MODELS OF KUMMER LINES AND GALOIS REPRESENTATIONS

RAZVAN BARBULESCU, DAMIEN ROBERT, AND NICOLAS SARKIS

Abstract. In order to compute a multiple of a point on an elliptic curve in Weierstrass form one can use formulas in only one of the two coordinates of the points. These x-only formulas can be seen as an arithmetic on the Kummer line associated to the curve.

In this paper, we look at models of Kummer lines, and define an intrinsic notion of isomorphisms of Kummer lines. This allows us to give conversion formulas between Kummer models in a unified manner. When there is one rational point T of 2-torsion on the curve, we also use Mumford's theory of theta groups to show that there are two type of models: the "symmetric" ones with respect to T and the "anti-symmetric" ones. We show how this recovers the Montgomery model and various variants of the theta model.

We also classify when curves admit these different models via Galois representations and modular curves. When an elliptic curve is viewed inside a 2-isogeny volcano, we give a criteria to say if it has a given Kummer model based solely on its position in the volcano. We also give applications to the ECM factorization algorithm.

1. Introduction

In many cryptographic protocols based on elliptic curves, one wants to compute $n \cdot P = P + \cdots + P$ in the most efficient way as possible. The applications include key exchange (ECDH), digital signature (ECDSA), pairings-based identity-based encryption (IBE) and isogeny-based key encapsulation methods (e.g. CSIDH). Between 1997 and 2020 the Workshop on elliptic curve cryptography (ECC)[1] gave a special place to the algorithms and implementations of the scalar product.

On the cryptanalytic side too, the scalar product is important. The elliptic curve method of factorization (ECM) — see Lenstra's seminal work [Len87] — is a building block which takes a non-negligible amount of time in the record computations against RSA and DSA.

The improvements to the scalar product (see e.g. [BSS99; BSS05]) include among others new systems of coordinates. Some of them are available to all elliptic curves, like the Weierstrass form, and some are restricted to certain families of curves, like the Montgomery form [Mon87], the Edwards form [Edw07; BL07b], the twisted Edwards form [Ber+08; His+08], the Hessian form [Sma01], the generalized Hessian form [FJ10], the theta coordinates [GL09] and theta squared coordinates [Bos+13; HR19]. We also mention a mixed system [CGF08] where the addition law takes coordinates in one form and returns coordinates in another form.

If the x-coordinate of $n \cdot P$ is computed one can recover its y-coordinate by a square root. Montgomery noted [Mon87] that the x-coordinate of $n \cdot P$ can be obtained more efficiently by using only the x-coordinate of intermediate points of the computation. Computing with the x-coordinate only is equivalent to computing on the set $E/\pm 1$ also known as the Kummer line. Our goal in this paper is to study models of Kummer lines and their arithmetic.

Key words and phrases. Elliptic curve cryptography, Kummer lines, theta functions, modular curves, Galois representation.

[1] `https://eccworkshop.org/`

Motivation. This article is part of a line of investigations on Kummer lines:

- It is easy to say what the Kummer line of an elliptic curve in Montgomery form, or Edwards form or theta coordinates looks like. Can one define the Kummer lines in a unified and abstract manner to encompass any model, *without* going back to a model of the curve E itself? Can one make a complete list of Kummer models up to some equivalence that has to be specified?
- It is known that Montgomery curves have a rational 2-torsion point and a fast doubling formula. Similarly it is known that Hessian curves have a 3-isogeny and have a fast tripling formula. It is part of the folklore that this is related to the fact that the doubling endomorphism factors as a composition of two isogenies and on a computer it is faster to evaluate the composition of two polynomials when compared to evaluating a random polynomial of the same degree as their composition. Can one find efficient 2-isogeny formulas on Kummer lines in all models having a rational 2-torsion point?
- It is known that if P and Q are two points on an elliptic curve and P, Q and $P-Q$ are known on the Kummer line, then one can compute $P+Q$. Can we exploit a rational point of 2-torsion to speed up differential additions on Kummer lines, similar to how it was exploited to speed up doublings?

In this work we answer the questions in the first item, i.e. we give a unified description of Kummer line models. Also, it allows to find in a unified manner conversion formulas from one model to another. Finally, it allows to revisit from a more geometric point of view classical models used in the literature: Montgomery models, theta, theta squared and theta twisted models.

We postponed the publication of this article, which gives a new point of view on old and new results, until two articles answering the other items were published. Indeed, having a good geometric understanding of the characterisation of the isomorphism class of a Kummer line, as explained in Section 2 and Appendix A, was key to obtain the arithmetic results from [RS24a] and [RS24b] which bring further cryptographic applications of this article.

Some applications. In isogeny based cryptography, a recent trend has been the use of higher dimensional isogenies, between product of elliptic curves. Currently, their implementation all use theta coordinates of level 2. By contrast, it is slightly more efficient to use the Montgomery models on elliptic curves. The change of coordinates from Section 4 have been used to convert between both models for the higher dimensional isogeny is required. Although conversion between Montgomery and theta coordinates where already given in [HR19], for the isogeny applications we really need to keep track of the associated level structure, in particular the extra level 4 information, which is easy to do with the tools we introduce in this paper. As an example, the conversion formulas used in 2d [Dar+24] or 4d [Dar24] come from results obtained during this work.

For the round 2 submission of SQISign, the contributors needed a method to select a Montgomery model from a theta model (obtained via a 2d isogeny computation). In order not to leak any information from the extra level information contained in the choice of a Montgomery model, it was needed to select one uniformly among the 6 possible ones. This was done using the results of Example 6.10.

Recently, it was observed in [Rob24] that one could also use the "cubical arithmetic" on abelian varieties, constructed via work of Mumford, Grothendeick and Breen, for algorithmic purpose. Indeed, the cubical arithmetic refines the standard arithmetic and give a unified framework for the computations of pairings and isogenies. It is easy to extend our results of Section 4 of isomorphisms of Kummer line to obtain isomorphism of the underlying cubical torsor structure. Indeed, by the unicity of the cubical torsor structure, it suffices to lift the isomorphism from a projective linear change of variable to an affine change of variable, such that the cubical neutral

point of the domain is sent to the cubical neutral point of the codomain. For instance, the map $(X : Z) \mapsto (bX + aZ : aZ - bX)$ from Proposition 4.2 for the conversion from a theta model to a Montgomery model can be lifted to a map $(X, Z) \mapsto (X/a + Z/b, Z/b - X/a)$. This sends the cubical neutral point (a, b) to $(1, 0)$, hence is an isomorphism of cubical torsor structure. This isomorphism was originally used in [Rob24] to obtain the cubical formulas for the Montgomery model from the ones from the theta model. In the end, a more direct proof of the Montgomery cubical formulas was given in that paper.

Roadmap. In Section 2, we discuss the general theory of Kummer lines. In Section 3 and 4, we describe the Kummer lines built from Montgomery curves and certain theta functions of level 2. We also provide the differential addition and doubling formulas in every model, as well as the correlations between them and the conversion formulas. Section 5 covers the classification of elliptic curves via Shimura theory and the easier Galois representation criteria for the previously introduced Kummer lines. Finally, we relate the different models to isogeny volcanos in Section 7 and describe how to find curves with theta squared model to use for instance in ECM, as well as some thoughts on stage 2 with Kummer lines in Section 8.

Notations. We will use the following notations for computational cost:

- **M** is a generic multiplication,
- **S** is a generic squaring,
- **m** is a multiplication by a constant that could change on a set curve, for instance the x-coordinate of a base point,
- $\mathbf{m_0}$ is a multiplication by a curve parameter, for instance the $\mathcal{A}$ parameter of a Montgomery curve,
- **c** is a multiplication by a constant less than a computer word.

A brief presentation of the results. The article is relatively long and the reader can benefit from a brief abstract of the results. To do so we use a a language which is more abstract than the rest of the article, where we introduce the concepts gradually.

The Kummer line $E/\pm 1$ is isomorphic, as a scheme, to $\mathbb{P}^1$. However, it is not possible to recover E from the projective line, we need extra data. We first show that it is (almost) enough to give as extra marking the 4-ramification points on $\mathbb{P}^1$ (the image of the 2-torsion point on E), along with which point out of those 4 is the point 0_E. (It is customary to send 0_E to the point at infinity $(1 : 0)$ on the Kummer line, but some of the models we will study won't have this property). This model will be rational (i.e. correspond to the Kummer line f a rational elliptic curve) whenever the ramification is stable under the Galois action, and the image of 0_E is rational. We note that from this data, we can only recover E up to a quadratic twist.

Although our proofs of the above facts are completely elementary, their underlying structural reason is that the Kummer line ought to be taken as a stacky quotient $[E/\mu_2]$, where $\mu_2 = \{-1, 1\}$ is the group scheme of square roots of the unity, rather than as a schematic quotient E/μ_2 (the later is the coarse space of the former). We explain this briefly in Appendix A. This also explains why the Kummer line can "see" E only up to a quadratic twist: the choice of E is determined by the stacky quotient $[E/\pm 1]$ along with a choice of map $[E/\mu_2] \to B\mu_2$, where $B\mu_2 = [k/\mu_2]$ is the classifying stack of étale μ_2-torsors. We stress that we won't use this more abstract point of view in the main part of the paper.

The ramification data thus gives us a very simple description of the Kummer line, while still allowing us to find formulas for the arithmetic. Let us start with isomorphisms of Kummer lines: to find an isomorphism between the Kummer coordinate $(X_1 : Z_1)$ of $E_1/\pm 1$ and $(X_2 : Z_2)$ of $E_2/\pm 1$, it suffices to find the homography that sends the ramification of $E_1/\pm 1$ to the ramification to $E_2/\pm 1$, and 0_{E_1} to 0_{E_2}; this boils down to linear algebra. Indeed, such an homography lifts

to an isomorphism of elliptic curves $E_1 \to E_2$ (maybe up to replacing them by quadratic twists), isomorphism that sends 0_{E_1} to 0_{E_2} by assumption, hence which automatically preserve the group law. In particular, this gives a much simplified proof of the change of coordinates from [HR19], where the authors used a formal calculus software to check that their conversion formula preserved the group law. Instead, we only need to check that the image of the ramification matches.

Next, the ramification data is also enough to find doubling and differential addition formulas on the Kummer line. Doublings were worked out in [RS24a], while differential additions in [RS24b]. As such, we won't expand on these arithmetic aspects in this paper, but focus on the models themselves. In Section 3 we give a list of some standard Kummer models used in the literature, like the Montgomery, theta, squared theta (and maybe less standard like the twisted theta) model, and refer to the existing formulas in the literature for the arithmetic (which were also rebuilt "from scratch" in [RS24a; RS24b]). Here our contribution is Section 4, where we give conversion map between these different models. We remark that most of these were already done in [HR19], descending the existing conversion formulas in the litterature from elliptic curves to Kummer lines. What we do in Section 4 is to instead recover the conversion formulas from scratch, simply from the ramification of these different models.

In [RS24a], using the general doubling framework on Kummer lines, it was observed that for some models doublings and translation by a point of 2-torsion could be faster than a doubling. This was used to adjust the usual Montgomery ladder by replacing doublings by doublings with translation. We mention that we can retrieve a particular case as follows: the Montgomery model has faster doublings than the theta squared model, but the theta squared model has faster differential additions. But, using the conversion formulas, we see in Proposition 4.7 that they have the exact same ramification, but with a different marked point for 0_E. This means that the identity $(X : Z) \mapsto (X : Z)$ behaves as translation by a point of 2-torsion when converting back and forth between these two models; and that using the Montgomery doubling formulas in the theta model behaves as doubling and translation, and similarly using the theta squared differential additions in the Montgomery model behaves as a differential addition + translation. Since the extra translation is easy to keep track (for instance it is killed by a subsequent doubling), it is easy to adjust the Montgomery ladder to use the translated formulas instead.

In Section 5 we study when the models of Section 3 are rational, and how they are parametrized. This is where Galois representation comes in: we show that each of the family correspond to the Galois representation in the 2-Tate module T_2E taking a specific form. In fact for these families it is enough to look at the Galois representation in $E[4]$. The Galois representation then gives matrices in $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ and the families correspond to matrices living in some specific subgroup G. By Shimura theory (see e.g. [Zyw15]) our families can then be described by modular curves. More precisely, in Section 5 we show that Montgomery models correspond to $G = \Gamma^0(4)$, theta squared models to $G = \Gamma^0(4) \cap \Gamma(2)$, and theta models to $G = \Gamma(2,4) = \Gamma^0(4) \cap \Gamma_0(4)$. We also reinterpret the condition to have Galois representation in $\Gamma^0(4)$ in terms of the 2-Tate pairing. These results are certainly folklore. For the theta model they are a consequence of the more general (analytic) result by Igusa that theta constants of level n in dimension g are modular forms for $\Gamma(n, 2n)$. (The algebraic interpretation of Igusa's result, as shown by Mumford in [Mum66], is having a rational symmetric theta structure of level n.) Furthermore, although most of the many equivalent conditions to having a rational Montgomery model given in Corollary 6.3 are certainly well known (see for instance the discussion in [CV11, § 2.2]), we haven't seen explicitly stated all of them in the literature.

This section also allows us to understand the link between Montgomery and theta models better: in dimension 1 and level 2, having a rational theta structure is equivalent to having two different Montgomery models (if $E/\pm 1$ has a Montgomery model, $(X : Z) \mapsto (-X : Z)$

automatically gives another one, that leaves $(0:0)$ invariant. By two different Montgomery model we mean an isomorphism of models that sends $(0:0)$ to another two torsion point). In Section 5, we consider the modular curves as schemes (hence as coarse spaces). For moduli problems the fine moduli spaces keep track of more information, but in presence of non trivial automorphisms this requires to work with stacks rather than schemes. We briefly survey stacky modular curves in Appendix B, and their parametrisation of the Kummer models (and twists).

In Section 6, we explain why the families studied in Section 3 are "natural". Recall that our Kummer lines are isomorphic as a scheme to $\mathbb{P}^1$. We certainly want to use a line as a model of $\mathbb{P}^1$, so use as coordinate a section of a divisor (t) of degree 1: either x (which has a pole at $\infty = (1:0)$) or an homography $(ax+b)/(cx+d)$ (which has a pole at $t=-d/c$). In practice, since we prefer to work with projective coordinates $(X:Z)$, this amounts to choosing a linear change of variable $(X:Z) \mapsto (aX+bZ : cX+dZ)$. From the elliptic curve point of view, if $\pi : E \to E/\pm 1 \simeq \mathbb{P}^1$ is the projection, (X,Z) can then be seen as sections of $\pi^*(t) \sim 2(0_E)$: they form coordinates of level 2. So for us a model of Kummer lines boils down to a choice of coordinate x, and looking at how the ramification behaves. This might seem rather boring, but there are actually some nice arithmetic considerations behind the choice of x.

We want to focus on models of Kummer lines which have at least one rational point of two-torsion T (because this allows us to split doublings into the composition of two 2-isogenies). Since our projective coordinates $(X:Z)$ are of level 2, the translation map $(X(P):Z(P)) \mapsto (X(P+T):Z(P+T))$ (which is well defined on the Kummer line because T is of 2-torsion) is given by a linear change of variable $(X(P+T):Z(P+T)) = M_T \cdot (X(P):Z(P))$ for a 2×2 matrix M_T (well defined up to a multiplications by $\lambda \,\mathrm{Id}$ because $(X:Z)$ are projective coordinates). Since T is of two-torsion, M_T^2 acts by the projective identity, so we have, $M_T^2 = \lambda_T \,\mathrm{Id}$. A natural question is whether we can find M_T such that $M_T^2 = \mathrm{Id}$, i.e. $\lambda_T = 1$? It is easy to see that changing M_T to λM_T changes λ_T to $\lambda^2 \lambda_T$, so λ_T is well defined up to squares: we call it the type of T. In particular, there is an *arithmetic obstruction* to finding such a M_T: namely whether the class of λ_T modulo squares is trivial (i.e. is λ_T a square)?

If this condition is satisfied, then up to a change of basis we have $M_T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and the translation by T is $(X:Z) \mapsto (Z:X)$. Putting 0_E at infinity $(1:0)$, we then have that $T=(0:1)$, and the other two torsion points are given by $(\alpha:1), (1:\alpha)$ (since $\{T_1,T_2\}$ is stable under the action of M_T). We have rediscovered the Montgomery model!

An alternative is to take $M'_T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, this matrix is conjugate to M_T and the conjugation gives the new variables $(X':Z') = (X+Z : X-Z)$ (which we will call the Hadamard transform). Taking the Montgomery model, the ramification is then given in the $(X':Z')$ coordinates by $0_E = (1:1)$, $T_1 = (-1:1)$, $T_2 = (\beta:1), T_3 = (-\beta:1)$ with $\beta = (\alpha+1)/(\alpha-1)$.

Now assume that we have two rational points of 2-torsion, T_1, T_2. We can try to further refine by asking that T_1, T_2 should both be of trivial type, so that we can find two matrices M_1, M_2 giving their translation map and such that $M_1^2 = M_2^2 = 1$. Then M_1 and M_2 have to anticommute (this can be seen by working out the form they can take given the ramification, but also result from the deeper theory that the commutator bracket of M_1, M_2 gives the Weil pairing $e_{W,2}(T_1,T_2) = -1$.) From general linear algebra, we can always find a basis (X,Z) such that $M_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. We remark that such a basis is uniquely determined (up to a common scalar), in particular we do not have extra degrees of liberty to put 0_E at infinity anymore. If we denote $(X(0_E):Z(0_E)) = (a:b)$, then by constructions of M_1, M_2, we have $T_1 = (b:a), T_2 = (-a:b), T_1+T_2 = (-b:a)$. We have just rediscovered the theta model! In other words: a Kummer line has a rational Montgomery model when its ramification is (up to a change of variable) symmetric for one of the two symmetries: $(X:Z) \mapsto (Z:X)$ or

$(X : Z) \mapsto (-X : Z)$, while it admits a rational theta model if its ramification is (up to a change of variable) symmetric for both symmetries at the same time.

Hidden behind this story is Mumford's theta group $G(2(0_E))$: our matrices M_T are given by the action of elements of the theta groups on the sections $\Gamma(2(0_E))$, and being able to find a matrix M_T such that $M_T^2 = 1$ amount to being able to find a symmetric element above T in the theta group. Unsurprisingly, we also show in Section 6 that the class of the type $\lambda_T \in k^*/k^{*,2}$ of T is given by the self Tate pairing $e_{T,2}(T,T)$. Yet another equivalent condition is to look at points of 4-torsion: a point T' on the Kummer line is of 4-torsion above T if and only if $(X(T') : Z(T'))$ are projectively invariant under the action of M_T, i.e. $(X(T'), Z(T'))$ is an eigenvector of M_T. There are two such eigenvectors, with eigenvalues $\pm\sqrt{\lambda_T} \in \overline{k}$ (because M_T is not projectively trivial, hence not diagonal), so these eigenvectors are rational if and only if λ_T is a square. We refer to Corollary 6.3 for other equivalent conditions. This explains why in Section 5 we are interested in the Galois representation in $E[4]$.

Using these algebraic and arithmetic tools, we revisit the families of Section 3 from the theta group point of view. We also explain how we can reinterpret them as twisted variant of the theta model, and how to count their number of rational models.

In Sections 5 and 6, we look at whether a Kummer line admitted a Montgomery or theta model. In Section 7, we tackle the question whether it is *isogeneous* to one such model. For that, we use the theory of isogeny volcano.

In Section 8 we study ECM with the level 2 theta model and some of its variants. Thanks to the modular curves from Section 5, we parametrize all the elliptic curves which are suitable for our coordinate systems. In particular, we can select curves with more torsion points and small parameters.

2. Models of Kummer lines

In this article, we fix a perfect field k of characteristic 0 or $p > 2$.

Let E/k be an elliptic curve, and $\pi : E \to E/\pm 1$ be the projection, it is a degree 2 cover. This map ramifies at the 2-torsion points $E[2]$. Since there are 4 of them on $\overline{k}$, $E/\pm 1$ is a marked curve of genus 0, the marked point being $\pi(\mathcal{O}_E)$, hence is isomorphic to $\mathbb{P}^1$ over k. In fact, taking an affine Weierstrass model $y^2 = h(x)$ with $h(x)$ of degree 3 and the neutral point $\mathcal{O}_E$ being at infinity, then since $-P = (x_P, -y_P)$, it is classical that the quotient $\pi : E \to E/\pm 1$ is given by $(X : Y : Z) \mapsto (X : Z)$; this is equivalent to checking that the field $k(x)$ is the subfield of $k(E)$ invariant by the involution $[-1]$.

Definition 2.1. *A Kummer line is a map $\pi : E \to \mathbb{P}^1$ defined over k through which $[-1]$ factorizes, modulo the identification of π with $\pi' : E' \to \mathbb{P}^1$ whenever there is an isomorphism (of elliptic curves) $\varphi : E \simeq E'$ defined over $\overline{k}$ such that $\pi' = \pi \circ \varphi$.*

An isomorphism of Kummer lines $\pi_1 : E_1 \to \mathbb{P}^1$ and $\pi_2 : E_2 \to \mathbb{P}^1$ is any isomorphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ defined over k, such that φ extends to an isomorphism $\psi : E_1 \to E_2$ over $\overline{k}$ such that $\pi_2 \circ \psi = \varphi \circ \pi_1$.

Remark 2.2. *Note that in Definition 2.1, the morphisms between elliptic curves are defined over the algebraic closure $\overline{k}$, whereas the maps to the projective line are defined over k.*

For instance let us consider an elliptic curve E defined over a finite field k and its quadratic twist E'. Then what the definition says is that we identify the Kummer lines of E and E' even if E, E' are only isomorphic on the algebraic closure but not on k itself.

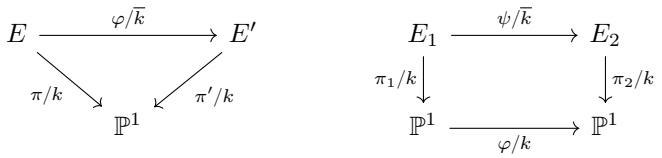


FIGURE 1. Commutative diagrams for Definition 2.1

Although the definition given above might seem ad hoc, it is quite natural if we consider the Kummer line as a stack quotient rather than a scheme quotient, we refer to Appendix A for more details.

Not every degree 2 cover $E \to \mathbb{P}^1$ factorizes through $[-1]$, hence define a Kummer line. Indeed, degree 2 covers are given by degree 2 divisors , as the pullback of (∞) on $\mathbb{P}^1$ (by Riemann-Roch a degree 2 divisor has two global sections, hence define a morphism to $\mathbb{P}^1$), and such a divisor D is, up to linear equivalence, of the form $D = (P) + (\mathcal{O}_E) = 2(P')$. It corresponds to the cover $R \mapsto x(R - P')$, which factorizes through $[-1]$ if and only if P' is a point of two torsion, that is D is linearly equivalent to $2(0_E)$.

