{ns}^{+}(p)$, then E has potentially good supersingular reduction at p (Corollary 3.2.13). To treat the remaining primes, we first prove the following lemma.

Lemma 6.1.3. *Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime such that E has potentially good ordinary reduction at p. If $p \geq 5$, we have $G(p^2) \not\subseteq C_{ns}^{+}(p^2)$. If $p = 3$, we have $G(27) \not\subseteq C_{ns}^{+}(27)$; moreover, if E has good ordinary reduction at 3 we have $G(9) \not\subseteq C_{ns}^{+}(9)$.*

Proof. Let $\mathbb{Q}_p^{nr}$ be the maximal unramified extension of $\mathbb{Q}_p$ and let K be the minimal extension of $\mathbb{Q}_p^{nr}$ over which E acquires good reduction. By Theorem 3.1.1 we know that $e := [K : \mathbb{Q}_p^{nr}] \in \{1, 2, 3, 4, 6, 12\}$. Let $I_K < \mathrm{Gal}\left(\overline{K}/K\right)$ be the inertia subgroup. By Lemma 3.2.7 we know that I_K acts on $E[p^n]$ as $\begin{pmatrix} \chi_{p^n} & * \\ 0 & 1 \end{pmatrix}$, where χ_{p^n} is the cyclotomic character modulo p^n. Suppose first that $p > 3$. If we consider $n = 2$, since $(e, p) = 1$ we notice that $p + 1 \in \mathrm{Im}\,\chi_{p^2} = \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times e}$. In particular, there exists an element g in $\rho_{E,p^2}(I_K)$ conjugate to $\begin{pmatrix} p+1 & k \\ 0 & 1 \end{pmatrix}$ that satisfies the polynomial equation $(g-1)(g-p-1) = 0$. Suppose by contradiction that $g \in C_{ns}^{+}(p^2)$. It is easy to check that $g \equiv I \pmod{p}$, and so also $k \equiv 0 \pmod{p}$. In particular, if we write $k = ph$ we have

$$\begin{pmatrix} p+1 & k \\ 0 & 1 \end{pmatrix} = I + p\begin{pmatrix} 1 & h \\ 0 & 0 \end{pmatrix} = I + pA.$$

By Proposition 6.1.1 we know that G is an N-Cartan lift, and by Remark 2.1.8 A must be conjugate to an element of $V_1 \oplus V_2$ described in Lemma 2.1.7. However, A has rank 1, which is impossible as elements of $V_1 \oplus V_2$ only have rank 0 or 2. Suppose now that $p = 3$: then either E has good reduction at 3, so we have $e = 1$ and we can repeat the same proof as for $p > 3$, or E has bad reduction at 3. In the latter case, since $v_3(e) \leq 1$, we notice that $3^2 + 1 \in \mathrm{Im}\,\chi_{27}$, and hence there is an element $g \in \rho_{E,27}(I_K)$ conjugate to $\begin{pmatrix} 3^2+1 & k \\ 0 & 1 \end{pmatrix}$. Suppose that $g \in C_{ns}^{+}(27)$. We see as before that $k \equiv 0 \pmod{3}$ and if $k \not\equiv 0 \pmod{9}$ we would have a non-zero element of the form

$\begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix}$ in $\mathfrak{g}_1$, which is impossible. We then conclude as before that we have an element conjugate to $\begin{pmatrix} 1 & h \\ 0 & 0 \end{pmatrix}$ inside $V_1 \oplus V_2$, which is impossible. □

Proof of Lemma 6.1.2. By Corollary 2.1.11 we know that $V_1 \subseteq \mathfrak{g}_1$, and hence $\dim \mathfrak{g}_1 > 0$. Suppose by contradiction that $\dim \mathfrak{g}_1 = 1$, and so that $\mathfrak{g}_1 = V_1$. By Proposition 1.3.2 we know that there exists a lift $\widetilde{G(p)} < G$ of $G(p)$ isomorphic to it via the projection such that $G = \widetilde{G(p)}G_1$, and up to conjugation of G in $\mathrm{GL}_2(\mathbb{Z}_p)$ we can assume that $\widetilde{G(p)} < C_{ns}^+$. Since $\mathfrak{g}_1 = V_1$, modulo p^2 we obtain that $G(p^2) = \widetilde{G(p)} \cdot \{(1 + p\alpha)I\}_{\alpha \in \mathbb{F}_p} < C_{ns}^+(p^2)$ and $[C_{ns}^+(p^2) : G(p^2)] = p$. If $p = 3$, the curve E corresponds to a rational point on [LMF24, Modular Curve 9.81.1.a.1], with equation $x^3 - 6x^2y + 3x^2z + 6xyz - 6xz^2 - y^3 - 6yz^2 + z^3 = 0$ in $\mathbb{P}^2$. However, this equation has no solutions modulo 27, and hence such a curve E does not exist. If instead $p > 3$, by Corollary 3.1.3, we know that the curve E has potentially good reduction modulo p. If E has potentially ordinary reduction at p, we can apply Lemma 6.1.3 to get a contradiction. If E has potentially supersingular reduction at p, we can use Proposition 3.2.9 to show that E does not have a canonical subgroup of order p, and so by [Smi23, Theorem 1.1] we have that if $R \in E[p^2] \setminus E[p]$, then $p^2 \mid [\mathbb{Q}(R) : \mathbb{Q}] \mid [\mathbb{Q}(E[p^2]) : \mathbb{Q}]$. We know that $|\mathfrak{g}_1| = [\mathbb{Q}(E[p^2]) : \mathbb{Q}(E[p])] = \frac{[\mathbb{Q}(E[p^2]):\mathbb{Q}]}{[\mathbb{Q}(E[p]):\mathbb{Q}]}$, and since $p \nmid [\mathbb{Q}(E[p]) : \mathbb{Q}]$ we obtain that $p^2 \mid |\mathfrak{g}_1|$. The conclusion follows from Lemma 2.1.4. □

Remark 6.1.4. In the proof above, the statement about ramification in division fields that allows us to show that $p^2 \mid [\mathbb{Q}(R) : \mathbb{Q}]$ is due to Lozano-Robledo [LR16, Theorem 1.2(2)]. However, as pointed out in [Smi23], his proof is incorrect. A correct version is provided in [Smi23, Theorem 1.1], which is the same we used in the proof.

Theorem 6.1.5. *Let $E/\mathbb{Q}$ be an elliptic curve without CM and set $G := \operatorname{Im} \rho_{E,p^\infty}$. Let p be an odd prime such that $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$ up to conjugation and let $n \geq 1$ be the smallest integer such that $\operatorname{Im} \rho_{E,p^\infty} \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$. One of the following holds:*

- *$G(p^n) = C_{ns}^+(p^n)$ up to conjugation.*
- *$n = 2$ and*

$$G(p^2) \cong C_{ns}^+(p) \ltimes \left\{ I + p \begin{pmatrix} a & \varepsilon b \\ -b & c \end{pmatrix} \right\},$$

with the semidirect product defined by the conjugation action.

- *$p = 5$ and G corresponds to the group with RSZB label* `5.30.0.2`.
- *$p = 3$ and $\pm G$ corresponds to one of the groups with RSZB labels* `3.6.0.1`, `3.12.0.1`, `9.18.0.1`, `9.18.0.2`, `9.36.0.1`, `9.36.0.2`, `9.36.0.3`.

Proof. We show that G satisfies the hypotheses of Theorem 2.1.14. First, we know by Proposition 6.1.1 that G is a non-split N-Cartan lift. By Lemma 6.1.2 we also know that $\dim \mathfrak{g}_1 > 1$. Moreover, by [LT22, Theorem 3.16] we know that for $p > 3$ we have $G \supseteq (1 + p\mathbb{Z}_p)I$.
Suppose first that $p > 5$. By Theorem 9 we know that $G(p) = C_{ns}^+(p)$, and hence the image of $G(p) \cap C_{ns}(p) = C_{ns}(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ contains an element of order greater than 2. We can then apply Theorem 2.1.14. As $G \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$, we have either $G(p^n) \subseteq C_{ns}^+(p^n)$ with $[C_{ns}^+(p^n) : G(p^n)] = [C_{ns}^+(p) : G(p)] = 1$, or $n = 2$ and $G(p^n) \cong G(p) \ltimes (V_1 \oplus V_3)$, and the conclusion follows.
If $p = 5$, then by Theorem 9 we have $[C_{ns}^+(p) : G(p)] \in \{1, 3\}$. If $G(p) = C_{ns}^+(p)$, we can repeat the argument above. If instead $[C_{ns}^+(p) : G(p)] = 3$, the argument above does not work anymore, because every element of $G(p) \cap C_{ns}(p)$ has order 2 in $\mathrm{PGL}_2(\mathbb{F}_p)$. Using [RSZB22, Theorem 1.6] we see that either G corresponds to a modular curve with infinitely many rational points, or $G(25) \subseteq C_{ns}^+(25)$, or G has RSZB label `25.50.2.1` or `25.75.2.1`. In the last case, we see that $G(5) \in \{C_{sp}^+(5), C_{ns}^+(5)\}$, and so we don't have $[C_{ns}^+(p) : G(p)] = 3$. In the first case we can check in [SZ17, Table 2] that the only possible case is the group with RSZB label `5.30.0.2`: indeed, this is the unique group with $G(5)$ contained in $C_{ns}^+(5)$ and index of the form $30 \cdot 5^k$. If $G(25) \subseteq C_{ns}^+(25)$, then G must be contained in the group with RSZB label `25.750.46.1`, which is, in turn, contained in the group with RSZB label `25.50.2.1`. However, this last group has been ruled out in [BDM$^+$23, Section 5.3]. Indeed, the modular curve associated with it has 2 rational points: one is a CM point, and the other corresponds to an elliptic curve with $G(5) = C_{ns}^+(5)$, as we can check in [RSZB22, Table 1].
If $p = 3$, by [Zyw15a, Theorem 1.2] we can consider the three following cases: $G(3) = C_{ns}^+(3)$, or $G(3) = C_{sp}^+(3)$, or $G(3)$ is contained in $C_{sp}(3)$. In the first case, we have that $E[3]$ is an irreducible Galois module, and then by [LT22, Proposition 3.12] we have again that $G \supseteq (1 + 3\mathbb{Z}_3)I$. Moreover, the image of $C_{ns}^+(3)$ in $\mathrm{PGL}_2(\mathbb{F}_3)$ contains an element of order 4, hence we can apply Theorem 2.1.14 and conclude as for $p > 5$. If $G(3) = C_{sp}^+(3)$, we can apply [RSZB22, Theorem 1.6] to show that either $G(9) \subset C_{ns}^+(9)$ or G appears in [SZ17, Table 1]. If $G(9) \subset C_{ns}^+(9)$, then $G(9)$ is contained in the group corresponding to the modular curve with RSZB label `9.54.2.2`, which has no non-cuspidal non-CM points by [RSZB22, Section 8.2]. If instead G appears in [SZ17, Table 1], we can notice that since $G(3) = C_{sp}^+(3)$ the index of G

must be of the form $6 \cdot 3^k$, and the only such groups in the table are those corresponding to the modular curves with RSZB labels `3.6.0.1`, `9.18.0.1`, `9.18.0.2`. Suppose now that $G(3) \subseteq C_{sp}(3)$. In particular, this implies that $G(3)$ is contained in a Borel subgroup, so $\pm G$ must correspond to a modular curve in the finite list given in [RSZB22, Corollary 1.1]. However, the only curves in the list for which $\pm G(3) \subseteq C_{sp}(3)$ are those with RSZB labels `3.12.0.1`, `9.36.0.1`, `9.36.0.2`, `9.36.0.3`. □

6.2 p-adic indices

In this section, we provide some bounds on the indices of the images of the p-adic Galois representations attached to E. In particular, we will mainly focus on the case where $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup.

Proposition 6.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let p be an odd prime such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$ up to conjugation, with equality holding in the case $p = 3$. Let $n \geq 1$ be the largest integer for which $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. We have*

$$[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] \in \begin{cases} \left\{\frac{p^2-p}{2}, \frac{p^3-p^2}{2}, 30\right\} & \text{for } n = 1 \\ \left\{\frac{p-1}{2} \cdot p^{2n-1}\right\} & \text{for } n > 1, \end{cases}$$

where $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] = 30$ for $p = 5$.

Proof. Suppose first that $\operatorname{Im}\rho_{E,p} = C_{ns}^+(p)$. This implies that we are in one of the first two cases of Theorem 6.1.5, and so if n is the smallest integer such that $\operatorname{Im}\rho_{E,p^\infty} \supseteq I + p^n M_{2\times 2}(\mathbb{Z}_p)$, then either $\operatorname{Im}\rho_{E,p^n} = C_{ns}^+(p^n)$, or $n = 2$ and $\operatorname{Im}\rho_{E,p^2}$ is a group of order $2(p^2-1)p^3$. In particular, we have that $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] \in \left\{\frac{p-1}{2} \cdot p^{2n-1}, \frac{p^3-p^2}{2}\right\}$. If instead $\operatorname{Im}\rho_{E,p} \subsetneq C_{ns}^+(p)$, by Theorem 6.1.5 we know that $p^n = 5$ and $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] = 30$. □

Corollary 6.2.2. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let p be an odd prime such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$ up to conjugation, with equality holding in the case $p = 3$. Let $n \geq 1$ be the largest integer for which $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. We have*

$$[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] \leq \frac{p-1}{2p} \cdot p^{3n}.$$

Proof. If $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] \neq 30$ the statement easily follows from Proposition 6.2.1. If instead $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im}\rho_{E,p^\infty}] = 30$, then $p^n = 5$ and $30 < \frac{5-1}{10} \cdot 5^3 = 50$. □

We now give two propositions to bound the p-adic index in some cases in which $\operatorname{Im}\rho_{E,p}$ is not contained in the normaliser of a non-split Cartan. These cases will be the only ones that can occur whenever there exists a large prime p for which $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$.

