Computing with necklaces on elliptic curves

Marusia Rebolledo and Christian Wuthrich

8th September 2026

Abstract

We present computational algorithms to work with points on the modular curve associated to the normaliser of a non-split Cartan group of prime level p. Rather than working with explicit equations, we represent these points using the moduli interpretation of necklaces in the p-torsion of elliptic curves. We use our methods to investigate for which primes $\ell \neq p$ two rational points with complex multiplication can have equal reduction modulo ℓ.

1 Introduction

Concrete calculations with modular curves have attracted a lot of attention in recent years. Specifically, the study of algorithms working with explicit isogenies and torsion points on elliptic curves both over number fields and finite fields are an active area. These correspond to points on the modular curves $X_0(N)$ and $X_1(N)$. The present article grew out of the attempt to work explicitly with points on a different modular curve, namely the one associated to the normaliser of a non-split Cartan subgroup. In [18], the authors have introduced a moduli interpretation for this curve, which is the starting point for the algorithms presented here.

Let p be an odd prime. We denote by X the modular curve $X^+_{\mathrm{nsp}}(p)$, which is a smooth projective curve defined over the rational numbers. A model can be obtained by taking the quotient of the modular curve $X(p)$ by the normaliser of a choice of a non-split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$. Let $Y = Y^+_{\mathrm{nsp}}(p)$ be the affine curve obtained by omitting the cusps. For a field of characteristic different from p, the points in $Y(\bar{k})$ can be viewed as $\bar{k}$-isomorphism classes of pairs $(E, \mathfrak{v})$ where E is an elliptic curve defined over $\bar{k}$ and $\mathfrak{v}$ is a **necklace** in $E[p]$. Here a necklace is a particular arrangement of the $p+1$ distinct cyclic subgroup of order p in E. The precise definition is given in [18] and repeated in Section 2.1.

Equations giving (possibly singular) models for this curve are currently only known for prime level up to 23 by the works of several authors [3, 11, 14, 17]. They are listed together with plenty of other information on the LMFDB data base [15]. Although this is not the focus of the article, the study of the curve $X = X^+_{\mathrm{nsp}}(p)$ is motivated by Serre's uniformity conjecture [21], which could be resolved if the $\mathbb{Q}$-rational points of X are shown to consist solely of CM points. The approach using explicit equations has allowed to determine $X(\mathbb{Q})$ in the cases of level 13 and 17 using the quadratic Chabauty method in [1, 2].

In this article, we will avoid the use of equations for X and instead, we make possible concrete calculations using our moduli description of X introduced in [18]. One way to give a concrete description of a necklace is by listing polynomials $f_0, f_1, \ldots, f_p$ defining the cyclic subgroup schemes $C_0, C_1, \ldots, C_p$ in the order they appear in the necklace. Even if the necklace is defined over k, these polynomials will have coefficients in an extension L which we call the p-isogeny field, the smallest extension over which all isogenies of degree p leaving E are defined. If their codomains, the elliptic curves E/C_k, have distinct j-invariants, we can also just give these j-invariants $j_0, j_1, \ldots, j_p$ as elements in L. If p is relatively small and $k = \mathbb{Q}$ or if k is a finite field, we can calculate L and determine all f_k; however, for

The first named author is supported by the ANR Projects ANR-20-CE40-0003 Jinvariant and ANR-23-CE40-0006 GAEC. The second named author is partially supported by the Engineering and Physical Sciences Research Council, Grant UKRI071.

larger p this turns out to be far from efficient. The use of the p-isogeny field compared to the larger field $k\big(E[p]\big)$ is a good gain: In our case the extension L/k has typically degree $2(p+1)$, which is much smaller than $2(p^2-1)$.

We present here a first algorithm for k being a number field, which works for any elliptic curve E with a unique k-rational necklace $\mathfrak{v}$. The implementation in Sage [24] for $k=\mathbb{Q}$ can be found at [19]. The ordering of the subgroups C_i is found using a Frobenius element at a suitable auxiliary prime ideal $\mathfrak{Q}$ in L. For any prime ideal ℓ in k, we can then calculate the reduction of $(E,\mathfrak{v})$ modulo ℓ to obtain a representation $(\tilde{E},\tilde{\mathfrak{v}})$ of a point in $X(\mathbb{F}_\ell)$ where $\mathbb{F}_\ell$ is the residue field at ℓ. We have to emphasise that this is really a global problem; we cannot work in a reduction or in a completion as there the curve will usually have more than one necklace and we cannot guess which one is the reduction of a k-rational necklace we are after. Unfortunately, this first algorithm is only really practical for small primes p and for them we know good models for X.

It is expected that for $p>11$, the only points in $Y(\mathbb{Q})$ are given by $(E,\mathfrak{v})$ with E having complex multiplication. Therefore, we present a second faster algorithm for such points called **CM points**. The algorithm discussed in Section 4.3 calculates the reduced point $(\tilde{E},\tilde{\mathfrak{v}})\in X(\mathbb{F}_\ell)$ directly without having to determine L globally. It only needs to work out the p-isogeny field for the curve $\tilde{E}$ over the finite field $\mathbb{F}_\ell$. We do not know a similar construction for curves without complex multiplication.

As an application of this algorithm, we can make predictions about the following question. For which distinct primes $p,\ell\geqslant 5$ do there exist two CM points x_1 and x_2 in $X(\mathbb{Q})$ such that their reductions in $X(\mathbb{F}_\ell)$ are equal? For instance, when using an explicit Chabauty methods as in [1, 2] to determine the rational point on X for a particular p, the auxiliary prime ℓ is best chosen such that all rational points have distinct reduction, since this results in ℓ-adic analytic functions with a single zero in a residue disc. One could hope that the moduli interpretation will help the use of the geometric Chabauty method as in [8] for larger p without having to rely on explicit equations. This is one of the main motivations of this paper.

When p increases, the number of points in $X(\mathbb{F}_\ell)$ increases quite quickly, which means that we do not expect equal reduction among the finitely many CM points x_1 and x_2 in $X(\mathbb{Q})$ to happen when p is large. Having tested all $5\leqslant p<50$ and all $\ell>3$, we found equal reductions only for $p=5$ and $p=7$ and for $\ell\leqslant 17$. The eight such pairs (x_1,x_2) we found are listed in Proposition 15; it is likely that these are the only examples that exist.

This question can be seen as the first step in a deeper investigation into the arithmetic intersection number of points on the curve X analogous to the work of Gross–Zagier in [10] for the modular curve $X_0(p)$. Recently, this has been studied by Love, Studnia, and Vonk in [16]. In particular, their work gives a theoretical understanding of these intersections and verifies indeed that our eight pairs are the only such cases of equal reduction among CM points.

The algorithms in this paper are to our knowledge the first methods found to do explicit calculations with points on $X^+_{\mathrm{nsp}}(p)$ without the use of equations defining the curve. They have their limitations, but do allow for experimentations on these curves. Of course, it would be very interesting to find faster or more general methods. At this stage, we do not know if there are any applications of these algorithms over finite fields, like the theory of isogeny volcanoes [23] has.

The paper is structured as follows. Section 2 recalls the definition of necklaces and reviews background results used later. The algorithm to calculate any necklace over a number field is explained in Section 3. The reduction of necklaces, both for general as well as CM points is contained in Section 4, while Section 5 considers the question of when two points have the same reduction. The short appendix A gives a table that allows to calculate $\#X(\mathbb{F}_\ell)$.

2 Background

In this section we recall the moduli interpretation of the modular curve $X=X^+_{\mathrm{nsp}}(p)$ described in [18] and state some preliminary results. We wish to point to [22] for basic facts

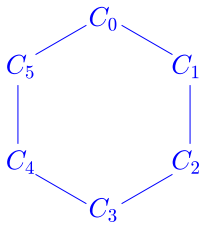
about the Galois representation $E[p]$ and the notions of Cartan subgroups and their normalisers.

2.1 Necklaces

Let p be an odd prime. We fix throughout the article a generator γ of the cyclic group $\mathbb{F}_{p^2}^\times$. By a **necklace** on an elliptic curve, we will understand a non-oriented γ-necklace as defined in [18] whose definition we are going to recall now.

Definition. Let E be an elliptic curve defined over a field k whose characteristic is different from p. A **necklace** in the p-torsion of E is defined to be an equivalence class $\mathfrak{v}$ of an ordering $(C_0, C_1, \ldots, C_p)$ of all cyclic subgroups of order p in $E(\bar{k})$ satisfying the condition that there is an element $h \in \mathrm{PGL}\big(E[p]\big)$ with $h(C_i) = C_{i+1 \bmod p+1}$ and such that there is a matrix in h whose characteristic polynomial is equal to the minimal polynomial of γ. Two such lists are equivalent if one can be obtained from the other by a cyclic permutation and a reversal $w\colon (C_0, C_1, \ldots, C_p) \mapsto (C_p, \ldots, C_1, C_0)$ if needed.

We view the cyclic subgroups C_i as pearls and the necklace as placing these pearls on a regular $(p+1)$-gon forming the picture of a pearl necklace:



Turning a necklace $\mathfrak{v}$ (acting by h) or flipping it from one side to the other (acting by the involution w) does not change the necklace by the equivalence introduced above. The subgroup of $\mathrm{PGL}(E[p])$ stabilising $\mathfrak{v}$ is generated by h and w: this is the normaliser of the non-split Cartan subgroup generated by h. Conversely, if N is the normaliser of a non-split Cartan subgroup C and h an element that generates C with characteristic polynomial equal to the minimal polynomial of γ, then acting successively by h on a given cyclic subgroup C_0 of order p gives the only necklace stabilised by N. There are $p(p-1)/2$ necklaces (see [18, Corollary 3]).

As the terminology is a little cumbersome to repeat often, we will introduce the neologism **nonoca** as an abbreviation for "normaliser of a non-split Cartan subgroup" in $\mathrm{PGL}\big(E[p]\big)$. Recall that any nonoca is isomorphic to a dihedral group of order $2(p+1)$.

There is a characterisation of necklaces without reference to h: Let $\xi = t^2/(t^2-n)$ where $t = \mathrm{Tr}(\gamma)$ and $n = \mathrm{N}(\gamma)$. A list $(C_0, C_1, \ldots, C_p)$ represents a necklace if the cross-ratio $[C_i, C_{i+1}; C_{i+2}, C_{i+3}]$ of any four consecutive pearls is equal to ξ. See Proposition 5 in [18].

Any choice of three pearls C_0, C_1 and C_2 yields a unique necklace such that C_1 is adjacent to C_0 and C_2. See Lemma 2 in [18].

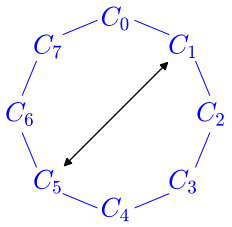
The absolute Galois group G_k of k acts on the cyclic subgroups of order p of E; we write $\rho\colon G_k \to \mathrm{PGL}\big(E[p]\big)$ for the corresponding map. This induces an action of G_k on the set of necklaces on E.

Let $X = X_{\mathrm{nsp}}^+(p)$ be the modular curve associated to the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. The affine curve obtained by removing the cusps is denoted by $Y = Y_{\mathrm{nsp}}^+(p)$. The following is proved in Section 2.3 in [18].

Proposition 1. Suppose that the characteristic of k is different from p. There is a bijection between points on $Y(\bar{k})$ and $\bar{k}$-isomorphism classes of pairs $(E, \mathfrak{v})$ where E is an elliptic curve defined over $\bar{k}$ and $\mathfrak{v}$ is a necklace in the p-torsion of E. Any point in $Y(k)$ is represented by $(E, \mathfrak{v})$ with E defined over k and, in case $j(E) \notin \{0, 1728\}$, the necklace $\mathfrak{v}$ is also defined over k.

For a point in Y with j-invariant different from 0 and 1728 to be k-rational is equivalent to asking that $\rho(G_k)$ is contained in a nonoca, namely the nonoca stabilising the corresponding necklace. The situation is more subtle for the points with j-invariant in $\{0, 1728\}$ as explained in Section 2.5.

Another important notion that we will be using is the following. Two pearls C_i and C_j are **antipodal** in a necklace $\mathfrak{v} = (C_0, C_1, \ldots, C_p)$ if $i \equiv j + (p+1)/2 \pmod{p+1}$. That is they are diametrically opposed when the necklace is represented as a regular $(p+1)$-gon:



2.2 The number of rational necklaces on a given elliptic curve

We aim to describe the number of k-rational necklaces on an elliptic curve defined over a field k. For instance, we will see that for $k = \mathbb{Q}$ there is usually at most one such necklace.