Here is the definition of Kummer line found in [RS24a]:

Definition 2.3. *A Kummer line is the datum of a degree* 2 *cover of* $\mathbb{P}^1$ *by* E *with* 4 *distinct ramification points, one of which is rational and marked:*

$$\pi : E \to \mathbb{P}^1 \text{ and } \exists \mathcal{O}_E \in E(k), \exists T, R, S \in E \text{ with } \#\pi^{-1}(\pi(P)) = \begin{cases} 1 & \text{if } P \in \{\mathcal{O}_E, T, R, S\}, \\ 2 & \text{otherwise.} \end{cases}$$

As we will see in Proposition 2.5, both definitions are equivalent, we will first need a lemma:

Lemma 2.4. *Let* E *be an algebraic curve defined over* k*, and* $\pi : E \to \mathbb{P}^1$ *a degree* 2 *cover defined over* k *with* 4 *ramification points, one of which is marked. Then* E *is an elliptic curve.*

Proof. This statement could be proved using Riemann-Hurwitz formula, but we will use another approach that will yield more information on the ramification in Proposition 2.5. Since π is a degree 2 cover and one of the ramification points is in $E(k)$, $\pi^* : k(\mathbb{P}^1) \to k(E)$ is a degree 2 extension. Because $\operatorname{char} k \neq 2$, one can write $k(\mathbb{P}^1) = k(x)$, $k(E) = k(x, y)$ and $y^2 = h(x)$, where $h \in k[x]$. The discriminant of this extension is $\Delta = 4h$. We now work over $\overline{k}$. The places in $\mathbb{P}^1$ are the $\mathfrak{p}_\alpha$ associated to the irreducible polynomial $x - \alpha$ with $\alpha \in \overline{k}$, and the place at infinity $\mathfrak{p}_\infty$. A place $\mathfrak{p}_\alpha$ ramifies if and only if $\mathfrak{p}_\alpha \mid \Delta$, i.e. $h(\alpha) = 0$ since the characteristic is not 2. With the place at infinity, this means that h has either 3 or 4 roots in $\overline{k}$, hence E is an elliptic curve. □

Proposition 2.5. *Let* E *be an elliptic curve and* $\pi : E \to \mathbb{P}^1$ *a map, both defined over* k*. The following assertions are equivalent:*

(1) π *is a Kummer line in the sense of Definition 2.1.*
(2) π *is a Kummer line in the sense of Definition 2.3.*

Moreover, the 4 *ramification points in Definition 2.3 are exactly the* 2*-torsion points and the fibres are given by* $\pi^{-1}(\pi(P)) = \{\pm P\}$ *for* $P \in E$*.*

Proof. Assume first that π is a Kummer line in the sense of Definition 2.1. We consider $p : E \to \mathbb{P}^1$ with $p(P) = (x : 1)$ if $P = (x, y) \in E$ and $p(\mathcal{O}) = (1 : 0)$. p is a degree 2 cover which factors by $[-1]$, hence because of the universal property defining π, we can identify them. If $P \in E$, the fibres are $p^{-1}(p(P)) = \{\pm P\}$, so ramification points must verify $P = -P$, i.e. $2 \cdot P = \mathcal{O}$, that is P is a ramification point if and only if P is a 2-torsion point. This gives exactly 4 ramification points, and $\mathcal{O}_E$ is rational, so p and π are Kummer lines in the sense of Definition 2.3.

Conversely, assume π is a Kummer line in the sense of Definition 2.3. We will reuse notations of the proof of Lemma 2.4, where $k(\mathbb{P}^1) = k(x)$, $k(E) = k(x, y)$, $y^2 = h(x)$ with $h \in k[x]$ and $\pi^* : k(\mathbb{P}^1) \to k(E)$ is the degree 2 extension. Let $\sigma \in \mathrm{Gal}(\overline{k}(x, y)/\overline{k}(x))$, then $\sigma(x) = x$ and because $y^2 \in k(x)$, we must have $\sigma(y)^2 = y^2$, that is $\sigma(y) = \pm y$. Hence, the non-trivial Galois automorphism is given by $\sigma(x) = x$ and $\sigma(y) = -y$. It is well known that this corresponds to the involution $\iota : E \to E$ with $\iota(P) = -P$, see [Sil86, § III.2.3]. Because $\pi^* = \sigma \circ \pi^*$, we recover that $\pi = \pi \circ \iota$, which implies $\pi^{-1}(\pi(P)) = \{\pm P\}$, and as before the ramification points are the 2-torsion points. Because of the fibres, $[-1]$ factorizes through π, hence it is a Kummer line in the sense of Definition 2.1. □

3. Some families of Kummer lines

We now give some examples of Kummer lines, from the classical Montgomery model to variants of theta models.

3.1. **Montgomery curves.**

Let $\mathcal{A}, B \in k$, an elliptic curve of the following form is known as a Montgomery curve:

$$M_{\mathcal{A},B} : By^2 = x(x^2 + \mathcal{A}x + 1)$$

Points are written in projective coordinates $(X : Y : Z)$ satisfying the following equation:

$$BY^2Z = X(X^2 + \mathcal{A}XZ + Z^2)$$

The neutral element for the addition law is $\mathcal{O} = (0 : 1 : 0)$.

The Kummer line associated to a Montgomery curve is the x-only system of coordinates:

$$M_{\mathcal{A},B} \xrightarrow{\pi} \mathbb{P}^1$$
$$(X : Y : Z) \mapsto \begin{cases} (1 : 0) & \text{if } (X : Y : Z) = \mathcal{O}, \\ (X : Z) & \text{otherwise.} \end{cases}$$

Because the ramification on the Kummer line is given by the 2-torsion, it corresponds to the point at infinity and the points with x-coordinate a root of $x(x^2 + \mathcal{A}x + 1)$.

Definition 3.1. *Let $\alpha \in \overline{k}$ be a root of $x^2 + \mathcal{A}x + 1$, then the ramification is:*

$$\mathcal{O} = (1 : 0)^*, \quad T = (0 : 1), \quad R = (\alpha : 1), \quad S = (1 : \alpha). \tag{1}$$

If $\alpha = (a : b) \in \mathbb{P}^1$, we will denote the Montgomery Kummer line model $M(a : b)$.

The arithmetic provided by Montgomery in [Mon87] and recalled in Algorithms 1 and 2 is efficient with this construction as a differential addition can be done in $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}$ and a doubling in $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$.

Remark 3.2. *The differential addition formulas do not hold if $[P - Q] = (0 : 1)$, in this case, $P - Q = T$ is a 2-torsion point and $[P + Q] = [2 \cdot Q + T]$. If $[2 \cdot Q] = (X : Z)$, then $[2 \cdot Q + T] = (Z : X)$ according to [RS24a, Eq. (4)].*

It can be noted that the constant B is never involved in the formulas, which is a specificity of Kummer lines, the twist we are working on does not matter. We refer to [CS18] for a survey on Montgomery curves.

Lastly, it will prove useful to determine when there are any rational 4-torsion points on the Kummer line T'. Of course, this implies that $T := 2T'$ is rational. To do that, the approach is the same as what is done in [RS24a, § 3.2, Main Example 4]. We first determine the translation $\tau : P \mapsto P + T$ on the Kummer line, where T is a 2-torsion point, therefore τ factors by $[-1]$ on both sides and hence is well-defined and is a homography γ_T. Then we look for a point $x(T') = (X(T') : Z(T'))$ that is invariant by γ_T. We stress that although we only look for T'

Algorithm 1: Differential addition in Montgomery xz-coordinates

Input: $[P] = (X_1 : Z_1)$, $[Q] = (X_2 : Z_2)$ and $[P - Q] = (X_0 : Z_0) \neq (0 : 1), (1 : 0)$
Output: $[P + Q] = (X : Z)$

Function `DiffAdd`$([P], [Q], [P - Q])$**:**
- $u \leftarrow (X_1 + Z_1)(X_2 - Z_2)$;
- $v \leftarrow (X_1 - Z_1)(X_2 + Z_2)$;
- $w \leftarrow (u + v)^2$;
- $t \leftarrow (u - v)^2$;
- $X \leftarrow w$;
- $Z \leftarrow \frac{X_0}{Z_0} t$;
- **return** $(X : Z)$;

Algorithm 2: Doubling in Montgomery xz-coordinates

Input: $[P] = (X_1 : Z_1)$
Output: $[2 \cdot P] = (X : Z)$
Data: On $M_{\mathcal{A},B}$, $d = \frac{\mathcal{A}+2}{4}$

Function `Doubling`$([P])$**:**
- $u \leftarrow (X_1 + Z_1)^2$;
- $v \leftarrow (X_1 - Z_1)^2$;
- $t \leftarrow u - v$;
- $X \leftarrow uv$;
- $Z \leftarrow t(v + dt)$;
- **return** $(X : Z)$;

rational on the Kummer line, i.e. $x(T')$ rational; T' itself may only be defined over a quadratic extension. We note the following easy lemma:

Lemma 3.3. *A 4-torsion point $T' \in E$ above a rational 2-torsion point $T = 2T'$ has $x(T') \in k$ if and only if $\sigma(T') = T'$ or $\sigma(T') = T' + T$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$, if and only if the cyclic subgroup of order 4, $\langle T' \rangle$, is rational.*

In this case there is also a second rational cyclic subgroup of order 4 containing T, generated by $T' + T_2$ for a 2-torsion point $T_2 \neq T$.

Proof. Note that if $\varphi : E \to E_2 = E/\langle T \rangle$ is the corresponding 2-isogeny, then the image of T_2 by φ is a rational point of 2-torsion (which gives the dual isogeny), the image of T' is also a rational point of 2-torsion, hence there is also a third rational point of 2-torsion on E_2, and composing the associated isogeny $E_2 \to E_3$ with φ gives a cyclic isogeny of degree 4. □

On the Montgomery model, for $T = (0 : 1)$, $\gamma_T : (X : Z) \mapsto (Z : X)$, and we find that there are always two points of 4-torsion: $T' = (1 : 1)$ and $T'' = (-1 : 1)$.

3.2. **Theta models.** It is easy to define from a Montgomery curve a Kummer line model with efficient arithmetic. Another way to build Kummer lines is via theta functions, which have already been used for instance in [GL09; KS20]. Their arithmetic is competitive with the Montgomery one, hence why we would like to study them. Another interesting aspect about these functions is that they generalize well to abelian varieties of higher dimension, but we will not discuss this aspect in this paper.

Theta functions can be naturally expressed as analytic functions over $\mathbb{C}$, hence an approach is to study and find formulas on complex numbers and check that those are still valid on more generic fields, especially finite ones. For the direct algebraic interpretation of theta functions we refer to [Mum66] for their construction via the theta group, and to [Bre83] for their construction via the cubical torsor structure.

Let $\mathbb{H}$ be the Poincaré half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \operatorname{im} \tau > 0\}$ and consider $\tau \in \mathbb{H}$. We can then define a lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ and an elliptic curve on $\mathbb{C}$ can be seen as $E_\tau = \mathbb{C}/\Lambda_\tau$. Our first objective is to define some mappings $E_\tau \to \mathbb{P}^{\ell-1}(\mathbb{C})$ with simple algebraic addition law. Theta functions will help us to do so, more details can be found in [Mum83, § II].

First, for $\tau \in \mathbb{H}$, the Jacobi theta function is defined as follows for every $z \in \mathbb{C}$:

$$\vartheta(z;\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi n^2\tau + 2i\pi nz). \tag{2}$$

This function is well-defined for every $z \in \mathbb{C}$ (see [Mum83, § II.1, Prop. 1.1]).

If $a, b \in \mathbb{Z}$, $\ell \in \mathbb{N}^*$, we also define theta functions with characteristics (we use the notations of Gaudry and Lubicz [GL09]):

$$\vartheta_\ell\left[a,b\right](z;\tau) = \sum_{n\in\mathbb{Z}} \exp\left(i\pi\Big(n+\frac{a}{\ell}\Big)^2\tau + 2i\pi\left(n+\frac{a}{\ell}\right)\left(z+\frac{b}{\ell}\right)\right). \tag{3}$$

Let us list a series of classical properties of the theta functions:

Proposition 3.4. *Let $z \in \mathbb{C}$, $\ell \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}$, then:*

$$\begin{aligned}
\vartheta_\ell\left[a,b\right](z;\tau) &= \exp(i\pi a^2\tau/\ell^2 + 2i\pi a(z+b/\ell)/\ell)\vartheta(z+a\tau/\ell+b/\ell;\tau),\\
\vartheta_\ell\left[a,b\right](z+m;\tau) &= \exp(2i\pi am/\ell)\vartheta_\ell\left[a,b\right](z;\tau),\\
\vartheta_\ell\left[a,b\right](z+m\tau;\tau) &= \exp(-2i\pi bm/\ell)\exp(-i\pi m^2\tau - 2i\pi mz)\vartheta_\ell\left[a,b\right](z;\tau).
\end{aligned}$$

These functions are still well-defined if $a, b \in \mathbb{R}$, but we generally restrict to the case where $a, b \in \mathbb{Z}$.

Theta functions with characteristic are a particular case of functions of level ℓ.

Definition 3.5. *Let $\tau \in \mathbb{H}$ and $\ell \in \mathbb{N}^*$. An entire function $f : \mathbb{C} \to \mathbb{C}$ is said to be of level ℓ if for all $z \in \mathbb{C}$, $m \in \mathbb{Z}$:*

$$f(z+m) = f(z) \text{ and } f(z+m\tau) = \exp(-i\pi\ell m^2\tau - 2i\pi\ell mz)f(z)$$

We call R_ℓ^τ the vector space of functions of level ℓ.

The point of defining such functions is that if we take a family $f_1, \dots, f_r \in R_\ell^\tau$ and $\lambda \in \Lambda_\tau$, then there is a function $c_\ell : \mathbb{C} \to \mathbb{C}$ such that for all $1 \leqslant i \leqslant r$, for all $z \in \mathbb{C}$, $f_i(z+\lambda) = c_\ell(z)f_i(z)$, hence in the projective space, $(f_1 : \cdots : f_r)$ is invariant by the lattice Λ_τ. Functions of level ℓ are interesting because up to a projective factor, they are invariant under the action of Λ_τ.

We will now relate theta functions with characteristics with functions of level ℓ. Because of the definition in Eq. (3), at a set ℓ and with integer characteristics, it is clear that we can define for a given τ exactly ℓ^2 functions. The following theorem shows that in fact we only require ℓ of them.

Theorem 3.6 ([Mum83], § II.1, Prop. 1.3)**.** *For every $\tau \in \mathbb{H}$, $\ell \in \mathbb{N}^*$, $\dim R_\ell^\tau = \ell$.*

Mumford's proof builds explicit bases via theta functions with characteristics. In the following, we will focus on level $\ell = 2$ because we will gain on several aspects, especially recovering easily Kummer lines. We will now give some of the families used in Mumford's proof:

Definition 3.7. *Let $\tau \in \mathbb{H}$, for every $z \in \mathbb{C}$, we define the following theta functions:*

$$\theta_0^\tau(z) = \vartheta_2\left[0,0\right](z;\tau/2), \qquad \theta_1^\tau(z) = \vartheta_2\left[0,1\right](z;\tau/2).$$

Proposition 3.8 ([Mum83], § II.1, Prop. 1.3)**.** *$(\theta_0^\tau, \theta_1^\tau)$ is a basis of R_2^τ.*

For every elliptic curve E on $\mathbb{C}$, there exists τ such that $E = E_\tau$, to which we associate the previously defined theta functions, giving a degree 2 cover thanks to the following theorem by Lefschetz proven in [Mum83, § II.1, Thm. 1.3] and [Mum70, § I.3]:

Theorem 3.9 (Lefschetz)**.** *Let $\tau \in \mathbb{H}$. If E_τ is an elliptic curve on $\mathbb{C}$, denote by $\mathcal{K}_\tau = E_\tau/\pm 1$, and $\overline{z} \in \mathcal{K}_\tau$ the class of $z \in E_\tau$. If (f, g) is a basis of R_2^τ, then the following map $\Phi : \mathcal{K}_\tau \to \mathbb{P}^1$ is well-defined and is an embedding:*

$$\Phi : \overline{z} \mapsto (f(z) : g(z)).$$

Equivalently, $\pi : E_\tau \to \mathbb{P}^1, z \mapsto (f(z) : g(z))$ is a Kummer line.

Remark 3.10. *The more general version of the theorem also states that if the level ℓ is greater than 3, then we directly have an embedding $E_\tau \to \mathbb{P}^{\ell-1}$.*

As for the arithmetic, we will need the following formulas relating theta functions with different characteristics and τ, we will only give them in level 2, however more general formulas can be found in [Igu72, § IV.1, Thm. 2]:

Proposition 3.11 (Duplication formulas)**.** *Let $a_1, b_1, a_2, b_2 \in \mathbb{Z}$, $z_1, z_2 \in \mathbb{C}$ and $\tau \in \mathbb{H}$. Let $2w_1 = z_1 + z_2$ and $2w_2 = z_1 - z_2$, then:*

$$2\vartheta_2\left[a_1, b_1\right](z_1;\tau)\vartheta_2\left[a_2, b_2\right](z_2;\tau) = \sum_{t\in\{0,1\}} e^{-i\pi a_1 t}\vartheta_2\left[a_1 + a_2, \frac{b_1+b_2}{2} + t\right](w_1;\tau/2)\cdot\vartheta_2\left[a_1 - a_2, \frac{b_1-b_2}{2} + t\right](w_2;\tau/2),$$

$$\vartheta_2\left[a_1, b_1\right](z_1;\tau)\vartheta_2\left[a_2, b_2\right](z_2;\tau) = \sum_{t\in\{0,1\}} \vartheta_2\left[\frac{a_1+a_2}{2} + t, b_1 + b_2\right](2w_1;2\tau)\cdot\vartheta_2\left[\frac{a_1-a_2}{2} + t, b_1 - b_2\right](2w_2;2\tau).$$

Proof. The first formula is [Igu72, § IV.1, Thm. 2]. The second one can then be derived from the first one, set:

$$A = \sum_{t\in\{0,1\}} \vartheta_2\left[\frac{a_1+a_2}{2} + t, b_1 + b_2\right](2w_1;2\tau)\cdot\vartheta_2\left[\frac{a_1-a_2}{2} + t, b_1 - b_2\right](2w_2;2\tau).$$

Also set, for $t \in \{0, 1\}$:

$$a_1' = \frac{a_1+a_2}{2} + t, \qquad a_2' = \frac{a_1-a_2}{2} + t, \qquad b_1' = b_1 + b_2, \qquad b_2' = b_1 - b_2.$$

A quick computation yields:

$$a_1' + a_2' = a_1 + 2t, \qquad a_1' - a_2' = a_2, \qquad b_1' + b_2' = 2b_1, \qquad b_1' - b_2' = 2b_2.$$

By applying the first formula inside the sum of A, since $2t = 0 \bmod 2$, we get:

$$A = \frac{1}{2}\sum_{t,r\in\{0,1\}} e^{-i\pi a_1' r}\vartheta_2\left[a_1, b_1 + r\right](z_1;\tau)\cdot\vartheta_2\left[a_2, b_2 + r\right](z_2;\tau).$$

We then split when $r = 0$ and $r = 1$. If $r = 0$, then there is no dependency on t, and we recover $2\vartheta_2\left[a_1, b_1\right](z_1;\tau)\vartheta_2\left[a_2, b_2\right](z_2;\tau)$ in the sum. If $r = 1$, the theta functions do not depend on t and the exponential is $\exp(-i\pi a_1' r) = \exp(-i\pi\frac{a_1+a_2}{2})\exp(-i\pi t)$. Because $1 + \exp(-i\pi) = 0$, we finally get:

$$A = \vartheta_2\left[a_1, b_1\right](z_1;\tau)\vartheta_2\left[a_2, b_2\right](z_2;\tau).$$

□

3.2.1. *Theta models and their duals.* A period $\tau \in \mathbb{H}$ is set for the rest of this section. Let us first consider the theta functions $(\theta_0^\tau, \theta_1^\tau)$. It is a basis of R_2^τ thanks to Proposition 3.8, so the map $\pi : z \in E_\tau \mapsto (\theta_0^\tau(z) : \theta_1^\tau(z))$ is a Kummer line by Theorem 3.9. For convenience, set $(a : b) := (\theta_0^\tau(0) : \theta_1^\tau(0))$, they are the theta constants. It can be shown using the definition of the theta functions that the ramification on the Kummer line is then:

$$\mathcal{O} = (a : b)^*, \quad T = (-a : b), \quad R = (b : a), \quad S = (-b : a). \tag{4}$$

Definition 3.12. *An elliptic curve E/k has a theta model with theta constants $(a : b) \in \mathbb{P}^1(k)$ if there exist a Kummer line $E \to \mathbb{P}^1$ with the following ramification points as in (4). The theta model will be written $\theta(a : b)$ generally, or $\theta^\tau(a : b)$ over E_τ.*

Another model that can be derived from this one is the dual one using the Hadamard transform.

Definition 3.13. *Let E/k be an elliptic curve with a theta model $\theta(a : b)$, the Kummer line is denoted π. The dual theta model is given by composing π with the Hadamard transform*

$$\begin{aligned} H : \mathbb{P}^1 &\to \mathbb{P}^1 \\ (X : Z) &\mapsto (X + Z : X - Z). \end{aligned} \tag{5}$$

The theta constants are $(a' : b') = (a + b : a - b)$, and the ramification is:

$$\mathcal{O} = (a' : b')^*, \quad T = (b' : a'), \quad R = (-a' : b'), \quad S = (-b' : a').$$

The dual model is written $\theta'(a : b)$ or $\theta'^\tau(a : b)$ over E_τ.

The corresponding theta functions are:

$$\theta'^\tau_0 = \theta_0^\tau + \theta_1^\tau, \qquad \theta'^\tau_1 = \theta_0^\tau - \theta_1^\tau.$$

It is a corollary from Proposition 3.8 that this is also a basis of R_2^τ.

Remark 3.14. *A computation with the analytic definition helps to express θ'^τ_0 and θ'^τ_1 as theta functions with characteristic:*

$$\theta'^\tau_0(z) = \vartheta_2\left[0, 0\right](2z; 2\tau), \qquad \theta'^\tau_1(z) = \vartheta_2\left[1, 0\right](2z; 2\tau).$$

With these new notations, and using Proposition 3.11 with $(a_1, b_1) = (a_2, b_2)$, one can relate the theta functions to get a differential addition and doubling:

Proposition 3.15. *Let $\tau \in \mathbb{H}$, for every $u, v \in \mathbb{C}$:*

$$\begin{cases} 2\theta'^{\tau/2}_0(u+v)\theta'^{\tau/2}_0(u-v) = \theta_0^\tau(2u)\theta_0^\tau(2v) + \theta_1^\tau(2u)\theta_1^\tau(2v), \\ 2\theta'^{\tau/2}_1(u+v)\theta'^{\tau/2}_1(u-v) = \theta_0^\tau(2u)\theta_0^\tau(2v) - \theta_1^\tau(2u)\theta_1^\tau(2v), \\ \theta_0^\tau(u+v)\theta_0^\tau(u-v) = \theta'^{\tau/2}_0(u)\theta'^{\tau/2}_0(v) + \theta'^{\tau/2}_1(u)\theta'^{\tau/2}_1(v), \\ \theta_1^\tau(u+v)\theta_1^\tau(u-v) = \theta'^{\tau/2}_0(u)\theta'^{\tau/2}_0(v) - \theta'^{\tau/2}_1(u)\theta'^{\tau/2}_1(v). \end{cases} \tag{6}$$

It is convenient to give names to the theta constants on the 2-isogeneous curve $E_{\tau/2}$. Let $(A : B) := (\theta_0^{\tau/2}(0) : \theta_1^{\tau/2}(0))$ and $(A' : B') := (A + B : A - B)$. Setting $u = v = 0$ in Eq. (6), one obtains[2]:

$$(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2).$$

[2]This relation is also in [GL09, § 6.2], however there is a typo in the published version as squares are missing on A' and B'. The preprint is fixed.

Remark 3.16. *The formulas in Eq.* (6)*, while obtained over* $\mathbb{C}$*, are purely algebraic in the end. This is what enables us to use them on more general fields, such as finite fields, thanks to Lefschetz' principle.*

Similarly to what Montgomery did, these formulas provide differential addition formulas as well as doubling ones, they are described in Algorithms 3 and 4. Differential addition costs $2\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$, while doubling is $4\mathbf{S} + 2\mathbf{m}_0$.

Algorithm 3: Differential addition on theta model

Input: $[P] = (X_1 : Z_1)$, $[Q] = (X_2 : Z_2)$ and $[P - Q] = (X_0 : Z_0)$
Output: $[P + Q] = (X : Z)$
Data: On $\theta^\tau(a : b)$, $(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2)$

Function `DiffAdd`$([P], [Q], [P - Q])$**:**
- $u \leftarrow (X_1^2 + Z_1^2)(X_2^2 + Z_2^2)$;
- $v \leftarrow \frac{A'^2}{B'^2}(X_1^2 - Z_1^2)(X_2^2 - Z_2^2)$;
- $X \leftarrow (u + v)$;
- $Z \leftarrow \frac{X_0}{Z_0}(u - v)$;
- **return** $(X : Z)$;

Algorithm 4: Doubling on theta model

Input: $[P] = (X_1 : Z_1)$
Output: $[2 \cdot P] = (X : Z)$
Data: On $\theta^\tau(a : b)$, $(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2)$

Function `Doubling`$([P])$**:**
- $u \leftarrow (X_1^2 + Z_1^2)^2$;
- $v \leftarrow \frac{A'^2}{B'^2}(X_1^2 - Z_1^2)^2$;
- $X \leftarrow (u + v)$;
- $Z \leftarrow \frac{a}{b}(u - v)$;
- **return** $(X : Z)$;

We can also study points of 4-torsion on the theta model $\theta^\tau(a : b)$. Recall that $T = (-a : b)$ and $R = (b : a)$ are two independent 2-torsion points, then $\tau : (X : Z) \mapsto (-X : Z)$ is the translation by T and $\tau' : (X : Z) \mapsto (Z : X)$ is the translation by R. Then, on the Kummer line, if we have a 4-torsion point T' above T, it verifies $T' + T = T'$. Hence, if $T' = (X : Z)$, we must have $(X : Z) = (-X : Z)$, that is $T' = (1 : 0)$ or $T' = (0 : 1)$. Similarly, if R' is above R, we find that $R' = (1 : 1)$ or $R' = (-1 : 1)$.