Proposition 6.2.3. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication that does not admit any rational 2-isogeny. Then either $[\mathrm{GL}_2(\mathbb{Z}_2) : \operatorname{Im}\rho_{E,2^\infty}]$ divides 32, or $j(E)$ is one among*

$$-\frac{3\cdot 18249920^3}{17^{16}},\ -\frac{7\cdot 1723187806080^3}{79^{16}}$$

and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] = 128$.

Proof. By [RZB15, Theorem 1.1], [RZB15, Corollary 1.3], and [RZB15, Remark 1.5] we know that either $j(E)$ is one among the two numbers in the statement, or the index $[\mathrm{GL}_2(\mathbb{Z}_2) : \operatorname{Im}\rho_{E,2^\infty}]$ divides 96. In the first case, we can compute the index of the adelic representation using the algorithm `FindOpenImage.m` developed in [Zyw22]. Indeed, by [Zyw15b, Corollary 2.3] we know that the index only depends on j-invariant. We now focus on the second case. Since E admits a rational 2-isogeny if and only if $\operatorname{Im}\rho_{E,2}$ is contained in a Borel subgroup, we notice that E admits a rational 2-isogeny if and only if the index $[\mathrm{GL}_2(\mathbb{Z}_2) : \operatorname{Im}\rho_{E,2^\infty}]$ is divisible by 3. The conclusion follows. □

Proposition 6.2.4. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication.*

- *If $\operatorname{Im}\rho_{E,3} = \mathrm{GL}_2(\mathbb{F}_3)$, then $[\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{Im}\rho_{E,3^\infty}] \leq 27$;*
- *If $\operatorname{Im}\rho_{E,5}$ is conjugate to the exceptional subgroup $5S4$, then*

$$[\mathrm{GL}_2(\mathbb{Z}_5) : \operatorname{Im}\rho_{E,5^\infty}] = [\mathrm{GL}_2(\mathbb{F}_5) : \operatorname{Im}\rho_{E,5}] = 5.$$

Proof. By [RSZB22, Theorem 1.6] we know that either $\operatorname{Im}\rho_{E,27} \subseteq C_{ns}^{+}(27)$ or $\operatorname{Im}\rho_{E,3^\infty}$ corresponds to a group in [SZ17, Table 1]. As $\operatorname{Im}\rho_{E,3}$ is equal to $\mathrm{GL}_2(\mathbb{F}_3)$, the index $[\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{Im}\rho_{E,3^\infty}]$ must be a power of 3. However, the largest power of 3 among the indices of [SZ17, Table 1] is 27, hence $[\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{Im}\rho_{E,3^\infty}] \leq 27$. If $\operatorname{Im}\rho_{E,5} = 5S4$ we have $[\mathrm{GL}_2(\mathbb{F}_5) : \operatorname{Im}\rho_{E,5}] = 5$. Similarly to Lemma 2.1.7 one can easily check that the only non-trivial $\mathbb{F}_5[5S4]$-submodules of $\mathfrak{gl}_2(\mathbb{F}_5)$ are $\mathbb{F}_5\cdot\mathrm{Id}$ and $\mathfrak{sl}_2(\mathbb{F}_5)$. However, if we set $G := \operatorname{Im}\rho_{E,5^\infty}$, by Lemma 2.1.10 we know that $\mathbb{F}_5\cdot\mathrm{Id}$ is contained in $\mathfrak{g}_1$, and so we have $\mathfrak{g}_1 \in \{\mathbb{F}_5\cdot\mathrm{Id}, \mathfrak{gl}_2(\mathbb{F}_5)\}$. If $\mathfrak{g}_1 = \mathbb{F}_5\cdot\mathrm{Id}$, then E corresponds to a rational point on the modular curve with RSZB label `25.625.36.1`, which has no rational points by [RSZB22, Section 8.6]. To conclude, we notice that if $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_5)$, by Lemma 2.1.12 we have that $[\mathrm{GL}_2(\mathbb{Z}_5) : G] = 5$. □

6.3 Entanglement

Let E be an elliptic curve defined over a number field K and let p be a prime for which $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ for some n. In this section, we study the entanglement between the p^n-torsion and the rest of the torsion. The key tool of our method is the ramification of primes of potentially good supersingular reduction in division fields. In particular, we will notice that p has high ramification index in $K(E[p^n])$: this relies on the work of Lozano-Robledo [LR16] and Smith [Smi23] on the valuation of the p^n-torsion points of the formal group associated with E. On the other hand, every other prime $q \neq p$ has very small ramification index in $K(E[p^n])$: this follows from a variant of the Néron–Ogg–Shafarevich criterion introduced in Theorem 3.1.1. This suggests that the intersection of two division fields $K(E[p^n]) \cap K(E[q^m])$ such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ and $\operatorname{Im}\rho_{E,q^m} \subseteq C_{ns}^+(q^m)$ should be very small.

Theorem 6.3.1. *Let E be an elliptic curve defined over a number field K and let p be a prime. Let $\mathfrak{p} \subseteq K$ be a prime above p such that E has potentially good supersingular reduction at $\mathfrak{p}$, and let $e := e(\mathfrak{p}|p)$ be its ramification index. Suppose that $p \geq 6e-1$ and that there exists an integer $n \geq 1$ such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ up to conjugation. Let F be the compositum*

$$F := \prod_{\substack{q \text{ prime} \\ q \neq p}} K(E[q^\infty]).$$

There exists $\eta \in \{1,2,3\}$ such that if E has good reduction at $\mathfrak{p}$ we have $\eta = 1$, and for every extension $K \subseteq K' \subseteq \overline{K}$ unramified at $\mathfrak{p}$, setting $F' = FK'$ we have that

$$\left[K'(E[p^n]) : F' \cap K'(E[p^n])\right] \text{ is a multiple of } \frac{p^{2n-2}(p^2-1)}{\gcd(2\eta e, p^2-1)}, \text{ and}$$

$$\operatorname{Gal}\left(K'(E[p^n])/F' \cap K'(E[p^n])\right) \text{ has an element of order } \frac{p^{n-1}(p^2-1)}{\gcd(2\eta e, p^2-1)}.$$

Moreover,

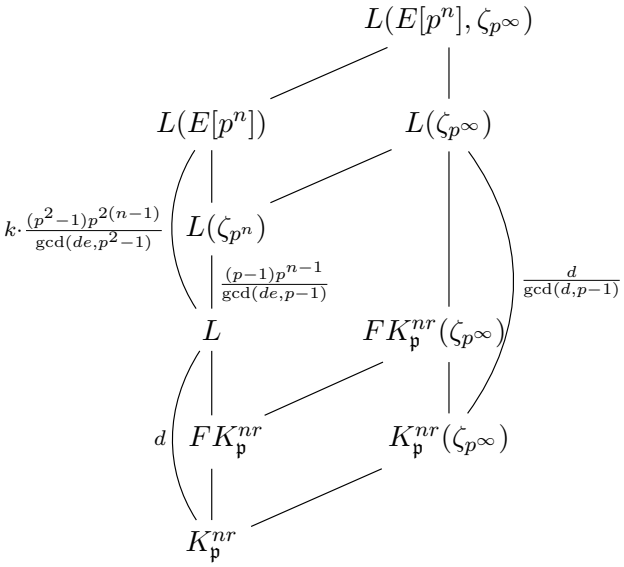
$$\operatorname{Gal}\left(K'(E[p^n])/F'(\zeta_{p^\infty}) \cap K'(E[p^n])\right) \text{ has an element of order } \frac{p^{n-1}(p+1)}{\gcd(\eta e, p+1)}.$$

Proof. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. Consider the maximal unramified extension $K_{\mathfrak{p}}^{nr}$ of $K_{\mathfrak{p}}$. We clearly have $K'K_{\mathfrak{p}} \subseteq K_{\mathfrak{p}}^{nr}$. Let $L/K_{\mathfrak{p}}^{nr}$ be the minimal extension over which E acquires good reduction. As $p \geq 6e-1 \geq 5$, by [Kra90, Proposition 1] we have $d := [L : K_{\mathfrak{p}}^{nr}] \in \{1,2,3,4,6\}$. By the Néron–Ogg–Shafarevich criterion, for every prime $q \neq p$, as $L(E[q^\infty])/L$ is unramified, we have $L(E[q^\infty]) = L$, and so $F'L = L$. By Proposition 3.2.9,

we know that E does not have a canonical subgroup, so by Lemma 3.2.8 we know that $\mathrm{Gal}\left(L(E[p^n])/L\right)$ contains an element of order $\frac{(p^2-1)p^{n-1}}{\gcd(de,p^2-1)}$. This proves the first part of the theorem, as $\mathrm{Gal}\left(L(E[p^n])/L\right)$ embeds into

$$\mathrm{Gal}\left(F'(E[p^n])/F'\right) \cong \mathrm{Gal}\left(K'(E[p^n])/F' \cap K'(E[p^n])\right).$$

We now prove that $L(E[p^n]) \cap L(\zeta_{p^\infty})$ is equal to $L(\zeta_{p^n})$. First we notice that $L(\zeta_{p^n}) \subseteq L(E[p^n])$. Since $L(\zeta_{p^\infty})/L(\zeta_{p^n})$ is a procyclic extension, every proper subextension must contain $L(\zeta_{p^{n+1}})$. It then suffices to show that $\zeta_{p^{n+1}} \notin L(E[p^n])$. However, this is true as $\mathrm{Gal}\left(L(\zeta_{p^{n+1}})/L\right)$ contains elements of order p^n, since $L/\mathbb{Q}_p^{nr}$ is a tamely ramified extension, while $\mathrm{Gal}\left(L(E[p^n])/L\right)$ is a subgroup of $C_{ns}^+(p^n)$, and hence does not contain elements of order p^n. Since $L(\zeta_p)/L$ is totally ramified, we have $[L(\zeta_p) : L] = \frac{(p-1)}{\gcd(de,p-1)}$. As $p \geq 6e-1 \geq de-1$, we necessarily have $p \nmid de$, and so $[L(\zeta_{p^n}) : L(\zeta_p)] = p^{n-1}$, because $L(\zeta_{p^n})/L(\zeta_p)$ is totally wildly ramified. This implies that $[L(\zeta_{p^n}) : L] = \frac{(p-1)p^{n-1}}{\gcd(de,p-1)}$.



We then obtain that the degree of $L(E[p^n])/L(\zeta_{p^n})$ is a multiple of

$$\frac{\gcd(de,p-1)}{\gcd(de,p^2-1)} \cdot (p+1)p^{n-1}.$$

Moreover, since $F' \subseteq L$, we have that

$$[K'(E[p^n]) : F'(\zeta_{p^\infty}) \cap K'(E[p^n])] = [F'(E[p^n], \zeta_{p^\infty}) : F'(\zeta_{p^\infty})]$$

is a multiple of

$$[L(E[p^n], \zeta_{p^\infty}) : L(\zeta_{p^\infty})] = [L(E[p^n]) : L(\zeta_{p^\infty}) \cap L(E[p^n])] = [L(E[p^n]) : L(\zeta_{p^n})].$$

In particular, we showed that the degree $[K'(E[p^n]) : F'(\zeta_{p^\infty}) \cap K'(E[p^n])]$ is a multiple of $\frac{\gcd(de, p-1)}{\gcd(de, p^2-1)} \cdot (p+1)p^{n-1}$. To conclude, it suffices to show that there exists $\eta \in \{1, 2, 3\}$ such that $D := \frac{\gcd(de, p^2-1)}{\gcd(de, p-1)}$ is a divisor of $\gcd(\eta e, p+1)$. Suppose first that de is odd: then $(de, p^2-1) = (de, p-1)(de, p+1)$, and so $D = (de, p+1)$. Moreover, d is odd and therefore $d \in \{1, 3\}$. We can then take $\eta = d$. Suppose now that de is even: then we can write

$$(de, p^2-1) = 2\left(\frac{de}{2}, \frac{p^2-1}{2}\right) = \begin{cases} \left(\frac{de}{2}, p-1\right)(de, p+1) & \text{if } p \equiv 1 \pmod 4 \\ (de, p-1)\left(\frac{de}{2}, p+1\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

If $p \equiv 3 \pmod 4$, we have $D = \left(\frac{de}{2}, p+1\right)$, and then we conclude, as for $d \in \{1, 2, 3, 4, 6\}$ we have that $\frac{de}{2}$ divides either $2e$ or $3e$. If instead $p \equiv 1 \pmod 4$, we treat separately the cases in which e is odd or e is even. If e is odd, then we must have $d \in \{2, 4, 6\}$, and so $v_2(de) \leq v_2(p-1)$. This implies that $\frac{\left(\frac{de}{2}, p-1\right)}{(de, p-1)} = \frac{1}{2}$, and in particular $D = \frac{1}{2}(de, p+1)$, which divides $\left(\frac{d}{2} \cdot e, p+1\right)$. We can then take $\eta = \frac{d}{2}$. If e is even, then either d is odd, and so $D = \frac{\left(\frac{de}{2}, p-1\right)}{(de, p-1)} \cdot (de, p+1)$ divides $(de, p+1)$, with $de \in \{e, 3e\}$ and $\eta = d$, or d is even. In the latter case, we have that $v_2(de) \geq 2 > 1 = v_2(p+1)$, and so $(de, p+1) = \left(\frac{de}{2}, p+1\right)$. This implies that D divides $(de, p+1) = \left(\frac{d}{2} \cdot e, p+1\right)$ and we can take $\eta = \frac{d}{2}$. To conclude, it suffices to show that when E has good reduction at $\mathfrak{p}$ we have $\eta = 1$. To do that, we notice that in all the cases above η is a divisor of d, and since E has good reduction the degree d must be 1. □

Corollary 6.3.2. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $p > 7$ and $n \geq 1$ be integers such that p is prime and $\operatorname{Im} \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. Let F be the compositum*

$$F := \prod_{\substack{q \text{ prime} \\ q \neq p}} \mathbb{Q}(E[q^\infty]).$$

There exists $\eta \in \{1, 2, 3\}$ such that

$$[F(E[p^n]) : F] \quad \textit{is a } \text{proper } \textit{multiple of} \quad \frac{p^{2n} - p^{2n-2}}{12}, \quad \textit{and}$$
$$[F\mathbb{Q}^{\mathrm{ab}}(E[p^n]) : F\mathbb{Q}^{\mathrm{ab}}] \quad \textit{is a multiple of} \quad \frac{p^n + p^{n-1}}{\eta}.$$

Moreover, if E has good reduction at p we have $\eta = 1$.