Lemma 2. Let E be an elliptic curve over a field k whose characteristic is coprime to p. The number of necklaces on E defined over k could be either 0, 1, 2 (only if $p \equiv 1 \pmod 4$), 3 (only if $p \equiv 3 \pmod 4$), $(p-1)/2$, $(p+3)/2$ or all $p(p-1)/2$ of them.

Denote by $G \leqslant \mathrm{PGL}\big(E[p]\big)$ the image of the Galois representation $\rho\colon G_k \to \mathrm{PGL}\big(E[p]\big)$. Given an element $g \in \mathrm{PGL}\big(E[p]\big)$ represented by an element $M \in \mathrm{GL}\big(E[p]\big)$, we will write

$$\delta(g) = \Big(\frac{\mathrm{Tr}(M)^2 - 4\det(M)}{p}\Big) \in \{-1, 0, 1\},$$

where $\big(\frac{\cdot}{\cdot}\big)$ denotes the Legendre symbol. If $\delta(g) \neq 0$, then g lies in a unique Cartan subgroup. The element g belongs to a split Cartan subgroup precisely when $\delta(g) = 1$, in which case we will say that g is **split**. Otherwise, when $\delta(g) = -1$, we will say that g is **non-split**. Recall that a non-trivial element of $\mathrm{PGL}(E[p])$ is split if and only if it fixes two subgroups of $E[p]$.

Proof. A necklace $\mathfrak{v}$ is defined over k if and only if G is contained in the nonoca stabilising $\mathfrak{v}$. Hence there is no necklace defined over k on $E[p]$ in the case when G is not contained in any nonoca and there is a unique one in the case when G is contained in a single nonoca. If G is trivial, then all $p(p-1)/2$ necklaces are defined over k. We may assume now that G is non-trivial.

Suppose now that E has at least two necklaces $\mathfrak{v}$ and $\mathfrak{v}'$ defined over k and hence $G \subset N \cap N'$ where N and N' are the nonocas stabilising $\mathfrak{v}$ and $\mathfrak{v}'$, respectively. As any two non-split Cartan subgroups intersect trivially, the only possible non-trivial elements in the intersection of two nonocas N and N' have order 2.

In what follows, we will say that an element of G **fixes** or **flips** a necklace $\mathfrak{v}$ if it fixes or flips the associated oriented necklace as defined in [18].

If a non-trivial element $g \in G$ is split, it is not in any non-split Cartan subgroup, hence any necklace defined over k is flipped by g, that is to say g appears as a reflection. It follows that the subgroups A and B fixed by g are antipodal in the necklace and g is the reflection whose axis is the line through A and B. By Lemma 8 in [18] there are $(p-1)/2$ such necklaces.

If g is non-split, it is in a unique non-split Cartan subgroup C_g and hence it fixes a unique necklace, namely the necklace stabilised by the normalizer of C_g. In this necklace, g appears as the rotation of angle π.

We count the number of necklaces that g flips as follows. The non-split elements of order 2 form a single conjugacy class in $\mathrm{PGL}_2(E[p])$ of cardinality $p(p-1)/2$; every non-split

Cartan subgroup contains exactly one such non-split element of order 2. Therefore, each of them flips the same number of necklaces. There are $(p+1)/2$ reflections of a regular $(p+1)$-gon that fix no corner. Therefore g, and any of its conjugate elements, will flip $(p+1)/2$ necklaces. In total, the non-split g belongs to $1+(p+1)/2 = (p+3)/2$ nonocas.

This concludes the case when G is cyclic generated by g: We obtain $(p-1)/2$ necklaces defined over k if g is split, or $(p+3)/2$ necklaces over k if g is non-split.

Suppose now that $G \subset N \cap N'$ contains two distinct non-trivial elements g_1 and g_2. In fact, G is then isomorphic to the abelian, but non-cyclic group of order 4 because these are the largest subgroups of a nonoca containing no elements of larger order. We claim that of the three elements g_1, g_2, and $g_3 = g_1 g_2$ at most one is split. Indeed, if there were two split elements, the two distinct necklaces $\mathfrak{v}$ and $\mathfrak{v}'$ would have two distinct antipodal pairs of pearls in common, which is impossible by Lemma 8 in [18].

Hence we may suppose that g_1 and g_2 are non-split. As elements of order 2 come from elements in $\mathrm{GL}\big(E[p]\big)$ with trace zero, we find $\delta(g_3) = \left(\frac{-1}{p}\right)\delta(g_1)\,\delta(g_2) = \left(\frac{-1}{p}\right)$. Thus g_3 is split if $p \equiv 1 \pmod 4$ and non-split if $p \equiv 3 \pmod 4$.

We claim that any necklace $\mathfrak{v}$ fixed by a non-split element $g \in G$ is automatically flipped by any other element $g' \in G$ using that they commute. Indeed, for any $A \in \mathbb{P}(E[p])$, A and $g(A)$ are antipodal in $\mathfrak{v}$, and so are $g'(A)$ and $gg'(A)$. In the necklace $g'(\mathfrak{v})$, it follows that $g'(A)$ and $g'g(A) = gg'(A)$ are antipodal and so are $A = g'g'(A)$ and $g(A) = g'g'g(A)$. However, by Lemma 8 in [18] there is at most one necklace with a fixed pair of antipodals. Hence $g'(\mathfrak{v}) = \mathfrak{v}$ and g' must flip $\mathfrak{v}$ as g already fixes it.

First the case $p \equiv 1 \pmod 4$: A necklace $\mathfrak{v}$ defined over k is flipped by g_3 since g_3 is split. If it were also flipped by g_1, then it is fixed by $g_2 = g_1 g_3$. Thus exactly one of g_1 or g_2 must fix $\mathfrak{v}$. We deduce that there are exactly two necklaces defined over k: one fixed by g_1, which is flipped by g_3 and g_2, and one fixed by g_2 and flipped by g_1 and g_3.

Finally the case $p \equiv 3 \pmod 4$: With the same argument as above, a necklace defined over k must be fixed by exactly one of g_1, g_2, g_3 and then, by the above claim, it is automatically flipped by the others. We conclude that there are exactly three necklaces defined over k. □

Lemma 3. Let E be an elliptic curve defined over a finite field $\mathbb{F}$ of cardinal ℓ^r with ℓ a prime distinct from p and $r \geqslant 1$ an integer. Let a be the trace of Frobenius such that $\#E(\mathbb{F}) = \ell^r + 1 - a$ and set $\delta = \left(\frac{a^2-4\ell^r}{p}\right) \in \{-1, 0, 1\}$. Denote by n_{isog} the number of isogenies of degree p defined over $\mathbb{F}$ leaving from E. The number $n_{\mathrm{necklaces}}$ of necklaces on E defined over $\mathbb{F}$ can be read off the following table:

a	δ	n_{isog}	$n_{\mathrm{necklaces}}$
0	$+1$		$(p-1)/2$
0	-1		$(p+3)/2$
$\neq 0$	$+1$		0
$\neq 0$	-1		1
$\neq 0$	0	$p+1$	$p(p-1)/2$
$\neq 0$	0	1	0

This lemma counts the number of $\mathbb{F}$-rational necklaces for $\mathbb{F}$ a finite field of characteristic different from p. For curves with j-invariant different from 0 and 1728, this is the same as the number of $\mathbb{F}$-rational points on X with that j-invariant. For the special two j-invariants this is more complicated and discussed in Section 2.5. In the case $\mathbb{F} = \mathbb{F}_\ell$, the complete table for all j-invariants is given in Appendix A, which contains the above as its final six lines.

Proof. As in the proof above, let G be the image of the absolute Galois group in $\mathrm{PGL}\big(E[p]\big)$. It is generated by the image g of the Frobenius, whose image in $\mathrm{GL}\big(E[p]\big)$ is a matrix M with characteristic polynomial $X^2 - a\,X + \ell^r \in \mathbb{F}_p[X]$. By definition $\delta(g) = \delta$. In the top row of the table, g is a split element of order 2. In the second row, it is a non-split element of order 2. If we are in the third row, then g is not in any nonoca since it is split of order

> 2. In the fourth row, g is non-split of order larger than 2; it belongs to a unique nonoca. The last two rows are matrices with repeated eigenvalues, they can either be diagonalisable matrices, that is $g = 1$ and all necklaces are rational over $\mathbb{F}$, or non-diagonalisable, in which case they are in no nonoca. In the first case, all $p + 1$ isogenies $E \to E'$ of degree p are defined over $\mathbb{F}$, in the second case, there is a unique such isogeny. □

Proposition 4. Let E be an elliptic curve defined over $\mathbb{Q}$ with $j(E) \notin \{0, 1728\}$. If $p > 5$, then there is at most one necklace defined over $\mathbb{Q}$ on E. If $p = 5$, then there are at most two.

Proof. Suppose first that E does not have complex multiplication. Theorem 1.5 in [9] by Furio and Lombardo, improving results of Zywina [25] and Le Fourn and Lemos [13], shows that for $p > 37$, either $\rho\colon G_{\mathbb{Q}} \to \mathrm{PGL}\big(E[p]\big)$ is surjective or it has image equal to a whole nonoca. They also proved in their Theorem 1.6 that for primes $5 < p \leqslant 37$ the image of ρ cannot be a proper subgroup of a nonoca. We deduce from this that if E does not have complex multiplication and $p > 5$, then there is at most one necklace defined over $\mathbb{Q}$ on E.

Suppose now that E has complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field F, by which we mean $\mathrm{End}_{\bar{\mathbb{Q}}}(E) \cong \mathcal{O}$. If the image of ρ is contained in a nonoca, then p is inert in $\mathcal{O}$ and $\rho(G_{\mathbb{Q}})$ is the whole nonoca as showed in Proposition 1.14 in [25] or in our Lemma 6 below. Again, we deduce that there is a unique necklace defined over $\mathbb{Q}$.

The image of complex conjugation under ρ is a class of matrices with trace 0 and determinant -1; therefore it is a split element of order 2. For $p = 5$, this fact together with the proof of Lemma 2 shows that there are at most $\frac{p-1}{2} = 2$ necklaces defined over $\mathbb{Q}$. □

Example. For $p = 5$, the image of ρ can be equal to $C_2 \times C_2$, a case denoted by $G(p) = G_3$ in Theorem 1.4 in [25]. In this case, there are exactly two necklaces defined over $\mathbb{Q}$ on E, as shown by the proof of Lemma 2. For example, the curve with Cremona label 6975d1 has two necklaces for $p = 5$ defined over $\mathbb{Q}$. There are infinitely many such examples as the modular curve in question is of genus 0.

Example. Note that the image of ρ for the curve 98a3 for $p = 3$ consists of only one non-split element of order 2. All three necklaces are defined over $\mathbb{Q}$ on that curve. The corresponding modular curve has genus 0, so there are infinitely many examples over $\mathbb{Q}$.

2.3 Elliptic curves with complex multiplication

For the convenience of the reader, we will recall some background results for elliptic curves with extra endomorphisms. We will say E has complex multiplication (CM) if the geometric endomorphism ring is not $\mathbb{Z}$, even if the endomorphisms are not defined over the base field of the curve.

Lemma 5. Let E be an elliptic curve defined over a number field K with complex multiplication by an order $\mathcal{O}$ with conductor f in an imaginary quadratic field F.

i) If p is split in $\mathcal{O}$, then the image of $\rho\colon G_K \to \mathrm{PGL}\big(E[p]\big)$ is contained in the normaliser of a split Cartan subgroup.
ii) If p is inert in $\mathcal{O}$, then the image of ρ is contained in a nonoca.
iii) If p ramifies in $\mathcal{O}$, then the image of ρ is contained in a Borel subgroup, but not in any normaliser of a Cartan subgroup.

In case i) and ii), if moreover p does not divide f nor the absolute discriminant Δ_{FK} of FK and E has good reduction above p, then ρ has image the whole Cartan subgroup if $F \subset K$ or its normalizer if $[FK : K] = 2$.

If p is inert in $\mathcal{O}$, the necklace $\mathfrak{v}^*$ fixed by the non-split Cartan of Lemma 5 is defined over K and the point $[(E, \mathfrak{v}^*)] \in X(K)$ is a Heegner point. (See also Section 4.3).