Proposition 3.17. *On the theta model* $\theta^\tau(a : b)$*, the* 4*-torsion is:*

$$T' = (1 : 0), \qquad T'' = (0 : 1), \qquad R' = (1 : 1), \qquad R'' = (-1 : 1)$$

where $2 \cdot T' = 2 \cdot T'' = T$ *and* $2 \cdot R' = 2 \cdot R'' = R$*. On the theta dual model* $\theta'^\tau(a' : b')$*, the* 4*-torsion is:*

$$T' = (1 : 1), \qquad T'' = (-1 : 1), \qquad R' = (1 : 0), \qquad R'' = (0 : 1).$$

On both model, the last points above S *may not be rational but are still given by* $S' = (i : 1)$ *and* $S'' = (-i : 1)$ *with* $i^2 = -1$*.*

3.2.2. *Theta squared model.* It appears in Algorithms 3 and 4 that one only needs the square of the coordinates. This is what leads to the theta squared model. For a set $\tau \in \mathbb{H}$, we define the following theta functions:

$$\widehat{\theta}_0^{\tau/2}(z) = \vartheta_2\left[0,0\right](z;\tau/2)^2, \qquad \widehat{\theta}_1^{\tau/2}(z) = \vartheta_2\left[0,1\right](z;\tau/2)^2,$$
$$\breve{\theta'}_0^{\tau}(z) = \vartheta_2\left[0,0\right](z;\tau)^2, \qquad \breve{\theta'}_1^{\tau}(z) = \vartheta_2\left[1,0\right](z;\tau)^2.$$

Proposition 3.18 ([Mum83], § II.1, Prop. 1.3)**.** *$(\breve{\theta'}_0^{\tau}, \breve{\theta'}_1^{\tau})$ is a basis of R_2^{τ} and $(\widehat{\theta}_0^{\tau/2}, \widehat{\theta}_1^{\tau/2})$ is a basis of $R_2^{\tau/2}$.*

This gives new theta models, but more importantly they are related to the previous ones via the following relations:

$$\widehat{\theta}_i^{\tau/2}(z) = \theta_i^{\tau}(z)^2, \qquad \breve{\theta'}_i^{\tau}(2z) = {\theta'}_i^{\tau/2}(z)^2.$$

The curve E_τ and $E_{\tau/2}$ are 2-isogeneous, the isogeny and its dual are given by:

$$f : z \bmod \Lambda_\tau \mapsto z \bmod \Lambda_{\tau/2}, \qquad \hat{f} : z \bmod \Lambda_{\tau/2} \mapsto 2z \bmod \Lambda_\tau.$$

If we relate this to the formulas above, we have just expressed f and $\hat{f}$ on certain theta models.

As for the ramification points, we use the additional 4-torsion given in Proposition 3.17.

Definition 3.19. *An elliptic curve E/k has a theta squared model with constants $(a^2 : b^2) \in \mathbb{P}^1(k)$ if there exist a Kummer line $E \to \mathbb{P}^1$ with the following ramification points:*

$$\mathcal{O} = (a^2 : b^2)^*, \quad T = (b^2 : a^2), \quad R = (1 : 0), \quad S = (0 : 1).$$

The theta squared model will be written $\widehat{\theta}(a^2 : b^2)$ generally, or $\widehat{\theta}^{\tau/2}(a^2 : b^2)$ over $E_{\tau/2}$, and $\breve{\theta'}^{\tau}(A'^2 : B'^2)$ over E_τ with the according constants.

Remark 3.20. *While as functions $\widehat{\theta}_i$ and $\breve{\theta'}_i$ are not exactly the same, they both correspond to squared coordinates of a theta model and have ramification in the same shape, hence the name and the association. The ramification points are exactly the same as in the Montgomery model Eq.* (1)*, but the marked point is different. We will develop this connection in the next section.*

Note that with this definition, an elliptic curve can admit a theta squared model $\widehat{\theta}(a^2 : b^2)$ without having a theta model $\theta(a : b)$: $(a : b)$ may not be rational.

Proposition 3.21. *The rational 4-torsion on the theta squared model $\widehat{\theta}(a^2 : b^2)$ is given by $T' = (1 : 1)$ and $T'' = (-1 : 1)$ where $2 \cdot T' = 2 \cdot T'' = T$.*

By adapting Algorithms 3 and 4, we can recover a more efficient differential addition in $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$ in this model with a doubling still in $4\mathbf{S} + 2\mathbf{m}_0$, they are in Algorithms 5 and 6.

3.2.3. *Theta twisted model.* While arithmetic on theta squared model is quite efficient, it is hard to go back to the original theta model if it exists because of the squares. We will then introduce a more natural model which is as efficient as the theta squared one and less restrictive to go back to the theta one.

If we have theta functions (θ_0, θ_1) which give a theta model, the associated theta constants are not zero, and we can then consider a new basis:

$$\widetilde{\theta}_0(z) := \theta_0(0)\theta_0(z), \qquad \widetilde{\theta}_1(z) := \theta_1(0)\theta_1(z).$$

This is clearly a basis of R_2^{τ} from Proposition 3.8, and define a new theta model named theta twisted. The ramification is as follows if we start from the theta model $\theta(a : b)$:

Algorithm 5: Differential addition on theta squared model

Input: $[P] = (X_1 : Z_1)$, $[Q] = (X_2 : Z_2)$ and $[P - Q] = (X_0 : Z_0)$
Output: $[P + Q] = (X : Z)$
Data: On $\breve{\theta'}^{\tau}(A'^2 : B'^2)$, $(a^2 : b^2) = (A'^2 + B'^2 : A'^2 - B'^2)$

Function `DiffAdd`$([P], [Q], [P - Q])$**:**
- $u \leftarrow (X_1 + Z_1)(X_2 + Z_2)$;
- $v \leftarrow \frac{a^2}{b^2}(X_1 - Z_1)(X_2 - Z_2)$;
- $X \leftarrow (u + v)^2$;
- $Z \leftarrow \frac{X_0}{Z_0}(u - v)^2$;
- **return** $(X : Z)$;

Algorithm 6: Doubling on theta squared model

Input: $[P] = (X_1 : Z_1)$
Output: $[2 \cdot P] = (X : Z)$
Data: On $\breve{\theta'}^{\tau}(A'^2 : B'^2)$, $(a^2 : b^2) = (A'^2 + B'^2 : A'^2 - B'^2)$

Function `Doubling`$([P])$**:**
- $u \leftarrow (X_1 + Z_1)^2$;
- $v \leftarrow \frac{a^2}{b^2}(X_1 - Z_1)^2$;
- $X \leftarrow (u + v)^2$;
- $Z \leftarrow \frac{A'^2}{B'^2}(u - v)^2$;
- **return** $(X : Z)$;

Definition 3.22. *An elliptic curve E/k has a theta twisted model with constants $(a^2 : b^2) \in \mathbb{P}^1(k)$ if there exist a Kummer line $E \to \mathbb{P}^1$ with the following ramification points:*

$$\mathcal{O} = (a^2 : b^2)^*, \quad T = (-a^2 : b^2), \quad R = (1 : 1), \quad S = (-1 : 1).$$

The theta twisted model will be written $\widetilde{\theta}(a^2 : b^2)$ generally, or $\widetilde{\theta}^{\tau}(a^2 : b^2)$ over E_τ.

The 4-torsion above T is always rational and is given by $T' = (1 : 0)$ and $T'' = (0 : 1)$. The 4-torsion above R may not be rational, but is given by $R' = (a : b)$ and $R'' = (-a : b)$.

Remark 3.23. *Similarly to the theta squared model, an elliptic curve can admit a theta twisted model $\widetilde{\theta}(a^2 : b^2)$ without having a theta model $\theta(a : b)$ if $(a : b)$ is not rational. However, it is much easier to recover the original model via $(X : Z) \in \widetilde{\theta}(a^2 : b^2) \mapsto (bX : aZ) \in \theta(a : b)$ if $(a : b) \in \mathbb{P}^1(k)$.*

If (θ'_0, θ'_1) are the dual theta functions, we can twist this basis too:

$$\widetilde{\theta}'_0(z) := \theta'_0(0)\theta'_0(z), \qquad \widetilde{\theta}'_1(z) := \theta'_1(0)\theta'_1(z).$$

It appears there are a lot of similarities between theta squared and theta twisted models. In fact, if we set $u = v$ in Eq. (6), we find:

$$(\widetilde{\theta'}_0^{\tau} : \widetilde{\theta'}_1^{\tau}) = (\widehat{\theta}_0^{\tau/2} + \widehat{\theta}_1^{\tau/2} : \widehat{\theta}_0^{\tau/2} - \widehat{\theta}_1^{\tau/2}), \qquad (\widetilde{\theta}_0^{\tau/2} : \widetilde{\theta}_1^{\tau/2}) = (\breve{\theta'}_0^{\tau} + \breve{\theta'}_1^{\tau} : \breve{\theta'}_0^{\tau} - \breve{\theta'}_1^{\tau}).$$

In the end, the theta twisted coordinates are just the Hadamard dual of the theta squared coordinates, hence why they behave similarly. But note in the above formula that they are

coordinates for different period matrices τ and $\tau/2$, hence they are also quite useful to study 2-isogenies in theta coordinates.

The differential addition and doubling in theta twisted coordinates are given in Algorithms 7 and 8 respectively. They are derived from the ones in theta squared and by applying Eq. (5).

In terms of complexity, Algorithm 7 costs $2\mathbf{M}+2\mathbf{S}+1\mathbf{m}+1\mathbf{m}_0$ and Algorithm 8 costs $4\mathbf{S}+2\mathbf{m}_0$, which is the same as in the squared model.

Algorithm 7: Differential addition in theta twisted coordinates

Input: $[P] = (X_1 : Z_1)$, $[Q] = (X_2 : Z_2)$ and $[P - Q] = (X_0 : Z_0)$
Output: $[P + Q] = (X : Z)$
Data: On $\widetilde{\theta}^\tau(a^2 : b^2)$, $(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2)$

Function `DiffAdd`$([P], [Q], [P - Q])$**:**
- $u \leftarrow X_1 X_2$;
- $v \leftarrow \frac{a^2}{b^2} Z_1 Z_2$;
- $\widetilde{X} \leftarrow X_0 + Z_0$;
- $\widetilde{Z} \leftarrow X_0 - Z_0$;
- $w \leftarrow (u + v)^2$;
- $t \leftarrow \frac{\widetilde{X}}{\widetilde{Z}}(u - v)^2$;
- $X \leftarrow w + t$;
- $Z \leftarrow w - t$;
- **return** $(X : Z)$;

Algorithm 8: Doubling in theta twisted coordinates

Input: $[P] = (X_1 : Z_1)$ a point
Output: $[2 \cdot P] = (X : Z)$
Data: On $\widetilde{\theta}^\tau(a^2 : b^2)$, $(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2)$

Function `Doubling`$([P])$**:**
- $u \leftarrow X_1^2$;
- $v \leftarrow \frac{a^2}{b^2} Z_1^2$;
- $w \leftarrow (u + v)^2$;
- $t \leftarrow \frac{A'^2}{B'^2}(u - v)^2$;
- $X \leftarrow w + t$;
- $Z \leftarrow w - t$;
- **return** $(X : Z)$;

A summary of the maps between various theta models is available in Fig. 2.

We remark that a similar figure first appeared in [RS17, § 4.3] (in dimension 2), and then in [HR19, Corollary 4, Theorem 5] in dimension 1. The "intermediate Kummer" introduced in these work is our twisted theta model. The explanation for that name will be given in Section 6.2.

4. Conversions between these models

As seen in Section 2, Kummer lines isomorphisms are given by homographies that preserve 2-torsion. This allows us to recover the existing formulas in the literature, notably those of [HR19].

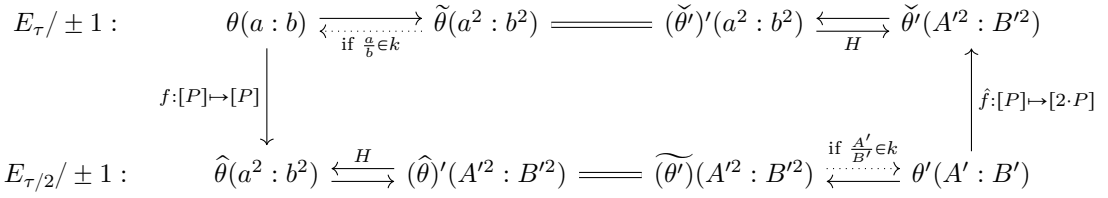


FIGURE 2. Relations among several models pf the Kummer line: the theta θ (Definition 3.12),

Remark 4.1. *There is a less direct way to convert from Montgomery to theta squared and theta twisted, by chaining isomorphisms from Montgomery to Legendre and then from Legendre to theta squared, which can be found in [EH22, § 2.8] for the Montgomery to Legendre maps, and in [GL09, § 6] and [KS20, § 2.6] for the Legendre to theta squared maps.*

With the 2-torsion data, we can then define our isomorphisms:

Proposition 4.2 (Montgomery and theta)**.** *Let $a, b \in k$ and set $(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2)$. Let M and θ be the Kummer line models in Definitions 3.1 and 3.12. There is a morphism φ given by:*

$$\begin{aligned}\varphi : \theta(a:b) &\to M(A'^2 : B'^2)\\ (X:Z) &\mapsto (bX + aZ : aZ - bX).\end{aligned}$$

Conversely, if $A'^2, B'^2 \in k$ and $(a^2 : b^2) = (A'^2 + B'^2 : A'^2 - B'^2)$ with $a, b \in \overline{k}$, the converse of φ is given by:

$$\begin{aligned}\varphi^{-1} : M(A'^2 : B'^2) &\to \theta(a:b)\\ (X:Z) &\mapsto (a(X-Z) : b(X+Z)).\end{aligned}$$

Proof. We are looking for a homography $\varphi : (X : Z) \mapsto (\alpha X + \beta Z : \gamma X + \delta Z)$ such that:

- $\varphi(a:b) = (1:0)$, that is $\gamma a + \delta b = 0$,
- $\varphi(-a:b) = (0:1)$, that is $-\alpha a + \beta b = 0$,
- $\varphi(b:a) = (A'^2 : B'^2)$, that is $(\alpha b + \beta a : \gamma b + \delta a) = (A'^2 : B'^2)$.

The last equation can be reformulated as:

$$(A'^2 : B'^2) = (\alpha b^2 + \beta ab : \gamma b^2 + \delta ab) = (\alpha(b^2 + a^2) : \gamma(b^2 - a^2)).$$

Thus, $(A'^2 : B'^2) = (-\alpha A'^2 : \gamma B'^2)$, i.e. $\alpha = -\gamma$, $\beta = \delta$, and since $\gamma a = -\delta b$, we end up with the expression of φ. We can then check that with this expression $\varphi(-b:a) = (B'^2 : A'^2)$.

For the converse, we give another method which is to check that the 2-torsion is mapped correctly and the point at infinity correspond:

$$\varphi^{-1}(1:0) = (a:b),\ \varphi^{-1}(0:1) = (-a:b),\ \varphi^{-1}(A'^2 : B'^2) = (b:a),\ \varphi^{-1}(B'^2 : A'^2) = (-b:a).$$

□

We can compose these conversion map with the map $M(A'^2 : B'^2) \to M(A'^2 : -B'^2), (X : Z) \mapsto (-X : Z)$, to obtain $\theta(a:b) \to M(A'^2 : -B'^2)$, $(X : Z) \mapsto (X/a + Z/b : X/a - Z/b)$, the Hadamard transform of another twisted variant of theta coordinates: $\theta_0/\theta_0(0), \theta_1/\theta_1(0)$.

Remark 4.3. *In Proposition 4.2, we chose to map $(A'^2 : B'^2)$ and $(-a : b)$ together, but we could have done it differently. Set $(a' : b') = (a + b : a - b)$. Transposing 2-torsion is the same as*

working on the dual theta model, so we apply φ and φ^{-1} to $\theta'(a' : b')$ and then use a Hadamard transform to go back to $\theta(a : b)$:

$$\begin{aligned}\varphi' : \theta(a : b) &\to M(\widetilde{A}^2 : \widetilde{B}^2)\\ (X : Z) &\mapsto (aX - bZ : bX - aZ),\end{aligned}$$

and:

$$\begin{aligned}\varphi'^{-1} : M(\widetilde{A}^2 : \widetilde{B}^2) &\to \theta(a : b)\\ (X : Z) &\mapsto (aX - bZ : bX - aZ).\end{aligned}$$

This time $(\widetilde{A}^2 : \widetilde{B}^2) = (a'^2 + b'^2 : a'^2 - b'^2) = (a^2 + b^2 : 2ab)$, $\varphi' = \varphi \circ H$, $\widetilde{A}^2, \widetilde{B}^2 \in k$ and $a, b \in \overline{k}$.

Remark 4.4. *The conversion formulas in Proposition 4.2 also help to express Montgomery XZ-coordinates via theta functions. Indeed, let $\tau \in \mathbb{H}$ and consider the theta model $\theta^\tau(a : b)$. We write $(X : Z) = (\theta_0^\tau(z) : \theta_1^\tau(z))$ and $(X_M : Z_M) = (bX + aZ : aZ - bX)$ the corresponding Montgomery coordinates. Using Proposition 3.11, with $\alpha = a_1 = a_2$ and $\beta = b_1 = b_2$, one gets:*

$$2\vartheta_2[\alpha,\beta](z;\tau)^2 = \vartheta_2[0,0](0;\tau/2)\vartheta_2[0,\beta](z;\tau/2) + e^{-i\pi\alpha}\vartheta_2[0,1](0;\tau/2)\vartheta_2[0,\beta+1](z;\tau/2).$$

Applying this to $(\alpha,\beta) = (0,1)$ and $(\alpha,\beta) = (1,1)$, one gets the two following formulas:

$$\begin{cases} 2\vartheta_2[0,1](z;\tau)^2 = \vartheta_2[0,0](0;\tau/2)\vartheta_2[0,1](z;\tau/2) + \vartheta_2[0,1](0;\tau/2)\vartheta_2[0,0](z;\tau/2)\\ 2\vartheta_2[1,1](z;\tau)^2 = \vartheta_2[0,0](0;\tau/2)\vartheta_2[0,1](z;\tau/2) - \vartheta_2[0,1](0;\tau/2)\vartheta_2[0,0](z;\tau/2).\end{cases}$$

Hence $(X_M : Z_M) = (aZ + bX : aZ - bX) = (\vartheta_2[0,1](z;\tau)^2 : \vartheta_2[1,1](z;\tau)^2)$ expresses the Montgomery coordinates via theta functions of level 2.

Proposition 4.5 (Montgomery and theta squared)**.** *Let $a, b \in \overline{k}$ with $a^2, b^2 \in k$. Let M and $\hat{\theta}$ be the Montgomery and theta squared models as in Definitions 3.1 and 3.19. There is an isomorphism $\widehat{\varphi}$ given by:*

$$\begin{aligned}\widehat{\varphi} : \widehat{\theta}(a^2 : b^2) &\to M(a^2 : b^2)\\ (X : Z) &\mapsto (a^2X - b^2Z : b^2X - a^2Z).\end{aligned}$$

The converse is:

$$\begin{aligned}\widehat{\varphi}^{-1} : M(a^2 : b^2) &\to \widehat{\theta}(a^2 : b^2)\\ (X : Z) &\mapsto (a^2X - b^2Z : b^2X - a^2Z).\end{aligned}$$

Proof. Similarly to Proposition 4.2, we will determine $\widehat{\varphi} : (X : Z) \mapsto (\alpha X + \beta Z : \gamma X + \delta Z)$ using the 2-torsion. We want:

- $\widehat{\varphi}(a^2 : b^2) = (1 : 0)$, that is $\gamma a^2 + \delta b^2 = 0$,
- $\widehat{\varphi}(1 : 0) = (a^2 : b^2)$, that is $(\alpha : \gamma) = (a^2 : b^2)$,
- $\widehat{\varphi}(0 : 1) = (b^2 : a^2)$, that is $(\beta : \delta) = (b^2 : a^2)$.

From the first two equations, we deduce $\alpha = -\delta$, and because $\beta a^2 = \delta b^2$, $\gamma a^2 = -\delta b^2$, we have:

$$(\alpha X + \beta Z : \gamma X + \delta Z) = (\delta(-a^2X + b^2Z) : \delta(-b^2X + a^2Z)) = (a^2X - b^2Z : b^2X - a^2Z).$$

It follows that $\widehat{\varphi}(b^2 : a^2) = (0 : 1)$.

For the converse, we will again just check that the point at infinity and the 2-torsion are correctly mapped:

$$\widehat{\varphi}^{-1}(1 : 0) = (a^2 : b^2), \quad \widehat{\varphi}^{-1}(0 : 1) = (b^2 : a^2), \quad \widehat{\varphi}^{-1}(a^2 : b^2) = (1 : 0), \quad \widehat{\varphi}^{-1}(b^2 : a^2) = (0 : 1).$$

□

The last conversion between theta twisted and Montgomery models can be derived from Proposition 4.5 thanks to the Hadamard transform:

Proposition 4.6 (Montgomery and theta twisted)**.** *Let $a, b \in \overline{k}$ such that $a^2, b^2 \in k$, and set $(A'^2 : B'^2) = (a^2 + b^2 : a^2 - b^2)$. Let M and $\widetilde{\theta}$ be the Montgomery and twisted theta models as in Definitions 3.1 and 3.22. There is an isomorphism $\widetilde{\varphi}$ given by:*

$$\begin{aligned}\widetilde{\varphi} : \widetilde{\theta}(a^2 : b^2) &\to M(A'^2 : B'^2)\\ (X : Z) &\mapsto (b^2X + a^2Z : a^2Z - b^2X).\end{aligned}$$

The converse is:

$$\begin{aligned}\widetilde{\varphi}^{-1} : M(A'^2 : B'^2) &\to \widetilde{\theta}(a^2 : b^2)\\ (X : Z) &\mapsto (a^2(X - Z) : b^2(X + Z)).\end{aligned}$$

Proof. Because of the isomorphism $H : \widetilde{\theta}(a^2 : b^2) \to \widehat{\theta}(A'^2 : B'^2), (X : Z) \mapsto (X + Z : X - Z)$, we just have to compose $\widehat{\varphi} : \widehat{\theta}(A^2 : B'^2) \to M(A'^2 : B'^2)$ with H to get $\widetilde{\varphi} = \widehat{\varphi} \circ H$ and $\widetilde{\varphi}^{-1} = H^{-1} \circ \widehat{\varphi}^{-1}$. We then have:

$$\widetilde{\varphi}(X : Z) = (A'^2(X + Z) - B'^2(X - Z) : B'^2(X + Z) - A'^2(X - Z)) = (b^2X + a^2Z : a^2Z - b^2X),$$

and:

$$\widetilde{\varphi}^{-1}(X : Z) = (A'^2X - B'^2Z + B'^2X - A'^2Z : A'^2X - B'^2 - B'^2X + A'^2Z) = (a^2(X - Z) : b^2(X + Z)).$$

□

To benefit from faster doubling formulas on the theta squared model while keeping the better differential addition on Montgomery model, one could do conversions, however this approach adds a lot of multiplications. However, there is one last conversion map that is interesting between theta squared and Montgomery models to tackle this issue:

Proposition 4.7. *Let $a, b \in \overline{k}$ such that $a^2, b^2 \in k$. Let $[P_\theta] \in \widehat{\theta}(a^2 : b^2)$ and $[P_M] = \widehat{\varphi}([P_\theta])$ from Proposition 4.5. Finally, let $[R_\theta] = (1 : 0) \in \widehat{\theta}(a^2 : b^2)$ and $[R_M] = (a^2 : b^2) \in M(a^2 : b^2)$ 2-torsion points on their respective models.*

The map $\tau : \widehat{\theta}(a^2 : b^2) \to M(a^2 : b^2), [P_\theta] \mapsto [P_M + R_M]$ is well-defined and given by $(X : Z) \mapsto (X : Z)$. It is a bijection and the converse is $\tau^{-1} : [P_M] \mapsto [P_\theta + R_\theta]$.