Proof. We notice that we can assume that E has potentially good supersingular reduction modulo p. Indeed, by Corollary 3.2.13 the prime p is always supersingular for $p > 7$ and $\neq 13$. However, by [BDM$^+$19, Corollary 1.3] we know that for $p = 13$ the image of $\rho_{E,p}$ is not contained in $C_{ns}^+(p)$. Consider the set $R := \{r \geq 1 \ : \ p \nmid r\}$ and define the extension $K = \mathbb{Q}(\{\zeta_r\}_{r\in R})$. As p is unramified in K, by Theorem 6.3.1 we know that there exists $\eta \in \{1, 2, 3\}$ such that

$$\begin{aligned}[F\mathbb{Q}^{\mathrm{ab}}(E[p^n]) : F\mathbb{Q}^{\mathrm{ab}}] &= [FK(\zeta_{p^\infty}, E[p^n]) : FK(\zeta_{p^\infty})] \\ &= [K(E[p^n]) : FK(\zeta_{p^\infty}) \cap K(E[p^n])]\end{aligned}$$

is a multiple of $\frac{p^n+p^{n-1}}{\eta}$. The fact that $[F(E[p^n]) : F]$ is a proper multiple of $\frac{p^{2n}-p^{2n-2}}{12}$ immediately follows from Theorem 6.3.1. □

Lemma 6.3.3. *Let E be an elliptic curve over a field K and let p be a prime. Let B be a set of primes such that for every $q \in B$ the prime p does not divide $q(q^2 - 1)$. Define $m := \prod_{q\in B} q$ (possibly a supernatural number) and consider the compositum $K(E[m^\infty]) := \prod_{q\in B} K(E[q^\infty])$. We have*

$$K(E[m^\infty], E[p]) \cap K(E[p^\infty]) = K(E[p]).$$

Proof. Set $F := K(E[m^\infty])$. We notice that for every $q \in B$ we have

$$p \nmid [K(E[q]) : K] \mid \#\,\mathrm{GL}_2(\mathbb{F}_q) = q(q-1)^2(q+1).$$

As F is the composite of $K(E[q^\infty])$ for $q \in B$ and $K(E[q^\infty])/K(E[q])$ is a pro-q extension, this implies that F does not contain any finite subextension with degree multiple of p. In particular, the same holds for $F(E[p])/K(E[p])$. On the other hand, $K(E[p^\infty])$ is a pro-p extension of $K(E[p])$, and so the field $F(E[p]) \cap K(E[p^\infty])$ must be equal to $K(E[p])$. □

Corollary 6.3.4. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $p > 7$ be a prime such that $\mathrm{Im}\,\rho_{E,p} = C_{ns}^+(p)$. Let B be a set of primes such that for every $q \in B$ the prime p does not divide $q(q^2 - 1)$. Define $m := \prod_{q\in B} q$ (possibly a supernatural number), and consider the compositum $\mathbb{Q}(E[m^\infty]) := \prod_{q\in B} \mathbb{Q}(E[q^\infty])$. We have*

$$[\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) : \mathbb{Q}^{\mathrm{ab}}] \leq 6.$$

Moreover, if E has good reduction at p we have

$$[\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) : \mathbb{Q}^{\mathrm{ab}}] \leq 2.$$

Proof. By Lemma 6.3.3 we know that

$$\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) \subseteq \mathbb{Q}^{\mathrm{ab}}(E[m^\infty], E[p]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) = \mathbb{Q}^{\mathrm{ab}}(E[p]).$$

In particular, we can rewrite

$$\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) = \mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p]),$$

and so it suffices to compute

$$\begin{aligned}\left[\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}\right] &= \frac{\left[\mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}\right]}{\left[\mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p])\right]} \\ &= \frac{\left[\mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}\right]}{\left[\mathbb{Q}^{\mathrm{ab}}(E[m^\infty], E[p]) : \mathbb{Q}^{\mathrm{ab}}(E[m^\infty])\right]}.\end{aligned}$$

However, by Corollary 6.3.2 we know that $\left[\mathbb{Q}^{\mathrm{ab}}(E[m^\infty], E[p]) : \mathbb{Q}^{\mathrm{ab}}(E[m^\infty])\right]$ is at least $\frac{p+1}{3}$ (and greater than or equal to $p+1$ in the case of good reduction), and

$$\begin{aligned}\left[\mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}\right] &= [\mathbb{Q}(E[p]) : \mathbb{Q}(E[p]) \cap \mathbb{Q}^{\mathrm{ab}}] \leq [\mathbb{Q}(E[p]) : \mathbb{Q}(\zeta_p)] \\ &= \frac{[\mathbb{Q}(E[p]) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]} = 2(p+1).\end{aligned}$$

□

Lemma 6.3.5. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $\mathcal{P}$ be a set of primes containing $2, 3, 5$ and all primes p for which $\rho_{E,p}$ is not surjective. Let m be the product of all the primes in $\mathcal{P}$ and write $\mathbb{Z}_m := \prod_{p\in\mathcal{P}} \mathbb{Z}_p$ and $\rho_{E,m^\infty} := \prod_{p\in\mathcal{P}} \rho_{E,p^\infty}$. Call $S := \rho_E\left(\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}\right)\right) < \mathrm{SL}_2(\mathbb{Z}_p)$ and $S_\mathcal{P}$ its image under the projection on $\mathrm{SL}_2(\mathbb{Z}_m)$. We have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] = \left[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S\right] = [\mathrm{SL}_2(\mathbb{Z}_m) : S_\mathcal{P}] = [\mathrm{GL}_2(\mathbb{Z}_m) : \mathrm{Im}\,\rho_{E,m^\infty}]\,.$$

Proof. The first and the third equalities follow from surjectivity of $\det\circ\rho_E$ onto $\widehat{\mathbb{Z}}^\times$. To prove the second inequality, it suffices to notice that we can view S as a closed subgroup of $\prod_p S_p \subseteq \prod_p \mathrm{SL}_2(\mathbb{Z}_p) = \mathrm{SL}_2(\widehat{\mathbb{Z}})$, and by [Ser98, IV §3.4 Lemma 5] we know that S contains the subgroup $\prod_{p\notin\mathcal{P}} \mathrm{SL}_2(\mathbb{Z}_p)$, concluding the proof. □

Lemma 6.3.6. *Let E be an elliptic curve defined over a field K. Let m, n be coprime squarefree supernatural numbers. Set $G := \mathrm{Im}\,\rho_E$ and define G_m, G_n, G_{mn} to be its projections on $\mathrm{GL}_2(\mathbb{Z}_m)$, $\mathrm{GL}_2(\mathbb{Z}_n)$, $\mathrm{GL}_2(\mathbb{Z}_{mn})$ respectively. We have*

$$[G_m \times G_n : G_{mn}] = [K(E[m^\infty]) \cap K(E[n^\infty]) : K].$$

Proof. Set $F := K(E[m^\infty]) \cap K(E[n^\infty])$. If we write

$$G_m = \mathrm{Gal}\left(K(E[m^\infty])/K\right) \quad \text{and} \quad G_n = \mathrm{Gal}\left(K(E[n^\infty])/K\right),$$

we know that $G_{mn} = \mathrm{Gal}\left(K(E[(mn)^\infty])/K\right)$ is isomorphic to the subgroup of $G_m \times G_n$ described as $\{(\sigma, \tau) \in G_m \times G_n \ : \ \sigma|_F = \tau|_F\}$. We conclude the proof noting that $[G_m \times G_n : G_{mn}] = [F : K]$. □

Corollary 6.3.7. *Let K be a number field and let E/K be an elliptic curve without CM. Let m, n be coprime squarefree supernatural numbers. Set $G := \mathrm{Im}\,\rho_E$ and $S := \rho_E(\mathrm{Gal}(\overline{K}/K\mathbb{Q}^{\mathrm{ab}}))$, and define G_m, G_n, G_{mn}, S_m, S_n, S_{mn} to be their projections on $\mathrm{GL}_2(\mathbb{Z}_m)$, $\mathrm{GL}_2(\mathbb{Z}_n)$, $\mathrm{GL}_2(\mathbb{Z}_{mn})$, $\mathrm{SL}_2(\mathbb{Z}_m)$, $\mathrm{SL}_2(\mathbb{Z}_n)$, $\mathrm{SL}_2(\mathbb{Z}_{mn})$ respectively. The index $[\mathrm{GL}_2(\mathbb{Z}_{mn}) : G_{mn}]$ is equal to*

$$[\mathrm{GL}_2(\mathbb{Z}_m) : G_m] \cdot [\mathrm{GL}_2(\mathbb{Z}_n) : G_n] \cdot [K(E[m^\infty]) \cap K(E[n^\infty]) : K]$$

and the index $[\mathrm{SL}_2(\mathbb{Z}_{mn}) : S_{mn}]$ is equal to

$$[\mathrm{SL}_2(\mathbb{Z}_m) : S_m] \cdot [\mathrm{SL}_2(\mathbb{Z}_n) : S_n] \cdot [K\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap K\mathbb{Q}^{\mathrm{ab}}(E[n^\infty]) : K\mathbb{Q}^{\mathrm{ab}}].$$

Proof. The first statement follows from Lemma 6.3.6 noting that

$$\begin{aligned}[\mathrm{GL}_2(\mathbb{Z}_{mn}) : G_{mn}] &= [\mathrm{GL}_2(\mathbb{Z}_{mn}) : G_m \times G_n] \cdot [G_m \times G_n : G_{mn}] \\ &= [\mathrm{GL}_2(\mathbb{Z}_m) : G_m] \cdot [\mathrm{GL}_2(\mathbb{Z}_n) : G_n] \cdot [G_m \times G_n : G_{mn}].\end{aligned}$$

The second statement is proved in the same way replacing K with $K\mathbb{Q}^{\mathrm{ab}}$. □

6.4 Bound on the adelic index

The aim of this section is to combine the results from the previous chapters to obtain a bound on the index of the image of the adelic Galois representation of an elliptic curve $E/\mathbb{Q}$ without CM. In particular, we will combine the classification of p-adic images (Theorem 6.1.5) and the effective surjectivity theorem (Theorem 4.2.5) to obtain a bound on the contribution given by those primes for which $\mathrm{Im}\,\rho_{E,p}$ is contained in the normaliser of a non-split Cartan. We will then give a bound for the index at the other non-surjective primes and a bound for the entanglement phenomenon among all primes. To do this, we will use some results about the degree of entanglement fields given in Section 6.3. The following theorem is the main result of this section.

Theorem 6.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. We have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 9.5 \cdot 10^{20}(\mathrm{h}_{\mathcal{F}}(E) + 40)^{4.42}.$$

Moreover, if we define

$$\delta(x) := \frac{1}{\log(\log(x+40)+7.6)-0.903}$$

for every $x > -0.75$*, we have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] < 3.4 \cdot 10^{20} \cdot (\mathrm{h}_{\mathcal{F}}(E) + 22.5)^{3+4.158\cdot\delta(\mathrm{h}_{\mathcal{F}}(E))}.$$

In particular, we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] < \mathrm{h}_{\mathcal{F}}(E)^{3+O\left(\frac{1}{\log\log \mathrm{h}_{\mathcal{F}}(E)}\right)}$ *as* $\mathrm{h}_{\mathcal{F}}(E)$ *tends to* ∞*.*

Remark 6.4.2. If we compare this result with Theorem 17 we see that the constant and the exponent are much better. In particular, $\exp(1.9 \cdot 10^{10})$ is replaced with $9.5 \cdot 10^{20}$, while the exponent 12395 is replaced with 4.42.

Before proving Theorem 6.4.1, we will give many intermediate lemmas and propositions, that allow us to organise the proof in different steps. We will treat separately the cases where the elliptic curve E satisfies the uniformity conjecture or not, and we will distinguish cases according to whether $j(E)$ is an integer or not.