Proof. Over FK, the action by G_{FK} and the action by the endomorphism ring $\mathcal{O}$ on $E[p]$ commute. This shows that the restriction of ρ to G_{FK} maps into the subgroup $C_{\mathcal{O}}$ in $\mathrm{PGL}\big(E[p]\big)$ which is the image of $\mathrm{Aut}_{\mathcal{O}}\big(E[p]\big) \cong (\mathcal{O}/p\mathcal{O})^{\times}$. If p splits in $\mathcal{O}$ this is a split Cartan subgroup and, if p is inert, it is a non-split Cartan subgroup. If $p = \mathfrak{p}^2$ for an ideal $\mathfrak{p}$ in $\mathcal{O}$, then the Galois action must fix the subgroup $E[\mathfrak{p}]$ inside $E[p]$ which shows that $\rho(G_{FK})$ lies inside a Borel subgroup, however it can not belong to a split Cartan subgroup as there is no other sub-$\mathcal{O}$-module in $E[p]$ of order p. Then any element of a Borel subgroup which is not split has order p, and hence it is not in a non-split Cartan.

As $[FK : K] \leqslant 2$, the subgroup $\rho(G_{FK})$ has index at most 2 in $\rho(G_K)$, which implies that it is normal. Hence that the image of ρ is in the normaliser of $\rho(G_{FK})$.

If, in addition, p does not divide $f\Delta_{FK}$ and E has good reduction above p, then the natural injection $G_{FK} \hookrightarrow C_{\mathcal{O}}$ is an isomorphism, as proved in [6, Proposition 3.3]. This gives the second part of the lemma if $F \subset K$. If $[FK : K] = 2$, it remains to show that $\rho(G_K)$ is the whole normaliser. Suppose it is not, hence $\rho(G_K) = \rho(G_{FK})$ and the action of G_K commutes with the action of $\mathcal{O}$ on $E[p]$. This contradicts the fact that the action of a non-trivial element of $\mathrm{Gal}(FK/K)$ and an element of degree 2 in $\mathcal{O}$ anti-commute. □

When E is defined over $\mathbb{Q}$, we can say a little more. The order $\mathcal{O}$ is one of the thirteen imaginary quadratic orders of class number one listed in the Table 1 below. We denote by $D = \Delta_F \cdot f^2$ the discriminant of $\mathcal{O}$. The elliptic curve E_D is one of minimal conductor among the elliptic curves with complex multiplication by $\mathcal{O}$ and they are listed with their Cremona label here.

Table 1: CM elliptic curves over $\mathbb{Q}$

$D = \Delta_F \cdot f^2$	j	E_D
-3	0	27a3
-4	1728	32a2
-7	-3375	49a1
-8	8000	256a1
-11	-32768	121b1
$-12 = -3 \cdot 2^2$	54000	36a2
$-16 = -4 \cdot 2^2$	287496	32a3
-19	-884736	361a1
$-27 = -3 \cdot 3^2$	-12288000	27a2
$-28 = -7 \cdot 2^2$	16581375	49a2
-43	-884736000	1849a1
-67	-147197952000	4489a1
-163	-262537412640768000	26569a1

Lemma 6. Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field F of discriminant Δ_F and let $p > 2$ be a prime number. Assume that $j(E) \notin \{0, 1728\}$.

i) If $\left(\frac{\Delta_F}{p}\right) = 1$ then the image of ρ is equal to the normaliser of a split Cartan subgroup.
ii) If $\left(\frac{\Delta_F}{p}\right) = -1$ then the image of ρ is equal to a nonoca.
iii) If $p \mid \Delta_F$ then the image of ρ is contained in a Borel, but not in any normaliser of a Cartan subgroup.

Hence, if $p > 3$, there is a $\mathbb{Q}$-rational necklace $\mathfrak{v}^*$ on E only in the case $\left(\frac{\Delta_F}{p}\right) = -1$ and it is then unique.

Proof. From Table 1, we see that $p \nmid \Delta_F$ implies $p \nmid f$ for all odd p. It follows that the condition on $\left(\frac{\Delta_F}{p}\right)$ corresponds to the splitting behaviour of p in $\mathcal{O}$, so $\rho(G_{\mathbb{Q}})$ is contained in the normaliser of a split Cartan, the normaliser of a non-split Cartan or a Borel as listed in Lemma 5.

The case $p \mid \Delta_F$ follows from Lemma 5. Now, we wish to show that if $p \nmid \Delta_F$, $\rho(G_{\mathbb{Q}})$ is the whole normaliser of the Cartan subgroup $C_{\mathcal{O}}$ (with the notation of the proof of Lemma 5).

As stated by Stevenhagen (see Theorem 1.4 in [4]), class field theory implies that the p-ray class field of $\mathcal{O}$ is included in $F(E[p])$ and has Galois group over F isomorphic to $(\mathcal{O}/p\mathcal{O})^\times/[\mathcal{O}^\times]$ where $[\mathcal{O}^\times]$ is the image of $\mathcal{O}^\times$ through $\mathcal{O} \longrightarrow \mathcal{O}/p\mathcal{O}$. Hence, the index of $\rho(G_F)$ in $C_{\mathcal{O}}$ divides $|\mathcal{O}^\times/\{\pm 1\}|$, which gives $\rho(G_F) = C_{\mathcal{O}}$ since $j(E) \notin \{0, 1728\}$. We conclude that $\rho(G_{\mathbb{Q}})$ is the whole normaliser of $C_{\mathcal{O}}$ as in the end of the proof of Lemma 5.

The following is an alternative proof: Since $j(E) \notin \{0, 1728\}$, the curve E is a quadratic twist of E_D. Therefore the image of ρ is isomorphic to the image of the representation associated to E_D. From Table 1, we see that E_D has good reduction for all odd primes $p \nmid \Delta_F$. Hence the result follows from the second part of Lemma 5 for $K = \mathbb{Q}$.

Finally, note that the normaliser of a split Cartan subgroup cannot be contained in a nonoca if $p > 3$, justifying the final statement of the Lemma. □

Recall that the cases $j \in \{0, 1728\}$, are discussed in Section 2.5.

Remark. We state and prove Lemmas 5 and 6 in the projective setting, which is sufficient for our purposes and slightly simpler, but they also hold for the representation into $\mathrm{GL}(E[p])$ instead of $\mathrm{PGL}(E[p])$. The proof of Lemma 5 remains unchanged, while the $\mathrm{GL}(E[p])$ version of Lemma 6 follows, for instance, from Theorem 6.3 in [6].

2.4 Distinct j-invariants

Since our goal is to represent necklaces algorithmically, we are particularly interested by the case when the j-invariants of the curves E/C for all C cyclic subgroup of order p are distinct. Indeed, in this case we may represent $\mathfrak{v} = (C_0, C_1, \ldots, C_p)$ by an ordered list of the j-invariants $\big(j(E/C_0), j(E/C_1), \ldots, j(E/C_p)\big)$. We will make use of this in Section 3.

Lemma 7. Let E be an elliptic curve defined over a field k, such that $j(E) \notin \{0, 1728\}$. Assume that k is of characteristic 0 or that k is of characteristic $\ell \neq p$ and E is ordinary. There exists two distinct cyclic subgroups C and C' of order p such that $j(E/C) = j(E/C')$ if and only if $\mathrm{End}(E)$ is an order in an imaginary quadratic field in which p splits.

Proof. Suppose that C and C' are two distinct cyclic subgroups of order p in E such that E/C and E/C' are $\bar{k}$-isomorphic, say by an isomorphism ι. If φ and φ' are choices of isogenies with $\ker(\varphi) = C$ and $\ker(\varphi') = C'$, then the composition $\alpha = \check{\varphi} \circ \iota \circ \varphi' \colon E \to E/C' \to E/C \to E$ gives an endomorphism on E.

If the ideal $I = (\alpha)$ is equal to (p) in $\mathrm{End}(E)$, then there is a unit $u \in \mathrm{End}(E)$ such that $\alpha = u\,p$. As we have excluded that $j(E)$ is 0 or 1728, we must have $u = \pm 1$, but this would imply that $\iota \circ \varphi' = \pm\varphi$, which is impossible if φ and φ' have distinct kernel.

It follows that the endomorphism ring of E is larger than $\mathbb{Z}$. Our hypothesis implies that it is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field. The ideal I is such that $\mathcal{O}/I$ is cyclic of order p^2. This implies that I is the square of a prime ideal of norm p and hence p splits in $\mathcal{O}$. In particular, the index of $\mathcal{O}$ in the maximal order is coprime to p.

Conversely, if $\mathrm{End}(E)$ is imaginary quadratic with p split, say $(p) = \mathfrak{p} \cdot \mathfrak{p}'$, then the isogenies given by the kernels $E[\mathfrak{p}]$ and $E[\mathfrak{p}']$ have the same codomain isomorphic to E. □

In the case of a supersingular elliptic curve, here is an example later discussed in Section 6.2: Take the elliptic curve E defined over $\mathbb{F}_{13}$ with j-invariant equal to 5. This is the unique supersingular j-invariant. This curve admits three necklaces defined over $\mathbb{F}_{13}$, however the j-invariants of E/C are all equal to 5 as well.

In terms of isogeny volcanoes [23], this means that if the j-invariants are not distinct, the curve sits on the rim of the volcano with at least one pair of vertices with multiple connected edges.

Proposition 8. Let E be an elliptic curve defined over a number field K and suppose $j(E) \notin \{0, 1728\}$. If the image of the representation $\rho \colon G_K \to \mathrm{PGL}\big(E[p]\big)$ is equal to a full nonoca, then the j-invariants $j(E/C)$ for C cyclic in $E[p]$ are pairwise distinct.

Proof. Suppose that there exists two distinct subgroups C and C' of order p such that $j(E/C) = j(E/C')$. Then, by the previous lemma, E has complex multiplication by an imaginary quadratic order $\mathcal{O}$ in which p splits. By Lemma 5, this implies that $\rho(G_K)$ is contained in the normaliser of a split Cartan subgroup. This is not possible since $\rho(G_K)$ is a nonoca. □

Proposition 9. Suppose $p > 3$. Let E be an elliptic curve defined over $\mathbb{Q}$ with $j(E) \notin \{0, 1728\}$. If E admits a necklace $\mathfrak{v}$ defined over $\mathbb{Q}$, then the j-invariants $j(E/C)$ for C cyclic in $E[p]$ are pairwise distinct.

Proof. As above, $j(E/C) = j(E/C')$ for $C \neq C'$ would imply that E has complex multiplication by an imaginary quadratic field F in which p splits. But Lemma 6 contradicts then the existence of a necklace defined over $\mathbb{Q}$. □

2.5 Curves with extra automorphisms

We discuss now the special cases when $\mathrm{Aut}(E)$ is strictly larger than $\{\pm 1\}$. Let $p > 3$ be a prime number and E be an elliptic curve defined over a field k of characteristic different from p, 2, and 3 and suppose that $j(E) = 0$ or 1728. Denote $F = \mathbb{Q}(\sqrt{D})$ and

$$\begin{array}{llll} D = -3, & \mathcal{O} = \mathcal{O}_F = \mathbb{Z}[\zeta], & n = 3 & \text{if } j(E) = 0 \\ D = -4, & \mathcal{O} = \mathcal{O}_F = \mathbb{Z}[i], & n = 2 & \text{if } j(E) = 1728 \end{array}$$

where ζ is a primitive cube root of unity in $\bar{k}$, and consider

$$E_{-3}\colon \quad y^2 = x^3 + 1 \qquad \text{and} \qquad E_{-4}\colon \quad y^2 = x^3 + x.$$

As E has complex multiplication by $\mathcal{O}$, it is a twist of E_D. It has an equation of the form $y^2 = x^3 + d$ if $j(E) = 0$ or of the form $y^2 = x^3 + dx$ if $j(E) = 1728$, with d a $(2n)$-th power-free integer.

As $[-1]$ acts trivially on $\mathbb{P}\big(E[p]\big)$, the cyclic group $\mathrm{Aut}(E)/\{\pm 1\}$ of order n acts on the set of necklaces on $E[p]$. Let $\alpha = [\zeta]$ if $j = 0$ and $\alpha = [i]$ if $j = 1728$. It induces an element $u \in \mathrm{PGL}\big(E[p]\big)$ which is of order n.

Proposition 10. Suppose $k = \mathbb{Q}$ and $p > 5$. If $j(E) = 0$ assume that $p > 7$. Then there is a necklace in the p-torsion of E defined over $\mathbb{Q}$ if and only if $p \equiv 2 \pmod 3$ when $j(E) = 0$ or $p \equiv 3 \pmod 4$ if $j = 1728$. This necklace $\mathfrak{v}^*$ is unique and the element u acts as a rotation on it.