Proof. The map is well-defined because R_M is a 2-torsion point, so $[P_M + R_M] = [P_M - R_M]$ and the map $P_\theta \mapsto P_M + R_M$ on the elliptic curves factors through $[-1]$, giving τ. Recall the ramification on each model:

$$[\mathcal{O}_\theta] = (a^2 : b^2)^*, \quad [T_\theta] = (b^2 : a^2), \quad [R_\theta] = (1 : 0), \quad [S_\theta] = [T_\theta + R_\theta] = (0 : 1),$$

$$[\mathcal{O}_M] = (1 : 0)^*, \quad [T_M] = (0 : 1), \quad [R_M] = (a^2 : b^2), \quad [S_M] = [T_M + R_M] = (b^2 : a^2).$$

It is then clear that $(X : Z) \mapsto (X : Z)$ and τ match on the 2-torsion, hence on the whole model. The converse τ^{-1} also matches with $(X : Z) \mapsto (X : Z)$. □

The idea to do the computations on several models up to a 2-torsion point has been developed in [RS24a, § 5] with the hybrid ladder.

The possible conversions between the Montgomery and Legendre model, we give one choice below. Combining this with the other conversion maps allows to obtain the conversion formulas between the theta model variants and the Legendre model.

Proposition 4.8 (Montgomery and Legendre)**.** *If $M(\alpha : 1)$ is a Montgomery model, the ramification is $\mathcal{O} = (1 : 0)^*$, $T = (0 : 1)$, $R = (\alpha : 1)$, $S = (1 : \alpha)$, and so the map $(X : Z) \mapsto (\alpha X : Z)$ gives an isomorphism (defined over the field of definition of α) with the Legendre Kummer line whose ramification is $\mathcal{O} = (1 : 0)^*$, $T = (0 : 1)$, $R = (\lambda : 1)$, $S = (1 : 1)$, and $\lambda = \alpha^2$.*

In particular, combining with Proposition 4.2, given a theta model $\theta(a : b)$ we see that it is isomorphic to the Legendre model with $\lambda = A'^4/B'^4$.

5. Interpretation in terms of Galois representation

Here we will give an interpretation of the models of Section 3 in terms of Galois representation. Let us introduce some notations first.

5.1. **Weil and Tate pairings.** k is as before a perfect field with $\mathrm{char}(k) \neq 2$, and we will consider an elliptic curve E defined over k. Let $n \geqslant 2$ be an integer, prime with $\mathrm{char}(k)$ if it is positive. We will note the n-torsion on E by $E[n]$ and the rational n-torsion $E[n](k)$, that is:

$$E[n] = \{P \in E \mid n \cdot P = \mathcal{O}\} \text{ and } E[n](k) = E[n] \cap E(k).$$

The structure of $E[n]$ is well known (see for instance [Sil86, Cor. III.6.4]):

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

If $P, Q \in E[n]$, one can define their Weil pairing $e_{W,n}(P, Q) \in \mu_n$ where μ_n are the n-th roots of unity, see [Sil86, § III.8]. We will mainly use the following properties:

Proposition 5.1. *$e_{W,n} : E[n] \times E[n] \to \mu_n$ is:*

(1) Bilinear:

$$e_{W,n}(P_1 + P_2, Q) = e_{W,n}(P_1, Q)e_{W,n}(P_2, Q)$$
$$e_{W,n}(P, Q_1 + Q_2) = e_{W,n}(P, Q_1)e_{W,n}(P, Q_2)$$

(2) Alternating:

$$e_{W,n}(P, P) = 1$$

(3) Non-degenerate:

$$(\forall P \in E[n], e_{W,n}(P, Q) = 1) \implies Q = \mathcal{O}$$

(4) Surjective: there are $P, Q \in E[n]$ such that $e_{W,n}(P, Q)$ is a primitive n-th root of unity.

There are many equivalent definitions of the Tate pairing. For our purposes, we will use the following definition (see for instance [Rob23, § 4.4, Eq. (10)]):

Definition 5.2. *Denote by $G_k = \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group of k and assume that there is a rational n-torsion point on E, that is $Q \in E[n](k)$. Let $P \in E(k)$ and $P_0 \in E$ such that $n \cdot P_0 = P$. The Tate pairing is then defined as:*

$$e_{T,n}(P, Q) : G_k \to \mu_n$$
$$\sigma \mapsto e_{W,n}(\sigma(P_0) - P_0, Q)$$

Remark 5.3. *The Tate pairing can be evaluated up to an n-th power because $H^1(G_k, \mu_n) \simeq k^\times/(k^\times)^n$, more details can be found in [Rob23, § 4.4] to switch between the different points of view.*

On a finite field, the Tate pairing can even be reduced to studying only the case $\sigma = \pi_q$ where π_q is the Frobenius map over $\mathbb{F}_q$. This is called the reduced Tate pairing (see [Rob23, § 4.5]), but we won't need it here.

One use of the Tate pairing to have a nice criterion about having a 4-isogeny (see also [Rob23, Ex. 5.9] which use the geometric definition to obtain the following result as an immediate corollary):

Lemma 5.4. *Assume E has a non-trivial rational 2-torsion point $P \in E[2](k)$ and set $P_0 \in E[4]$ such that $2 \cdot P_0 = P$. The following conditions are equivalent:*

(1) $e_{T,2}(P, P)$ is trivial.

(2) For all $\sigma \in G_k$, $\sigma(P_0) = P_0$.
(3) $K = \langle P_0 \rangle$ is a rational cyclic subgroup of $E[4]$ of order 4 (i.e. $\sigma(K) = K$ for all $\sigma \in G_k$).
(4) E has a 4-isogeny which is cyclic and rational.

Moreover, E has a rational cyclic 4-isogeny if and only if there is a rational 4-torsion point $[P_0]$ on the associated Kummer line $\mathcal{K} = E/\{\pm 1\}$.

Proof. Let $\sigma \in G_k$. Since $P \in E[2](k) \subseteq E[2]$, we can consider $Q \in E[2]$ such that $E[2] = \langle P, Q \rangle$. The non-degeneracy of the Weil pairing imposes that $e_{W,2}(P, Q)$ is a primitive root of unity, i.e. $e_{W,2}(P, Q) = -1$.

Because $\sigma(P_0) - P_0 \in E[2]$, we write it as $aP + bQ$ with $a, b \in \mathbb{Z}/2\mathbb{Z}$, then $e_{T,n}(P, P)(\sigma) = (-1)^b$. $e_{T,n}(P, P)$ is trivial if and only if for all $\sigma \in G_k$, $\sigma(P_0) - P_0 \in \langle P \rangle$, and because $P + P_0 = -P_0$:

$$e_{T,n}(P, P) = 1 \iff \forall \sigma \in G_k, \sigma(P_0) = \pm P_0.$$

The rest of the equivalence follows from Lemma 3.3.

□

5.2. **Galois representation and modular curves.** For this section we refer to [Zyw15, § 2, § 3] which gives a modern point of view of Shimura's theory developed in [Shi94].

5.2.1. *Galois representation.* Let E be an elliptic curve defined over k a field with $\mathrm{char}(k) \neq 2$ and $n \geqslant 2$. As stated above, the structure of $E[n]$ is well known. We will fix a basis of $E[n] = \langle P, Q \rangle$ for the rest of this section. G_k acts on points of E coordinate-wise and is compatible with the addition law. Therefore, if $\sigma \in G_k$, $\sigma(E[n]) = E[n]$. So one only needs to know the image of P and Q by σ to get the full image of $E[n]$.

If $\sigma(P) = aP + cQ$ and $\sigma(Q) = bP + dQ$ with $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$, we can set:

$$M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Definition 5.5 (Galois representation)**.** *The following map defines a representation of G_k on $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, known as the Galois representation modulo n:*

$$\begin{array}{rccc} \rho_{E,n} : & G_k & \to & \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ & \sigma & \mapsto & M_\sigma. \end{array}$$

The morphism $\rho_{E,n}(G_k)$ plays a key role in the classification of elliptic curves E, but to explain why we first introduce modular curves.

5.2.2. *Modular curves over $\mathbb{Q}$.* Here we assume that $k = \mathbb{Q}$. Recall that $\mathbb{H}$ is the upper half-plane of $\mathbb{C}$, then $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ via $\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}$ if $\tau \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Let $\Gamma(N)$ be the kernel of the reduction modulo N map $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, that is the set of matrices of determinant 1 which reduce to the identity modulo N. The quotient $Y(N) = \Gamma(N)\backslash\mathbb{H}$ is a Riemann surface which can be compactified in a smooth compact Riemann surface denoted $X(N)$. If $\tau \in \mathbb{H}$, every meromorphic function f on $X(N)$ can be written in q-expansion ($q^{1/N} = e^{2i\pi\tau/N}$), that is there is a sequence of complex numbers $(c_n)_{n \geqslant n_0}$ with $n_0 \in \mathbb{Z}$ such that:

$$f(\tau) = \sum_{n \geqslant n_0} c_n q^{n/N}.$$

We denote by $\mathcal{F}_N$ the field of meromorphic functions over $X(N)$ that has q-expansion coefficients in $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2i\pi/N}$. Its elements are called the modular functions of level N. If $j = j(\tau)$ is the modular j-invariant, then $\mathcal{F}_1 = \mathbb{Q}(j)$. According to [Zyw15, Prop. 3.1], $\mathcal{F}_N$ is a Galois extension of $\mathbb{Q}(j)$ with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

For G a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$ and such that $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, we can then define $\mathcal{F}_N^G$ the subfield of $\mathcal{F}_N$ fixed by the action of G seen as a part of $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$. By the assumption on $\det(G)$, $\mathbb{Q}$ is algebraically closed in $\mathcal{F}_N^G$ and $X_G = G\backslash X(N)$ is well-defined as the smooth projective curve over $\mathbb{Q}$ with function field $\mathcal{F}_N^G$. Because of the inclusion $\mathbb{Q}(j) \subseteq \mathcal{F}_N^G$, there is also a non-constant morphism of degree $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$:

$$\pi_G : X_G \to \mathbb{P}^1(\mathbb{Q})$$

The core of the classification of models relies on this theorem from [Zyw15, Prop. 3.3]:

Theorem 5.6 (Modular interpretation)**.** *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $-I$ and satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, and let E be an elliptic curve defined over $\mathbb{Q}$ such that its j-invariant is different from 0, 1728. Then $\rho_{E,N}(G_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G if and only if $j_E \in \pi_G(X_G(\mathbb{Q}))$.*

Remark 5.7. *Theorem 5.6 can be generalized to more general fields, but requires developing the theory of modular curves over a generic field k. For completeness, this is done in Appendix B.*

We will introduce some notations for specific curves, we have already seen $X(N)$. Let $T_+(N)$ be the set of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $X_0(N) = X_{T_+(N)}$. Set also $T_-(N)$ be the set of lower triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $D(N) = T_+(N) \cap T_-(N)$ the diagonal matrices. Let $T_1(N) = \{\left(\begin{smallmatrix}1 & * \\ 0 & *\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})\}$ and $X_1(N) = X_{T_1(N)}$. Finally, if $M \geqslant 1$ is another integer, we set:

$$H(M, MN) = \{g \in T_+(MN) \mid g \equiv I \bmod M\} \text{ and } X(M, MN) = X_{H(M,MN)}.$$

Definition 5.8. *Γ is said to be a congruence subgroup if there exists $N \geqslant 1$ such that $\Gamma(N) \subset \Gamma$.*

Modular curves over $\mathbb{C}$ can be seen as the compactification of $Y(\Gamma) = \Gamma\backslash\mathbb{H}$, i.e. $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$ where $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ is the completed upper half plane, as done in [DS05]. Congruence subgroups then help to describe complex points of such curves. The following result can be computed with a computer algebra software like Magma and is tabulated in LMFDB.

Proposition 5.9. *When $N = 4$, the 19 possible images of congruence subgroups in $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ have been represented in Fig. 6 in Appendix C.*

Because of Theorem 5.6, some of these subgroups give families of elliptic curves with Kummer lines we would like to classify, as we will see in the next section.

5.3. **Classification of models.** Here we give description of the models of Section 3 in terms of modular curves. k is a field with $\mathrm{char}(k) \neq 2$.

It is an open question whether all the efficient families of curves in cryptography are associated to congruence subgroups, especially those in Fig. 6. In Section 8, we will come back to this classification where we will want both good arithmetic, such as Montgomery or theta coordinates, and also good torsion properties, so we may need to intersect some of these families.

An example of such classification is Legendre curves:

Proposition 5.10. *Let E be an elliptic curve over k with j-invariant different from 0, 1728. Then E is a Legendre curve if and only if it has full rational 2-torsion or equivalently if $j \in \pi_G(X(2))$.*

5.3.1. *Montgomery curves.* To describe Montgomery curves, we will first need a criterion shown in [OKS00, Prop. 1]:

Lemma 5.11. *Let E be an elliptic curve over k and written in Weierstrass form $y^2 = h(x)$. Then E can be put in Montgomery form if and only if there exists $\alpha \in k$ such that $h(\alpha) = 0$ and $h'(\alpha)$ is a square different from zero.*

The first condition means there is a non-trivial rational 2-torsion point, which is clear with the equation of a Montgomery curve. We will explicit the second condition using the Tate pairing:

Proposition 5.12. *Let E be an elliptic curve over k with j-invariant different from 0, 1728. Then E is a Montgomery curve if and only if it admits a rational cyclic subgroup K of order 4. Every Montgomery curve is described by a rational point $x \in X_0(4)(k)$ and vice-versa.*

Proof. We will write $E : y^2 = h(x)$ in Weierstrass form.

First assume E is a Montgomery curve. By Lemma 5.11, $P = (\alpha, 0)$ is a rational 2-torsion point in Weierstrass coordinates with $\alpha \in k$ and such that $h'(\alpha) \in (k^\times)^2$. Now recall Remark 5.3, the Tate pairing $e_{T,2}(P, P) \in H^1(G, \mu_2)$ is trivial if and only if it is a square. But if P is a rational 2-torsion point, thanks to some computation done in [Rob23, Ex. 5.8.1], we have $e_{T,2}(P, P) \equiv h'(\alpha)$, which is a square. So $e_{T,2}(P, P)$ is trivial and using Lemma 5.4 we have a rational subgroup $K \simeq \mathbb{Z}/4\mathbb{Z}$.

Conversely, assume that E has such a subgroup K, and denote its generator by $P_0 \in E[4]$. By Lemma 5.4, $\sigma(P_0) = \pm P_0$ for all $\sigma \in G_k$ because K is rational. Setting $P = 2 \cdot P_0$, we then have $\sigma(P) = P$, that is P is a non-trivial rational 2-torsion point on E. We write it $(\alpha, 0)$ in Weierstrass coordinates with $\alpha \in k$. Again, by Lemma 5.4, $e_{T,2}(P, P)$ is trivial, i.e. it is a square. This implies that $h'(\alpha)$ is also a square because of $e_{T,2}(P, P) \equiv h'(\alpha)$, and we conclude with Lemma 5.11.

If we set the basis of $E[4] = \langle P_0, Q\rangle$ where $K = \langle P_0\rangle$, then for all $\sigma \in G_k$, $\sigma(P_0) = \pm P_0$. Therefore, $\rho_{E,4}(\sigma)$ is upper triangular, i.e. $\rho_{E,4}(G_k) \subset T_+(4)$. Thanks to Theorem 5.6 applied to $G = T_+(4)$, E being in Montgomery form is equivalent to its j-invariant j_E being in $\pi_G(X_0(4)(k))$. □

Remark 5.13. *In terms of congruence subgroups, we are on the curve associated to $T_+(4) = \left\langle \Gamma_0(4), \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\rangle$ which is group* 4.6.0.c.1 *in Fig. 6.*

5.3.2. *Theta and theta squared models.* As seen before, rational torsion is really helpful to determine on which modular curve we are. In addition to that, as shown in Lemma 5.4 the Tate pairing also gives useful information on the Galois representation. We will consider the theta model $\theta(a : b)$ and the theta squared model $\widehat{\theta}(a^2 : b^2)$. These two models have full 2-torsion, and some rational 4-torsion points, as already seen in Propositions 3.17 and 3.21.

We have the following proposition:

Proposition 5.14. *Let E be an elliptic curve over k, with j-invariant j_E different from 0, 1728.*

1. *E admits a theta model if and only if it has two rational subgroups $K_1, K_2 \simeq \mathbb{Z}/4\mathbb{Z}$ with trivial intersection. Every theta model can then be described by a rational point $j_E \in \pi_{D(4)}(X_{D(4)}(k))$ and vice-versa.*
2. *E admits a theta squared model if and only if $E[2](k) = E[2]$ and E has a rational subgroup $K \simeq \mathbb{Z}/4\mathbb{Z}$. Every theta squared model can then be described by a rational point $j_E \in \pi_{H(2,4)}(X(2, 4)(k))$ and vice-versa.*

Proof. If E admits a theta model $\theta(a : b)$, we have two rational independent 4-torsion points on the Kummer line which are $(1 : 0)$ and $(1 : 1)$ according to Proposition 3.17. They can be lifted to points $P_0, Q_0 \in E[4]$ which generates two rational cyclic kernels $K_1 = \langle P_0\rangle$ and $K_2 = \langle Q_0\rangle$ thanks to Lemma 5.4 (the points P_0, Q_0 may not be rational however). The kernels now have trivial intersection because the torsion points are independent, they do not lie above the same 2-torsion point. We also recover that E has full rational 2-torsion generated by $P = 2 \cdot P_0$ and $Q = 2 \cdot Q_0$, which are rational because the kernels are too.

If E only has a theta squared model, we still have the full rational 2-torsion by lifting $(b^2 : a^2)$ and $(1 : 0)$ to E. The points are rational on the curve too because they are of order 2. We then

set $K = \langle P_0 \rangle$ where P_0 is a lift of the rational 4-torsion point $(1 : 1)$ on the Kummer line. Then K is rational because of Lemma 5.4.

Conversely, assume that E has a rational kernel $K \simeq \mathbb{Z}/4\mathbb{Z}$ and full rational 2-torsion. Then E can be put in Montgomery form using Proposition 5.12:

$$E : By^2 = x(x^2 + \mathcal{A}x + 1).$$

Moreover, non-trivial 2-torsion points on a Montgomery curve are given by $y = 0$, i.e. $x = 0$ or $x^2 + \mathcal{A}x + 1 = 0$. Because the 2-torsion is rational, $x^2 + \mathcal{A}x + 1$ is split, and we have $\alpha \in k^\times$ such that:

$$E : By^2 = x(x - \alpha)(x - \alpha^{-1}).$$

From that point, we know that the Kummer line associated to E is $M(\alpha : 1)$, as defined in Section 3. This model is isomorphic to $\widehat{\theta}(\alpha : 1)$ via Proposition 4.5, hence E admits a theta squared model.

If we have the stronger hypothesis that E has two rational kernels $K_1, K_2 \simeq \mathbb{Z}/4\mathbb{Z}$ with trivial intersection, we write $K_1 = \langle P_0 \rangle$ and $K_2 = \langle Q_0 \rangle$, $P = 2 \cdot P_0$ and $Q = 2 \cdot Q_0$. Since for all $\sigma \in G_k$, $\sigma(K_i) = K_i$, when looking at the order we must have $\sigma(P) = P$ and $\sigma(Q) = Q$, so these points are rational, and because they are distinct they are generators of the 2-torsion. We then are in the previous case with $\alpha \in k^\times$ such that:

$$E : By^2 = x(x - \alpha)(x - \alpha^{-1}) = h(x).$$

We would like to prove that $\frac{\alpha+1}{\alpha-1}$ is a square. Up to transposing P and Q, assume that $Q = (\alpha, 0)$. Because K_2 is cyclic rational of degree 4, $e_{T,2}(Q, Q)$ is trivial thanks to Lemma 5.4. With the computation done in [Rob23, Ex. 5.8.1], we know that $e_{T,2}(Q, Q) \equiv h'(\alpha)$ is a square.

Because $h'(x) = 3x^2 + 2\mathcal{A}x + 1$ where $\mathcal{A} = -\alpha - \alpha^{-1}$, when evaluated in α, we get:

$$h'(\alpha) = \alpha^2 - 1 = \frac{\alpha + 1}{\alpha - 1}(\alpha - 1)^2.$$

Thus, $\beta = \sqrt{\frac{\alpha+1}{\alpha-1}} \in k$, and $M(\alpha : 1)$ is isomorphic to $\theta(\beta : 1)$ thanks to Proposition 4.2, so E admits a theta model.

The interpretation in terms of modular curves is straight-forward:

- If E has a theta model, denote $K_1 = \langle P_0 \rangle$ and $K_2 = \langle Q_0 \rangle$ with $P_0, Q_0 \in E[4]$ the two rational kernels. We have $E[4] = \langle P_0, Q_0 \rangle$. Because both K_1 and K_2 are rational, for all $\sigma \in G_k$, $\sigma(P_0) = \pm P_0$ and $\sigma(Q_0) = \pm Q_0$, so $\rho_{E,4}(G_k) \subset D(4)$, which is equivalent to $j_E \in \pi_{D(4)}(X_{D(4)}(k))$ with Theorem 5.6.
- If E has a theta squared model, let $K = \langle P_0 \rangle$ with $P_0 \in E[4]$ be the rational kernel. Set $P = 2 \cdot P_0 \in E[2](k)$, write $E[2](k) = \langle P, Q \rangle$ and take $Q_0 \in E[4]$ such that $2 \cdot Q_0 = Q$ and $E[4] = \langle P_0, Q_0 \rangle$. Then for all $\sigma \in G_k$, $\sigma(P_0) = \pm P_0$, $\sigma(P) = P$ and $\sigma(Q) = Q$, so $\rho_{E,2}(\sigma) = I$ and $\rho_{E,4}(\sigma) \in T_+(4)$, i.e. $\rho_{E,4}(G_k) \subset H(2, 4)$. This is again equivalent to $j_E \in \pi_{H(2,4)}(X(2, 4)(k))$ with Theorem 5.6.

□

We remark that Proposition 5.14, for the theta model, is a particular case of a general result from Igusa that states that the theta constants of level n are modular forms for the subgroup $\Gamma(n, 2n) \subset \mathrm{Sp}_{2g}(\mathbb{Z})$. Indeed, in the particular case when $n = 2$ and $g = 1$, we have $\Gamma(2, 4)$ which is conjugated to $D(4) = T_+(4) \cap T_-(4)$.

Remark 5.15. *By Propositions 5.12 and 5.14, we see that the theta squared (or equivalently the theta twisted) model correspond to a Montgomery model with full rational 2-torsion (i.e. in Montgomery ∩ Legendre). This can be seen directly from the conversion formulas from Section 4.*

6. Interpretation in terms of the theta group

In this section, we reinterpret the results of Section 5 in term of the theta group.

6.1. **The theta group and the type of a point.** We refer to [Mum66] for the definition of the theta group of an abelian variety, and to [RS24a, § 2.2; RS24b, § 5.1, § 5.2] for more details on Mumford's theta group of an elliptic curve.

We briefly recall the definitions we'll need here, we'll only need to work with theta groups of level $n = 2$. Let $D = 2(0_E)$, then theta group $G(D)$ is the group of functions g_P on $k(E)$ such that $P \in E[2]$, and $\operatorname{div} g_P = t_{-P}^* D - D$. The addition law of $G(D)$ is given by $(g_P \cdot g_Q)(R) = g_P(R)g_Q(R-P)$, it is a function with divisor $t_{-P-Q}^* D - D$. We have a canonical faithful action of $G(D)$ on $\Gamma(D)$ given by $(g_P \cdot s)(R) = g_P(R)s(R-P)$.