Lemma 6.4.3. *Let* $E/\mathbb{Q}$ *be an elliptic curve without CM and let* p *be a prime number such that* $\operatorname{Im}\rho_{E,p}$ *is contained in an exceptional subgroup, i.e. a proper subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$ *which is not contained in a Borel subgroup or in the normaliser of a Cartan subgroup. There are two possible cases:*

- $p = 5$ *and* $[\mathrm{GL}_2(\mathbb{F}_5) : \operatorname{Im}\rho_{E,5}] = 5$*;*
- $p = 13$*, the* j*-invariant* $j(E)$ *is one among*

$$\frac{2^4\cdot 5\cdot 13^4\cdot 17^3}{3^{13}},\quad -\frac{2^{12}\cdot 5^3\cdot 11\cdot 13^4}{3^{13}},\quad \frac{2^{18}\cdot 3^3\cdot 13^4\cdot 127^3\cdot 139^3\cdot 157^3\cdot 283^3\cdot 929}{5^{13}\cdot 61^{13}}, \tag{6.4.1}$$

  and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] = 182$*.*

Proof. By [Ser81, §8.4, Lemme 18] we know that $p \leq 13$. Using [Zyw15a, Theorems 1.1, 1.2, 1.4, 1.5, 1.6, 1.8] and [Zyw15a, Remark 1.9], we note that there are just two possible groups: one for $p = 5$ with index 5 and one for $p = 13$ with index 91 (respectively 5S4 and 13S4). However, by [BDM+23, Theorem 1.1] we know that in the case $p = 13$ the j-invariant must belong to the list (6.4.1). We can then apply the algorithm `FindOpenImage` developed in [Zyw22] to compute the index of $\operatorname{Im}\rho_E$, which is 182. Indeed, by [Zyw15b, Corollary 2.3] the index only depends on the j-invariant. □

We collect together the facts we know about the possible images of $\rho_{E,p}$ in the following proposition.

Proposition 6.4.4. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. If $j(E)$ is one of the j-invariants of the following list*

$$\begin{gathered} -11\cdot 131^3,\quad -11^2,\quad -\frac{17^2\cdot 101^3}{2},\quad -\frac{17\cdot 373^3}{2^{17}},\quad -7\cdot 11^3 \\ -7\cdot 137^3\cdot 2083^3,\quad \frac{2^4\cdot 5\cdot 13^4\cdot 17^3}{3^{13}},\quad -\frac{2^{12}\cdot 5^3\cdot 11\cdot 13^4}{3^{13}}, \\ \frac{2^{18}\cdot 3^3\cdot 13^4\cdot 127^3\cdot 139^3\cdot 157^3\cdot 283^3\cdot 929}{5^{13}\cdot 61^{13}}, \end{gathered} \tag{6.4.2}$$

then $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 2736$. Suppose now that $j(E)$ is not in the list above.

- *If $\operatorname{Im}\rho_{E,p}$ is contained in a Borel subgroup, then $p \in \{2,3,5,7,13\}$.*
- *If $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a split Cartan subgroup, then $p \leq 7$.*
- *If $\operatorname{Im}\rho_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup and $p \geq 5$, then either $\operatorname{Im}\rho_{E,p} = C_{ns}^+(p)$ and $p \in \{5,7,11\} \cup \{N \geq 19\}$, or $[C_{ns}^+(p) : \operatorname{Im}\rho_{E,p}] = 3$ and $p = 5$.*
- *If $\operatorname{Im}\rho_{E,p}$ is contained in an exceptional subgroup but is not contained in one of the groups in the cases above, then $p = 5$ and $[\mathrm{GL}_2(\mathbb{Z}_5) : \operatorname{Im}\rho_{E,5^\infty}] = 5$.*

Proof. To prove that the j-invariants in the list have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 2736$, it suffices to notice that by [Zyw15b, Corollary 2.3] the index only depends on the j-invariant, and then we can compute it using the algorithm `FindOpenImage` developed in [Zyw22]. If $j(E)$ is not in the list, the statement follows combining Theorem 3, Theorem 4, Theorem 9, [BDM$^+$19, Corollary 1.3], [BDM$^+$23, Theorem 1.2], and Lemma 6.4.3. □

Another result we will use is the following theorem by Lemos ([Lem19a, Theorem 1.1] and [Lem19b, Theorem 1.4]).

Theorem 6.4.5 (Lemos)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Suppose that there exists a prime q for which $\operatorname{Im}\rho_{E,q}$ is contained either in a Borel subgroup or in the normaliser of a split Cartan subgroup: then $\rho_{E,p}$ is surjective for every $p > 37$.*

Lemos's arguments actually show the following stronger statement.

Theorem 6.4.6. *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let $p > 13$ be a prime such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. For every prime $q \neq p$, the image of $\rho_{E,q}$ is contained neither in a Borel subgroup nor in the normaliser of a split Cartan subgroup.*

Proof. By Theorem 3, we know that if E admits a rational q-isogeny then q belongs to the set $\{2, 3, 5, 7, 11, 13, 17, 37\}$. However, by [Lem19a, Proposition 2.1] we know that either $j(E) \in \mathbb{Z}$ or $q \in \{11, 17, 37\}$. If E admits a rational isogeny of degree $q \in \{11, 17, 37\}$, by Theorem 3 we know that $j(E)$ is one among

$$-11 \cdot 131^3, -11^2, -\frac{17^2 \cdot 101^3}{2}, -\frac{17 \cdot 373^3}{2^{17}}, -7 \cdot 137^3 \cdot 2083^3, -7 \cdot 11^3.$$

One can check on the LMFDB [LMF24] that in these cases $\operatorname{Im}\rho_{E,p}$ is not contained in $C_{ns}^{+}(p)$ for $p > 13$. If instead $\operatorname{Im}\rho_{E,q}$ is contained in the normaliser of a split Cartan subgroup, then by [Lem19b, Proposition 1.5] we know that $j(E) \in \mathbb{Z}$. From now on, we can therefore assume that $j(E) \in \mathbb{Z}$. Following the proof of [Lem19b, Theorem 1.4] we have that if $\operatorname{Im}\rho_{E,q} \subseteq C_{sp}^{+}(q)$ then $j(E) \in \{-5000, -1728\}$, for which $\operatorname{Im}\rho_{E,p}$ is not contained in $C_{ns}^{+}(p)$ for $p > 13$. If $j(E) \in \mathbb{Z}$ and the image of $\rho_{E,q}$ is contained in a Borel subgroup, then following the proof of [Lem19a, Theorem 1.1] we have that $j(E)$ belongs to the list in [Lem19a, p. 142], and one can check again on the LMFDB that none of those curves admits a prime $p > 13$ for which $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. □

Combining Proposition 6.4.4 and Theorem 6.4.6 we obtain the following.

Proposition 6.4.7. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Suppose that $j(E)$ does not belong to the list* (6.4.2)*. One of the following holds.*

(A) There exists $p > 13$ such that $\operatorname{Im}\rho_{E,p} = C_{ns}^{+}(p)$, and for every $q \neq 5$ for which $\rho_{E,q}$ is not surjective we have $\operatorname{Im}\rho_{E,q} \subseteq C_{ns}^{+}(q)$.

(B) For every $p > 13$ the representation ρ_{E,p^∞} is surjective.

Proof. Suppose first that there exists $p > 13$ such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. By Theorem 9 we know that $\operatorname{Im}\rho_{E,p} = C_{ns}^{+}(p)$. Using Theorem 6.4.6 we see that if q is a prime for which $\rho_{E,q}$ is not surjective and its image is not contained in $C_{ns}^{+}(q)$, then it must be contained in an exceptional subgroup. By Proposition 6.4.4 this implies that $q = 5$. If instead there are no primes $p > 13$ for which $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$, by Proposition 6.4.4 we see that $\rho_{E,p}$ is surjective for every $p > 13$. By [Ser98, IV-23, Lemma 3] we have that $\rho_{E,p^\infty}\left(\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}\right)\right) = \mathrm{SL}_2(\mathbb{Z}_p)$, and by surjectivity of the determinant this implies that $\operatorname{Im}\rho_{E,p^\infty} = \mathrm{GL}_2(\mathbb{Z}_p)$. □

Definition 6.4.8. Let $E/\mathbb{Q}$ be an elliptic curve without CM. For every integer $n > 1$ set $\mathbb{Z}_n = \prod_{p|n} \mathbb{Z}_p$ and $\rho_{E,n^\infty} = \prod_{p|n} \rho_{E,p^\infty} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_2(\mathbb{Z}_n)$. For any coprime integers $m, n > 1$, using Corollary 6.3.7 and the surjectivity of $\det \circ \rho_E$ define

$$\begin{aligned}
\mathrm{Ind}(m) &:= [\mathrm{GL}_2(\mathbb{Z}_m) : \mathrm{Im}\,\rho_{E,m^\infty}] = [\mathrm{SL}_2(\mathbb{Z}_m) : \mathrm{Im}\,\rho_{E,m^\infty} \cap \mathrm{SL}_2(\mathbb{Z}_m)]\,, \\
\mathrm{Ent}(m,n) &:= \frac{\mathrm{Ind}(mn)}{\mathrm{Ind}(m)\,\mathrm{Ind}(n)} = [\mathbb{Q}(E[m^\infty]) \cap \mathbb{Q}(E[n^\infty]) : \mathbb{Q}] \\
&= [\mathbb{Q}^{\mathrm{ab}}(E[m^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[n^\infty]) : \mathbb{Q}^{\mathrm{ab}}].
\end{aligned}$$

We are now ready to prove Theorem 6.4.1. We will split the proof in multiple step and cases, to make it clearer.

Proposition 6.4.9. *Let E be an elliptic curve without CM and suppose that $j(E)$ does not belong to the list* (6.4.2)*. Consider the two cases (A) and (B) of Proposition 6.4.7. In the respective cases we have*

(A) Let $\mathcal{C}_{ns}$ be the set of the primes $p \geq 7$ such that $\mathrm{Im}\,\rho_{E,p} \subseteq C_{ns}^+(p)$, and let β be the number of primes in $\mathcal{C}_{ns}$ at which E has bad reduction. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq \Delta_7 \cdot 2^{|\mathcal{C}_{ns}|-\beta} \cdot 6^\beta \cdot \mathrm{Ind}(30) \cdot \prod_{p \in \mathcal{C}_{ns}} \mathrm{Ind}(p),$$

where

$$\Delta_7 := \begin{cases} 1 & \text{if } 7 \notin \mathcal{C}, \\ 8 & \text{if } 7 \in \mathcal{C} \text{ and } E \text{ has good reduction at } 7, \\ \frac{8}{3} & \text{if } 7 \in \mathcal{C} \text{ and } E \text{ has bad reduction at } 7. \end{cases}$$

(B) Let $\{2,3,5\} \subseteq \mathcal{L} \subseteq \{2,3,5,7,11,13\}$ be the set of primes containing $2,3,5$ and every p for which $\rho_{E,p}$ is not surjective. Let m_p be the product of primes $q < p$ that belong to $\mathcal{L}$. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_{E,p}] \leq \prod_{p \in \mathcal{L}} \mathrm{Ent}(m_p, p)\,\mathrm{Ind}(p).$$

Proof. Case (B) follows from the definition of $\mathrm{Ent}(m_p, p)$ and $\mathrm{Ind}(p)$, we then focus on case (A). By Theorem 6.4.6 we know that for every prime p, if the representation $\rho_{E,p}$ is not surjective, its image is contained either in the normaliser of a non-split Cartan or in an exceptional subgroup. If $\mathrm{Im}\,\rho_{E,p}$ is contained in an exceptional subgroup, we know by Lemma 6.4.3 that either

$p = 5$ and $\operatorname{Im}\rho_{E,5^\infty}$ has index 5 or the index of $\operatorname{Im}\rho_E$ is 182, and hence satisfies the inequality in the statement of the lemma. We will then assume that for every prime p for which $\rho_{E,p}$ is not surjective, either $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$ or $p = 5$ and $[\mathrm{GL}_2(\mathbb{Z}_5) : \operatorname{Im}\rho_{E,5^\infty}] = 5$. Define the set $\mathcal{P} := \{2, 3, 5\} \cup \mathcal{C}$ and consider $m := \prod_{p\in\mathcal{P}} p$. Lemma 6.3.5 yields

$$\left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E\right] = \left[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S\right] = \mathrm{Ind}(m). \tag{6.4.3}$$

Define $\mathcal{C}_{ns} := \mathcal{C} \setminus \{3, 5\}$, let p be the largest prime in $\mathcal{C}_{ns}$ and set $B := \mathcal{P} \setminus \{p\}$. If $p > 7$, by Corollary 6.3.7 and Corollary 6.3.4 we have

$$\mathrm{Ind}(m) = \mathrm{Ent}(m/p, p) \cdot \mathrm{Ind}(m/p) \cdot \mathrm{Ind}(p) \leq 6 \cdot \mathrm{Ind}(m/p) \cdot \mathrm{Ind}(p). \tag{6.4.4}$$