Proof. As $p > 3$, the prime cannot be ramified in $\mathcal{O}$. As seen in the proof of Lemma 5, $\rho(G_F)$ is a subgroup of a Cartan subgroup $C_{\mathcal{O}}$, which is split if p is split in $\mathcal{O}$ and non-split if p is inert. From Stevenhagen's theorem cited in [4], we know that the index of $\rho(G_F)$ in $C_{\mathcal{O}}$ is either 1 or n.

Suppose p is inert. Then $\rho(G_F)$ has at least $(p+1)/n$ elements. The lower bounds on p ensure that this is greater than 2. As $\rho(G_F)$ contains more than 2 elements, $\rho(G_{\mathbb{Q}})$ cannot be contained in a nonoca other than the normaliser of $C_{\mathcal{O}}$. Therefore there is a unique necklace defined over $\mathbb{Q}$.

If p is split, then there are at least $(p-1)/n > 2$ elements. This implies that $\rho(G_{\mathbb{Q}})$ cannot be contained in a nonoca and hence there is no $\mathbb{Q}$-rational necklace on E.

The congruence conditions come from the fact that p is inert in $\mathcal{O}$ if and only if $\left(\frac{D}{p}\right) = -1$.

If E admits a necklace $\mathfrak{v}$, the element u belongs to $\mathrm{Aut}_{\mathcal{O}}\big(E[p]\big) = \big(\mathcal{O}/p\mathcal{O}\big)^\times$ inside $\mathrm{PGL}\big(E[p]\big)$ and not just its normaliser. It then acts as a rotation on $\mathfrak{v}$. □

One can find some curves $E/\mathbb{Q}$ with $j(E) = 0$ with a single and some that have two $\mathbb{Q}$-rational necklaces for $p = 5$. Moreover, some have a $\mathbb{Q}$-rational necklace for $p = 7$ despite $7 \equiv 1 \pmod 3$. Compare with Example 4.4 in [4].

Lemma 11. If u is of order 2, then its action on $\mathbb{P}\big(E[p]\big)$ commutes with the action of the Galois group of k. If u is of order 3 and k contains the third roots of unity, then u commutes with the Galois group. Otherwise the Galois group may invert u.

Proof. As $[-1]$ acts trivially on $\mathbb{P}\big(E[p]\big)$, it is the group $\mathrm{Aut}_{\bar{k}}(E)/\pm 1$ that acts. As a Galois module this is either isomorphic to $\mu_4/\mu_2 \cong \mu_2$ which has a trivial action by the Galois group or $\mu_6/\mu_2 \cong \mu_3$ which is trivial only if k contains the third roots of unity. □

Let us now consider the points $x \in X$ in $\pi^{-1}(\{0, 1728\})$ for $\pi\colon X \longrightarrow \mathbb{P}^1$. Such a point can be represented by a pair $(E, \mathfrak{v})$ with $E = E_{-3}$ or E_{-4}. We have $x \in X(k)$ if and only if for each $\sigma \in G_k$, there exists an automorphism $\psi_\sigma \in \mathrm{Aut}(E)$ such that $\psi_\sigma(\mathfrak{v}) = \sigma(\mathfrak{v})$.

Denote by Ω the $\mathrm{Aut}(E)/\{\pm 1\}$-orbit of $\mathfrak{v}$, which is either a sigleton or it contains n necklaces. The ramification index of x above $\pi(x)$ is $|\mathrm{Aut}(E)|/|\mathrm{Stab}(\mathfrak{v})| = \#\Omega$. If $\Omega = \{\mathfrak{v}\}$, then the point x is an elliptic point of X as it is unramified above $\pi(x)$. We already counted these points in Proposition 12 in [18]. In this case, $x \in X(k)$ if and only if $\mathfrak{v}$ is defined over k.

If $\#\Omega = n$, then x is a ramified point of index n; it is represented by $(E, \mathfrak{w})$ for each $\mathfrak{w} \in \Omega$. Such a point is in $X(k)$ if either each necklace in Ω is defined over k, in which case G is contained in the intersection of the corresponding n nonocas, or Ω forms a single G_k-orbit.

- Above $j = 0$ there is no elliptic point if $p \equiv 1 \pmod 3$ and only one if $p \equiv 2 \pmod 3$. In this last case, the unique necklace $\mathfrak{v}^*$ is fixed by u, that is to say u acts as a rotation of angle $\pm 2\pi/3$. It can be visualized by folding the necklace three times over itself. Since $u(C_i) = C_{i+(p+1)/3}$, we have $j(E/C_i) = j\big(E/C_{i+(p+1)/3}\big)$ for all i. The other points are ramified points $x = \big[(E, \mathfrak{v})\big] = \big[(E, u(\mathfrak{v}))\big] = \big[(E, u^2(\mathfrak{v}))\big]$.
- Above $j = 1728$, the automorphism u may either fix or flip the necklace for an elliptic point. If $p \equiv 1 \pmod 4$, there are no such necklaces fixed by u, while for $p \equiv 3 \pmod 4$ there is exactly one such necklace, as explained in Section 3.5.1 in [18] where it appears as a pair of two oriented necklaces. On this necklace u acts as a rotation of angle π and we may picture it like folding this necklace $\mathfrak{v}^*$ twice on itself. Here $j(E/C_i) = j\big(E/C_{i+(p+1)/2}\big)$ for all i.
  Moreover, there are $\big(p - (\frac{-1}{p})\big)/2$ elliptic points such that u acts as a reflection on the necklace. These are the flipped necklaces in Section 3.5.2 of [18]. The number of them is obtained by subtracting from the number e_2^+ in Proposition 12 in [18] the number of fixed necklaces.
  Finally, the other points in the fibre are ramified points $x = \big[(E, \mathfrak{v})\big] = \big[(E, u(\mathfrak{v}))\big]$.

In the case where $k = \mathbb{Q}$, the necklace $\mathfrak{v}^*$ above is the unique necklace of Proposition 10.

Lemma 12. Let $p > 7$. When $p \equiv 2 \pmod 3$ the only point of $X(\mathbb{Q})$ above $j = 0$ is $[(E_{-3}, \mathfrak{v}^*)]$, and there is no such point if $p \equiv 1 \pmod 3$. Similarly, $[(E_{-4}, \mathfrak{v}^*)]$ is the unique point above $j = 1728$ when $p \equiv 3 \pmod 4$ and there is none when $p \equiv 1 \pmod 4$.

Proof. As we are no longer concerned with the specific curve, but only the points in X, we may take the curve to be E_D. Recall that we denote $\pi\colon X \longrightarrow \mathbb{P}^1$. An unramified point in $\pi^{-1}(\{0, 1728\})$ is defined over $\mathbb{Q}$ if and only if it is represented by $(E_D, \mathfrak{v})$ with $\mathfrak{v}$ defined over $\mathbb{Q}$: There is only one such point obtained for $\mathfrak{v} = \mathfrak{v}^*$ if $p \equiv -1 \pmod D$, and none otherwise by Proposition 10.

We are left to prove that no ramified point $x = [(E_D, \mathfrak{v})]$ is defined over $\mathbb{Q}$ when $\mathfrak{v} \neq \mathfrak{v}^*$, in other words we want to exclude the possibility that the $\mathrm{Aut}(E)/\{\pm 1\}$-orbit Ω of $\mathfrak{v}$ is a $G_{\mathbb{Q}}$-orbit. For our particular curve E_D, the reduction is good at p and p is not ramified in $\mathcal{O}$. Therefore, Lemma 5 implies that $G = \rho(G_{\mathbb{Q}})$ is equal to the normaliser of a Cartan subgroup in $\mathrm{PGL}\big(E[p]\big)$. It is dihedral of order $2(p+1)$ or order $2(p-1)$. Since $\mathfrak{v}$ is not fixed by G, its stabiliser under the Galois action is of order 2 or 4, since it is in the intersection of G with the nonoca stabilizing $\mathfrak{v}$. Hence the Galois orbit of $\mathfrak{v}$ has order $(p \pm 1)/2$ or $(p \pm 1)$. For $p > 7$, the Galois orbit has at least $(7-1)/2 = 4$ elements, which implies that Ω cannot be such an orbit as Ω has at most 3 elements. □

The fibres for smaller primes p can be exceptionally. For $p = 7$, the fibre above $j = 0$ contains one rational point and it is ramified despite $p \equiv 1 \pmod 3$. For $p = 5$, the fibre above $j = 0$ has two rational points, one ramified and one unramified. This can be checked on the explicit models or with the same method as in the proof above.

3 Representation of necklaces over number fields

Let E be an elliptic curve defined over a number field K, such that $j(E) \notin \{0, 1728\}$. We suppose that E admits a necklace $\mathfrak{v}$ defined over K. The aim of the following algorithm is to represent $\mathfrak{v}$. In this section, we suppose that the j-invariants $j(E/C)$ for C cyclic in $E[p]$ are pairwise distinct (see Lemma 7): in this case, we may represent $\mathfrak{v} = (C_0, C_1, \ldots, C_p)$ by an ordered list of the j-invariants

$$\big(j(E/C_0),\, j(E/C_1),\, \ldots,\, j(E/C_p)\big).$$

Actually, for algorithmic purposes, we will make a stronger assumption: We suppose that the image G of the representation $\rho\colon G_K \to \mathrm{PGL}\big(E[p]\big)$ is the full nonoca stabilising $\mathfrak{v}$. In this case, the j-invariants are automatically distinct by Proposition 8. See also Proposition 9.

Let $\mathfrak{q} \mid q$ be a prime ideal of K of good reduction for E with $q \neq p$. Denote by $\mathbb{F}_\mathfrak{q}$ the residue field of K at $\mathfrak{q}$ and $\widetilde{E}$ the reduction of E modulo $\mathfrak{q}$. Then $E[p] \cong \widetilde{E}[p]$ as G_K-modules, where G_K acts on $\widetilde{E}[p]$ via the canonical surjection $G_K \to G_{\mathbb{F}_\mathfrak{q}}$. On $\mathbb{P}\big(E[p]\big) \cong \mathbb{P}\big(\widetilde{E}[p]\big)$ this action will factor through the **p-isogeny field** L, that is to say the smallest extension of K over which all cyclic subgroups of E of order p are defined. Since E has good reduction at $\mathfrak{q}$, the inertia group at $\mathfrak{q}$ acts trivially on $E[p]$. Hence the action of G_K on $\widetilde{E}[p]$ is cyclic generated by any choice of a Frobenius element $\mathrm{Fr}_\mathfrak{Q} \in \mathrm{Gal}(L/K)$ for $\mathfrak{Q} \mid \mathfrak{q}$ an ideal of L.

The basic idea of the algorithm described below as Algorithm 1 is the following:

Step 1: We calculate L as the splitting field of the polynomial $f(x) = \Phi_p\big(j(E), x\big)$, where Φ_p is the standard modular polynomial for $Y_0(p)$. These polynomials have been calculated by Bröker, Lauter, and Sutherland as explained in [5] and can simply be read off a file which can be found on Sutherland's webpage.

Step 2: We determine a prime ideal $\mathfrak{q}$ in K such that the roots of f have distinct reduction modulo a prime $\mathfrak{Q}$ in L above $\mathfrak{q}$ and such that a Frobenius $\mathrm{Fr}_\mathfrak{Q} \in \mathrm{Gal}(L/K)$ is the class of an element of order $p+1$. More precisely, we want $\mathrm{Fr}_\mathfrak{Q}$ to have characteristic polynomial on $E[p]$ equal to the minimal polynomial of γ. To obtain this, we try the primes $\mathfrak{q}$ of good reduction such that $\mathrm{N}(\mathfrak{q}) \equiv \mathrm{N}(\gamma) \pmod p$ and $a_\mathfrak{q} \equiv \mathrm{Tr}(\gamma) \pmod p$, each time checking if the reduced roots of f are distinct. Here $a_\mathfrak{q} = \mathrm{N}(\mathfrak{q}) + 1 - \#\tilde{E}(\mathbb{F}_\mathfrak{q})$.

Step 3: In the last step, we order the roots $j(E/C) \in L$ of f according to the necklace $\mathfrak{v}$: We pick a first root j_0 among them. Then we pick j_1 to be the unique root whose reduction modulo $\mathfrak{q}$ is $\mathrm{Fr}_\mathfrak{Q}(j_0)$ in the residue field. Then j_2 and so forth.

The bottleneck of the algorithm is the complete factorisation of f in the field L.