If $P \in E[2]$, we have the translation map $R \mapsto R + P$ which induces a linear map on $\Gamma(D) = \langle X, Z\rangle$, hence an homography γ_P on the Kummer line $E/\pm 1$. We can represent the homography γ_P as an element of PGL_2. A choice of theta group element g_P is then equivalent to the choice of a matrix $M_P \in \mathrm{GL}_2$ above γ_P.

Since P is a point of 2-torsion, we have $M_P^2 = \lambda_P$. If P is rational and we take $M_P \in \mathrm{GL}_2(k)$, then changing M_P by a scalar changes λ_P by a square; we see that the class of $\lambda_P \in k^*/k^{*,2}$ depends only on P, not on G_P, and is called the type of P (see [RS24a, Definition 2]). Since the type of P can be recovered from the equation $g_P^2 = \lambda_P$ for a rational element g_P in the theta group above P, we see that it does not depend on the choice of basis of $\Gamma(D)$.

Theorem 6.1. *Assume that $P \neq 0_E \in E[2](k)$. The type $\lambda_P \in k^*/k^{*,2}$ of P is also the class of the non reduced self Tate pairing $e_{T,2}(P,P) \in k^*/k^{*,2}$. If we take a representative λ_P of the type, then there is a model of the Kummer line $E/\pm 1$ where 0_E is sent to ∞ P to 0_E, and the other two torsion points are given by $(\alpha : 1), (1/(\lambda_P\alpha) : 1)$ (where $\alpha \in \overline{k}$).*

Conversely, if we have a model of the Kummer line $E/\pm 1$ such that the ramification is stable by $(X : Z) \mapsto (Z : \lambda_P X)$ with 0_E sent to P, then P is of type λ_P. In particular, P is of type λ_P if and only if there is a rational Weierstrass equation of E of the form $By^2 = x(x^2 + Ax + 1/\lambda_P)$ with $x(P) = 0$.

Proof. Recall that the type of P is given by $g_P^2 = \lambda_P$ where g_P is any theta group element above P. By the definition of the theta group law, we have $\lambda_P = e_{T,2}(P,P)$ (see [RS24a, p. 8]).

Now looking at the matrix M_P given by the action of g_P on $\Gamma(2)$, we also have $M_P^2 = \lambda_P$. This is the minimal polynomial of M_P because M_P cannot be a diagonal matrix since $P \neq 0_E$. So we can find a basis of sections of D such that $M_P = \left(\begin{smallmatrix} 0 & \lambda_P \\ 1 & 0 \end{smallmatrix}\right)$.

If $0_E = (a : b)$ with this basis, then $P = \gamma_P \cdot 0_E = (b : \lambda_P a)$. Then change of basis $(X, Z) \mapsto (X - \frac{b}{\lambda_P a} Z : Z - \frac{b}{a} X)$ sends 0_E to $(1 : 0)$ and P to $(0 : 1)$, while M_P is invariant by the corresponding conjugation. It follows that if one other two-torsion as coordinates $T_2 = (\alpha : 1)$, then $T_3 = \gamma_P \cdot T_2 = (1 : \lambda_P\alpha)$.

Conversely, an homography of order 2 that stabilizes the ramification and sends 0_E to P has to be the one induced by the translation by P, and by our assumptions we can take $M_P = \left(\begin{smallmatrix} 0 & \lambda_P \\ 1 & 0 \end{smallmatrix}\right)$. □

Remark 6.2. *Pick up g_P such that $g_P^2 = \lambda_P$. One way to find a basis $(X, Z) \in \Gamma(D)$ so that the ramification is as Theorem 6.1 is as follows. First let $Z_1 \in \Gamma((0_E))$ be a section, and let $Z = Z_1^2$. Then we let $X = g_P \cdot Z$. Since $Z(0_E) = 0$, we have $0_E = (1 : 0)$, and $P = (0 : 1)$. If T_2 is another two-torsion point, $T_3 = g_P \cdot T_2$.*

Theorem 6.1 explains how the structure of the ramification on the Kummer line, the action of the theta group on $\Gamma(D)$, and the Tate self-pairing are all linked together. A particularly

important case is when the type of P is a square, in which case we say that P is of *Montgomery type*.

Corollary 6.3. *If $P \in E[2](k)$ is a rational two torsion point, the following conditions are equivalent:*

1. *the type of P is a square;*
2. *E has a Montgomery model $By^2 = x(x^2 + Ax + 1)$ with $x(P) = 0$;*
3. *there is a model of the Kummer line of E which has its ramification invariant by $(X : Z) \mapsto (Z : X)$ with 0_E sent to P*
4. *there is a model of the Kummer line of E such that $0_E = (1 : 0)$, $P = (0 : 1)$, and the other points of 2-torsion are given by $T_2 = (\alpha : 1), T_3 = (1 : \alpha)$*
5. *there is a model of the Kummer line of E which has its ramification invariant by $(X : Z) \mapsto (-X : Z)$ with 0_E sent to P*
6. *there is a model of the Kummer line of E such that $0_E = (1 : 1)$, $P = (-1 : 1)$, and the other points of 2-torsion are given by $T_2 = (\beta : 1), T_3 = (-\beta : 1)$*
7. *there exists a rational element $g_P \in G(D)$ such that $g_P^2 = 1$ (equivalently: the two symmetric elements $\pm g_P \in G(D)$ above P are rational);*
8. *the reduced Tate self pairing is trivial: $e_{T,2}(P, P) = 1$;*
9. *there exists a rational cyclic subgroup K of degree 4 containing P;*
10. *there exists a point of 4-torsion P' above P which is rational on the Kummer line (i.e. such that if $E : By^2 = x^3+a_2x^2+a_4x+a_6$, $x(P')$ is rational). Equivalently, $\sigma(P') = \pm P'$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$.*
11. *$E/\langle P\rangle$ has its full 2-torsion rational (i.e. admits a rational Legendre model);*
12. *The isogeny $\varphi_P : E \to E/\langle P\rangle$ can be extended to a rational cyclic isogeny of degree 4 (automatically in two different ways).*

Proof. The first eight equivalences are consequences of the definition of the type of P and of Theorem 6.1: if P has type a square, we can take $\lambda_P = 1$ and $M_P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then the Hadamard change of basis $(X, Z) \mapsto (X + Z, X - Z)$ shows that we can also take $M_P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

The link between the Tate pairing and having a rational cyclic group is given by Lemma 5.4, but we can use the above result to give an alternative proof: if P is a 2-torsion point, then an element $g_P \in G(D)$ such that $g_P^2 = 1$ is completely determined by a choice of 4-torsion point P' above P (more precisely, the choice of P' determines a symmetric element g_P, but for $n = 2$, g_P is symmetric if and only if $g_P^2 = 1$, see [RS24a]). If $P'' = P' + T$ is a different choice of 4-torsion point, so that $T \in E[2]$, the element induced by P'' is the same one as the one by P' if and only if $e_{W,2}(T, P) = 1$. It follows that we can find a rational g_P if and only if we can find P' such that $\sigma(P') = \pm P'$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Yet another alternative proof is to use descent theory: we can find a rational symmetric g_P if and only if $2(0_E)$ descends to a symmetric divisor on $E' = E/\langle P\rangle$, i.e. there is a rational divisor D' linearly equivalent to $D = 2(0_E)$ of the form $\varphi_P^*((T'))$ for $T' \in E'[2]$ where $\varphi_P : E \to E'$ is the 2-isogeny. But then $D' = (P') + (P' + P)$, for some point of 4-torsion P', and since D' is rational we recover that $\sigma(P') = \pm P'$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

We already saw that (9) is equivalent to (10).

For the last two statements, notice that on $E' = E/\langle P\rangle$ there is always a rational 2-torsion point T_1' giving the dual isogeny $E' \to E$. The isogeny φ_P can be extended to a cyclic isogeny of degree 4 if and only if there is another rational point of 2-torsion T_2' on E', but then $T_3' = T_1' + T_2'$ is rational too, so this is equivalent to E' having full rational 2-torsion. □

If $k = \mathbb{F}_q$ is a finite field, then $\mathbb{F}_q^*/\mathbb{F}_q^{*,2}$ is of cardinal two. Pick up a $\lambda_- \in \mathbb{F}_q^*$ that is not a square, for instance if $q \equiv 3 \mod 4$ we will pick $\lambda_- = -1$. Then if $P \in E[2](\mathbb{F}_q)$, it is either of

type a square (i.e. of Montgomery type) in which case we can choose $\lambda_P = 1$, or not a square, in which case we can choose $\lambda_P = \lambda_-$ and we say that P is of anti-Montgomery type. The pendant of Corollary 6.3 is:

Corollary 6.4. *If $P \in E[2](k)$ is a rational two torsion point, the following conditions are equivalent:*

(1) the type of P is not a square;
(2) E has a "anti-Montgomery" model $By^2 = x(x^2 + Ax + 1/\lambda_-)$ with $x(P) = 0$;
(3) there is a model of the Kummer line of E which has its ramification invariant by $(X : Z) \mapsto (\lambda_- Z : X)$ with 0_E sent to P
(4) there is a model of the Kummer line of E such that $0_E = (1 : 0)$, $P = (0 : 1)$, and the other points of 2-torsion are given by $T_2 = (\alpha : 1), T_3 = (\lambda_- : \alpha)$
(5) there does not exist a rational element $g_P \in G(D)$ such that $g_P^2 = 1$ (equivalently: the two symmetric elements $\pm g_P \in G(D)$ above P are not rational);
(6) the reduced Tate self pairing is not trivial: $e_{T,2}(P, P) = -1$;
(7) there does not exists a rational cyclic subgroup K of degree 4 containing P;
(8) $E/\langle P\rangle$ has only one rational point of 2-torsion;
(9) The isogeny $\varphi_P : E \to E/\langle P\rangle$ cannot be extended to a rational cyclic isogeny of degree 4.

The results of Corollaries 6.3 and 6.4 allow to recover the discussion on the Montgomery and Montgomery$^-$ models of [CD20].

6.2. **Twisted theta models.** We continue our reinterpretation of the results of Section 5 in terms of the theta group.

Let, E/k be an elliptic curve, and denote, as above, $D = 2(0_E)$. By definition ([Mum66]), a symmetric theta structure on (E, D) is a (symmetric) isomorphism between the theta group $G(D)$ and the Heisenberg group $H(2)$ of level 2. In this very particular case, an isomorphism between $G(D)$ and $H(2)$ has to be symmetric. By [Mum66], $G(D)$ is always isomorphic to $H(2)$ over $\overline{k}$, and picking up an isomorphism amount to:

- Choose a basis T_1, T_2 of $E[2]$
- Choose two symmetric elements $g_1, g_2 \in G(D)$ above T_1, T_2. (We recall that in our case g is symmetric if and only if $g^2 = 1$).

In which case, the canonical basis of theta functions θ_0, θ_1 can be defined as follows: we pick up θ_0 as a generator of $\Gamma(D)$ invariant under the action of g_1, and $\theta_1 = g_2 \cdot \theta_0$.

It follows:

Lemma 6.5. *E admits a rational symmetric theta structure of level 2 if and only if there exists two rational points $T_1, T_2 \in E[2](k)$ that are both of Montgomery type.*

In particular, by Corollary 6.3, we recover the first part of Proposition 5.14. In fact, we can refine it: if E has such a rational theta structure, let $T_1, T_2, g_1, g_2 \in G(D)$ be rational elements given by the rational isomorphism of $G(D)$ with $H(2)$. Then $T_1 + T_2$ is certainly rational, $g_1 g_2$ is above $T_1 + T_2$, and we have $(g_1 g_2)^2 = -1$, hence $T_1 + T_2$ is of type -1. It follows that $T_1 + T_2$ is also of Montgomery type if and only if -1 is a square in k (and then we will denote by i a square root).

Corollary 6.6. *Assume that E/k has a rational symmetric theta model of level 2. Then if -1 is a square in k, E/k has 24 different theta models; otherwise it has 8.*

(We implicitely count theta models with multiplicities if E has non trivial automorphisms.)

Proof. If -1 is a square, all three points of 2-torsion are of Montgomery type. The choice of a theta model amount to choosing two points (T_1, T_2) out ofh the three (where the ordering count),

for a total of 6 choices, and then for each T_i to fix a choice of symmetric element $\pm g_1, \pm g_2$, for a total of 4 choices. This gives 24 possible choices. If -1 is not a square, only two points are of Montgomery type, and now we have $2 \times 4 = 8$ choices. □

Example 6.7 (The number of rational Montgomery models)**.** *More generally, if we have two rational two torsion points T_1, T_2, of type λ_1, λ_2, then $T_1 + T_2$ is rational of type $-\lambda_1\lambda_2$.*

Also, if T_1 is of type λ_1 and we select $g_1 \in G(D)$ such that $g_1^2 = \lambda_1$ to construct the (X, Z) coordinates as in Remark 6.2, which gives the equation $E : By^2 = x^3 + Ax^2 + x/\lambda_1$, then picking up $-g_1$ instead changes X to $-X$, and gives the equation $E : -By^2 = x^3 - Ax^2 + x/\lambda_1$

It follows that, if $k = \mathbb{F}_q$ is a finite field, and -1 is a square in $\mathbb{F}_q$:

- *If T_1, T_2 are of Montgomery type, $T_1 + T_2$ too, and there are 6 rational Montgomery models.*
- *If T_1 is of Montgomery type and T_2 of anti-Montgomery type, then $T_1 + T_2$ if of anti-Montgomery type, and there are 2 rational Montgomery models and 4 rational Montgomery$^-$ models.*
- *If T_1, T_2 are of anti-Montgomery type, then $T_1 + T_2$ if of Montgomery type, and there are 2 rational Montgomery models and 4 rational Montgomery$^-$ models.*

And if -1 is not a square in $\mathbb{F}_q$:

- *If T_1, T_2 are of Montgomery type, $T_1 + T_2$ is of anti-Montgomery type, and there are 4 rational Montgomery models and 2 rational Montgomery$^-$ models.*
- *If T_1 is of Montgomery type and T_2 of anti-Montgomery type, then $T_1 + T_2$ if of Montgomery type, and there are 4 rational Montgomery models and 2 rational Montgomery$^-$ models.*
- *If T_1, T_2 are of anti-Montgomery type, then $T_1 + T_2$ if of anti-Montgomery type, and there are 6 rational Montgomery$^-$ models.*

Now, if $G(D)$ is not isomorphic to $H(2)$ over k, we know that it is an (étale) twist of it (since it is isomorphic over the separable closure). Picking up such an automorphism γ, we see that for each $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we obtain a (symmetric) automorphism $\xi(\sigma) = \gamma^\sigma \gamma^{-1}$ of $H(2)$, and $\sigma \to \xi(\sigma)$ form a cocyle.

Assume, for the sake of simplicity, that -1 is a square in k, so that the symmetric automorphisms of $H(2)$ are rational, and the coboundaries are trivial. We can identify these automorphisms with $\Gamma/\Gamma(2,4)$ where $\Gamma = \mathrm{Sp}_2(\mathbb{Z})$ and, in our special case, and $\Gamma(2,4) = \Gamma^0(4) \cap \Gamma_0(4)$ (see the discussion after Proposition 5.14).

In particular, $\xi(\sigma)$ explains how σ acts on the canonical theta basis (θ_0, θ_1) given by γ: unless $\xi(\sigma) = \mathrm{Id}$ for all σ, this basis is not rational in general. Pick a subgroup G such that $\Gamma(2,4) \subset G \subset \Gamma$. We say that $G(D)$ is of type G if $\xi(\sigma) \in G$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$. In that case, we can try to build a basis θ_0', θ_1' as a linear combination of θ_0, θ_1 such that θ_0', θ_1' is invariant under the action of the automorphisms in G. It follows that we obtain a rational basis of sections on E, and we call (θ_0', θ_1') a twisted theta model. We stress that in a "twisted theta model", we still describe a model of E (or its Kummer line), rather than a twist E' of E. Here the twist refer instead to the fact that for these models the theta group is a twist of the standard Heisenberg group.

Example 6.8 (Automorphisms of the theta group)**.** *We list all 24 automorphisms of $H(2)$, for each give a representative in $\Gamma/\Gamma(2,4)$, and how it acts on the theta coordinates θ_0, θ_1 (hence on the theta constants). We give six blocks of four automorphisms. Each block correspond to a choice of a representative of $\Gamma/\Gamma(2)$ (which is of cardinal $3! = 6$), and where the first block corresponds to $\gamma = \mathrm{Id}$. Then for these choices of $\gamma \in \Gamma/\Gamma(2)$, we list 4 possible lifts of γ to*

$\Gamma/\Gamma(2,4)$. *More precisely, once we have picked up one possible lift γ', we then give the other ones via the action of the first block of automorphisms.*

The change of coordinate follows from the explicit construction of θ_0, θ_1 once g_1, g_2 has been chosen. Analytically, it also follows from the theta transformation formula [Igu72; Mum83] (which is more precise since it also keep track of the theta constants as modular forms*).*

(1) $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0,\theta_1)$.
(2) $\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_1,\theta_0)$. *This amounts to keeping g_2 and changing g_1 to $-g_1$.*
(3) $\left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0,-\theta_1)$. *This amounts to keeping g_1 and changing g_2 to $-g_2$.*
(4) $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_1,-\theta_0)$. *This amounts to changing g_1 to $-g_1$ and changing g_2 to $-g_2$.*

(5) $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+\theta_1,\theta_0-\theta_1)$. *This amounts to permuting g_1, g_2.*
(6) $\left(\begin{smallmatrix}2&1\\-1&0\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0-\theta_1,\theta_0+\theta_1)$.
(7) $\left(\begin{smallmatrix}0&1\\-1&2\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+\theta_1,-\theta_0+\theta_1)$.
(8) $\left(\begin{smallmatrix}2&-1\\1&2\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(-\theta_0+\theta_1,\theta_0+\theta_1)$.

(9) $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0,i\theta_1)$. *This amounts to keeping g_1 and changing g_2 to ig_2g_1.*
(10) $\left(\begin{smallmatrix}1&2\\1&-1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(i\theta_1,\theta_0)$.
(11) $\left(\begin{smallmatrix}1&0\\-1&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0,-i\theta_1)$.
(12) $\left(\begin{smallmatrix}-1&2\\1&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(i\theta_1,-\theta_0)$.

(13) $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(i\theta_0+\theta_1,\theta_0+i\theta_1)$. *This amounts to changing g_1 to ig_1g_2 and keeping g_2, i.e., applying (5) then (9) then (5).*
(14) $\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+i\theta_1,i\theta_0+\theta_1)$.
(15) $\left(\begin{smallmatrix}1&1\\2&-1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(i\theta_0+\theta_1,-\theta_0-i\theta_1)$.
(16) $\left(\begin{smallmatrix}1&-1\\2&-1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+i\theta_1,-i\theta_0-\theta_1)$.

(17) $\left(\begin{smallmatrix}1&-1\\1&0\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+i\theta_1,\theta_0-i\theta_1)$. *This amounts to sending g_1 to ig_2g_1 and g_2 to g_1, i.e., applying (9) then (5).*
(18) $\left(\begin{smallmatrix}1&1\\-1&0\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0-i\theta_1,\theta_0+i\theta_1)$.
(19) $\left(\begin{smallmatrix}-1&1\\1&2\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+i\theta_1,-\theta_0+i\theta_1)$.
(20) $\left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0-i\theta_1,-\theta_0-i\theta_1)$.

(21) $\left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+\theta_1,i\theta_0-i\theta_1)$. *This amounts to changing g_1 to g_2 and g_2 to ig_1g_2, i.e., applying (5) then (9).*
(22) $\left(\begin{smallmatrix}2&-1\\-1&-1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(i\theta_0-i\theta_1,\theta_0+\theta_1)$.
(23) $\left(\begin{smallmatrix}0&1\\-1&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(\theta_0+\theta_1,-i\theta_0+i\theta_1)$.
(24) $\left(\begin{smallmatrix}2&-1\\-1&1\end{smallmatrix}\right)$ *acts by* $(\theta_0,\theta_1)\mapsto(i\theta_0-i\theta_1,-\theta_0-\theta_1)$.

We can use Example 6.8 to recover the families from Section 3.

Example 6.9.

- *The coordinates $\theta'_0=\theta_0\theta_0(0),\theta'_1=\theta_1\theta_1(0)$ are invariant under the action of the automorphisms (1, 3). They are thus rational when E is of type $\Gamma(2)\cap\Gamma^0(4)$, which is of index 12 in Γ. We recover the coordinates of the twisted theta model from Section 3.*
- *The coordinates $\theta'_0=\theta_0/\theta_0(0),\theta'_1=\theta_1/\theta_1(0)$ are invariant under the action of the automorphisms (1, 3, 9, 11). They are thus rational when E is of type $\Gamma^0(4)$, which is of index 6 in Γ. In that case we know by Section 5 that E has a Montgomery model, and indeed we saw in Section 4 that the Montgomery coordinates are given by the Hadamard transform of θ'_0,θ'_1.*

- *The coordinates* $\theta'_0 = \theta_0\theta_0(0)+\theta_1\theta_1(0)$ $\theta'_1 = (\theta_0\theta_0(0)-\theta_1\theta_1(0))\frac{\theta_0(0)^2+\theta_1(0)^2}{\theta_0(0)^2-\theta_1(0)^2}$*, are invariant under the action of the automorphisms (1, 2, 3, 4). They are thus rational when* E *is of type* $\Gamma(2)$*.*

  And indeed, looking at the ramification in the $(\theta'_0 : \theta'_1)$ *we get that* 0_E *is sent to* $(1:1)$ *and the other ramified points are* $(1:0), (0:1), ((a^2-b^2)^2 : (a^2+b^2)^2)$*, so it is isomorphic to the Legendre model with* $\lambda = (a^2-b^2)^2/(a^2+b^2)^2$ *via the change of variable given by the 2-torsion translation between* $(1:1)$ *and* $(1:0)$*.*

We now explain how to, given an elliptic curve equation over k, compute the Galois action on a theta model defined over an extension of k. First, by Lemma 6.5, the theta model is defined by the choice of two rational points $T_1, T_2 \in E[2](k')$, both of Montgomey type over k', and the choice of two symmetric elements g_1, g_2 above T_1, T_2. By Section 6.1, The choice of g_i is itself equivalent to the choice of a cyclic subgroup K_i of degree 4 containing T_i defined over k', or (via its generator) a choice of four torsion point $\pm U'_i$ above T_i (i.e. by the image T'_i of U'_i on the Kummer). If $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$, and we take the standard basis of $\Gamma(2(0_E))$ given by $Z = Z_1^2$ (Z_1 a section of $\Gamma(0_E)$) and $X = xZ$, then the action of the symmetric theta group element g_i associated to $\pm T'_i$ is given by [Dar+24, p. 9] as the matrix

$$\frac{1}{x_iw_i - z_iu_i}\begin{pmatrix} u_iz_i & z_iw_i \\ w_ix_i^2/z_i - 2u_ix_i & -u_iz_i \end{pmatrix},$$

where on the Kummer line $T'_i = (x_i : z_i)$, $T_i = (u_i : w_i)$. Conversely, given a choice of g_i, then T'_i is the unique two point of 4-torsion on the Kummer above T_i such that $g_i \cdot (x_i, z_i) = (x_i, z_i)$ rather than $(-x_i, -z_i)$. Recall also that the choice of theta coordinate is given by θ_0 is a non trivial linear combination of X, Z invariant by g_1, and $\theta_1 = g_2 \cdot \theta_0$. From this data, looking at the Galois action of $\sigma \in \mathrm{Gal}(k'/k)$ on T'_1, T'_2, it is easy to check which automorphism from Example 6.8 it induces on the theta group and so the action of σ on the theta coordinates.

For instance, if $\sigma(T'_1) = T'_1$, i.e. $\sigma(K_1) = K_1$, then $\sigma(g_1) = g_1$. If $\sigma(T'_1) = T''_1 = T'_1 + T_2$, i.e. $\sigma(T_1) = T_1$ pour $\sigma(K_1) \neq K_1$, then $\sigma(g_1) = -g_1$. If $\sigma(T'_1) = T'_2$, i.e. $\sigma(K_1) = K_2$, then $\sigma(g_1) = g_2$. If $\sigma(T'_1) = T'_2 + T_1$, i.e. $\sigma(T_1) = T_2$ but $\sigma(K_1) \neq K_2$, then $\sigma(g_1) = -g_2$. Finally, if $\sigma(T_1) = T_1 + T_2$, we define $i = e_{W,4}(U_1, U_2)$ (where we use the sign convention given by the commutator of the theta group of level 4), and $K_3 = \langle U_1 + U_2 \rangle$, T'_3 the image of $U_1 + U_2$ on the Kummer. Then if $\sigma(T'_1) = T'_3$, i.e, $\sigma(K_1) = K_3$, then $\sigma(g_1) = ig_2g_1$. Otherwise $\sigma(g_1) = -ig_2g_1$.