Similarly, if we further assume that E has good reduction at p, we have

$$\mathrm{Ind}(m) \leq 2 \cdot \mathrm{Ind}(m/p) \cdot \mathrm{Ind}(p).$$

If instead $p = 7$, we have that $\frac{m}{p} = 30$, and so we can apply Lemma 6.3.3. In particular, we obtain

$$\begin{aligned}\mathrm{Ent}(m/p, p) &= [\mathbb{Q}^{\mathrm{ab}}(E[(m/p)^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) : \mathbb{Q}^{\mathrm{ab}}] \\ &= [\mathbb{Q}^{\mathrm{ab}}(E[(m/p)^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}] \\ &\leq [\mathbb{Q}^{\mathrm{ab}}(E[p]) : \mathbb{Q}^{\mathrm{ab}}] \leq |C_{ns}^+(7)| = 16,\end{aligned}$$

and so

$$\mathrm{Ind}(m) \leq 16 \cdot \mathrm{Ind}(30) \cdot \mathrm{Ind}(7).$$

We can now iterate this argument on $\frac{m}{p}$ in place of m, so that we obtain

$$\mathrm{Ind}(m) \leq \Delta_7 \cdot 2^{|\mathcal{C}_{ns}|-\beta} \cdot 6^\beta \cdot \mathrm{Ind}(30) \cdot \prod_{p\in\mathcal{C}_{ns}} \mathrm{Ind}(p)$$

as desired. □

Lemma 6.4.10. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Define $\mathcal{C}$ as the set of all odd primes p for which $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$. Let β be the number of primes $p > 5$ in $\mathcal{C}$ for which E has bad reduction at p. For every $p \in \mathcal{C}$, call n_p the largest integer n for which $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$, and define $\Lambda := \prod_{p\in\mathcal{C}} p^{n_p}$. Suppose that $\mathcal{C}$ contains a prime greater than 13 (Case (A) of Proposition 6.4.7). We have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 2488320 \cdot \Delta_7 \cdot 3^\beta \cdot \Lambda^3,$$

where

$$\Delta_7 := \begin{cases} 1 & \text{if } 7 \notin \mathcal{C}, \\ 8 & \text{if } 7 \in \mathcal{C} \text{ and } E \text{ has good reduction at } 7, \\ \frac{8}{3} & \text{if } 7 \in \mathcal{C} \text{ and } E \text{ has bad reduction at } 7. \end{cases}$$

Proof. Set $\mathcal{C}_{ns} = \mathcal{C} \setminus \{3,5\}$. As we are in case (A) of Proposition 6.4.9, we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq \Delta_7 \cdot 2^{|\mathcal{C}_{ns}|-\beta} \cdot 6^{\beta} \cdot \mathrm{Ind}(30) \cdot \prod_{p \in \mathcal{C}_{ns}} \mathrm{Ind}(p).$$

We notice that

$$\mathrm{Ind}(30) = \mathrm{Ind}(5) \cdot \mathrm{Ind}(6) \cdot \mathrm{Ent}(6,5).$$

Call S_m the projection of $\mathrm{Im}\,\rho_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\mathbb{Z}_m)$. We know that $\mathrm{Im}\,\rho_{E,5}$ is $\mathrm{SL}_2(\mathbb{F}_5)$, or it is conjugate to either a subgroup of $C_{ns}^+(5)$, or to the exceptional subgroup $5S4$. If $\mathrm{Im}\,\rho_{E,5} = \mathrm{SL}_2(\mathbb{F}_5)$ we know by [Ser98, IV §3.4 Lemma 3] that $S_5 = \mathrm{SL}_2(\mathbb{Z}_5)$. We can apply Goursat's lemma to show that the image of S_{30} in the product $\frac{S_6}{N_6} \times \frac{\mathrm{SL}_2(\mathbb{Z}_5)}{N_5}$ corresponds to the graph of an isomorphism $\frac{S_6}{N_6} \cong \frac{\mathrm{SL}_2(\mathbb{Z}_5)}{N_5}$, where N_6 and N_5 are the kernels of the projections on S_5 and S_6 respectively. However, the group S_6 is solvable, while following the description of $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p))$ in [Ser98, IV-25] we see that $\mathrm{SL}_2(\mathbb{Z}_5)$ contains $\mathrm{PSL}_2(\mathbb{F}_5)$ in its composition series. This implies that N_5 must surject onto $\mathrm{PSL}_2(\mathbb{F}_5)$. In particular, by [Ser98, IV §3.4 Lemmas 2 and 3] this implies that $N_5 = \mathrm{SL}_2(\mathbb{Z}_5)$, and so

$$\mathrm{Ind}(30) = \mathrm{Ind}(6) \cdot \mathrm{Ind}(5) = \mathrm{Ind}(6).$$

In the non-split Cartan case, we can apply Lemma 6.3.3 and obtain

$$\begin{aligned} \mathrm{Ent}(6,5) &= [\mathbb{Q}^{\mathrm{ab}}(E[6^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[5^\infty]) : \mathbb{Q}^{\mathrm{ab}}] \\ &= [\mathbb{Q}^{\mathrm{ab}}(E[6^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[5]) : \mathbb{Q}^{\mathrm{ab}}] \\ &\leq [\mathbb{Q}^{\mathrm{ab}}(E[5]) : \mathbb{Q}^{\mathrm{ab}}] \leq |C_{ns}^+(5)| = 12. \end{aligned}$$

In the exceptional case, in the same way as for the Cartan we have $\mathrm{Ent}(6,5) \leq 24$. Define Δ_5 as 12 if $\mathrm{Im}\,\rho_{E,5} \subseteq C_{ns}^+(5)$, as $\Delta_5 := 24$ if $\mathrm{Im}\,\rho_{E,5} = 5S4$, and as 1 otherwise. Combining all cases we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq \Delta_5\Delta_7 \cdot 2^{|\mathcal{C}_{ns}|-\beta} \cdot 6^{\beta} \cdot \mathrm{Ind}(6) \prod_{p \in \mathcal{C}\setminus\{3\}} \mathrm{Ind}(p).$$

We now notice that both S_2 and S_3 are solvable, and that S_2 has just one copy of $\mathbb{Z}/3\mathbb{Z}$ in its composition series, while S_3 has 3 copies of $\frac{\mathbb{Z}}{2\mathbb{Z}}$ in its composition series. The quotients $\frac{S_2}{N_2} \cong \frac{S_3}{N_3}$ will then have order less than or equal to 24. In particular, we have $\mathrm{Ent}(6) \leq 24$, and so $\mathrm{Ind}(6) \leq 24 \cdot \mathrm{Ind}(2) \cdot \mathrm{Ind}(3)$. If we set $\mathcal{P} := \mathcal{C} \cup \{2,3,5\}$ we obtain

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq 24\Delta_5\Delta_7 \cdot 2^{|\mathcal{C}_{ns}|-\beta} \cdot 6^{\beta} \cdot \prod_{p \in \mathcal{P}} [\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{Im}\,\rho_{E,p^\infty}]. \quad (6.4.5)$$

By Theorem 6.4.6 we know that $\mathrm{Im}\,\rho_{E,3}$ is contained neither in a Borel subgroup nor in the normaliser of a split Cartan subgroup. In particular, by

[Zyw15a, Theorem 1.2] we know that it must be either equal to the normaliser of a non-split Cartan or to $\mathrm{GL}_2(\mathbb{F}_3)$. By Proposition 6.2.4 we know that if $3 \notin \mathcal{C}$, then $\mathrm{Ind}(3) \leq 27$. On the other hand, if $3 \in \mathcal{C}$ then by Corollary 6.2.2 we have $\mathrm{Ind}(3) \leq 3^{3n_3-1}$. In all cases, we can write $\mathrm{Ind}(3) \leq 3^{\max\{3,3n_3-1\}} \leq 27 \cdot 3^{3n_3}$. Similarly, if $\rho_{E,5}$ is not surjective and $5 \notin \mathcal{C}$, we can apply Proposition 6.2.4 to obtain that $\mathrm{Ind}(5) = 5$, and so $\Delta_5 \mathrm{Ind}(5) = 120$. If instead $5 \in \mathcal{C}$, by Corollary 6.2.2 we have $\mathrm{Ind}(5) \leq \frac{2}{5} \cdot 5^{3n_5}$, and $\Delta_5 \mathrm{Ind}(5) \leq \frac{24}{5} \cdot 5^{3n_5}$. Since if $\rho_{E,5}$ is surjective we have $\mathrm{Ind}(5) = 1$, in all cases we can write $\Delta_5 \mathrm{Ind}(5) \leq 120 \cdot 5^{3n_5}$. By Proposition 6.2.3, we know that either $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] = 128$ or $\mathrm{Ind}(2) \leq 32$. We can exclude the first case, as it is better than the inequality in the statement of the lemma. For all the other $p \in \mathcal{P}$, we know that $p \in \mathcal{C}$, and by Corollary 6.2.2 we have $\mathrm{Ind}(p) \leq \frac{p^{3n_p}}{2}$. Replacing all these bounds in equation (6.4.5) we obtain

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] &\leq 24 \cdot 32 \cdot 27 \cdot 120 \cdot \Delta_7 \cdot 2^{|\mathcal{C}_{ns}|-\beta} \cdot 6^{\beta} \cdot 3^{3n_3} \cdot 5^{3n_5} \prod_{p \in \mathcal{C}_{ns}} \frac{p^{3n_p}}{2} \\ &= 2488320 \cdot \Delta_7 \cdot 3^{\beta} \cdot \Lambda^3. \end{aligned}$$

□

Lemma 6.4.11. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Define $\mathcal{C}$ as the set of all odd primes p for which $\mathrm{Im}\,\rho_{E,p} \subseteq C_{ns}^+(p)$. For every $p \in \mathcal{C}$, call n_p the largest integer n for which $\mathrm{Im}\,\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$, and define $\Lambda := \prod_{p \in \mathcal{C}} p^{n_p}$. Suppose that $j(E)$ does not belong to the list* (6.4.2) *and that $\rho_{E,p}$ is surjective for every prime $p > 13$ (Case (B) of Proposition 6.4.7). We have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq 4.3 \cdot 10^{12} \cdot \Lambda^2.$$

Proof. By Theorem 3, we know that if p is an odd prime for which E has a rational p-isogeny, then $p \in \{3, 5, 7, 13\}$. Define the set $\mathcal{P} = \{2, 3, 5\} \cup \{p \mid \rho_{E,p} \text{ is not surjective}\} \subseteq \{2, 3, 5, 7, 11, 13\}$, and set as before $m := \prod_{p \in \mathcal{P}} p$ and $S := \rho_E\left(\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}\right)\right)$. By Lemma 6.3.5 we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] = \mathrm{Ind}(m)$. Define the set $B_p := \{q \in \mathcal{P} : q < p\}$ and write $m_p := \prod_{q \in B_p} q$ (where $m_2 = 1$). By Proposition 6.4.7 we have

$$\mathrm{Ind}(m) = \prod_{p \in \mathcal{P}} \mathrm{Ind}(p) \cdot \mathrm{Ent}(m_p, p). \tag{6.4.6}$$

If $p \geq 5$ we can apply Lemma 6.3.3 and obtain

$$K_p := \mathbb{Q}^{\mathrm{ab}}(E[p^\infty]) \cap \mathbb{Q}^{\mathrm{ab}}(E[m_p^\infty]) = \mathbb{Q}^{\mathrm{ab}}(E[p]) \cap \mathbb{Q}^{\mathrm{ab}}(E[m_p^\infty]).$$

Moreover, similarly to the proof of Lemma 6.3.3, since the Galois group $\mathrm{Gal}\left(\mathbb{Q}^{\mathrm{ab}}(E[m_p^\infty])/\mathbb{Q}^{\mathrm{ab}}\right)$ does not contain any finite group of order divisible by p in its composition series, the field K_p must be a subextension of

$\mathbb{Q}^{\mathrm{ab}}(E[p])/\mathbb{Q}^{\mathrm{ab}}$ of degree coprime with p. In particular, if P_p is a p-Sylow of S_p, we have that $[K_p : \mathbb{Q}^{\mathrm{ab}}] \leq [S_p : P_p]$, and so

$$\mathrm{Ind}(p) \cdot \mathrm{Ent}(m_p, p) = [\mathrm{SL}_2(\mathbb{Z}_p) : S_p] \cdot [K_p : \mathbb{Q}^{\mathrm{ab}}] \leq [\mathrm{SL}_2(\mathbb{Z}_p) : P_p]. \quad (6.4.7)$$

We now proceed by providing a bound on the indices of the groups P_p prime by prime, assuming that ρ_{E,p^∞} is not surjective. To optimise the bound, we will bound the degree $[K_3 : \mathbb{Q}^{\mathrm{ab}}]$ together with the index $[\mathrm{SL}_2(\mathbb{Z}_2) : S_2]$, even if they correspond to different primes.

- $\underline{p = 13}$. We can apply Proposition 6.4.4 to show that $\mathrm{Im}\,\rho_{E,13}$ is contained in a Borel subgroup. By Theorem 11 we have that the 13-Sylow of $\mathrm{GL}_2(\mathbb{Z}_{13})$ is contained in $\mathrm{Im}\,\rho_{E,13^\infty}$, and so by Lemma 2.1.10 and Lemma 2.1.4 we have that P_{13} is the 13-Sylow of $\mathrm{SL}_2(\mathbb{Z}_{13})$. We then obtain $[\mathrm{SL}_2(\mathbb{Z}_{13}) : P_{13}] \leq 12 \cdot 14$.

- $\underline{p = 11}$. By Proposition 6.4.4, $\mathrm{Im}\,\rho_{E,11}$ is equal to the normaliser of a non-split Cartan subgroup. In particular, by Proposition 6.2.1 and Corollary 6.3.4 we have $[\mathrm{SL}_2(\mathbb{Z}_{11}) : S_{11}] \cdot [K_{11} : \mathbb{Q}^{\mathrm{ab}}] \leq 5 \cdot 11^{2n_{11}} \cdot 6 = 30 \cdot 11^{2n_{11}}$.