Remark. The condition on $\mathrm{Fr}_\mathfrak{Q}$ to be of order $p+1$ implies that the prime of good reduction $\mathfrak{q}$ for E is ordinary, and by Lemma 7, the condition on the roots of $f \pmod \mathfrak{Q}$ implies that p is not split in $\mathrm{End}(\tilde{E})$.

4 Reduction of a necklace

Let E be an elliptic curve defined over a number field K with $j(E) \notin \{0, 1728\}$. Suppose $\mathfrak{v}$ is a necklace in $E[p]$ defined over K.

4.1 Good reduction

Let λ be a prime ideal in K not dividing p, $\mathbb{F}_\lambda$ the residue field at λ and suppose that E has good reduction at λ. Then the point $[(E, \mathfrak{v})] \in Y(K)$ can be reduced to a point

Algorithm 1: Computing necklaces over number fields

Input: E/K elliptic curve as above, a prime p, and a generator γ of $\mathbb{F}_{p^2}^{\times}$.
Output: A list $(j_0, j_1, \ldots, j_p)$ of elements in a number field representing the necklace $\mathfrak{v}$ in $E[p]$

Read Φ_p in the file described above `/* Step 1 */`
$f(x) \leftarrow \Phi_p(j(E), x) \in K[x]$
$L \leftarrow$ the splitting field of f
$J \leftarrow$ the set of all roots of f in L
Set $t \leftarrow \mathrm{Tr}(\gamma)$ and $n \leftarrow \mathrm{N}(\gamma)$ `/* Step 2 */`
repeat
  repeat
    Advance to the next prime ideal $\mathfrak{q} \nmid p$ in K for which E has good reduction
  until $\mathrm{N}(\mathfrak{q}) \equiv n \pmod{p}$ and $a_{\mathfrak{q}} \equiv t \pmod{p}$
  Pick a prime $\mathfrak{Q}$ in L above $\mathfrak{q}$
until the reduction of elements in J are distinct modulo $\mathfrak{Q}$
$j_0 \leftarrow$ one element in J `/* Step 3 */`
for k **from** 1 **to** p **do**
  $y \leftarrow \mathrm{Fr}_{\mathfrak{Q}}(j_{k-1} + \mathfrak{Q})$
  Set j_k to be the element in J that reduces to y modulo $\mathfrak{Q}$.
return the necklace $(j_0, j_1, \ldots, j_p)$

$\left[(\tilde{E}, \tilde{\mathfrak{v}})\right] \in Y(\mathbb{F}_\lambda)$. If the necklace is given by the above Algorithm 1, then we can try obtaining a representation of $\tilde{\mathfrak{v}}$ simply as follows: Pick a prime $\mathfrak{L}$ above λ in the p-isogeny field L and reduce the values $j_k = j(E/C_k)$ modulo $\mathfrak{L}$. If we are lucky the reduced values are distinct. We would then have a list $(\tilde{j}_0, \tilde{j}_1, \ldots, \tilde{j}_p)$ belonging to a finite extension of $\mathbb{F}_\lambda$ representing the necklace $\tilde{\mathfrak{v}}$ by listing the j-invariants of the curves which are the codomains of p-isogenies leaving the reduced curve $\tilde{E}/\mathbb{F}_\lambda$.

However, we may be unlucky. If the reduction of E at λ is supersingular, we may expect that the j-invariants do not reduce to distinct elements modulo $\mathfrak{L}$. Lemma 7 explains that even when the reduction at λ is good ordinary, the j-invariant may no longer pairwise distinct in the reduction.

In this situation, we need to do extra work. First, we can write down explicitly isogenies $\varphi_k \colon E \to E/C_k$ given that we know the degree and the two elliptic curves involved. There are two choices for the isogeny, φ_k and $-\varphi_k$, with the same kernel C_k as we have no extra automorphisms by assumption. However, this choice will not matter as we care for C_k rather than for φ_k. We obtain this way a kernel polynomial f_k defining the cyclic subgroup C_k as a subgroup scheme of E and this does not depend on the above choice of φ_k. This kernel polynomial can be reduced modulo $\mathfrak{L}$. We obtain a list of polynomials $\left(\tilde{f}_0, \tilde{f}_1, \ldots, \tilde{f}_p\right)$ defined over a finite field. This represents the reduced necklace $\tilde{\mathfrak{v}}$. We could also reduce the isogenies and represent it as a list $\left(\tilde{\varphi}_0, \tilde{\varphi}_1, \ldots, \tilde{\varphi}_p\right)$.

4.2 Bad reduction

Suppose now that E has bad reduction at λ.

First, if the reduction of E is potentially multiplicative, i.e., $j(E)$ has negative valuation at λ, then the reduction will be one of the cusps of X over $\mathbb{F}_\lambda$. We could use the description of necklaces on Tate curves as in the proof of Proposition 6 in [18] to decide which of the $\frac{p-1}{2}$ cusps the point reduces to, but we have not implemented this.

Otherwise, $j(E)$ is integral at λ. We will need to reduce the j-invariants $j(E/C)$, which belong to the p-isogeny field L, or the kernel polynomials, whose coefficients are in L. Over L the elliptic curve E will acquire good reduction at primes above λ due to the following lemma. Therefore the j-invariants and polynomials can be reduced at the chosen prime $\mathfrak{L}$ above λ. The obtained reduced elliptic curve $\tilde{E}/\mathbb{F}_{\mathfrak{L}}$ will admit a non-singular model defined

Algorithm 2: Reduce a necklace

Input: E/K elliptic curve as above, a prime p, necklace represented by distinct j-invariants $(j_0, j_1, \ldots, j_p)$ and a prime λ.

Output: Either a list of $p+1$ distinct elements $(\tilde{j}_0, \ldots, \tilde{j}_p)$ or an ordered list of $p+1$ polynomials $\left(\tilde{f}_0, \tilde{f}_1, \ldots, \tilde{f}_p\right)$ defined over a finite extension of $\mathbb{F}_\lambda$

$L \leftarrow$ p-isogeny field of E
Pick a prime $\mathfrak{L}$ in L above λ
Reduce the j-invariants modulo $\mathfrak{L}$ to $\tilde{J} = (\tilde{j}_0, \tilde{j}_1, \ldots, \tilde{j}_p)$
if all reduced values in $\tilde{J}$ are distinct **then**
    return $\tilde{J}$
for j **from** 0 **to** p **do**
    Determine the isogeny $\varphi_k \colon E \to E/C_k$ given the codomain and degree
    Calculate the kernel polynomial f_k defining C_k in $L[x]$
    Reduce the kernel polynomial modulo $\mathfrak{L}$
return $\left(\tilde{f}_0, \tilde{f}_1, \ldots, \tilde{f}_p\right)$

over $\mathbb{F}_\lambda$ as its j-invariant lies in $\mathbb{F}_\lambda$. Thus the reduced information will look exactly like in the case of good reduction.

Lemma 13. Let E be an elliptic curve defined over a local field k of residual characteristic ℓ. If E admits an isogeny $E \to E'$ defined over k of prime degree $p > 3$ with $(p, \lambda) = 1$, then E has semistable reduction.

Proof. Let C be the kernel of the isogeny viewed as a subgroup scheme of the Néron model $\mathcal{E}$. Assume that $\mathcal{E}$ has additive reduction. As the group of components has order at most 4 and $p > 3$, the subgroup C lies in the connected component of the identity $\mathcal{E}^0$. Since p is coprime to ℓ, the special fibre of C is étale. This is impossible as $\mathbb{G}_a$ over a field of characteristic ℓ has no subgroup of order p. □

4.3 Reduction of necklaces on CM elliptic curves

We now present a quicker algorithm to calculate reductions of necklaces on CM elliptic curves avoiding Algorithm 1. Instead we use the reduction of the endomorphism ring.

Let E be an elliptic curve defined over a number field K. Assume that E has complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field F and that p is inert in $\mathcal{O}$. Then, as discussed in Section 2.3, there exists a special necklace $\mathfrak{v}^*$ defined over K on $E[p]$ coming from the fact that $E[p]$ is a free $\mathcal{O}/p\mathcal{O}$-module of rank 1. This is the necklace fixed by the non-split Cartan subgroup $C_\mathcal{O}$ in $\mathrm{PGL}\big(E[p]\big)$ coming from the $\mathcal{O}$-structure. Although we do not elaborate further in this article, we note that the point $[(E, \mathfrak{v}^*)] \in X(K)$ is a Heegner point.

If $\rho(G_K) = C_\mathcal{O}$, then $\mathfrak{v}^*$ is the unique necklace on $E[p]$ defined over K. This is the case for instance if $K = \mathbb{Q}$ by Lemma 6 or more generally if $p \nmid f\Delta_{FK}$ is a place of good reduction for E by Lemma 5.

Let $\lambda \nmid p$ be a prime ideal of K of good reduction for E. Denote by $\mathbb{F}_\lambda$ the residue field of K at λ. By reducing $\mathfrak{v}^*$ modulo λ, we obtain the necklace $\tilde{\mathfrak{v}}^*$ on the reduction $\tilde{E}$. The aim of this section is to present an algorithm to calculate $\tilde{\mathfrak{v}}^*$ from only data of the CM elliptic curve E without having to calculate $\mathfrak{v}^*$ beforehand, that is without executing the costly Algorithm 1. By Proposition 3.4 in [20], the reduction map $\mathcal{O} \cong \mathrm{End}(E) \hookrightarrow \mathrm{End}(\tilde{E})$ is injective. Hence $\tilde{\mathfrak{v}}^*$ is the unique necklace on $\tilde{E}[p]$ stabilised by $(\mathcal{O}/p\mathcal{O})^\times$. It is then given by the action of any element of $\mathcal{O} \hookrightarrow \mathrm{End}(\tilde{E})$ which modulo p maps to the chosen generator γ of $\mathbb{F}_{p^2}^\times$ through the isomorphism with $(\mathcal{O}/p\mathcal{O})^\times$.

The method is presented in Algorithm 3, for elliptic curves over $\mathbb{Q}$.

Algorithm 3: Construct the reduced necklace for a curve with complex multiplication

Input: Two distinct primes p and ℓ, an elliptic curve $E/\mathbb{Q}$ with complex multiplication, and a unique necklace $\mathfrak{v}$ in its p-torsion

Output: A representation of the necklace $\tilde{\mathfrak{v}}$ on $\tilde{E}$ over $\mathbb{F}_\ell$

1 Determine $\mathrm{End}(E)$ and find a $\mathbb{Z}$-basis $\{1, \psi\}$ for it
2 Find an element $\varphi = a + b\,\psi \in \mathrm{End}(E)$ such that the reduction in $\mathrm{End}(E)/p\,\mathrm{End}(E) \cong \mathbb{F}_{p^2}$ maps to γ
3 Reduce φ to $\tilde{\varphi} \in \mathrm{End}(\tilde{E})$ defined over $\mathbb{F}_{\ell^2}$
4 Determine the p-isogeny field for $\tilde{E}$ and all p-isogenies leaving $\tilde{E}$
5 Order them as in the necklace $\tilde{\mathfrak{v}}$ by acting with $\tilde{\varphi}$ on p-isogenies

Again some remarks should be made. First of all, we opt to represent isogenies, and in particular endomorphisms on elliptic curves, as formal sums of compositions of easier isogenies. This is done effectively in Sage [24]. For instance only $[a]$, $[b]$ and ψ are used and the actual rational map $\varphi = a + b\psi$ is never directly calculated.

For line 1, one needs to construct an endomorphism ψ which is not in $\mathbb{Z}$. For $j = 0$ and $j = 1728$ one can take an automorphism of E other than $[\pm 1]$; this is a simple change of variables in the Weierstrass equation. For all other curves, we pick a small prime $q \neq \ell$ which splits in $\mathcal{O}$. There is an endomorphism of degree q on E/F which can be constructed explicitly. The hardest case for this is for the curve with $F = \mathbb{Q}\big(\sqrt{-163}\big)$ and $\ell = 41$, but the requested endomorphism of degree $q = 43$ is not difficult to calculate either. The identification $[\cdot]\colon \mathcal{O} \to \mathrm{End}(E)$ obtained in this way has to be normalised such that $[a]^*(\omega) = a \cdot \omega$ for a differential ω on E.

In line 2, any lift of our γ to $\mathcal{O}$ will do. However, the reduction to an $\mathbb{F}_p$-scalar multiple of γ will have the same action on the pearls, and hence any lift of those will also work. The possible elements in $\mathrm{End}(E)$ are all elements in a subgroup of index p which do not belong to $p\,\mathrm{End}(E)$. Therefore the values of a and b can be chosen fairly small compared to p; although in practice these values do not matter too much as we will work with the formal sum as explained above.