We conclude this section by combining the change of coordinates from Section 4 with the automorphisms from Example 6.8 to give the conversion between a theta model and all 6 possible Montgomery models.

Example 6.10 (Conversions between the theta model and the Montgomery model)**.** *We first recall that a choice of rational symmetric element* g_T *above a two torsion point* T *is the same as a choice of* 4*-torsion point* T' *above* T *such that* $x(T')$ *is rational. The Montgomery model associated to* g_T *is the one that sends* T *to* $(0:0)$ *and* T' *to* $(1:1)$*.*

A choice of theta model is the choice of two rational symmetric elements g_1, g_2*. Once we have fixed the theta model, the theta constant* $(a:b)$ *determines the two torsion:* $T_1 = (-a:b), T_2 = (b:a), T_3 = (-b:a)$*, but also the 4-torsion points* T'_1, T'_2 *that induces* g_1, g_2 *respectively. We can recover* T'_i *as the 4-torsion point such that its coordinates* $(X(T'_i), Z(T'_i))$ *are invariant under the action of* g_i*. Recall that by definition* $X = \theta_0$ *is invariant by* g_1 *while* $Z = \theta_1 = g \cdot \theta_0$*, so* $g_1 \cdot (X, Z) = (X, -Z)$ *and* $g_2 \cdot (X, Z) = (Z, X)$*. We thus have (see Proposition 3.17)* $T'_1 = (1:0)$ *(while* $T''_1 = (0:1)$ *induces* $-g_1$*), and* $T'_2 = (1:1)$ *(while* $T''_2 = (-1:1)$ *induces* $-g_2$*). Finally, we also have, if* -1 *is a square, the additional four torsion points on the Kummer line:* $T'_3 = (i:-1)$ *and* $T''_3 = (-1:i)$*.*

Then we let M_1 be the Montgomery model where T_1' is sent to $(1:1)$, and so T_1'' to $(-1:1)$. We have $\theta(a:b) \to M_1 : (X:Z) \mapsto (bX+aZ : bX-aZ)$, and the converse is $M_1 \to \theta(a:b) : (X:Z) \to (a(X+Z) : b(X-Z))$.

This sends T_2' to $(b+a : b-a)$, T_2'' to $(b-a : b+a)$, and T_2 to $(a^2+b^2 : b^2-a^2)$. And T_3' to $(-a-ib : a-ib)$, T_3'' to $(a-ib : -a-ib)$, T_3 to $(b^2-a^2 : a^2+b^2)$. It follows that $M_1 : By^2 = x(x-\alpha_1)(x-1/\alpha_1) = x^3+A_1x^2+x$ with $\alpha_1 = (a^2+b^2)/(b^2-a^2)$ and $A_1 = 2(a^4+b^4)/(a^4-b^4)$.

Of course, if we want to send T_1'' to $(-1:1)$, we just need to compose with $M_1 \to M_1' : (X:Z) \mapsto (-X:Z)$, we have $\alpha_1' = (a^2+b^2)/(a^2-b^2)$, $A_1' = -2(a^4+b^4)/(a^4-b^4)$. The conversion is $\theta(a:b) \to M_1' : (X:Z) \mapsto (aZ+bX : aZ-bX)$, $M_1' \to \theta(a:b) : (X:Z) \to (a(Z-X) : b(X+Z))$. This is the map from Proposition 4.2.

Now, if we want to send T_2' to $(1:1)$ and T_2'' to $(-1:1)$, we obtain the Montgomery curve M_2, and the change of variable is given by: $\theta(a:b) \to M_2 : (X:Z) \mapsto (bZ-aX : bX-aZ)$, and $M_2 \to \theta(a:b) : (X:Z) \mapsto (bZ-aX : bX-aZ)$. Then $\alpha_2 = -(a^2+b^2)/(2ab), A_2 = (a^4+6a^2b^2+b^4)/(2a^3b+2ab^3)$ (Of course we have a similar map $\theta(a:b) \to M_2'$ where $A_2' = -A_2$, which is the same as the map described in Remark 4.3).

And T_1' is sent to $(-a:b)$, T_1'' to $(-b:a)$, T_1 to $(a^2+b^2 : -2ab)$, T_3' to $(-ai+b : -a+bi)$, T_3'' to $(-a+bi : -ai+b)$, T_3 to $(-2ab : a^2+b^2)$.

Finally, if we want to send T_3' to $(1:1)$ and T_3'' to $(-1:1)$, we obtain the Montgomery curve M_3, and the change of variable is given by: $\theta(a:b) \to M_3 : (X:Z) \mapsto (iaX+ibZ : aZ-bX)$, and $M_3 \to \theta(a:b) : (X:Z) \mapsto (aX+ibZ : iaZ-bX)$. Then $\alpha_3 = (2iab)/(a^2-b^2), A_3 = (a^4-6a^2b^2+b^4)/(-2ia^3b+2iab^3)$.

And T_1' is sent to $(ia:-b)$, T_1'' to $(-b:ia)$, T_1 to $(a^2-b^2 : 2iab)$, T_2' to $(ia+ib : a-b)$, T_2'' to $(a-b, i(a+b)$, T_2 to $(2iab : a^2-b^2)$.

We remark that if we start from an elliptic curve $E : y^2 = x^3+a_2x^2+a_4x+a_6$ in Weierstrass equation, picking a Montgomery model for E first involve finding a root of $x^3+a_2x^2+a_4x+a_6$ to find a two torsion point T_1, then another square root to find $x(T_1')$ for T_1' a four-torsion point above T_1. This is coherent with the fact that $\Gamma^0(4)$ is of index 6 in Γ. To go from the Montgomery model to the theta model, we need another square root to find another two torsion point T_2, and a square root again to find $x(T_2')$. This is coherent with the fact that $\Gamma(2,4)$ is of index 24 in Γ. On the other hand, since the theta model is given, from the moduli point of view, by the level structure information of $T_1, T_2, x(T_1'), x(T_2')$, it contains enough level structure information to reconstruct 4 Montgomery models. If -1 is a square, this above level structure is enough to determine $x(T_3')$, which gives us the 2 other remaining Montgomery models. This explains why the explicit conversion formulas above are rational.

Keeping track of this level structure across the change of theta models from Example 6.8, we see that applying the automorphisms (1,3,9,11) to $\theta(a,b)$ before the change of coordinates $\theta(a,b) \to M_1$ gives the same Montgomery curve M_1, the automorphisms (2,4,10,12) give M_1', the automorphisms (5,7,21,23) give M_2, the automorphisms (6,8,22,24) give M_2', the automorphisms (13,15,18,20) give M_3, the automorphisms (16,17,19,21) give M_3'.

Example 6.11 (Conversions between the theta model and the Legendre model)**.** *Using the last formula of Example 6.9, we can also look at the different conversions between the theta model and the Legendre model. Given $\theta(a:b)$, assume that we pick the conversion that gives the Legendre parameter $\lambda = (a^2-b^2)^2/(a^2+b^2)^2$.*

If we act by an automorphism before computing λ, then (1,2,3,4) give λ, (5,6,7,8) give $1-\lambda$, (9, 10, 11, 12) give $1/\lambda$, (13, 14, 15, 16) give $\lambda/(\lambda-1)$, (17, 18, 19, 20) give $1-1/\lambda$, (21, 22, 23, 24) give $1/(1-\lambda)$.

7. The point of view of isogeny volcanoes

In Sections 5 and 6, we saw conditions for when a Kummer line of E has a Montgomery model, a Montgomery$^-$ model, a theta model, a theta squared model etc. When that is not the case, a natural condition is whether E is isogeneous to a curve that admits such a model.

In this section, we use the theory of volcanoes to answer this question: namely depending on the shape of the volcano and the position of an elliptic curve in its 2-isogeny volcano we can determine if it has a Montgomery model, a Montgomery$^-$ model or a theta model (and even how many).

One application is the following: if we need to use some fast arithmetic formulas that are only available on some models, and our current Kummer line does not admit such a rational model, we may try to find an isogeny in the volcano that leads to a curve having a rational model of the suitable type. Such a strategy is used in [RS24b], where fast "half" differential addition formulas are available on Montgomery models with full two torsion: if we start with a curve E with one rational point (on the Kummer) of 8-torsion P, then $E/\langle 4P\rangle$ is such a Montgomery curve.

7.1. **Volcanoes.** Being a Montgomery curve or having a theta model are properties that can be easily read on isogeny volcanoes, which we will recall in this section. We refer to [IJ13; Sut13] for the definitions and properties of these structures. Assume in this section that $k = \mathbb{F}_q$ is a finite field of odd characteristic p.

Definition 7.1. *Let ℓ be a prime, an ℓ-volcano is a connected undirected graph V with vertices partitioned in $V_0, \dots, V_h$ and such that:*

1. *The subgraph V_0 is regular of degree at most 2.*
2. *For every $i > 0$, each vertex in V_i has exactly one neighbour in V_{i-1}, and every edge that is not on V_0 is of this form.*
3. *For every $i < h$, each vertex in V_i is of degree $\ell + 1$.*

V_0 is called the crater or the surface, V_h the floor and h the height or the depth. The height will be denoted either h or $h(V)$.

Examples of 2-volcanoes are available in Fig. 3. To relate them to elliptic curves, we need to introduce a bit more material.

We will first look at elliptic curves up to isomorphism over $\overline{k}$, hence we will identify them by their j-invariant. If $\pi : E \to E$ is the Frobenius endomorphism given by $\pi(x, y) = (x^q, y^q)$ then its trace t verifies $t = q + 1 - \#E(\mathbb{F}_q)$. We are only interested in ordinary elliptic curves in this section[3], i.e. curves E such that $t \neq 0$. For a given $t \neq 0$, we define the set of vertices as follows:

$$\mathrm{Ell}_t(\mathbb{F}_q) = \{j(E) \mid \#E(\mathbb{F}_q) = q + 1 - t\}.$$

Tate's theorem [Tat66] states that two elliptic curves E and E' over $\mathbb{F}_q$ are isogenous if and only if they have the same cardinal. Since we want to restrict to ℓ-isogenies where $\ell \neq p$ is prime, two elliptic curves in $\mathrm{Ell}_t(\mathbb{F}_q)$ are connected by an edge if they are ℓ-isogenous over $\mathbb{F}_q$. We denote the resulting graph by $G_{\ell,t}(\mathbb{F}_q)$.

Note that the data of the j-invariant and the cardinal helps to fully recover the curve. Let consider a curve E over $\mathbb{F}_q$ with trace $t \neq 0$. Its quadratic twist E' has the same j-invariant, however its trace will be $-t \neq t$ since we assumed the curve to be ordinary and the characteristic to be odd.

Assume E is a curve with j-invariant 0 or 1728, and that it has a rational 2-torsion point T. It then has non-trivial automorphisms φ and ψ such that $E[2](k) = \{\mathcal{O}, T, R = \varphi(T), S = \psi(T)\}$, see [Sil86, Chap. III, Thm. 10.1]. If f is the 2-isogeny with kernel T, then $g = f \circ \varphi$ and $h = f \circ \psi$

[3]Although our results also hold for supersingular curves defined over the base field $\mathbb{F}_p$, because they also form a volcano structure

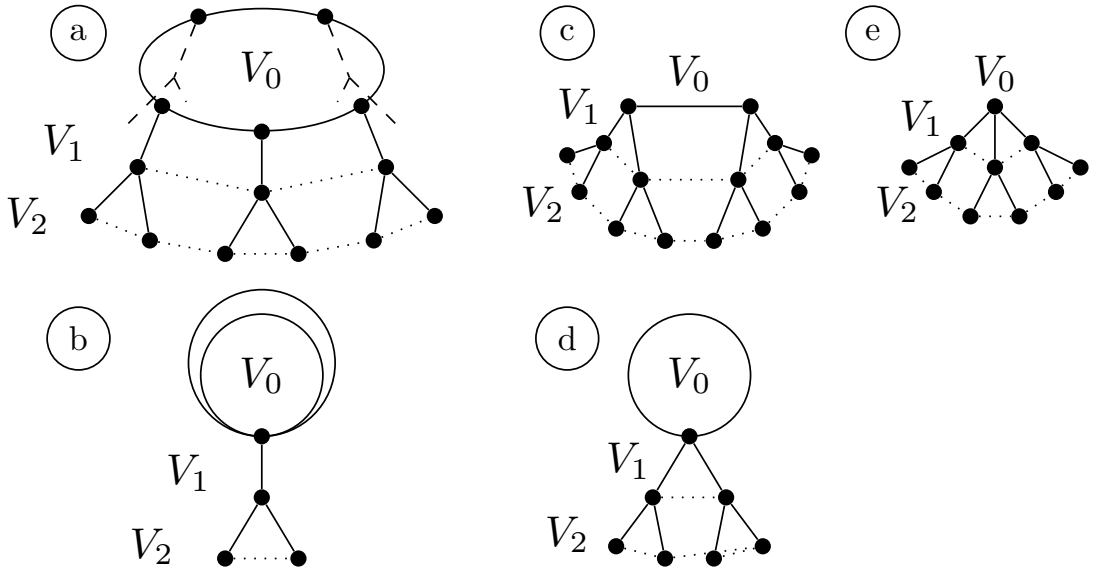


FIGURE 3. Examples of 2-volcanoes of height 2 with the possible crater shapes — dotted lines do not represent edges, only volcano levels.

are also 2-isogenies with kernel respectively R and S, they all share the same codomain. However, if the codomain E' does not have j-invariant 0 or 1728, the dual isogenies all have the same kernel T', hence $\hat{f} = \hat{g} = \hat{h}$. This is a particular case where a 2-isogeny on E yields three rational 2-isogenies, but only one going backward.

When $j \notin \{0, 1728\}$, there are no non-trivial automorphism, and therefore to one rational 2-isogeny corresponds one backward rational 2-isogeny given by the dual. Therefore, we will not deal with connected components of $G_{\ell,t}(\mathbb{F}_q)$ containing j-invariants 0 and 1728, and we will consider the graphs undirected.

The last notion is the one of orders. If E is an ordinary elliptic curve, then $\mathrm{End}(E)$ is an order $\mathcal{O}$ in a quadratic imaginary field K (more precisely, $K = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\pi)$). Let $\mathcal{O}_K$ be the ring of integers of K. Since π is an endomorphism, $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ holds. Let d_π, d and d_K be respectively the discriminant of $\mathbb{Z}[\pi]$, $\mathcal{O}$ and $\mathcal{O}_K$. Since the Frobenius satisfies $\pi^2 - t\pi + q = 0$, we know that $d_\pi = t^2 - 4q$. Let

$$\omega = \begin{cases} \sqrt{\frac{d_K}{4}} & \text{if } d_K \equiv 0 \bmod 4, \\ \frac{1+\sqrt{d_K}}{2} & \text{if } d_K \equiv 1 \bmod 4. \end{cases}$$

Then $\mathcal{O}_K = \mathbb{Z}[\omega]$, and we can write $\mathbb{Z}[\pi] = \mathbb{Z}[f_\pi \omega]$ and $\mathcal{O} = \mathbb{Z}[f\omega]$ with $f_\pi, f \geqslant 0$, they are respectively the conductor of $\mathbb{Z}[\pi]$ and $\mathcal{O}$. We also have $f_\pi = [\mathcal{O}_K : \mathbb{Z}[\pi]]$ and $f = [\mathcal{O}_K : \mathcal{O}]$, therefore $f \mid f_\pi$ and $d_\pi = f_\pi^2 d_K$, $d = f^2 d_K$.

The following result is due to Kohel who studied isogeny graphs in his thesis [Koh96, Prop. 21–23]:

Lemma 7.2 (Kohel, see e.g. Th 7 in [Sut13])**.** *Let V be a connected component of $G_{\ell,t}(\mathbb{F}_q)$ not containing j-invariants* 0 *and* 1728*. Then V is an ℓ-volcano with levels $V_0, \ldots, V_h$ verifying the following properties:*

(1) *Every curve in V_i has the same endomorphism ring $\mathcal{O}_i$ with discriminant d_i and conductor f_i.*
(2) *The subgraph V_0 has degree $1 + \left(\frac{d_0}{\ell}\right)$.*
(3) *If $\left(\frac{d_0}{\ell}\right) \neq -1$, then ℓ is split or ramified and $\#V_0$ is the order of $[\mathfrak{l}]$ in $\mathrm{Cl}(\mathcal{O}_0)$ where $\mathfrak{l} \mid \ell$ is prime, otherwise $\#V_0 = 1$.*
(4) *The height h is the ℓ-valuation of the conductor of $\mathbb{Z}[\pi]$.*
(5) *$\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$, and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ for $0 \leqslant i < h$, that is $d_i = \ell^{2i} d_0$ or $f_i = \ell^i f_0$.*

Using (2), since the discriminant d_i only differs from d_K by a square, the degree of V_0 depends only on whether ℓ is split, ramified or inert in $\mathcal{O}_K$. If ℓ is split, then V_0 has degree 2, if it is ramified V_0 has degree 1, and otherwise it is inert and V_0 is a point. From (4) and (5), we can also derive $h = v_\ell\left(\frac{d_\pi}{d_K}\right)/2 = v_\ell\left(\frac{d_\pi}{d_0}\right)/2$ since ℓ does not divide the conductor of $\mathcal{O}_0$.

Lemma 7.2 justifies the following terminology, let E and E' be two ℓ-isogenous elliptic curves via $f : E \to E'$, and $\mathcal{O}$ and $\mathcal{O}'$ there endomorphism rings. f is said to be horizontal if $\mathcal{O} = \mathcal{O}'$, descending if $[\mathcal{O} : \mathcal{O}'] = \ell$ and ascending if $[\mathcal{O}' : \mathcal{O}] = \ell$.

Formulas for the cardinal depending on its height and the size of the crater can be easily derived:

Proposition 7.3. *Let V be an ℓ-isogeny volcano with height h and levels $V_0, \dots, V_h$. Then:*

$$\#V = \begin{cases} \#V_0\, \ell^h & \text{if } \deg V_0 = 2, \\ \#V_0 \left(1 + \ell \frac{\ell^h - 1}{\ell - 1}\right) & \text{if } \deg V_0 = 1, \\ 1 + (\ell + 1)\frac{\ell^h - 1}{\ell - 1} & \text{if } \deg V_0 = 0. \end{cases}$$

Proof. If $h = 0$, the formulas indeed give $\#V = \#V_0$. We will assume $h \geqslant 1$. Let $u_i = \#V_i$. We have $\#V = u_0 + \cdots + u_h$. If $i = 1$, then each vertex on the crater has degree $\ell + 1$, and taking into account the degree of the subgraph V_0:

$$u_1 = \begin{cases} (\ell - 1)\#V_0 & \text{if } \deg V_0 = 2, \\ \ell\, \#V_0 & \text{if } \deg V_0 = 1, \\ (\ell + 1)\#V_0 & \text{if } \deg V_0 = 0. \end{cases}$$

Now if $1 \leqslant i < h$, each vertex on level V_i has only one ascending isogeny, and because the degree is $\ell + 1$, there must be ℓ descending isogenies, hence $u_{i+1} = \ell u_i$. The result then comes from summing a geometric series. □

From the theorem, one could wonder if every kind of volcano occurs. The answer is yes, even in the degenerate cases as we can see in Table 1. We consider a connected component V of $G_{\ell,t}(\mathbb{F}_p)$ where $\ell = 2$. These examples where found by looking for convenient quadratic fields and discriminant, using Lemma 7.2.

7.1.1. *Information on the ℓ-torsion.* Finally, we want to deduce information on a curve based on its position in a volcano, notably its ℓ-torsion. If E is an ordinary elliptic curve over $\mathbb{F}_q$ with endomorphism ring isomorphic to $\mathcal{O}$, it is known that $E(\mathbb{F}_q) \simeq \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ with $N \mid M$, then $\#E(\mathbb{F}_q) = MN$ thanks to a Tate result stating that $E(\mathbb{F}_q) \simeq \mathcal{O}/(\pi - 1)$. We are interested in the ℓ-valuation of N. We can write $\pi = a + f_\pi \omega$ where:

$$a = \begin{cases} t/2 & \text{if } d_K \equiv 0 \bmod 4, \\ (t - f_\pi)/2 & \text{if } d_K \equiv 1 \bmod 4. \end{cases}$$

If f is the conductor of the endomorphism ring $\mathcal{O}$, then $N = \gcd(a - 1, f_\pi/f)$. It is known [Mir+06, Thm. 1] (their proof holds for any ℓ) that $v_\ell(a - 1) \geqslant \min(v_\ell(f_\pi), v_\ell(\#E(\mathbb{F}_q))/2)$. If

p	t	$j(E)$	h	$\deg(V_0)$	$\#V$	$\#V_0$	Fig. 3 example
450361	1094	300824	3	2	176	22	a
3049	102	591	4		16	1	b
155209	506	83458	3	1	30	2	c
521	6	354	4		31	1	d
464069	164	93759	0		2	2	—
182641	194	135674	3	0	22	1	e
159629	9	63979	0		1	1	—

TABLE 1. Some examples of 2-isogeny volcanoes

we further assume that $v_\ell(N) < v_\ell(M)$, then $v_\ell(N) < v_\ell(\#E(\mathbb{F}_q))/2$, and because of the gcd, we must have $v_\ell(N) = v_\ell(f_\pi/f)$.

If we go down the volcano, the conductor is multiplied by ℓ, so the ℓ-valuation of N decreases by 1, whereas the one of M increases by 1. On the floor, because $h = v_\ell(f_\pi)$, ℓ does not divide N any more. Let $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ denote the ℓ-Sylow of $E(\mathbb{F}_q)$.

7.2. **Reading model of curves on a volcano.** We will now focus on the case $\ell = 2$ in this section. Let $t \neq 0$, we consider a volcano V of a connected component of $G_{2,t}(\mathbb{F}_q)$ not containing j-invariants 0 and 1728. The levels will be denoted $V_0, \dots, V_h$. Preparing next proposition, we start with a useful lemma:

Lemma 7.4. *If* $\deg V_0 = 2$*, then* $h(V) \geqslant 1$*.*

Proof. Let E be a curve on V_0. Because $\deg V_0 = 2$, there are two distinct rational kernels of order 2 in E. But having a rational kernel of order 2 is equivalent to having a rational 2-torsion point, so E has complete 2-torsion generated by T and R. But then $S = T + R$ is also a rational 2-torsion point, giving a third rational 2-isogeny. Because $\deg V_0 = 2$, this isogeny must be a descending one, hence $h(V) \geqslant 1$. □

Remark 7.5. *In the following proofs, we will be chaining isogenies in the volcano. One important thing to note is that, once we consider a descending isogeny, we must chain descending ones afterwards because there are no more horizontal isogenies at that level and the only ascending one available is going backwards.*

Legendre curves are simple to classify since they are the one with full 2-torsion.

Proposition 7.6 (Legendre curves)**.** *The elliptic curves in a* 2*-volcano are Legendre if and only if they are not on the floor i.e. the don't belong to* V_h *where* h *is the height of the volcano. In particular, a* 2*-volcano has no Legendre curve if and only if* $h = 0$*. In this case one also has* $\deg V_0 \leqslant 1$*.*

Proof. If $h \geqslant 1$, then for all $0 \leqslant i < h$, every curve in V_i has degree 3, hence 3 rational 2-torsion points, so the curve is in Legendre form. On the floor, the degree is 1, so they are not Legendre because they only have one rational 2-torsion point. If $h = 0$, because of Lemma 7.4, $\deg V_0 \leqslant 1$ and curves have at most one horizontal 2-isogeny, and no descending one, which does not give the full 2-torsion. □

For Montgomery curves and onwards, we will need the following lemma:

Lemma 7.7. *Let* f_1 *and* f_2 *be two* 2*-isogenies that are not dual, then* $f = f_1 \circ f_2$ *is a cyclic* 4*-isogeny.*

Proof. f has degree 4, so its kernel is either isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But in the second case, that would imply that $f = [2]$ and therefore f_1 and f_2 would be dual. Hence, f is cyclic. □

Montgomery curves are described as curves with a rational cyclic 4-isogeny thanks to Proposition 5.12.