- $\underline{p = 7}$. By [RSZB22, Theorem 1.6] we see that there are three possible cases: the index $[\mathrm{SL}_2(\mathbb{Z}_7) : S_7]$ has 7-adic valuation at most 1 (as we can check in the online supplement of [SZ17]), the image of $\rho_{E,7}$ is contained in $C_{ns}^+(7)$, or E corresponds to one of the two exceptional points in [RSZB22, Table 1]. In the last case, we can compute that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] = 224$. In the Cartan case, using Proposition 6.2.1 we have $[\mathrm{SL}_2(\mathbb{Z}_7) : P_7] \leq (7^2 - 1) \cdot 7^{2n_7}$. If instead the 7-adic valuation of the index is at most 1, we obtain $[\mathrm{SL}_2(\mathbb{Z}_7) : P_7] \leq (7^2 - 1) \cdot 7$. In all cases, we have $[\mathrm{SL}_2(\mathbb{Z}_7) : P_7] \leq 7 \cdot 48 \cdot 7^{2n_7}$.

- $\underline{p = 5}$. Similarly to the case $p = 7$, by [RSZB22, Theorem 1.6] we have three cases: $[\mathrm{SL}_2(\mathbb{Z}_5) : S_5]$ has 5-adic valuation at most 1, or $\mathrm{Im}\,\rho_{E,25} \subseteq C_{ns}^+(25)$, or E corresponds to one of two exceptional points with $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \in \{200, 300\}$. In the Cartan case we have $n_5 \geq 2$, so by Proposition 6.2.1 we have $[\mathrm{SL}_2(\mathbb{Z}_5) : P_5] \leq (5^2 - 1) \cdot 5^{2n_5 - 1}$. As in the first case we have $[\mathrm{SL}_2(\mathbb{Z}_5) : P_5] \leq 24 \cdot 5$, we obtain that in all cases $[\mathrm{SL}_2(\mathbb{Z}_5) : P_5] \leq 5 \cdot 24 \cdot 5^{2n_5}$.

- $\underline{p = 3}$. Again, by [RSZB22, Theorem 1.6] we have that either $[\mathrm{SL}_2(\mathbb{Z}_3) : S_3] \leq 27$, or $\mathrm{Im}\,\rho_{E,27} \subseteq C_{ns}^+(27)$. By Theorem 6.1.5 and Proposition 6.2.1, in both cases we have $[\mathrm{SL}_2(\mathbb{Z}_3) : S_3] \leq 27 \cdot 3^{2n_3}$.

- $\underline{p = 2}$. Since $m_2 = 1$ by definition, we have $[K_2 : \mathbb{Q}^{\mathrm{ab}}] = 1$. As shown in the proof of Proposition 6.4.10, we know that $[K_3 : \mathbb{Q}^{\mathrm{ab}}] = \mathrm{Ent}(3, 2)$

divides 24. We recall that the index $[\mathrm{SL}_2(\mathbb{Z}_2) : S_2]$ is divisible by 3 if and only if E admits a rational 2-isogeny (i.e. if $\mathrm{Im}\,\rho_{E,2}$ is contained in a Borel subgroup). Equivalently, the extension $\mathbb{Q}^{\mathrm{ab}}(E[2^\infty])/\mathbb{Q}^{\mathrm{ab}}$ is a pro-2 extension if and only if E admits a rational 2-isogeny. If E has a rational 2-isogeny, $[K_3 : \mathbb{Q}^{\mathrm{ab}}]$ divides 8, and by [RZB15, Corollary 1.3] the index $[\mathrm{SL}_2(\mathbb{Z}_2) : S_2]$ must divide 96. If instead E has no rational 2-isogenies, by Proposition 6.2.3 we can assume that the index $[\mathrm{SL}_2(\mathbb{Z}_2) : S_2]$ divides 32. In both cases, we have $[\mathrm{SL}_2(\mathbb{Z}_2) : S_2]\cdot[K_3 : \mathbb{Q}^{\mathrm{ab}}]\cdot[K_2 : \mathbb{Q}^{\mathrm{ab}}] \leq 96\cdot 8 = 32 \cdot 24 = 768$.

Writing $\Lambda = \prod_{p\in\mathcal{P}} p^{n_p}$, combining the bounds above with equations (6.4.6) and (6.4.7), we obtain

$$[\mathrm{SL}_2(\mathbb{Z}_m) : S_{\mathcal{P}}] \leq 168 \cdot 30 \cdot 336 \cdot 120 \cdot 27 \cdot 768 \cdot \Lambda^2 \leq 4.3 \cdot 10^{12} \cdot \Lambda^2, \quad (6.4.8)$$

concluding the proof. □

Proposition 6.4.12. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. If there exists a prime $q > 13$ such that $\mathrm{Im}\,\rho_{E,q} \subseteq C_{ns}^+(q)$, then Theorem 6.4.1 holds.*

We now give the final part of the proof of Theorem 6.4.1, treating separately cases (A) and (B) of Proposition 6.4.7.

Proof of Theorem 6.4.1. We notice that if $j(E)$ belongs to the list (6.4.2), by Proposition 6.4.4 we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq 2736$, hence we can assume that $j(E)$ is not in the list.
Suppose first that case (A) of Proposition 6.4.7 holds. Let $\mathcal{C}$ be the set of all odd primes p such that $\mathrm{Im}\,\rho_{E,p} \subseteq C_{ns}^+(p)$ and let $\mathcal{C}_{ns} = \mathcal{C} \setminus \{3, 5\}$. For every $p \in \mathcal{C}$, define n_p as the largest integer n for which $\mathrm{Im}\,\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$, and let $\Lambda := \prod_{p\in\mathcal{C}} p^{n_p}$. By Lemma 6.4.10 we know that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq 2488320 \cdot \Delta_7' \cdot 3^{|\mathcal{C}_{ns}|} \cdot \Lambda^3, \quad (6.4.9)$$

where we can assume that $\Delta_7' := 1$ if $7 \notin \mathcal{C}$ and $\Delta_7' := \frac{8}{3}$ otherwise: indeed, we have $\Delta_7 \cdot 3^\beta \leq \max\{1 \cdot 3^{|C_{ns}|}, \frac{8}{3} \cdot 3^{|C_{ns}|}, 8 \cdot 3^{|C_{ns}|-1}\}$, so we can set $\Delta_7' := \min\{\Delta_7, \frac{8}{3}\}$. As in the proof of Theorem 4.2.5, we treat separately the cases in which $j(E) \in \mathbb{Z}$ and $j(E) \notin \mathbb{Z}$.
Suppose first that $j(E) \notin \mathbb{Z}$. We can write $2488320 \cdot \Delta_7' \leq 6635520$. By Proposition 6.4.4 we know that $\mathcal{C}_{ns} \subseteq \{7, 11\} \cup \{p \in \mathcal{C}_{ns} \mid p \geq 19\}$, and so, as in the proof of Theorem 4.2.5 we have

$$\begin{aligned} |\mathcal{C}_{ns}| &\leq \max\left\{\log_{19}\Lambda, 1 + \log_{19}\frac{\Lambda}{7}, 1 + \log_{19}\frac{\Lambda}{11}, 2 + \log_{19}\frac{\Lambda}{77}\right\} \\ &\leq \log_{19}\Lambda + 1 - \log_{19} 7 < \log_{19}\Lambda + 0.525. \end{aligned}$$

Applying Theorem 4.2.4 we obtain

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &< 6635520 \cdot 3^{\log_{19}\Lambda + 0.525} \cdot \Lambda^3 < 6635520 \cdot 3^{0.525} \cdot \Lambda^{3+\log_{19} 3} \\ &< 6635520 \cdot 3^{0.525} \cdot \left(\frac{12}{\log 2}\right)^{3+\log_{19} 3} \cdot (\mathrm{h}_{\mathcal{F}}(E) + 1.5)^{3+\log_{19} 3} \\ &< 1.78 \cdot 10^{11} \cdot (\mathrm{h}_{\mathcal{F}}(E) + 1.5)^{3.38}. \end{aligned} \tag{6.4.10}$$

We can now write $|\mathcal{C}_{ns}| \leq |\mathcal{C}| = \omega(\Lambda)$, which is the function counting the distinct prime divisors of Λ. We can assume that $\Lambda \geq 26$, otherwise we would get a stronger statement, hence by [Rob83, Théorème 13] and Theorem 4.2.5 we have

$$\begin{aligned}\omega(\Lambda) &< \frac{\log \Lambda}{\log\log \Lambda - 1.1714} < \frac{1.308 \log(\mathrm{h}_{\mathcal{F}}(E) + 40) + \log 21000}{\log(1.308 \log(\mathrm{h}_{\mathcal{F}}(E) + 40) + \log 21000) - 1.1714} \\ &< (1.308 \log(\mathrm{h}_{\mathcal{F}}(E) + 40) + \log 21000)\delta(\mathrm{h}_{\mathcal{F}}(E)).\end{aligned}$$

Using this bound in equation (6.4.9) and applying again Theorem 4.2.4 we obtain

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &< 6635520 \cdot 3^{\log 21000 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E) + 40)^{1.308 \cdot \log 3 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} \cdot \Lambda^3 \\ &< 9 \cdot 10^9 (\mathrm{h}_{\mathcal{F}}(E) + 40)^{1.308 \cdot \log 3 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} \cdot \Lambda^3 \\ &< 9 \cdot 10^9 \left(\frac{12}{\log 2}\right)^3 (\mathrm{h}_{\mathcal{F}}(E) + 40)^{1.437 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E) + 1.5)^3 \\ &< 5 \cdot 10^{13} (\mathrm{h}_{\mathcal{F}}(E) + 40)^{1.437 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E) + 1.5)^3,\end{aligned}$$

where we used that $3^{\log 21000 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} < 1340$ for $\mathrm{h}_{\mathcal{F}}(E) > -0.75$ (which can be assumed by Remark 1.2.9). This inequality is better than the statement of the theorem.

Suppose now that $j(E) \in \mathbb{Z}$. By Lemma 5.3.3(2) we know that either $j(E)$ belongs to the list (5.3.1) and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 504$, or $7 \notin \mathcal{C}_{ns}$. In the former case, the theorem trivially holds, hence we can assume that $7 \notin \mathcal{C}_{ns}$. By [ST12] we also have that $11 \notin \mathcal{C}_{ns}$. Using again Proposition 6.4.4, we obtain that $|\mathcal{C}_{ns}| \leq \log_{19} \Lambda$ and $\Delta_7' = 1$, hence applying Theorem 4.2.5 to equation (6.4.9) we have

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &< 2488320 \cdot 3^{\log_{19}\Lambda} \cdot \Lambda^3 < 2488320 \cdot \Lambda^{3+\log_{19} 3} \\ &< 2488320 \cdot (21000)^{3+\log_{19} 3} \cdot (\mathrm{h}_{\mathcal{F}}(E) + 40)^{1.308 \cdot (3+\log_{19} 3)} \\ &< 9.5 \cdot 10^{20} \cdot (\mathrm{h}_{\mathcal{F}}(E) + 40)^{4.42}.\end{aligned}$$

Assume now that $\mathrm{h}_{\mathcal{F}}(E) > 4 \cdot 10^{15}$. We have

$$2488320 \cdot 3^{\log 21000 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} < 1.13 \cdot 10^8.$$

As before, we can apply Theorem 4.2.5 in equation (6.4.9) to obtain

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &< 2488320 \cdot 3^{\log 21000 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E)+40)^{1.308 \cdot \log 3 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} \Lambda^3 \\ &< 1.13 \cdot 10^8 \cdot 14400^3 (\mathrm{h}_{\mathcal{F}}(E)+40)^{4.158 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E)+22.5)^3 \\ &< 3.38 \cdot 10^{20} (\mathrm{h}_{\mathcal{F}}(E)+40)^{4.158 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E)+22.5)^3.\end{aligned}$$

To conclude, it suffices to notice that for $\mathrm{h}_{\mathcal{F}}(E) \geq 10^{15}$ we have

$$\left(\frac{x+40}{x+22.5}\right)^{4.158 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} < 1 + 10^{-5}$$

and for $\mathrm{h}_{\mathcal{F}}(E) \leq 10^{15}$ we have

$$9.5 \cdot 10^{20} (\mathrm{h}_{\mathcal{F}}(E)+40)^{4.42} < 3.4 \cdot 10^{20} (\mathrm{h}_{\mathcal{F}}(E)+22.5)^{3+4.158 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))}.$$

Assume now that we are in case (B) of Proposition 6.4.7. By Lemma 6.4.11 and Theorem 4.2.5 we have

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &< 4.3 \cdot 10^{12} \cdot 21000^2 \cdot (\mathrm{h}_{\mathcal{F}}(E)+40)^{2.616} \\ &< 1.9 \cdot 10^{21} \cdot (\mathrm{h}_{\mathcal{F}}(E)+40)^{2.616},\end{aligned}$$

which is better than the first statement of the theorem for $\mathrm{h}_{\mathcal{F}}(E) > -0.75$. Similarly, we have

$$\begin{aligned}[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &\leq 4.3 \cdot 10^{12} \cdot \Lambda^2 \\ &< 4.3 \cdot 10^{12} \cdot 14400^2 (\mathrm{h}_{\mathcal{F}}(E)+40)^{1.814 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E)+22.5)^2 \\ &< 9 \cdot 10^{20} \cdot (\mathrm{h}_{\mathcal{F}}(E)+40)^{1.814 \cdot \delta(\mathrm{h}_{\mathcal{F}}(E))} (\mathrm{h}_{\mathcal{F}}(E)+22.5)^2,\end{aligned}$$

which is again better than the second statement of the theorem for $\mathrm{h}_{\mathcal{F}}(E) > -0.75$. □

A bound in terms of the conductor

We conclude this chapter by giving another bound on the index of the adelic representation ρ_E. This new bound is given in terms of the conductor and not in terms of the height as before. In particular, we prove an effective and improved version of [Zyw11, Theorem 1.1(ii)].