In step 3, we reduce the endomorphism modulo a prime ideal λ in F above ℓ. In practice, as the isogeny is given as a sum of compositions, it is best to reduce these components and still represent it as a sum of composition over the residue field $\mathbb{F}_\lambda$. As we have avoided that ψ has degree divisible by ℓ, the reduced isogeny is obtained as a composition of separable isogenies.

In the actual implementation in [19] of step 4, we construct the p-division field $\mathbb{F}_\ell\big(\tilde{E}[p]\big)$ and consider the action of $\tilde{\varphi}$ on the p-torsion points. This is because it would be extra work to implement the Galois action directly on isogenies. Since points and isogenies are efficiently implemented over finite fields, this does not significantly reduce the speed of this algorithm.

We have assumed so far that the reduction of E is good at ℓ. However, it is easy to pass by. From Corollary 5.22 in [20], we know that there is an elliptic curve E' over F which is isomorphic to E and which has good reduction at the fixed prime ℓ. In practice, the curve E' can be obtained by a quadratic twist.

5 Comparing reduced points on the modular curve

5.1 Algorithm for comparing points over a finite field

In the previous section, we saw how we can obtain points in Y defined over the residue field $\mathbb{F}_\lambda$ of a number field. We will present an algorithm to test if two points $x_1 = \big[(E_1, \mathfrak{v}_1)\big]$ and $x_2 = \big[(E_2, \mathfrak{v}_2)\big]$ in $Y(K)$ reduce to the same point in $Y(\mathbb{F}_\lambda)$ at a given prime ideal λ in K not dividing p. For this we will explain Algorithm 4 which compares points on Y over finite

fields.

Note first that, as seen in Lemma 3, in some cases there is a single necklace on the elliptic curve, in which case we only need to check if the curves are isomorphic. But most elliptic curves over a finite field will have more than one necklace defined over that field.

We are given two elliptic curves E_1 and E_2 over a finite field $\mathbb{F}$ of characteristic $\ell \neq p$, respectively endowed with a necklace $\mathfrak{v}_1$ and $\mathfrak{v}_2$ also defined over $\mathbb{F}$. In practice, these necklaces are either given as a list of distinct j-invariants in an extension of $\mathbb{F}$ or as a list of kernel polynomials with coefficients in an extension of $\mathbb{F}$. We treat here first the case when both are given by list of distinct j-invariants.

First, we check that E_1 and E_2 are $\overline{\mathbb{F}}$-isomorphic by checking if $j(E_1) = j(E_2)$ in $\mathbb{F}$. Next, we can check if the p-isogeny fields of E_1 and E_2 are isomorphic. Finally, we may use an isomorphism between them to check if the list of j-invariants represents the same necklace by checking whether one list is a cyclic shift or a cyclic shift composed with reversing of the other list.

Algorithm 4: Test if two reduced necklaces are equal

Input: Two elliptic curves E_1 and E_2 over a finite field $\mathbb{F}$ each with a necklace $\mathfrak{v}_1$ and $\mathfrak{v}_2$ given by a list J_1 and J_2 of $p+1$ elements in an extension of $\mathbb{F}$.
Output: Boolean deciding if $(E_1, \mathfrak{v}_1)$ and $(E_1, \mathfrak{v}_2)$ represent the same point in $Y(\mathbb{F})$

if $j(E_1) \neq j(E_2)$ **then**
  return False
$F_1 \leftarrow$ the p-isogeny field of E_1
$F_2 \leftarrow$ the p-isogeny field of E_2
if $F_1 \ncong F_2$ **then**
  return False
Identify F_1 and F_2 and use it to convert elements in J_1 and J_2 to the same field
if J_1 differs from J_2 as a set **then**
  return False
if the permutation from J_1 to J_2 is either a $(p+1)$-cycle or a $(p+1)$-cycle composed with reversing the order **then**
  return True
else
  return False

If the j-invariants are not all distinct, we have to work with two lists of polynomials $(f_0, f_1, \ldots, f_p)$ instead. The basic comparison is as above: First checking if the curves are isomorphic, then if they have the same p-isogeny field and, finally, if the two kernel polynomial lists are linked by the correct permutation. Note that one has to make sure that the polynomials are consistently normalised to compare correctly if they give the same subgroup under an isomorphism of E_1 and E_2.

In this last step, one has to treat the special case that the j-invariant may be 0 or 1728; a case that can never appear in the first version of the algorithm as the j-invariants $j(E/C_k)$ will not be distinct. For this situation, one needs to account for extra automorphisms as explained in Section 2.5. In practice we check if the second list of polynomials is the right sort of permutation of $(u^*(f_0), u^*(f_1), \ldots, u^*(f_p))$ for any automorphism u of E_1 defined over the same field as f_k. Here $u^*(f_k)$ is the polynomial defining $u(C_k)$.

Remark. We have fixed a generator γ at the start and our comparison assumes that both necklaces were constructed with the same choice of γ. If this were not the case, one could check equality by finding an n coprime to $p+1$ and a k such that $j(E_1/C_i) = j(E_2/C_{ni+k})$ for all i and similar for the composition with reversing the order. See Lemma 1 in [18].

5.2 Injectivity of reduction

Let p and ℓ be two distinct prime numbers larger than 3. Denote again by X a model of X over $\mathbb{Z}[\frac{1}{p}]$ and by $\mathrm{red}_\ell \colon X(\mathbb{Q}) = X\big(\mathbb{Z}[\frac{1}{p}]\big) \to X(\mathbb{F}_\ell)$ the reduction map.

For $p = 5$ or $p = 7$, when $X \cong \mathbb{P}^1$ as a $\mathbb{Z}\left[\frac{1}{p}\right]$-scheme, this map is the obvious surjective reduction map. Similar for $p = 11$, when the genus is 1 and $X(\mathbb{Q})$ is an elliptic curve with positive rank. The situation is different for $p > 11$, when $X(\mathbb{Q})$ is finite.

It is conjectured that for $p > 11$, the set $X(\mathbb{Q})$ is equal to the set $\mathcal{CM}$ of rational points represented by $(E, \mathfrak{v})$ such that E has complex multiplication. In view of this conjecture, we are interested in $\mathrm{red}_\ell\,|_{\mathcal{CM}}$. In particular, we can ask for which ℓ this map is injective. In other words, we discuss the question for which ℓ are there two distinct points $x = [(E, \mathfrak{v})]$ and $x' = [(E', \mathfrak{v}')]$ in $X(\mathbb{Q})$ both with complex multiplication and having the same reduction in $X(\mathbb{F}_\ell)$.

Suppose that x, x', and ℓ are as above and $p > 7$. Since, by Lemma 6 and Lemma 12, there is only one point in $\mathcal{CM}$ with a given j-invariant, we represent $x = \big[(E, \mathfrak{v})\big]$ and $x' = \big[(E', \mathfrak{v}')\big]$ with $j(E) \neq j(E')$. Write $\tilde{E}$ for the common reduction modulo ℓ. The prime number ℓ must divide $j(E) - j(E')$, hence ℓ is in the finite list $\mathcal{L}$ of all prime divisors of the finitely many differences of CM j-invariants over $\mathbb{Q}$:

$$\mathcal{L} = \big\{3 \leqslant \ell \leqslant 127 \ : \ \ell \text{ is prime } \big\} \cup \big\{137, 139, 157, 163, 173, 193, 197, 211, 229, 233\big\} \cup \big\{241, 257, 277, 283, 293, 317, 331, 389, 433, 571, 643, 997\big\}$$

Lemma 14. Let $(E, \mathfrak{v})$ and $(E', \mathfrak{v}')$ be two CM points in $X(\mathbb{Q})$ and $\ell \neq p$ an odd prime such that their common reduction $\tilde{E}$ at ℓ is ordinary. Then the reductions $(\tilde{E}, \tilde{\mathfrak{v}})$ and $(\tilde{E}, \tilde{\mathfrak{v}}')$ in $X(\mathbb{F}_\ell)$ are distinct.

Proof. We can assume that $E = E_D$ and $E' = E_{D'}$ from our list in Table 1. From this table, we see that no ordinary prime ℓ divides the conductor of $\mathrm{End}(E)$ as its divisors are ramified in $\mathrm{End}(E) \otimes \mathbb{Q}$. By Deuring's result, as stated in Theorem 12 of section 13.4 in [12], it follows that $\mathrm{End}(E) \cong \mathrm{End}(\tilde{E}) \cong \mathrm{End}(E')$ and hence $j(E) = j(E')$ since the endomorphism rings have class number 1. □

Also we have checked algorithmically that the only case when $(E, \mathfrak{v})$ and $(E', \mathfrak{v}')$ have equal reduction and both good ordinary reduction is when $\ell = 2$ and E and E' are the curves E_{-7} and E_{-28}.

For each fixed p, as we will explain below, with our Algorithms 4 and 3, we can effectively determine all the finitely many primes $\ell \in \mathcal{L}$ for which $\mathrm{red}_\ell\,|_{\mathcal{CM}}$ is not injective.

Proposition 15. Among the curves X for primes $3 < p < 50$, there are only eight cases of $(\ell, E, \mathfrak{v}, E', \mathfrak{v}')$ such that $x = \big[(E, \mathfrak{v})\big]$ and $x' = \big[(E', \mathfrak{v}')\big]$ are in $\mathcal{CM} \subset X(\mathbb{Q})$ and such that $\mathrm{red}_\ell(x) = \mathrm{red}_\ell(x')$. They are all listed in the following table.

p	ℓ	j	$\#X_j$	r_j	curves
5	7	6	4	6	(E_{-7}, E_{-163}); (E_{-43}, E_{-67})
5	11	1	2	3	(E_{-27}, E_{-163})
5	13	5	4	5	(E_{-28}, E_{-67}); (E_{-8}, E_{-163})
5	17	8	4	4	(E_{-12}, E_{-163})
7	5	0	3	4	(E_{-8}, E_{-163})
7	13	5	3	4	(E_{-67}, E_{-163})

In this table, X_j denotes the fibre in $X(\mathbb{F}_\ell)$ of $X \to \mathbb{P}^1$ above $j \in \mathbb{F}_\ell$. The column r_j counts the number of CM points in $X(\mathbb{Q})$ which have this j-invariant modulo ℓ. In all but one of the above cases, the number r_j is larger than $\#X_j$ and hence the reduction cannot possibly be injective. We have not found an example of non-injectivity when $r_j < \#X_j$, but also no explanation as to why this should not occur.

Remark. In all those cases, as seen in Lemma 3, since $\tilde{E}$ is supersingular, the image of the Frobenius has order 2 in $\mathrm{PGL}\big(\tilde{E}[p]\big)$. If it is split, it flips $(p-1)/2$ necklaces, acting like a

reflection of axis passing through two antipodal pearls. If it is non-split, it fixes one necklace as an angle π rotation, and it flips $(p+1)/2$ necklaces acting like a reflection of axis passing between two couples of antipodal pairs. See Section 6 for an illustration of this.

The proof of the proposition is an explicit computer calculation using the implementation of Algorithm 3. Many of these instances are also explained in Section 6 as examples of necklaces. For $p = 5$, 7, and 11, we have also verified this result on the models as we can explain here in some details. For $p = 5$, in the LMFDB there is an explicit description of the j-map from a model of X as $\mathbb{P}^1$ over $\mathbb{Z}\left[\frac{1}{30}\right]$, which can be characterised by saying that the nine CM points have the following coordinates: $E_{-3} = (-1 : 2)$, $E_{-7} = (1 : 0)$, $E_{-8} = (0 : 1)$, $E_{-12} = (1 : 2)$, $E_{-27} = (1 : 1)$, $E_{-28} = (-1 : 4)$, $E_{-43} = (-1, 3)$, $E_{-67} = (5 : 6)$, and $E_{-163} = (-13 : 42)$. From this is it easy to verify the assertion for $p = 5$ made in the top four lines of the table.

For $p = 7$, there is a model found in the LMFDB which gives the CM points as $E_{-4} = (0 : 1)$, $E_{-8} = (1 : 0)$, $E_{-11} = (-8 : 5)$, $E_{-16} = (-16 : 5)$, $E_{-43} = (8 : 5)$, $E_{-67} = (-4 : 5)$ and $E_{-163} = (-72 : 25)$. The only congruences modulo prime $\ell > 3$ are $(1 : 0) \equiv (-72 : 25)$ modulo 5 and $(-4 : 5) \equiv (-72 : 25) \pmod{13}$ as expected.