Proposition 7.8 (Montgomery curves)**.** *Let V be a 2-isogeny volcano not containing curves with j-invariant 0 and 1728 and with levels $V_0, \dots V_h$:*

(1) If $\deg V_0 = 2$, every curve on the volcano has a Montgomery form.
(2) If $\deg V_0 = 1$, then either $h \geqslant 1$ and every curve on the volcano has a Montgomery form, otherwise $h = 0$ and no curve on the volcano has a Montgomery form.
(3) If $\deg V_0 = 0$, then either $h \geqslant 2$ and every curve on the volcano has a Montgomery form. Otherwise, if the height is 1 then every curve on the floor V_1 has a Montgomery form and finally if $h = 0$ no curve has a Montgomery form.

Proof. Lemma 7.7 helps to translate the property of having a rational 4-isogeny in terms of graph theory on the volcano: if we can follow a path of length 2 on the volcano, then the starting curve will have a 4-isogeny. Fig. 4 illustrates the different cases that can occur.

- If $\deg V_0 = 2$ and E is a curve on V_0, since the height is always greater than 1 with Lemma 7.4 and there is always a horizontal isogeny, it is possible to chain a horizontal and a descending one, see Fig. 4a.
- If $\deg V_0 = 2$ and E is a curve on V_1, it is possible to chain the ascending 2-isogeny with a horizontal one since we land on the crater after the first step.
- Assume $\deg V_0 = 1$ and E is a curve on V_0. Since there is only one horizontal isogeny, we must chain it with a descending one to get a 4-isogeny, so the height of the volcano must be greater than 1 in that case.
- If $\deg V_0 = 0$ and E is a curve on V_0, since there is no horizontal isogeny, we must consider two descending ones to build a 4-isogeny, this requires the height to be at least 2.
- If $\deg V_0 = 0$ or 1 and E is a curve on V_1, since curves on the crater have at least two descending isogenies, it is possible to chain first an ascending one starting from E and then a descending one, see Fig. 4d.
- Finally, assume that $i \geqslant 2$ and that E is a curve on V_i. It is then possible to chain two ascending 2-isogenies, giving a cyclic 4-isogeny.

□

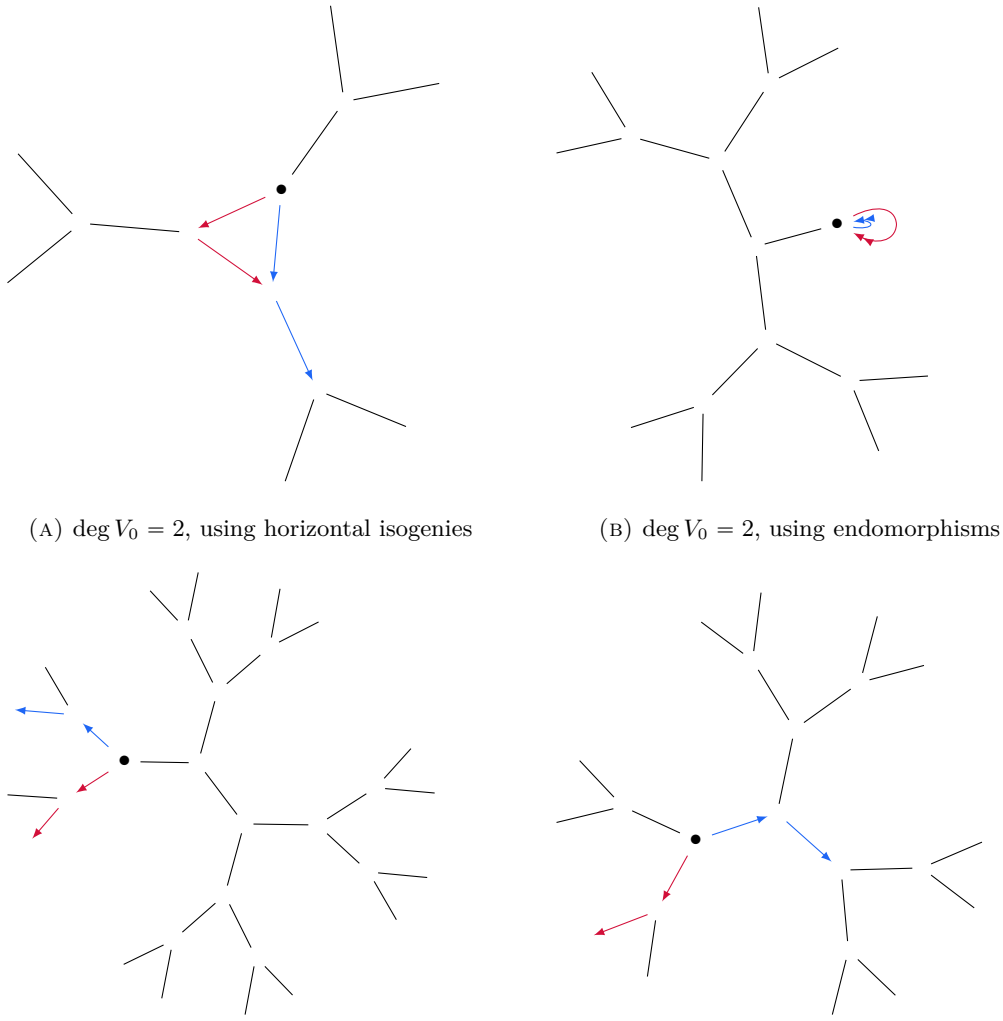
Recall from Corollary 6.4 that a curve admit a Montgomery$^-$ model if and only if there exists a rational 2-isogeny that does not extend to a rational cyclic 4-isogeny. We leave to the reader how to adapt Proposition 7.8 to the Montgomery$^-$ case.

A direct consequence is the characterization of curves having a theta squared model:

Proposition 7.9 (Theta squared model)**.** *Let V be a 2-isogeny volcano not containing curves with j-invariant 0 and 1728 and with levels $V_0, \dots V_h$:*

(1) If $\deg V_0 = 2$, every curve in $V_0 \cup \dots \cup V_{h-1}$ has a theta squared model.
(2) If $\deg V_0 = 1$, then either $h \geqslant 1$ and every curve in $V_0 \cup \dots \cup V_{h-1}$ has a theta squared model, otherwise $h = 0$ and no curve on the volcano has a theta squared model.
(3) If $\deg V_0 = 0$, then either $h \geqslant 2$ and every curve in $V_0 \cup \dots \cup V_{h-1}$ has a theta squared model. Otherwise, $h \leqslant 1$ and no curve on the volcano has a theta squared model.

Proof. Thanks to Proposition 5.14, an elliptic curve E has a theta squared model if and only if it has a Montgomery form with full rational 2-torsion, hence it also has a Legendre form. The result is then deduced from Propositions 7.6 and 7.8. □



(A) $\deg V_0 = 2$, using horizontal isogenies

(B) $\deg V_0 = 2$, using endomorphisms

(C) $\deg V_0 = 2$, using only descending isogenies

(D) $\deg V_0 = 0$, going through the crater

FIGURE 4. Some examples of cyclic 4-isogenies on different volcanoes

Finally, having a theta model is the most restrictive proposition since the curve requires two independent 4-isogenies thanks to Proposition 5.14. There is a particular case to address before looking at characterizing curves with a theta model.

Lemma 7.10. *Assume $\#V_0 = 1$, let E be the elliptic curve in V_0. If $\deg V_0 = 2$, then E admits exactly two non-trivial endomorphisms f and $\hat{f}$ of degree 2, where $\hat{f}$ is the dual of f. If $\deg V_0 = 1$ then E admits exactly one non-trivial endomorphism f of degree 2 which is self-dual, i.e. $f = \hat{f}$.*

Proof. When $\deg V_0 = 2$, there are two 2-isogenies on the crater with domain and codomain E. Denote them f and g, and their kernel generators P and Q. They are distinct rational 2-torsion points, hence generators of $E[2]$. The last 2-isogeny with kernel $P + Q$ can't be an

endomorphism because of the volcano structure, it must be descending. Because $\hat{f}$ is also a non-trivial endomorphism, we must have $\hat{f} = f$ or $\hat{f} = g$. But in the first case, if $\hat{f} = f$, looking at isogenies as ideals thanks to Deuring correspondence [Deu41], this would imply that $2\mathcal{O}_K = \mathfrak{p}^2$ where $\mathfrak{p}$ is the ideal corresponding to f, so 2 would be ramified in $\mathcal{O}_K$. But this is not the case according to Lemma 7.2, 2 is split when $\deg V_0 = 2$. Hence, $g = \hat{f}$.

When $\deg V_0 = 1$, there is only one 2-isogeny on E that is a non-trivial endomorphism, we denote it by f. Then $\hat{f}$ is also a non-trivial endomorphism and by uniqueness must verify $\hat{f} = f$. □

Proposition 7.11 (Theta model)**.** *Let V be a 2-isogeny volcano not containing curves with j-invariant 0 and 1728 and with levels $V_0, \dots V_h$:*

- *If $h \geqslant 2$, then every curve in $V_0 \cup V_1 \cup \dots \cup V_{h-2}$ have a theta model.*
- *If $\deg V_0 = 2$ and $h = 1$, only curves on V_0 have a theta model.*
- *If $\deg V_0 \leqslant 1$ and $h \leqslant 1$, no curve on the volcano has a theta model.*

Proof. For 4-isogenies to be independent, they must not share an edge in the same direction, but they can share a vertex. Because of Lemma 7.7, they will be cyclic. We once again refer to Fig. 4 for several illustrations.

- If E is a curve not on the crater — say E is in V_i with $i \geqslant 1$ — since there is only one edge ascending, this implies that the second isogeny must start by descending, and by Remark 7.5, at least one of the two isogenies will descend two levels. In that case if E admits a theta model we must have $h \geqslant i + 2$, i.e. $1 \leqslant i \leqslant h - 2$.
- If E is in V_0 and $\deg V_0 = 2$, there are two horizontal 2-isogenies starting from E.
  - Assume $\#V_0 \geqslant 2$, in that case there are two horizontal 2-isogenies starting from E. Since the height is at least 1 thanks to Lemma 7.4, it is possible to build the first 4-isogeny by chaining a horizontal one and a descending one. The second 4-isogeny is obtained by chaining two horizontal 2-isogenies, which is always possible because $\#V_0 \geqslant 2$, see Fig. 4a.
  - Otherwise, if $\#V_0 = 1$, Lemma 7.10 shows that there are two 2-isogenies on the crater that are endomorphisms and dual one another. Hence, if f and $\hat{f}$ are those two endomorphisms, $f \circ f$ and $\hat{f} \circ \hat{f}$ are two independent cyclic 4-isogenies, and E has a theta model, see Fig. 4b.
- If E is in V_0 and $\deg V_0 \leqslant 1$, there are two descending branches stemming from E. Moreover, there is at most one horizontal isogeny, therefore one of the 4-isogeny must start with a descending 2-isogeny. Hence, either $h \geqslant 2$ and E has a theta model, or $h \leqslant 1$ and it is not possible to construct both 4-isogenies, E does not have a theta model in that case.

□

All these properties are summarized in Table 2.

Remark 7.12 (The number of Montgomery and Montgomery$^-$ models)**.** *Using Example 6.7, we can refine the discussion about whether a curve, depending on its position in the volcano, admit a Montgomery or Montgomery$^-$ or theta model, to how many such models it may admit.*

Consider the case when the volcano is not a single point, which happens when the cardinal of $E(\mathbb{F}_q)$ is odd, and so there is not even a rational 2-torsion point.

On the bottom of the volanco, the 2-Sylow is cyclic so there is only one rational 2-torsion point T_1. Depending on whether the isogeny generated by T_1 extends to a rational 4-isogeny (which can be read as above from the shape of the volcano), then E admit 2 Montgomery models or 2 Montgomery$^-$ models. And E does not have a rational theta model.

$\deg V_0$	Legendre curves h	Legendre curves Volcano Levels	Montgomery curves h	Montgomery curves Volcano Levels	Theta squared model h	Theta squared model Volcano Levels	Theta model h	Theta model Volcano Levels
2	$\geqslant 1$	$\{0,\dots,h-1\}$	$\geqslant 1$	$\{0,\dots,h\}$	$\geqslant 1$	$\{0,\dots,h-1\}$	$\geqslant 2$ 1	$\{0,\dots,h-2\}$ $\{0\}$
1	$\geqslant 1$ 0	$\{0,\dots,h-1\}$ $\varnothing$	$\geqslant 1$ 0	$\{0,\dots,h\}$ $\varnothing$	$\geqslant 1$ 0	$\{0,\dots,h-1\}$ $\varnothing$	$\geqslant 2$ $\leqslant 1$	$\{0,\dots,h-2\}$ $\varnothing$
0	$\geqslant 1$ 0	$\{0,\dots,h-1\}$ $\varnothing$	$\geqslant 2$ 1 0	$\{0,\dots,h\}$ $\{1\}$ $\varnothing$	$\geqslant 2$ $\leqslant 1$	$\{0,\dots,h-1\}$ $\varnothing$	$\geqslant 2$ $\leqslant 1$	$\{0,\dots,h-2\}$ $\varnothing$

TABLE 2. Curves on a volcano $V = V_0 \cup \ldots \cup V_h$ with different models

When not on the bottom, then E has full rational 2-torsion T_1, T_2, T_3. It admits 6 Montgomery + Montgomery$^-$ model, and the exact number of Montgomery vs Montgomery$^-$ model depends on the type of T_1, T_2, T_3, which again can be read from the volcano.

Remark 7.13 (The supersingular case)**.** *We conclude by a discussion about the supersingular case. If $E/\mathbb{F}_p$ is a supersingular curve its 2-isogeny graph behaves similarly to the ordinary curve and in particular it has a volcano structure.*

If $p \equiv 1 \mod 4$, the volcano has height 1 (and 2 split in the maximal order), and if $p \equiv 3 \mod 4$, the volcano has height 2. If $p \equiv 3 \mod 8$, 2 is inert in the maximal order, so the volcano consist of one node on the top and three nodes on the bottom (all 2-isogenies from the top are descending), whereas if $p \equiv 7 \mod 8$, 2 splits in the maximal order, so we have a cycle at the top, and each curve on the top has two horizontal 2-isogenies, and one descending 2-isogeny.

The arguments from Remark 7.12 counting the number of Montgomery and Montgomery$^-$ models recover the results from [CD20, Figs. 1-2]. We also see that E admits a rational theta model if and only if $p \equiv 1 \mod 4$, or $p \equiv 7 \mod 8$ and E is at the top of the volcano (and the 2-cycle is not degenerate).

If $E/\mathbb{F}_{p^2}$ is a maximal or minimal supersingular curve, then the 2-torsion is rational, and the self Tate pairings are trivial. It follows that E always has a rational theta model, and in fact all 24 possible theta models on E are rational.

8. Application to the Elliptic Curve Method

As it is shown in [RS24a], combining arithmetic of theta squared and Montgomery models can speed up the Montgomery ladder. However, while the ladder is useful when constant time is required — for instance in cryptographic protocols — PRAC is preferred in other contexts, like Elliptic Curve Method. If the arithmetic can be improved using theta squared model, we are interested in finding curves with small coefficients and good torsion properties for ECM.

8.1. **Elliptic Curve Method.** ECM is an algorithm for integer factorization inspired by Pollard's $p-1$ method, whish is due to Lenstra [Len87]. The initial algorithm is called "stage 1" because it has been continued with a procedure called the "stage 2". Consider the factorization of an odd integer N which is not a prime power.

(1) One chooses $A, x, y \in \mathbb{Z}/N\mathbb{Z}$ and set B so that $By^2 = x^3 + Ax^2 + x$. One calls E the corresponding scheme over $\mathbb{Z}/N\mathbb{Z}$ and P the point $(x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.
(2) One chooses a positive integer M and compute $M \cdot P = (X : Y : Z)$ using the elliptic curve addition formulas.

There are two possible outcomes:

(1) In the usual addition law, divisions occurs and may not be defined modulo N, that means we have an element d which has a common factor with N. In that case, one computes $\gcd(d, N) \neq 1$, if it is not N, then this is a non-trivial factor.
(2) Otherwise, no error is raised while computing $M \cdot P$. If there is a prime factor $p \mid N$ such that $M \cdot P$ reduces to $\mathcal{O} = (0 : 1 : 0)$ modulo p, then $\gcd(Z, N)$ may yield a factor greater than 1 (a carefull analysis [Len87] shows that it is almost certainly not N).

The major difference with the $p - 1$ method is that if no factor is found on a curve, it can be iterated again by choosing a new curve. Note that since it is possible to compute multiples on the Kummer line with operations defined in Section 3, ECM stage 1 is usually done on the Kummer line. Note that in theta squared coordinates $\widehat{\theta}(a^2 : b^2)$, the origin is $(a^2 : b^2)$, so if $[M \cdot P] = (X : Z)$, we will look at the quantity $\gcd(b^2X - a^2Z, N)$.

Generally, $M = \operatorname{lcm}(\{p^{\lfloor \log_p B \rfloor : p < B}\})$ where B is a positive integer. This amounts to expecting the cardinal of the curve reduced modulo a prime $p \mid N$ to be B-smooth, i.e. every prime factor is less than B. This is reasonable because of the Hasse bound, see [Sil86, Thm V.1.1]: for any elliptic curve E over $\mathbb{F}_p$, $|\#E(\mathbb{F}_p) - p - 1| \leqslant 2\sqrt{p}$.

8.2. **Curves with fast arithmetic and large success probability.** We are interested here in finding elliptic curves E which are ECM-friendly i.e. with a fast arithmetic and a large success probability (see e.g. [Mon92, Sec 6.3], [Ber+13, Fig 9.1] and [Bar+13]). An analysis based on the Galois representation [BS22] estimated how the success probability of several families compares to each other.

We represent in Fig. 5 the subgroups of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ which contain $X_{\mathrm{sp}}(4)$, in particular those which characterize elliptic curves having a Montgomery, theta and respectively theta squared model (the data is extracted from the LMFDB site). For the full diagram of subgroups of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, see Fig. 6.

Kubert (see e.g. [Mon92, Th 6.2.4]) parametrized the elliptic curves whose rational torsion contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or equivalently those corresponding to $X(2, 8)$, as depicted in Table 3.

Equation	Kummer model or torsion
$y^2 = x(x^2 - \mathcal{A}x + \gamma)$	Torsion $\mathbb{Z}/2\mathbb{Z}$
$y^2 = x(x^2 - \mathcal{A}x + 1)$	Montgomery model
$y^2 = x(x - \frac{a}{b})(x - \frac{b}{a})$, $a \neq b$	Theta squared model
$y^2 = x(x - \frac{a^2}{b^2})(x - \frac{b^2}{a^2})$, $a \neq b$	Theta model
$y^2 = x(x - \frac{a^2}{b^2})(x - \frac{b^2}{a^2})$, $a^2 + b^2 = \square$	Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

TABLE 3. Different elliptic curves and their corresponding Kummer line model or torsion

We search for small integer values of a and b to exploit the fact that the multiplication by very small constants as 2 and 3 can be done by additions and is negligible compared to a full multiplication.

In a numerical experiment, we first generated a set of curves with $a^2 + b^2$ a square, a starting point for ECM $P = (X : Y : Z)$, and with the constraint that a^2, b^2, X and Z are less than a computer word. We found around 3 million of Pythagorean triplets, but by testing only 120000 of them, we got 91 curves with small constants. We then dropped the constraint $a^2 + b^2$ is a square. This was giving a lot of tuples (a, b), so we tested only the first 15600 and got 2861 more curves. Finally, we tried to set $b^2 = 1$, and out of 60000 tuples (a, b), we found 90 more curves.

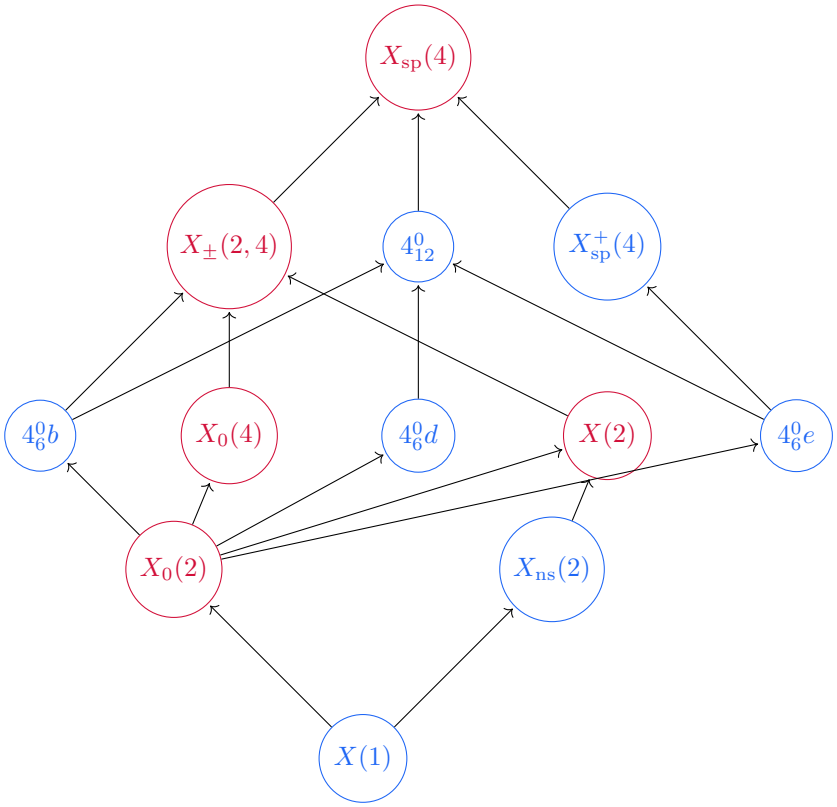


FIGURE 5. The diagram of the subgroups of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ containing $D(4) = \Gamma(2,4) = X_{\mathrm{sp}}(4)$. The subgroups which characterize the elliptic curves having Kummer models studied in this article are as follows: $X(1)$ is the set of all the curves, $X_0(2)$ corresponds to the curves with a rational point of order 2, $X(2)$ corresponds to the Legendre curves (Proposition 5.10) $X_0(4)$ corresponds to the Montgomery model M (Proposition 5.12), $D(4) = X_{\mathrm{sp}}(4)$ corresponds to the theta model θ (Proposition 5.14), $X(2,4)$ coresponds to the theta squared model $\widehat{\theta}$ (Proposition 5.14(2)).

Given the number of curves found in the second case, we'd like them to be as efficient as the first family. To do so, we will compare the following quantity, where G is a subgroup of $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$: $\mathrm{Prob}(E(\mathbb{F}_p)[2^n] \simeq G)$. If we have equal probabilities for 2 and 4-torsion, because we are working on level 4 modular curves, this will be sufficient to say that the efficiency will be similar for these two families. Thanks to Chebotarev density theorem and [Bar+13, Thm. 2.7.1], we know that this quantity is written (with $a \in \mathbb{N}$):

$$\mathrm{Prob}(E(\mathbb{F}_p)[2^n] \simeq G) = \frac{a}{\#\,\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})} = \frac{a}{96}.$$

To achieve that, we compute an experimental probability over many primes for each family of curves, and then look for the closest fraction in the form $\frac{a}{96}$. If we choose a large enough number of primes — which is known thanks to an effective version under GRH of Chebotarev theorem by Lagarias and Odlyzko [LO77, Thm. 1.1] and with explicit constants by Winckler [Win13, Thm. 1.2] — we then know that this is the exact value.

Results are given in Table 4. We can conclude that the second family, i.e. torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$,

Subgroup G of $\mathbb{Z}/2^n\mathbb{Z}\times\mathbb{Z}/2^n\mathbb{Z}$	Prob with $a^2+b^2=\square$	Prob with generic a^2+b^2
2-torsion		
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	1	1
4-torsion		
$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	0.75	0.75
$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$	0.25	0.25

TABLE 4. Comparison of the 2 and 4-torsions of the two families of curves

has the same success probability as the first one, i.e. curves with a theta model. One can therefore use the theta model if it has a better arithmetic cost.