Theorem 6.4.13. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let N be the product of the primes of bad reduction of E and let $\omega(N)$ be the number of prime factors of N. We have*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] < 2488320 \left(51N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)}.$$

To prove this result, we improve Proposition 3.3 of the article of Zywina [Zyw11] applying the sharpened version of a lemma of Kraus [Kra95] obtained in Chapter 1. The proof is very similar to that of Zywina, however, we have to slightly modify his argument to make it work for the prime $p = 3$.

Let p be an odd prime such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$ and consider the quadratic character ε_p defined as

$$\varepsilon_p : \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \xrightarrow{\rho_{E,p}} C_{ns}^+(p) \longrightarrow \frac{C_{ns}^+(p)}{C_{ns}(p)} \cong \{\pm 1\}.$$

We can identify ε_p with a Dirichlet character of the absolute Galois group of $\mathbb{Q}$. If $p > 3$, Serre showed that the character ε_p is unramified at all primes ℓ that do not divide N (see [Ser72, Section 5.8, (c_2)]). If instead $p = 3$, by the Néron–Ogg-Shafarevich criterion ε_p is unramified at all primes ℓ such that $\ell \nmid 3N$. We will show that, for our purpose, we can assume that ε_3 is unramified at 3 whenever $3 \nmid N$.

Lemma 6.4.14. *Let p be an odd prime and let ε_p be defined as above. The character ε_p is unramified at all primes $\ell \nmid pN$. Moreover, we have the following.*

- *If $p > 3$ and $p \nmid N$, the character ε_p is unramified at p.*
- *If $3 \nmid N$ and $\operatorname{Im}\rho_{E,9} \subseteq C_{ns}^+(9)$, the character ε_3 is unramified at 3.*

Proof. We follow the proof of Serre for $p > 3$ and we show that in our case the argument also works for $p = 3$. The fact that ε_p is unramified at $\ell \nmid pN$ follows from the Néron–Ogg–Shafarevich criterion. Since $p \nmid N$, the curve E has good reduction at p. By [Ser72, Section 1.11, Propositions 11 and 12] we know that the image $I := \rho_{E,p}(I_p)$ of the inertia subgroup I_p at p is either a group of the form $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ or a group of order $p^2 - 1$, depending on whether the curve E has ordinary or supersingular reduction respectively. In the latter case, the group I is contained in $C_{ns}(p)$, because every element in $C_{ns}^+(p) \setminus C_{ns}(p)$ has order dividing $2(p-1)$ and $p^2 - 1 > 2(p-1)$ (see also [Ser72, Section 2.2, Proposition 14]). If instead E has ordinary reduction at p, for $p > 3$ there exists an element in I with eigenvalues $\lambda_1, \lambda_2 \in \mathbb{F}_p$ such that $\lambda_1 \neq \pm\lambda_2$. However, every element in $C_{ns}^+(p)$ has eigenvalues conjugate over $\mathbb{F}_{p^2}$ up to sign, and hence this case never occurs (see also again [Ser72, Section 2.2, Proposition 14]). On the other hand, if $p = 3$ and $\operatorname{Im}\rho_{E,9} \subseteq C_{ns}^+(9)$, by Lemma 6.1.3 the curve E cannot have ordinary reduction at 3. □

If $\ell \nmid N$, we can consider the reduction $\widetilde{E}$ of E modulo ℓ. As usual, we define the number $a_\ell(E) := \ell + 1 - |\widetilde{E}(\mathbb{F}_\ell)|$.

Lemma 6.4.15. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ and let $p^n \neq 3$ be an odd prime power such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. Let N be the product of the primes for which E has bad reduction and let ε_p be defined as above. If $\ell \nmid N$ is a prime for which $\varepsilon_p(\ell) = -1$, then $a_\ell(E) \equiv 0 \pmod{p^n}$.*

Proof. By Lemma 6.4.14, for every $\ell \nmid N$ we have that ε_p and ρ_{E,p^n} are unramified. The condition $\varepsilon_p(\ell) = -1$ means that $\rho_{E,p^n}(\mathrm{Frob}_\ell) \in C_{ns}^+(p^n) \setminus C_{ns}(p^n)$, and hence it is an element with trace equal to 0. This implies that $a_\ell(E) \equiv \operatorname{tr}(\rho_{E,p^n}(\mathrm{Frob}_\ell)) \equiv 0 \pmod{p^n}$. □

Lemma 6.4.16. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ and let N be the product of the primes for which E has bad reduction. If there exists an odd prime p such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$, then $N > 5$.*

Proof. As there are no elliptic curves defined over $\mathbb{Q}$ with good reduction at all primes, it suffices to show that $N \notin \{2, 3, 5\}$. If $N = 2$, as proved in [Ogg66], we must have that $j(E) \in \{12^3, 20^3, 66^3, 2^7, 2^5 \cdot 7^3\}$, and since E does not have CM we have $j(E) \in \{2^7, 2^5 \cdot 7^3\}$. We can use the algorithm `FindOpenImage.m` from [Zyw22] to show that in these cases there are no primes $p > 2$ such that $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)$. Indeed, by Lemma 5.4.27 this property only depends on the j-invariant of E. If $N = 3$, we can use the classification of elliptic curves with conductor of the form $2^a \cdot 3^b$ given by Coghlan [Cog67], and republished in [BK06, Table 4], which shows that there are no non-CM elliptic curves with conductor a power of 3. If $N = 5$, by modularity theorem [BCDT01] we know that E corresponds to a non-trivial cusp form for one of the modular groups $\Gamma_0(5)$ and $\Gamma_0(25)$. However, the vector spaces $S_2(\Gamma_0(5))$ and $S_2(\Gamma_0(25))$ are trivial, and hence there are no elliptic curves with $N = 5$. □

Proposition 6.4.17. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Let N be the product of the primes for which E has bad reduction and let ε be a quadratic Dirichlet character with conductor dividing $N \cdot \operatorname{lcm}(N, 2)$. If $N > 2$, there exists a prime $\ell \nmid N$ with*

$$\ell < 312 \cdot N^2(1 + \log\log N)$$

such that $\varepsilon(\ell) = -1$ and $a_\ell(E) \neq 0$.

Proof. Set $E_1 := E$ and consider the elliptic curve E_2 obtained by twisting E_1 by the character ε. Let ℓ be a prime that does not divide N. By definition, E_2 has good reduction at ℓ and $a_\ell(E_2) = \varepsilon(\ell)a_\ell(E_1)$. In particular, we notice that $a_\ell(E_2) \neq a_\ell(E_1)$ if and only if $a_\ell(E) \neq 0$ and $\varepsilon(\ell) = -1$. Hence, it suffices to prove that there exists a small prime ℓ such that $a_\ell(E_2) \neq a_\ell(E_1)$. First, we notice that there exists a prime $\ell \nmid N$ such that $a_\ell(E) \neq 0$ and $\varepsilon(\ell) = -1$, otherwise E would have complex multiplication by the quadratic field that corresponds to ε. Let N_i be the conductor of E_i and define $N_i' :=$

$N_i \prod_{q|N} q^{d_i(q)}$, where $d_i(q) = 0$, 1 or 2 if E_i has additive, multiplicative or good reduction respectively, at q. If M is the least common multiple of N_1' and N_2', by [Del85b, Section 5 C] there exists a prime $\ell \leq \frac{M}{6} \prod_{q|M} \left(1 + \frac{1}{q}\right)$ such that $a_\ell(E_1) \neq a_\ell(E_2)$. This last property is implied by the modularity of E_1 and E_2, which follows by [BCDT01]. We see that M divides the number $2^6 \cdot 3^3 \cdot N^2$. In particular, since $N > 2$, we can apply Lemma 1.1.4 to obtain

$$\ell \leq 2^5 \cdot 3^2 \cdot N^2 \prod_{q|N} \left(1 + \frac{1}{q}\right) < 312 \cdot N^2(1 + \log\log N). \qquad \square$$

Remark 6.4.18. Notice that by the proof of Proposition 6.4.17 we can actually deduce that if N is a prime greater than 3, then

$$\ell \leq \frac{N(N+1)}{6}.$$

Indeed, this follows from the fact that M actually divides N^2.

Proposition 6.4.19. *Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let N be the product of the primes for which E has bad reduction. Let $\omega(N)$ be the number of prime divisors of N. Let M be the minimum positive integer such that if $\rho_{E,p^n}(G_\mathbb{Q}) \subseteq C_{ns}^+(p^n)$ for an odd prime power $p^n \neq 3$, then p^n divides M. We have*

$$M < \left(35.33 \cdot N(1 + \log\log N)^{\frac{1}{2}}\right)^{\omega(N)} \quad \text{for every } N, \text{ and}$$

$$M \leq \sqrt{\frac{2N(N+1)}{3}} \qquad \text{for } N \text{ prime.}$$

Moreover, if $j(E) \notin \mathbb{Z}$ we have $M \leq \frac{N^2}{4} - 1$.

Proof. By Lemma 6.4.16 we notice that we can assume that $N > 5$. Set $N_0 := N$ if N is odd, and $N_0 := 2N$ if N is even. Let V_1 be the group of quadratic characters of $\left(\mathbb{Z}/N_0\mathbb{Z}\right)^\times$. We may view V_1 as a vector space of dimension $\omega(N)$ over $\mathbb{F}_2$. We define a sequence of primes $\ell_1, \ldots, \ell_{\omega(N)}$ relatively prime to N such that $a_{\ell_i}(E) \neq 0$ for every i and for every non-trivial character $\varepsilon \in V_1$ there exists an i for which $\varepsilon(\ell_i) = -1$. We proceed by induction on i. Choose a non-trivial character $\alpha_i \in V_i$. By Proposition 6.4.17 there exists a prime $\ell_i \nmid N$ smaller than $312 \cdot N^2(1 + \log\log N)$ such that $\alpha_i(\ell_i) = -1$ and $a_{\ell_i}(E) \neq 0$. Let V_{i+1} be the subspace of V_i consisting of characters ε such that $\varepsilon(\ell_i) = 1$. The space V_{i+1} has dimension at most $\omega(N) - i$ over $\mathbb{F}_2$. In particular, $V_{\omega(N)+1} = 1$, and so the sequence of primes $\ell_1, \ldots, \ell_{\omega(N)}$ has the desired property. Define the integer $M' := \prod_{i=1}^{\omega(N)} |a_{\ell_i}(E)|$. If $p^n \neq 3$ is a prime power such that $\operatorname{Im} \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$, there exists i such that $\varepsilon_p(\ell_i) = -1$, and

hence by Lemma 6.4.15 we have $p^n \mid |a_{\ell_i}(E)|$, that implies $p^n \mid M'$, and in particular $M \leq M'$. By the Hasse's bound, for every ℓ_i we have

$$|a_{\ell_i}(E)| \leq 2\sqrt{\ell_i} < 35.33 \cdot N\sqrt{1+\log\log N},$$

and hence $M' < \left(35.33 \cdot N(1+\log\log N)^{\frac{1}{2}}\right)^{\omega(N)}$. Notice that by Remark 6.4.18, if $N = \ell$ is prime we have the stronger inequality $M' = |a_\ell(E)| \leq \sqrt{\frac{2\ell(\ell+1)}{3}}$.
Suppose now that $j(E) \notin \mathbb{Z}$. By Proposition 3.1.2 we know that if ℓ is a prime of potentially multiplicative reduction, for every odd prime power p^n such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ we have $p^n \mid \ell^2 - 1$. We then notice that $M \mid \ell^2 - 1$. If N is composite, we have $\ell \leq \frac{N}{2}$, and hence $M \leq \frac{N^2}{4} - 1$. If $N = \ell$ is prime, we have $M \leq \sqrt{\frac{2\ell(\ell+1)}{3}} \leq \frac{\ell^2}{4} - 1$, where the last inequality holds because by Lemma 6.4.16 we can assume that $\ell > 5$. □

We now divide the proof of Theorem 6.4.13 in two cases, according to whether we are in case (A) or (B) of Proposition 6.4.7.