Finally for $p = 11$, the curve X is isomorphic to the elliptic curve with Cremona label 121b1 given by

$$y^2 + y = x^3 - x^2 - 7\,x - 10$$

as found in [14, Prop. 4.3.8.1]. This curve has $X(\mathbb{Q}) = \mathbb{Z}\,Q$ with $Q = (4, 5)$. There is an isomorphism such that E_{-12} maps to O. The other CM points map to $E_{-3} = \left(\frac{5}{4}, \frac{7}{8}\right) = 3Q$, $E_{-4} = (2, 0) = 2Q$, $E_{-16} = (4, -6) = -Q$, $E_{-27} = (2, -1) = -2Q$, $E_{-67} = (4, 5) = Q$, and $E_{-167} = (-2, 3) = 4Q$. The question if two points reduce to the same point modulo ℓ becomes the question if the coordinates of their difference have ℓ as a prime in the denominator. The only points involved in such differences are the above points and $\pm 6Q$ and $\pm 5Q$. Since $6Q = \left(\frac{25}{16}, -\frac{85}{64}\right)$ and $5Q = \left(-\frac{8}{9}, -\frac{118}{27}\right)$ are also $\{2, 3\}$-integral, we can confirm that no two CM points reduce to equal points modulo any prime $\ell > 3$.

Maybe it should not be surprising that we found very few instances of non-injectivity as the number of points of $X(\mathbb{F}_\ell)$ even for small ℓ increases quickly as p grows. With the table presented in Appendix A, it is easy to count the number of points in the reduction.

In the following table, we list $\#X(\mathbb{F}_\ell)$ for $3 < p \neq \ell < 50$. The number $r = \#\mathcal{CM}$ counts the number of CM points in $X(\mathbb{Q})$. The boldface number are the ones for which the reduction map on CM points is not injective.

p	r	$\ell = 5$	7	11	13	17	19	23	29	31	37	41	43	47
5	9		**8**	**12**	**14**	**18**	20	24	30	32	38	42	44	48
7	7	**6**		12	**14**	18	20	24	30	32	38	42	44	48
11	7	9	8		14	18	20	33	30	37	31	42	44	60
13	7	10	11	20		20	24	29	31	37	26	49	31	66
17	7	11	15	24	13		23	41	45	45	27	54	37	63
19	7	14	13	27	14	27		40	45	41	38	54	39	69
23	7	13	16	25	22	34	30		47	51	31	69	44	93
29	8	16	18	37	20	37	46	52		64	30	85	57	100
31	8	20	18	38	21	42	42	56	65		32	90	51	99
37	4	21	21	41	23	50	49	73	72	69		83	65	111
41	8	22	28	49	27	48	54	74	75	83	35		59	129
43	4	24	23	50	27	56	49	78	75	78	40	110		140
47	8	25	30	49	34	60	56	78	79	81	48	116	69	

Note that for the top two rows when $p = 5$ or $p = 7$, we have $\#X(\mathbb{F}_\ell) = \ell + 1$; this confirms that these two curves are isomorphic to $\mathbb{P}^1$. As expected, the row for $p = 11$ coincides with the number of points on the elliptic curve 121b1 given above.

6 Examples

Throughout this final section, we will give elliptic curves with their label from Cremona's tables [7] together with links to the corresponding page at [15]. The rational CM points, i.e., points in $X(\mathbb{Q})$ whose elliptic curves are defined over $\mathbb{Q}$ and have complex multiplication, appear frequently; they will be denoted by E_D where D is the discriminant of the order. The list of all of them was given in Table 1.

6.1 A necklace on an elliptic curve over $\mathbb{Q}$

Among the easiest examples to present is the necklace on the curve $E\colon y^2 = x^3 - 3\,x + 6$ for $p = 3$. The 3-isogeny field is given by

$$K = \mathbb{Q}[s]/\big(s^8 - 6\,s^5 + 3\,s^4 + 18\,s^3 + 18\,s^2 + 18\,s + 9\big)$$

whose Galois group is D_4 over $\mathbb{Q}$. It is listed in the LMFDB. The four subgroups of order 3 are defined by the following kernel polynomials:

$$\begin{aligned}
C_0\colon&\ x - \tfrac{12}{11}s^7 + \tfrac{26}{33}s^6 - \tfrac{14}{33}s^5 + \tfrac{76}{11}s^4 - \tfrac{94}{11}s^3 - 14s^2 - \tfrac{104}{11}s - \tfrac{105}{11} = 0,\\
C_1\colon&\ x + \tfrac{2}{33}s^7 - \tfrac{2}{33}s^6 - \tfrac{2}{33}s^5 - \tfrac{8}{33}s^4 + \tfrac{10}{11}s^3 + \tfrac{10}{11}s^2 - \tfrac{14}{11}s - \tfrac{13}{11} = 0,\\
C_2\colon&\ x + \tfrac{8}{11}s^7 - \tfrac{8}{11}s^6 + \tfrac{20}{33}s^5 - \tfrac{54}{11}s^4 + \tfrac{76}{11}s^3 + \tfrac{76}{11}s^2 + \tfrac{74}{11}s + \tfrac{75}{11} = 0,\\
C_3\colon&\ x + \tfrac{10}{33}s^7 - \tfrac{4}{33}s^5 - \tfrac{58}{33}s^4 + \tfrac{8}{11}s^3 + \tfrac{68}{11}s^2 + 4s + \tfrac{43}{11} = 0
\end{aligned}$$

The necklace (C_0, C_1, C_2, C_3) is the only necklace defined over $\mathbb{Q}$. The corresponding j-invariants are

$$\begin{aligned}
j(E/C_1) &= \tfrac{1}{11}\big(218818080s^7 - 67867696s^6 - 146242512s^5 - 1250596464s^4\\
&\qquad + 1173069456s^3 + 4543203600s^2 + 1837676880s - 318777768\big),\\
j(E/C_2) &= \tfrac{1}{11}\big(-3174080s^7 - 33133776s^6 + 68459664s^5 + 34515312s^4\\
&\qquad - 112554000s^3 - 113068176s^2 - 130229424s - 75810888\big),\\
j(E/C_3) &= \tfrac{1}{11}\big(5891808s^7 + 30416048s^6 + 33887568s^5 + 14692080s^4\\
&\qquad - 161874960s^3 - 161360784s^2 - 152352720s - 97934184\big),\\
j(E/C_4) &= \tfrac{1}{11}\big(-221535808s^7 + 70585424s^6 + 43895280s^5 + 1201389072s^4\\
&\qquad - 898640496s^3 - 4268774640s^2 - 1555094736s - 3711549384\big).
\end{aligned}$$

It is difficult to present examples with larger p. Typically the coefficients of the polynomial defining the p-isogeny field and the j-invariants (or the kernel polynomials) have very large height. The code file at [19] contains more complicated examples.

6.2 Reduction to a supersingular curve without extra automorphisms

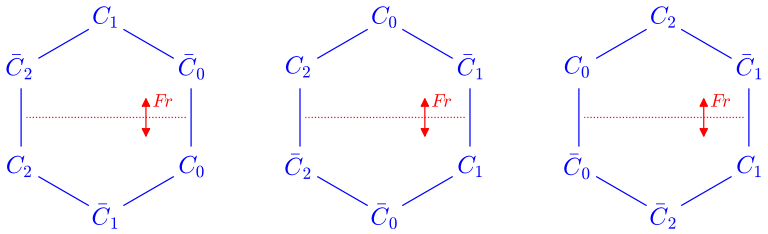
This example is for $p = 5$ and we will consider the reduction modulo $\ell = 13$ of necklaces on curves with complex multiplication. The CM points correponding to the curves E_{-7}, E_{-8}, E_{-28}, E_{-67}, and E_{-163} as listed above all have reduction at $\ell = 13$ isomorphic to the unique supersingular curve

$$\tilde{E}\colon y^2 = x^3 + x + 4$$

whose j-invariant is $5 \in \mathbb{F}_{13}$. This curve has no extra automorphisms. All six pearls are defined over the quadratic extension $\mathbb{F}_{169} = \mathbb{F}_{13}[\theta]/(\theta^2 - \theta + 2)$. Here we list the polynomials that define these subgroups on the above model of $\tilde{E}$.

$$\begin{aligned}
C_0\colon&\ x^2 + (9 + 5\theta)\,x + 8 + 12\theta & \bar{C}_0\colon&\ x^2 + (1 + 8\theta)\,x + 7 + \theta\\
C_1\colon&\ x^2 + (8 + 7\theta)\,x + 11 + 2\theta & \bar{C}_1\colon&\ x^2 + (2 + 6\theta)\,x + 11\theta\\
C_2\colon&\ x^2 + (7 + 5\theta)\,x + 1 + 6\theta & \bar{C}_2\colon&\ x^2 + (12 + 8\theta)\,x + 7 + 7\theta
\end{aligned}$$

Here the bar denotes the conjugate over $\mathbb{F}_{13}$. The three necklaces on $\tilde{E}$ pictured below are defined over $\mathbb{F}_{13}$.



The pictures are arranged such that the Galois action of $\mathbb{F}_{169}/\mathbb{F}_{13}$ is the reflection with respect to the horizontal symmetry. The unique necklace on the curve E_{-7} reduces to the left-hand necklace. For the curves E_{-28} and E_{-67}, it reduces to the middle necklace, while the necklaces of E_{-8} and E_{-163} have the right-hand necklace as their reduction.

Note that, further than the three necklaces above, the curve $\tilde{E}$ has one more $\mathbb{F}_{13}$-rational necklace, namely $(C_0, C_1, C_2, \bar{C}_0, \bar{C}_1, \bar{C}_2)$. Frobenius acts on it by rotation. No curve defined over $\mathbb{Q}$ with complex multiplication reduces to that necklace. The remaining six necklaces form three pairs of conjugate necklaces defined over $\mathbb{F}_{13^2}$.

6.3 Reduction to a curve with extra automorphism of order 4

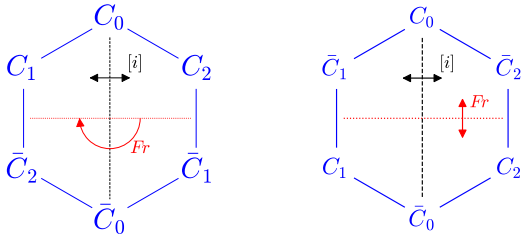
Now we consider again $p = 5$ but $\ell = 7$. The six CM points with curves E_{-7}, E_{-8}, E_{-28}, E_{-43}, E_{-67}, and E_{-163} all reduce to the curve $\tilde{E}\colon\ y^2 = x^3 + x$ with $j = 6 = 1728 \in \mathbb{F}_7$. This curve has an automorphism $[i]$ of order 4. The pearls are defined over $\mathbb{F}_{49} = \mathbb{F}_7[\theta]/(\theta^2 - \theta + 3)$.

$$
\begin{aligned}
C_0&\colon\ x^2 + 6\theta & \bar{C}_0&\colon\ x^2 + 6 + \theta \\
C_1&\colon\ x^2 + 2\theta\, x + 3\theta & \bar{C}_1&\colon\ x^2 + (2 + 5\theta)\, x + 3 + 4\theta \\
C_2&\colon\ x^2 + 5\theta\, x + 3\theta & \bar{C}_2&\colon\ x^2 + (5 + 2\theta)\, x + 3 + 4\theta
\end{aligned}
$$

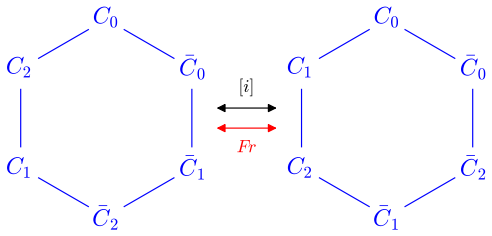
The action by the Frobenius of $\mathbb{F}_{49}/\mathbb{F}_7$ is indicated by the bar. The extra automorphism acts as an involution:

$$[i](C_0) = C_0,\ \ [i](C_1) = C_2,\ \ [i](\bar{C}_1) = \bar{C}_2.$$

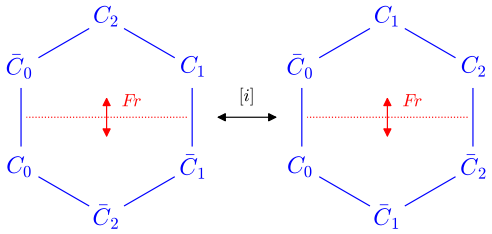
The left necklace below is the reduction of E_{-28}; it is fixed by both $[i]$ and the Frobenius and hence it represents on its own a point of $X(\mathbb{F}_7)$. The picture on the right is the reduced necklace for E_{-7} and E_{-163}, which is distinct from E_{-28}, but has the same sort of action by Galois and the automorphisms.



The next picture is the reduction of E_{-8}. The point in the modular curve is represented by a pair of necklaces exchanged by $[i]$. Frobenius exchanges the two necklaces, which shows that the point is $\mathbb{F}_7$-rational.



The final picture is the reduction of both E_{-43} and E_{-67}. Here the point in $X(\mathbb{F}_7)$ is again formed by a pair of necklaces exchanged by $[i]$. Instead each necklace is already defined over $\mathbb{F}_7$.



These four are all the $\mathbb{F}_7$-rational points on X, the remaining four necklaces produce two conjugate points in $X(\mathbb{F}_{49})$.

6.4 Reduction to a curve with extra automorphism of order 6

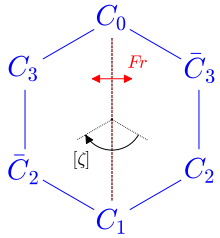
In this example, we consider again $p = 5$, but now $\ell = 11$, and we concentrate on the curve $\tilde{E}\colon y^2 = x^3 + 1$ with $j = 0$. It has extra endomorphisms and we denote $[\zeta]$ one of the elements of order 3. Two pearls are defined over $\mathbb{F}_{11}$, while the other four are defined over $\mathbb{F}_{121} = \mathbb{F}_{11}[\theta]/(\theta^2 + 7\theta + 2)$:

$$C_0\colon\ x^2 + 5\,x + 1 \qquad C_1\colon\ x^2 + 7\,x + 8$$
$$C_2\colon\ x^2 + (4 + 5\theta)\,x + 7 + 10\theta \qquad \bar{C}_2\colon x^2 + (2 + 6\theta)\,x + 3 + \theta$$
$$C_3\colon\ x^2 + (10 + 7\theta)\,x + 1 + 3\theta \qquad \bar{C}_3\colon x^2 + (5 + 4\theta)\,x + 2 + 8\theta$$

The action of the automorphisms satisfies

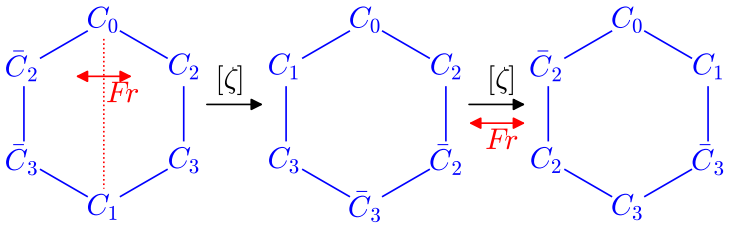
$$[\zeta](C_0) = C_2,\quad [\zeta](C_2) = \bar{C}_2,\quad [\zeta](C_1) = C_3,\quad \text{and}\quad [\zeta](C_3) = \bar{C}_3.$$

The reduction of E_{-3} gives the following necklace:



This necklace is flipped by Frobenius and fixed by $[\zeta]$; therefore it represents a point in $X(\mathbb{F}_{11})$.

Instead, the reduction of E_{-67} is the point in $X(\mathbb{F}_{11})$ represented by the triple of necklaces in the following picture:



While the first necklace is fixed by Frobenius, the other two are exchanged by it.

These are the only two $\mathbb{F}_{11}$-rational points on X, the remaining six necklaces on $\tilde{E}$ form two conjugate points in $X(\mathbb{F}_{121})$. While no other rational elliptic curves with complex multiplication that reduce to $\tilde{E}$, there are of course plenty of curves without complex multiplication.

6.5 Examples of a necklace with $p = 7$

There are four CM points corresponding to the curves E_{-8}, E_{-11}, E_{-67}, and E_{-163}, that reduce to the supersingular curve with $j = 5$ modulo $\ell = 13$.

As in Section 6.2, the pearls are defined over $\mathbb{F}_{169} = \mathbb{F}_{13}[\theta]/(\theta^2 - \theta + 2)$:

$C_0\colon\ x^3 + 10\,x^2 + 11\,x$

$C_1\colon\ x^3 + 7\,x^2 + 5\,x + 12$

$C_2\colon\ x^3 + (4 + 11\theta)x^2 + (11 + 9\theta)x + 2 + 3\theta$

$\bar{C}_2\colon\ x^3 + (2 + 2\theta)x^2 + (7 + 4\theta)x + 5 + 10\theta$

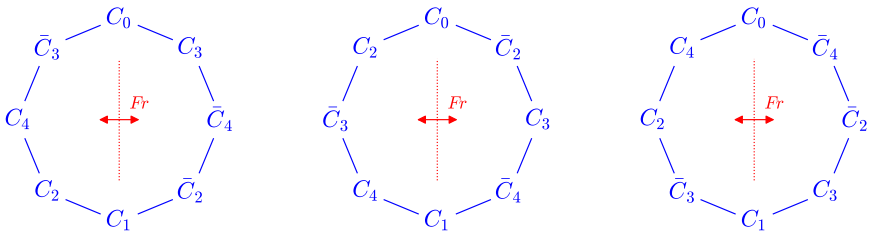
$C_3\colon\ x^3 + (10 + 4\theta)x^2 + (8 + 10\theta)x + 3 + 12\theta$

$\bar{C}_3\colon\ x^3 + (1 + 9\theta)x^2 + (5 + 3\theta)x + 2 + \theta$

$C_4\colon\ x^3 + 9\,x^2 + (8 + \theta)x + 10 + 8\theta$

$\bar{C}_4\colon\ x^3 + 9\,x^2 + (9 + 12\theta)x + 5 + 5\theta$

There are three necklaces defined over $\mathbb{F}_{13}$ on this curve:



The left is the reduction of the necklace on E_{-11}, the middle is the reduction of the necklace on E_{-8}, while the right necklace is the reduction of the necklaces of both E_{-67} and E_{-163}.

A Appendix: Number of points in the reduction

Here is a table that allows for a simple algorithm to count the number of points in $X(\mathbb{F}_\ell)$ for a prime number $\ell \neq p$.

For $j \in \mathbb{P}^1(\mathbb{F}_p)$, we write X_j for the fibre of $X(\mathbb{F}_\ell) \to \mathbb{P}^1(\mathbb{F}_\ell)$ above j. Therefore $X(\mathbb{F}_\ell) = \bigcup_{j \in \mathbb{P}^1(\mathbb{F}_\ell)} X_j$.

The following table determines $\#X_j$ in all cases. Here $a \in \mathbb{F}_p$ is the reduction modulo p of the trace of Frobenius of the elliptic curve E with the corresponding j-invariant. We define $\delta = \left(\frac{a^2 - 4\ell}{p}\right) \in \{-1, 0, 1\}$ and i to denote the number of isogenies on E of degree p defined over $\mathbb{F}_\ell$. The last invariant can take longer to calculate, but we need it only rarely.

The cases for $j \notin \{0, 1728\}$ at the bottom of the table were obtained in Lemma 3. the other entries can be calculated by analysing the Galois action on elliptic and ramified points in the special fibres above $j = 0$ and $j = 1728$. The calculations are fairly simple, but too tedious to reproduce here.

j	conditions	$\#X_j$
∞	$\ell \equiv \pm 1 \pmod{p}$	$(p-1)/2$
∞	$\ell \not\equiv \pm 1 \pmod{p}$	0
0	$\ell \equiv 2 \pmod 3$ and $\delta = 1$	$(p-1)/2$
0	$\ell \equiv 2 \pmod 3$ and $\delta = -1$	$(p+3)/2$
	$\ell \equiv p \equiv 1 \pmod 3$ and $a = 0$	$(p-1)/6$
	$\ell \equiv p \equiv 1 \pmod 3$ and $a^2 \equiv 3\ell \pmod{p}$	$(p-1)/6$
	$\ell \equiv p \equiv 1 \pmod 3$ and $a^2 \equiv \ell \pmod{p}$	$p(p-1)/6$
	$\ell \equiv p \equiv 1 \pmod 3$ and $a^2 \equiv 4\ell \pmod{p}$	$p(p-1)/6$
	$\ell \equiv p \equiv 1 \pmod 3$ and not above	0
	$\ell \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$ and $a = 0$	$(p+7)/6$
	$\ell \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$ and $a^2 \equiv 3\ell \pmod{p}$	$(p+7)/6$
	$\ell \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$ and $a^2 \equiv \ell \pmod{p}$	$(p^2-p+4)/6$
	$\ell \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$ and $a^2 \equiv 4\ell \pmod{p}$	$(p^2-p+4)/6$
0	$\ell \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$ and not above	1
1728	$p \equiv 1 \pmod 4$ and $a \neq 0$ and $\delta = 0$	$(p^2-1)/4$
1728	$p \equiv 1 \pmod 4$ and $a \neq 0$ and $\delta = 1$	0
	$p \equiv 1 \pmod 4$ and $a = 0$ and $\delta = -1$	$(p+3)/2$
	$p \equiv \ell \equiv 1 \pmod 4$ and $a = 0$ and $\delta = 1$	$(p^2-1)/4$
	$p \equiv 1 \pmod 4$ and not above	$(p-1)/2$
	$p \equiv 3 \pmod 4$ and $a \neq 0$ and $\delta = 0$	$(p^2+3)/4$
	$p \equiv 3 \pmod 4$ and $a \neq 0$ and $\delta \neq 0$	1
	$p \equiv 3 \pmod 4$ and $a = 0$ and $\delta = 1$	$(p-1)/2$
	$p \equiv \ell \equiv 3 \pmod 4$ and $a = 0$ and $\delta - 1$	$(p+3)/4$
1728	$p \equiv 3 \pmod 4$ and not above	$(p^2+3)/4$
others	$a = 0$ and $\delta = 1$	$(p-1)/2$
others	$a = 0$ and $\delta = -1$	$(p+3)/2$
	$a \neq 0$ and $\delta = 1$	0
	$a \neq 0$ and $\delta = -1$	1
	$a \neq 0$, $\delta = 0$ and $i > 2$	$p(p-1)/2$
others	$a \neq 0$, $\delta = 0$ and $i \leqslant 1$	0

References

[1] 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** (2019), no. 3, 885–944.

[2] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Quadratic Chabauty for modular curves: algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152.

[3] Burcu Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772.

[4] Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. **305** (2020), no. 1, 43–88.

[5] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231, the files we use can be found at `https://math.mit.edu/~drew/ClassicalModPolys.html`.

[6] Francesco Campagna and Riccardo Pengo, *Entanglement in the family of division fields of elliptic curves with complex multiplication*, Pacific J. Math. **317** (2022), no. 1, 21–66.

[7] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[8] Bas Edixhoven and Guido Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu **22** (2023), no. 1, 279–333.

[9] Lorenzo Furio and Davide Lombardo, *Serre's uniformity question and proper subgroups of $C_{ns}^{+}(p)$*, 2023, available at `https://arxiv.org/abs/2305.17780`.

[10] Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

[11] Emmanuel Halberstadt, *Sur la courbe modulaire $X_{ndép}(11)$*, Experiment. Math. **7** (1998), no. 2, 163–174.

[12] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate.

[13] 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** (2021), no. 3, 747–771.

[14] Gérard Ligozat, *Courbes modulaires de niveau* 11, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 149–237. Lecture Notes in Math., Vol. 601.

[15] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2025, information about modular curves are currently only available at `https://beta.lmfdb.org/ModularCurve/Q/?family=Xnsplus`.

[16] Jonathan Love, Elie Studnia, and Jan Vonk, *Arithmetic intersections on non-split cartan modular curves*, 2026, available at `https://arxiv.org/abs/2604.06963`.

[17] Pietro Mercuri and René Schoof, *Modular forms invariant under non-split Cartan subgroups*, Math. Comp. **89** (2020), no. 324, 1969–1991.

[18] Marusia Rebolledo and Christian Wuthrich, *A moduli interpretation for the non-split Cartan modular curve*, Glasg. Math. J. **60** (2018), no. 2, 411–434.

[19] ———, *SageMath implementation of necklaces on elliptic curves*, available at `https://www.maths.nottingham.ac.uk/plp/pmzcw/`, 2025.

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

[21] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[22] ———, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[23] Andrew V. Sutherland, *Isogeny volcanoes*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530.

[24] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.5)*, 2025, `https://www.sagemath.org`.

[25] David Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, 2015, available at `https://arxiv.org/abs/1508.07660`.