Proof of Theorem 6.4.13. Define the set $\mathcal{C} := \{p \geq 3 \mid \operatorname{Im}\rho_{E,p} \subseteq C_{ns}^+(p)\}$. For every $p \in \mathcal{C}$, let n_p be the largest integer n such that $\operatorname{Im}\rho_{E,p^n} \subseteq C_{ns}^+(p^n)$, and define $\Lambda := \prod_{p\in\mathcal{C}} p^{n_p}$. Set

$$\beta := |\{p \in \mathcal{C} \ : \ p > 5 \text{ and } E \text{ has bad reduction at } p\}| \leq \min\{\omega(\Lambda), \omega(N)\}.$$

We notice that $j(E)$ does not belong to the list (6.4.2), otherwise by Proposition 6.4.4 we would have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 2736$, which is better than the statement of the theorem. Suppose first that we are in case (A) of Proposition 6.4.7, i.e. that $\mathcal{C}$ contains a prime $p > 13$. By Lemma 6.4.10 we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 2488320 \cdot \Delta_7 \cdot 3^\beta \cdot \Lambda^3,$$

where $\Delta_7 \in \left\{1, \frac{8}{3}, 8\right\}$. If $j(E) \in \mathbb{Z}$, we can assume that $7 \notin \mathcal{C}$: indeed, using Lemma 5.3.3(1) we have that either $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] \leq 504$, which is better than the statement of the theorem, or $7 \notin \mathcal{C}$. In particular, we may assume that $\Delta_7 = 1$. Moreover, in the proof of Lemma 6.4.10 we used the bound $[\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{Im}\rho_{E,3^\infty}] \leq 3^{\max\{3,3n_3-1\}} \leq 27 \cdot 3^{3n_3}$, hence we can assume that $n_3 \neq 1$. We can then apply Proposition 6.4.19 and obtain

$$\begin{aligned}
[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] &\leq 2488320 \cdot 3^{\omega(N)} \cdot \left(35.33 \cdot N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)} \\
&= 2488320 \left(35.33\sqrt[3]{3} \cdot N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)} \\
&< 2488320 \left(51N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)}.
\end{aligned}$$

If $j(E) \notin \mathbb{Z}$ then we can bound $\Delta_7 \leq 8$ and using Proposition 6.4.19 we obtain

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 8 \cdot 2488320 \left(\frac{N^2}{4} - 1\right)^3 < 2488320 \left(51N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)} \tag{6.4.11}$$

for $\omega(N) > 1$, and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 8 \cdot 2488320 \left(\frac{2N(N+1)}{3}\right)^{\frac{3}{2}} < 2488320 \left(51N(1+\log\log N)^{\frac{1}{2}}\right)^{3\omega(N)} \tag{6.4.12}$$

for $\omega(N) = 1$.
Suppose now that we are in case (B) of Proposition 6.4.7, i.e. that for every prime $p > 13$ the representation $\rho_{E,p}$ is surjective. By Lemma 6.4.11 we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 4.3 \cdot 10^{12} \cdot \Lambda^2$. Moreover, we notice that in the proof of Lemma 6.4.11, in the case '$p = 3$', we used the bound $[\mathrm{SL}_2(\mathbb{Z}_3) : S_3] \leq 3^{\max\{3,2n_3-1\}} \leq 27 \cdot 3^{2n_3}$, and hence we can assume that $n_3 \neq 1$. We treat again separately the cases $j(E) \in \mathbb{Z}$ and $j(E) \notin \mathbb{Z}$. If $j(E)$ is not an integer, we can apply Proposition 6.4.19 to obtain

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 4.3 \cdot 10^{12} \cdot \Lambda^2 < 4.3 \cdot 10^{12} \cdot \left(\frac{N^2}{4} - 1\right)^2 \quad \text{for every } N, \text{ and}$$

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < 4.3 \cdot 10^{12} \cdot \frac{2}{3} N\,(N+1) \qquad \text{for } N \text{ prime.}$$

One can verify that the first inequality is always better than the statement of the theorem for $\omega(N) > 1$, while for $\omega(N) = 1$ we can use the second inequality, which is better than the statement of the theorem for $N > 5$ (which we can assume by Lemma 6.4.16). If instead $j(E)$ is an integer, by [BDM$^+$19, Corollary 1.3] and [ST12] we can assume that $11, 13 \notin \mathcal{C}$. In particular, if we look at the case '$p = 11$' in the proof of Lemma 6.4.11, we deduce that $\rho_{E,11}$ must be surjective (otherwise its image would be contained in a Borel and we would have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \leq 2736$), and hence we can save a factor 30 in equation (6.4.8). We then obtain

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < \frac{4.3 \cdot 10^{12}}{30} \cdot \Lambda^2 < \frac{4.3 \cdot 10^{12}}{30} \left(51N(1+\log\log N)^{\frac{1}{2}}\right)^{2\omega(N)}$$

for every N, and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < \frac{4.3 \cdot 10^{12}}{30} \left(\frac{2N(N+1)}{3}\right)^{\omega(N)} \quad \text{for } N \text{ prime.}$$

The first inequality is always better than the statement for $\omega(N) > 1$, and the second is better as well for $\omega(N) = 1$. Indeed, in both cases we have $N > 5$ by Lemma 6.4.16. $\square$

Bibliography

[Ara08] Keisuke Arai. On uniform lower bound of the Galois images associated to elliptic curves. *J. Théor. Nombres Bordeaux*, 20(1):23–43, 2008.

[Bar09] Burcu Baran. A modular curve of level 9 and the class number one problem. *J. Number Theory*, 129(3):715–728, 2009.

[Bar10] Burcu Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *J. Number Theory*, 130(12):2753–2772, 2010.

[BBM21] Aurélien Bajolet, Yuri Bilu, and Benjamin Matschke. Computing integral points on $X_{ns}^{+}(p)$. *Algebra & Number Theory*, 15(3):569–608, 2021.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[BDM+23] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Quadratic Chabauty for modular curves: algorithms and examples. *Compositio Mathematica*, 159(6):1111–1152, 2023.

[BJ16] Julio Brau and Nathan Jones. Elliptic curves with 2-torsion contained in the 3-torsion field. *Proc. Amer. Math. Soc.*, 144(3):925–936, 2016.

[BK06] Bryan J. Birch and Willem Kuyk. *Modular Functions of One Variable IV: Proceedings of the International Summer School, University of Antwerp, July 17-August 3, 1972*, volume 476. Springer, 2006.

[BP11a] Yuri Bilu and Pierre Parent. Runge's method and modular curves. *International Mathematics Research Notices*, 2011(9):1997–2027, 2011.

[BP11b] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Annals of Mathematics*, pages 569–584, 2011.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[BS14] Aurélien Bajolet and Min Sha. Bounding the j-invariant of integral points on $X_{ns}^+(p)$. *Proc. Amer. Math. Soc.*, 142(10):3395–3410, 2014.

[Cai22] Yulin Cai. An explicit bound of integral points on modular curves. *Commun. Math.*, 30(1):161–174, 2022.

[Che99] Imin Chen. On Siegel's modular curve of level 5 and the class number one problem. *J. Number Theory*, 74(2):278–297, 1999.

[Cog67] Francis B. Coghlan. *Elliptic Curves with Conductor $N = 2^m 3^n$*. ProQuest LLC, Ann Arbor, MI, 1967. Thesis (Ph.D.)–The University of Manchester (United Kingdom).

[Coj05] Alina Carmen Cojocaru. On the surjectivity of the Galois representations associated to non-CM elliptic curves. *Canad. Math. Bull.*, 48(1):16–31, 2005. With an appendix by Ernst Kani.

[Deb14] Christophe Debry. Beyond two criteria for supersingularity: coefficients of division polynomials. *J. Théor. Nombres Bordeaux*, 26(3):595–606, 2014.

[Del85a] Pierre Deligne. Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings). Number 121-122, pages 25–41. 1985. Seminar Bourbaki, Vol. 1983/84.

[Del85b] Pierre Deligne. Représentations l-adiques. Number 127, pages 249–255. 1985. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84).

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DLR23] Harris B. Daniels and Álvaro Lozano-Robledo. Coincidences of division fields. *Ann. Inst. Fourier (Grenoble)*, 73(1):163–202, 2023.

[DM22] Harris B. Daniels and Jackson S. Morrow. A group theoretic perspective on entanglements of division fields. *Trans. Amer. Math. Soc. Ser. B*, 9:827–858, 2022.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 349, pages 143–316. Springer, Berlin, 1973.

[Ejd22] Özlem Ejder. Isolated points on $X_1(\ell^n)$ with rational j-invariant. *Res. Number Theory*, 8(1):Paper No. 16, 7, 2022.

[Elk99] Noam D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 51–101. Cambridge Univ. Press, Cambridge, 1999.

[FL23a] Lorenzo Furio and Davide Lombardo. Computational data accompanying the paper 'Serre's uniformity question and proper subgroups of $C_{ns}^+(p)$', 2023. Available at `https://github.com/DavideLombardoMath/Cartan-cubes`.

[FL23b] Lorenzo Furio and Davide Lombardo. Serre's uniformity question and proper subgroups of $C_{ns}^+(p)$. *arXiv preprint arXiv:2305.17780*, 2023.

[GR14] Éric Gaudron and Gaël Rémond. Théorème des périodes et degrés minimaux d'isogénies. *Comment. Math. Helv.*, 89(2):343–403, 2014.

[Gre12] Ralph Greenberg. The image of Galois representations attached to elliptic curves with an isogeny. *Amer. J. Math.*, 134(5):1167–1196, 2012.

[GRSS14] Ralph Greenberg, Karl Rubin, Alice Silverberg, and Michael Stoll. On elliptic curves with an isogeny of degree 7. *Amer. J. Math.*, 136(1):77–109, 2014.

[HH08] Abdolhossein Hoorfar and Mehdi Hassani. Inequalities on the Lambert W function and hyperpower function. *JIPAM. J. Inequal. Pure Appl. Math.*, 9(2):Article 51, 5, 2008.

[JM22] Nathan Jones and Ken McMurdy. Elliptic curves with non-abelian entanglements. *New York J. Math.*, 28:182–229, 2022.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 350, pages 69–190. Springer, Berlin, 1973.

[Ken85] Monsur A. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32(1):45–48, 1985.

[KL81] Daniel S. Kubert and Serge Lang. *Modular units*, volume 244 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York-Berlin, 1981.

[Kra90] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta mathematica*, 69(1):353–385, 1990.

[Kra95] Alain Kraus. Une remarque sur les points de torsion des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 321(9):1143–1146, 1995.

[Lem19a] Pedro Lemos. Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies. *Trans. Amer. Math. Soc.*, 371(1):137–146, 2019.

[Lem19b] Pedro Lemos. Some cases of Serre's uniformity problem. *Math. Z.*, 292(1-2):739–762, 2019.

[LF16] Samuel Le Fourn. Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves. *Mathematische Annalen*, 365(1):173–214, 2016.

[LFL21] Samuel Le Fourn and Pedro Lemos. Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan. *Algebra & Number Theory*, 15(3):747–771, 2021.

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2024. [Online; accessed 6 September 2024].

[Lom15] Davide Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra Number Theory*, 9(10):2347–2395, 2015.

[LR16] Álvaro Lozano-Robledo. Ramification in the division fields of elliptic curves with potential supersingular reduction. *Res. Number Theory*, 2:Paper No. 8, 25, 2016.

[LT22] Davide Lombardo and Sebastiano Tronto. Some uniform bounds for elliptic curves over $\mathbb{Q}$. *Pacific J. Math.*, 320(1):133–175, 2022.

[Lub79] Jonathan Lubin. Canonical subgroups of formal groups. *Trans. Amer. Math. Soc.*, 251:103–127, 1979.

[Maz77] Barry Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, volume Vol. 601 of *Lecture Notes in Math.*, pages 107–148. Springer, Berlin-New York, 1977.

[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mor19] Jackson S. Morrow. Composite images of Galois for elliptic curves over $\mathbf{Q}$ and entanglement fields. *Math. Comp.*, 88(319):2389–2421, 2019.

[MW93a] David W. Masser and Gisbert Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[MW93b] David W. Masser and Gisbert Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[MW24] Jacob Mayle and Tian Wang. On the effective version of Serre's open image theorem. *Bull. Lond. Math. Soc.*, 56(4):1399–1416, 2024.

[Naj18] Filip Najman. Isogenies of non-CM elliptic curves with rational j-invariants over number fields. *Math. Proc. Cambridge Philos. Soc.*, 164(1):179–184, 2018.

[Ogg66] Andrew P. Ogg. Abelian curves of 2-power conductor. *Proc. Cambridge Philos. Soc.*, 62:143–148, 1966.

[Paz19] Fabien Pazuki. Modular invariants and isogenies. *International Journal of Number Theory*, 15(03):569–584, 2019.

[Per69] G. I. Perel'muter. Estimation of a sum along an algebraic curve. *Mathematical notes of the Academy of Sciences of the USSR*, 5(3):223–227, 1969.

[Rad68] Charles M Rader. Discrete fourier transforms when the number of data samples is prime. *Proceedings of the IEEE*, 56(6):1107–1108, 1968.

[Rob83] Guy Robin. Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arith.*, 42(4):367–389, 1983.

[RS62] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight). *Forum Math. Sigma*, 10:Paper No. e62, 63, 2022. With an appendix with John Voight.

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory*, 1:Paper No. 12, 34, 2015.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sha14] Min Sha. Bounding the j-invariant of integral points on modular curves. *Int. Math. Res. Not. IMRN*, (16):4492–4520, 2014.

[Sil86] Joseph H. Silverman. Heights and elliptic curves. In *Arithmetic geometry*, pages 253–265. Springer, 1986.

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

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

[Sma98] Nigel P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[Smi23] Hanson Smith. Ramification in division fields and sporadic points on modular curves. *Research in Number Theory*, 9(1):17, 2023.

[SP11] Patrick Solé and Michel Planat. Extreme values of the Dedekind Ψ function. *J. Comb. Number Theory*, 3(1):33–38, 2011.

[ST12] René Schoof and Nikos Tzanakis. Integral points of a modular curve of level 11. *Acta Arith.*, 152(1):39–49, 2012.

[Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:Paper No. e4, 79, 2016.

[SZ17] Andrew V. Sutherland and David Zywina. Modular curves of prime-power level with infinitely many rational points. *Algebra Number Theory*, 11(5):1199–1229, 2017.

[Wei48] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.*, 34:204–207, 1948.

[Wil98] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1998.

[Zyw11] David Zywina. Bounds for Serre's open image theorem. *arXiv preprint arXiv:1102.4656*, 2011.

[Zyw15a] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015.

[Zyw15b] David Zywina. Possible indices for the galois image of elliptic curves over q. *arXiv preprint arXiv:1508.07663*, 2015.

[Zyw22] David Zywina. Explicit open images for elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:2206.14959*, 2022.