Remark 8.1. *We studied ECM with theta coordinates in the first place because of its genus* 2 *generalization HECM [Cos11, Ch. 4]. Indeed, we believe there is a small mistake in [Cos11, Tab. 3.2], the first column about genus* 1 *should be* $2\mathbf{M}+6\mathbf{S}+1\mathbf{m}_P+3\mathbf{m}$ *on the first line, which is the sum of the cost of Algorithms 5 and 6. With this complexity, two instances of ECM should be a little bit faster than one pass of HECM, contrary to what is claimed in [Cos11].*

9. PERSPECTIVES

This paper concludes, with [RS24a; RS24b] a trilogy of papers looking at models of Kummer lines and their arithmetic. (Or a tetralogy if one also counts [Rob24] which deals with pairings on Kummer lines, but that papers also deal with higher dimension and other levels than two).

This study can be recast as a study of models of elliptic curves of level 2, that is given by a choice of basis of $\Gamma(E,2(0_E))$. All coordinates of level 2 are even, so descend to the Kummer line.

Through this study, a unifying theme was the role that the theta group $G(2(0_E))$ of level 2 played, along with its action on our sections, to understand the arithmetic of our models.

There are two natural generalisations we plan to tackle in the future. The first one is to stay in dimension 1 but to increase the level, in particular to obtain models of the elliptic curve itself. It is shown in [LR16] that if $\pi : E \to E/\pm 1 \simeq \mathbb{P}^1$ is the projection, and $P_0 \in E(k)$ is not a point of 2-torsion, then $P \mapsto (\pi(P), \pi(P+P_0)) \in \mathbb{P}^1\times\mathbb{P}^1$ is an embedding. If P_0 is a point of n-torsion, taking coordinates on $E/\pm 1$ of level 2, this gives coordinates of level $2\vee n$. The most well known example of this embedding is given by Edwards curves [BL07a], or more precisely the completed Edwards curve [Ber+13, § 2.7]. Indeed, up to a small change of variable, the completed Edwards model is precisely given by the embedding $E \to \mathbb{P}^1\times\mathbb{P}^1, P \mapsto ((X(P):Z(P)), X(P+T):Z(P+T))$ where (X,Z) are the Kummer line coordinates of a Montgomery model, and $T=(1:1)$ is the canonical point of 4-torsion (this seems to have been first noticed by Kohel in [Koh11]). It is therefore natural to look at similar level 4 embeddings via the other Kummer models studied in Section 3.

The other natural generalisation will be to stay in level $n=2$ but to move from dimension $g=1$ to $g=2$. In that case the Kummer surface $A/\pm 1$ (where A is an abelian surface) can be described as a surface in $\mathbb{P}^3$. In a similar manner to the Kummer lines, there is a combinatorial description of the Kummer surfaces [Gau07], namely via the $(16,6,2)$-design induced by their two torsion points and (translation) of their Θ-divisor. However, this is less tractable than the simple 4 points of ramification in $\mathbb{P}^1$ we had in dimension 1. Still, the theta model is characterised

by symmetry conditions on the (ramification locus of) the Kummer surface: this time it has to satisfy four different symmetries at the same time. Then it could be useful to look at models of Kummer surfaces where the theta group is a twist of the Heisenberg group, as in Section 6.2.

References

[AOV08] Dan Abramovich, Martin Olsson, and Angelo Vistoli. "Tame stacks in positive characteristic". In: *Annales de l'institut Fourier*. Vol. 58. 4. 2008, pp. 1057–1091.

[Bar+13] Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery. "Finding ECM-friendly curves through a study of Galois properties". English. In: *ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012*. Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013, pp. 63–86. ISBN: 978-1-935107-00-2; 978-1-935107-01-9.

[Ber+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. "Twisted Edwards Curves". In: *AFRICACRYPT 08*. Ed. by Serge Vaudenay. Vol. 5023. LNCS. Springer, Berlin, Heidelberg, June 2008, pp. 389–405. DOI: 10.1007/978-3-540-68164-9_26.

[Ber+13] Daniel Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. "ECM using Edwards curves". In: *Mathematics of Computation* 82.282 (2013), pp. 1139–1179.

[BL07a] Daniel J. Bernstein and Tanja Lange. "Faster Addition and Doubling on Elliptic Curves". In: *ASIACRYPT 2007*. Ed. by Kaoru Kurosawa. Vol. 4833. LNCS. Springer, Berlin, Heidelberg, Dec. 2007, pp. 29–50. DOI: 10.1007/978-3-540-76900-2_3.

[BL07b] Daniel J. Bernstein and Tanja Lange. "Inverted Edwards Coordinates". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007, Proceedings*. Ed. by Serdar Boztas and Hsiao-feng Lu. Vol. 4851. Lecture Notes in Computer Science. Springer, 2007, pp. 20–27. DOI: 10.1007/978-3-540-77224-8_4.

[BL24] Daniel Bragg and Max Lieblich. "Murphy's Law for Algebraic Stacks". In: *arXiv preprint arXiv:2402.00862* (2024).

[Bos+13] Joppe W. Bos, Craig Costello, Hüseyin Hisil, and Kristin Lauter. "Fast Cryptography in Genus 2". In: *EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. LNCS. Springer, Berlin, Heidelberg, May 2013, pp. 194–210. DOI: 10.1007/978-3-642-38348-9_12.

[Bre83] Lawrence Breen. *Fonctions thêta et théoreme du cube*. Vol. 980. Springer, 1983.

[BS22] Razvan Barbulescu and Sudarshan Shinde. "A classification of ECM-friendly families of elliptic curves using modular curves". In: *Mathematics of Computation* 91.335 (2022), pp. 1405–1436.

[BSS05] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Advances in elliptic curve cryptography*. English. Vol. 317. Lond. Math. Soc. Lect. Note Ser. Cambridge: Cambridge University Press, 2005. ISBN: 0-521-60415-X. DOI: 10.1017/CBO9780511546570.

[BSS99] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic curves in cryptography*. English. Vol. 265. Lond. Math. Soc. Lect. Note Ser. Cambridge: Cambridge University Press, 1999. ISBN: 0-521-65374-6.

[CD20] Wouter Castryck and Thomas Decru. "CSIDH on the Surface". In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*. Ed. by Jintai Ding and Jean-Pierre Tillich. Springer, Cham, 2020, pp. 111–129. DOI: 10.1007/978-3-030-44223-1_7.

[CGF08] Wouter Castryck, Steven Galbraith, and Reza Rezaeian Farashahi. *Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation*. Cryptology ePrint Archive, Report 2008/218. 2008. URL: https://eprint.iacr.org/2008/218.

[Cos11] Romain Cosset. "Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques. (Applications of theta functions for hyperelliptic curve cryptography)". PhD thesis. Henri Poincaré University, Nancy, France, 2011. URL: https://tel.archives-ouvertes.fr/tel-00642951.

[CS18] Craig Costello and Benjamin Smith. "Montgomery curves and their arithmetic - The case of large characteristic fields". In: *Journal of Cryptographic Engineering* 8.3 (Sept. 2018), pp. 227–240. DOI: 10.1007/s13389-017-0157-6.

[CV11] Wouter Castryck and Frederik Vercauteren. "Toric forms of elliptic curves and their arithmetic". In: *Journal of Symbolic Computation* 46.8 (2011), pp. 943–966.

[Dar+24] Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. "An Algorithmic Approach to (2, 2)-Isogenies in the Theta Model and Applications to Isogeny-Based Cryptography". In: *ASIACRYPT 2024, Part III*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15486. LNCS. Springer, Singapore, Dec. 2024, pp. 304–338. DOI: 10.1007/978-981-96-0891-1_10.

[Dar24] Pierrick Dartois. *Fast computation of 2-isogenies in dimension 4 and cryptographic applications*. Cryptology ePrint Archive, Report 2024/1180. 2024. URL: https://eprint.iacr.org/2024/1180.

[Deu41] Max Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkö rper". German. In: *Abh. Math. Semin. Univ. Hamb.* 14 (1941), pp. 197–272. ISSN: 0025-5858. DOI: 10.1007/BF02940746.

[DR73] Pierre Deligne and Michael Rapoport. "Les schémas de modules de courbes elliptiques". In: *Modular Functions of One Variable II: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*. Springer, 1973, pp. 143–316.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*. English. Vol. 228. Grad. Texts Math. Berlin: Springer, 2005. ISBN: 0-387-23229-X.

[Edw07] Harold M. Edwards. "A normal form for elliptic curves". English. In: *Bulletin of the American Mathematical Society. New Series* 44.3 (2007), pp. 393–422. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-07-01153-6.

[EH22] Jesse Elliott and Aaron Hutchinson. *Supersingular Isogeny Diffie-Hellman with Legendre Form*. Cryptology ePrint Archive, Report 2022/870. 2022. URL: https://eprint.iacr.org/2022/870.

[FJ10] Reza Rezaeian Farashahi and Marc Joye. "Efficient Arithmetic on Hessian Curves". In: *PKC 2010*. Ed. by Phong Q. Nguyen and David Pointcheval. Vol. 6056. LNCS. Springer, Berlin, Heidelberg, May 2010, pp. 243–260. DOI: 10.1007/978-3-642-13013-7_15.

[Gau07] Pierrick Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265.

[GL09] Pierrick Gaudry and David Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields Their Appl.* 15.2 (2009), pp. 246–260. DOI: 10.1016/J.FFA.2008.12.006.

[His+08] Hüseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. "Twisted Edwards Curves Revisited". In: *ASIACRYPT 2008*. Ed. by Josef Pieprzyk. Vol. 5350. LNCS. Springer, Berlin, Heidelberg, Dec. 2008, pp. 326–343. DOI: 10.1007/978-3-540-89255-7_20.

[HR19] Hüseyin Hisil and Joost Renes. "On Kummer Lines with Full Rational 2-torsion and Their Usage in Cryptography". In: *ACM Trans. Math. Softw.* 45.4 (2019), 39:1–39:17. DOI: 10.1145/3361680.

[Igu72] Jun-ichi Igusa. *Theta functions*. English. Vol. 194. Grundlehren Math. Wiss. Springer, Cham, 1972.

[IJ13] Sorina Ionica and Antoine Joux. "Pairing the volcano". In: *Math. Comput.* 82.281 (2013), pp. 581–603. DOI: 10.1090/S0025-5718-2012-02622-6.

[Koh11] David Kohel. "Arithmetic of split Kummer surfaces: Montgomery endomorphism of Edwards products". In: *International Conference on Coding and Cryptology*. Springer. 2011, pp. 238–245.

[Koh96] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley, 1996.

[KS20] Sabyasachi Karati and Palash Sarkar. "Kummer for Genus One Over Prime-Order Fields". In: *Journal of Cryptology* 33.1 (Jan. 2020), pp. 92–129. DOI: 10.1007/s00145-019-09320-4.

[Len87] Hendrik W. Lenstra Jr. "Factoring integers with elliptic curves". English. In: *Annals of Mathematics. Second Series* 126 (1987), pp. 649–673. ISSN: 0003-486X. DOI: 10.2307/1971363.

[LO77] Jeffrey C. Lagarias and Andrew M. Odlyzko. *Effective versions of the Chebotarev density theorem*. English. Algebr. Number Fields, Proc. Symp. London math. Soc ., Univ. Durham 1975, 409-464 (1977). 1977.

[LR16] David Lubicz and Damien Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (May 2016), pp. 130–158. DOI: 10.1016/j.ffa.2016.01.009.

[Mir+06] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. "An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields". In: *Appl. Math. Comput.* 176.2 (2006), pp. 739–750. DOI: 10.1016/J.AMC.2005.10.020.

[Mon87] Peter L. Montgomery. "Speeding the Pollard and elliptic curve methods of factorization". English. In: *Mathematics of Computation* 48 (1987), pp. 243–264. ISSN: 0025-5718. DOI: 10.2307/2007888.

[Mon92] Peter L. Montgomery. *An FFT extension of the elliptic curve method of factorization*. Thesis (Ph.D.)–University of California, Los Angeles. ProQuest LLC, Ann Arbor, MI, 1992, p. 162. URL: https://cr.yp.to/bib/1992/montgomery.pdf.

[Mum66] David Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354.

[Mum70] David Mumford. *Abelian varieties*. English. Vol. 5. Tata Inst. Fundam. Res., Stud. Math. London: Oxford University Press, 1970.

[Mum83] David Mumford. *Tata lectures on theta. I: Introduction and motivation: Theta functions in one variable. Basic results on theta functions in several variables. With the assistance of C. Musili, M. Nori , E. Previato, and M. Stillman*. English. Vol. 28. Prog. Math. Birkhäuser, Cham, 1983. DOI: 10.1007/978-1-4899-2843-6.

[OKS00] Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai. "Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications". In: *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Proceedings*. Ed. by Hideki Imai and Yuliang Zheng. Vol. 1751. Lecture Notes in Computer Science. Springer, 2000, pp. 238–257. DOI: 10.1007/978-3-540-46588-1_17.

[Rob23] Damien Robert. *The geometric interpretation of the Tate pairing and its applications.* Cryptology ePrint Archive, Report 2023/177. 2023. URL: https://eprint.iacr.org/2023/177.

[Rob24] Damien Robert. "Fast pairings via biextensions and cubical arithmetic". Apr. 2024. eprint: 2024/517, HAL: hal-04848028.

[RS17] Joost Renes and Benjamin Smith. "qDSA: Small and Secure Digital Signatures with Curve-Based Diffie-Hellman Key Pairs". In: *ASIACRYPT 2017, Part II*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10625. LNCS. Springer, Cham, Dec. 2017, pp. 273–302. DOI: 10.1007/978-3-319-70697-9_10.

[RS24a] Damien Robert and Nicolas Sarkis. "Computing 2-isogenies between Kummer lines". In: *IACR Communications in Cryptology* 1.1 (Apr. 9, 2024). ISSN: 3006-5496. DOI: 10.62056/abvua69p1.

[RS24b] Damien Robert and Nicolas Sarkis. "Halving differential additions on Kummer lines". Oct. 2024. eprint: 2024/1582, HAL: hal-04724019.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions.* English. Repr. of the 1971 orig. Vol. 11. Publ. Math. Soc. Japan. Princeton, NJ: Princeton Univ. Press, 1994. ISBN: 0-691-08092-5.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate texts in mathematics. Springer, 1986. ISBN: 978-3-540-96203-8.

[Sma01] Nigel P. Smart. "The Hessian Form of an Elliptic Curve". In: *CHES 2001*. Ed. by Çetin Kaya Koç, David Naccache, and Christof Paar. Vol. 2162. LNCS. Springer, Berlin, Heidelberg, May 2001, pp. 118–125. DOI: 10.1007/3-540-44709-1_11.

[Sut13] Andrew V. Sutherland. "Isogeny volcanoes". English. In: *ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012*. Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013, pp. 507–530. ISBN: 978-1-935107-00-2; 978-1-935107-01-9.

[Tat66] John Tate. "Endomorphisms of Abelian varieties over finite fields". English. In: *Inventiones Mathematicae* 2 (1966), pp. 134–144. ISSN: 0020-9910. DOI: 10.1007/BF01404549.

[VZ22] John Voight and David Zureick-Brown. *The canonical ring of a stacky curve*. Vol. 277. 1362. American Mathematical Society, 2022.

[Win13] Bruno Winckler. *Théorème de Chebotarev effectif*. 2013. DOI: 10.48550/ARXIV.1311.5715. arXiv: 1311.5715 [math.NT].

[Zyw15] David Zywina. *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*. 2015. DOI: 10.48550/ARXIV.1508.07660. arXiv: 1508.07660 [math.NT].

Appendix A. Kummer lines as stacky curves

In this section, we reinterpret the definitions of Section 2 in term of stack quotients. We will assume that we are not in characteristic two.

If E is an elliptic curve, the group scheme $\mu_2 = \{1, -1\}$ acts via $-1 \cdot P = -P$. The scheme quotient E/μ_2 (both as a geometric and categorical quotient) is the projective line $\mathbb{P}^1$.

This means that we cannot recover E directly from E/μ_2. In particular, although the action of μ_2 is ramified on the points of two torsion, E/μ_2 is still smooth. By the Nagata-Zariski purity theorem, this can happen only because the ramification locus is of codimension 1. And indeed, in dimension $g \geqslant 2$, the scheme quotient A/μ_2 of an abelian variety is no longer smooth: the non smooth locus is precisely the image of the 2-torsion.

A way to remember the ramification points is to take the stack quotient $[E/\mu_2]$. Its coarse moduli space is E/μ_2. Hence $[E/\mu_2]$ is a smooth stacky curve, and so is completely determined by the data of the coarse space $E/\mu_2 \simeq \mathbb{P}^1$, the ramification points on $\mathbb{P}^1$, and for each ramified points P_i its associated (non trivial) inertia [VZ22, Lemma 5.3.10] (the tameness condition is automatic in our case since we are not in characteristic two). In our case the inertia can only be μ_2, so it follows that $[E/\mu_2]$ is completely determined by the image of the 2-torsion points on $\mathbb{P}^1$. We recover the more elementary definition from Definition 2.3.

Now the stack quotient $[E/\mu_2]$ "remembers" E. More precisely, the map $E \to k$ yields a canonical map $\varphi : [E/\mu_2] \to B\mu_2 = [k/\mu_2]$. Recall that $B\mu_2$ is the classifying stack of (étale) μ_2-torsors: a μ_2-torsor $T \to S$ is the same as a point $S \to B\mu_2$, where T can be recovered as the pullback of the trivial torsor $i_0 : \operatorname{Spec} k \to B\mu_2$ by $S \to B\mu_2$. Likewise, a S-point $S \to [E/\mu_2]$ corresponds to a μ_2-torsor $T \to S$ with an μ_2-equivariant map $T \to E$. Like above T is given by the pullback of $E \to [E/\mu_2]$ by the point $S \to [E/\mu_2]$. We remark also that T is also the μ_2-torsor associated to the S-point $S \to [E/\mu_2] \to B\mu_2$. If k is perfect, by Hilbert 90 and Kummer theory, we have $H^1_{et}(k, \mu_n) \simeq k^*/k^{*,n}$, and if $\mu_n \subset k$, to give a μ_n-torsor X is the same as giving the smallest field extension k'/k that trivializes it (i.e. the subfield of $\overline{k}$ invariant by the inertia of the map $\operatorname{Gal}(\overline{k}/k) \to \mu_n$ associated to the torsor), whose Galois group is isomorphic to a subgroup μ_d of μ_n, and also to give the induced isomorphism $\operatorname{Gal}(k'/k) \to \mu_d$. If $n = 2$, there are only two possibilities, either $d = 1$ and $k' = k$ (X is the trivial torsor), or k'/k and k' uniquely determines X, since $\operatorname{Aut} \mu_2 = \{\mathrm{Id}\}$.

A scheme X/S can be recovered from its stack quotient $[X/G]$ via the pullback $X \simeq [X/G] \times_{BG} S$. Thus we have that $E = [E/\mu_2] \times_{B\mu_2} k$ is the pullback of $[E/\mu_2] \to B\mu_2$ by the canonical map $i_0 : \operatorname{Spec} k \to B\mu_2$ associated to the trivial torsor.

It is important to note that the reconstruction of E depends on the forgettnig map $\varphi : [E/\mu_2] \to B\mu_2$. For instance, consider k'/k the étale μ_2-torsor associated to a quadratic extension of k, then we have a corresponding map $i' : \operatorname{Spec} k \to B\mu_2$. This time, the pullback of i' by the canonical map φ gives a quadratic twist E' of E, precisely the quadratic twist associated to the μ_2-torsor k'/k.

Now, the stack quotient $[E'/\mu_2]$ is isomorphic to $[E/\mu_2]$. However, the isomorphism is not above their respective canonical maps φ, φ' to $B\mu_2$. Instead, we have the following diagram, where the leftmost and rightmost squares are pullbacks:

$$\begin{array}{ccccccccc}
E \times \mu_2 & \longrightarrow & E & & & & E' & \longleftarrow & E' \times \mu_2 \\
\downarrow & & \downarrow{\scriptstyle \pi} & & & & \downarrow{\scriptstyle \pi'} & & \downarrow \\
E & \xrightarrow{\pi} & [E/\mu_2] & \xrightarrow{\sim} & [E'/\mu_2] & & & \xleftarrow{\pi'} & E' \\
\downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} & & & & \downarrow \\
\operatorname{Spec} k & \xrightarrow{i_0} & B\mu_2 & \xleftarrow[\alpha]{\sim} & B\mu_2 & & & \xleftarrow{i_0} & \operatorname{Spec} k
\end{array}$$

Recall that if we have a G-torsor X/k corresponding to a map $x : \operatorname{Spec} k \to BG$, then x factors through $\operatorname{Spec} k \to BG \to BG$ where the first map is the canonical one $x_0 : \operatorname{Spec} k \to BG$ corresponding to the trivial torsor $\operatorname{Spec} k \times G \to \operatorname{Spec} k$, and the second one sends a G-torsor $T \to S$ to the G-torsor $T \times_G X_S \to S$. Here, $\alpha : B\mu_2 \to B\mu_2$ is the isomorphism constructed as above for the μ_2-torsor k'/k, so that $i' = \alpha \circ i_0$. Since pulling back the torsor $\operatorname{Spec} k' \to \operatorname{Spec} k$ to itself trivializes it, if we pullback the diagram above by $\operatorname{Spec} k' \to \operatorname{Spec} k$, α becomes trivial and we obtain an isomorphism $E' \to E$ over k'.

In elementary terms, given the description of $[E/\mu_2]$ in terms of the ramification locus $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in $\mathbb{P}^1$ the choice of forgetting map $[E/\mu_2] \to B\mu_2$ (hence of elliptic curve E) amount to the choice of $B \in k^*/k^{*,2}$: given $E : By^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) = h(x)$, the map $[E/\mu_2] \to B\mu_2$ is simply the map that sends $[P] : \operatorname{Spec} k \to [E/\mu_2]$ to the μ_2-torsor defined by $By^2 = h(x(P))$ (i.e. by $\pi^{-1}(x(P))$ where $\pi : E \to E/\pm 1$ is the canonical projection), where $x(P)$ is the image of $[P]$ composed with the forgetting map $[E/\mu_2] \to E/\mu_2 \simeq \mathbb{P}^1$ (this assumes that $x(P)$ is not in the ramification locus, in which case $[E/\mu_2]$ is étale locally isomorphic to E/μ_2 around $[P]$).

Once we have fixed E, hence the map $[E/\mu_2] \to B\mu_2$, then given $[P] : \operatorname{Spec} k \to [E/\mu_2]$ (not above the ramification), the torsor $\pi^{-1}([P]) = \pi^{-1}(x(P))$ associated to the map $i : \operatorname{Spec} k \to [E/\mu_2] \to B\mu_2$ determines if $x(P)$ lifts to two rational points $\pm P$ in $E(k)$. This is the case precisely when the torsor is trivial, i.e. isomorphic to $\operatorname{Spec} k \times \mu_2$. In the other cases it corresponds to a quadratic extension k'/k, and $\pm P$ live in $E(k')$. Alternatively, by the diagram above, $x(P)$ lifts to a rational point in the quadratic twist E' defined by k' (because the map $i' : \operatorname{Spec} k \to [E/\mu_2] \to B\mu_2 \to B\mu_2$, where the last map is the isomorphism induced by the torsor k'/k, corresponds to the trivial torsor). In particular, this quadratic twist E' is the unique one to which $x(P)$ lifts (over k).

In summary, the fibers of $E \to [E/\mu_2] \to E/\mu_2$ are as follows. If P is not above the ramification, we have the following pullback diagram:

$$\begin{array}{ccc}
\pi^{-1}([P]) = \pi^{-1}(x(P)) = \{P, -P\} & \longrightarrow & E \\
\downarrow & & \downarrow{\scriptstyle \pi} \\
\operatorname{Spec} k & \xrightarrow{[P]} & [E/\mu_2] \\
\downarrow & & \downarrow \\
\operatorname{Spec} k & \xrightarrow{x(P)} & E/\mu_2
\end{array}$$

And if $P = T$ is a point of two-torsion, we have instead the pullback diagram:

$$\begin{array}{ccc}
\operatorname{Spec} k & \xrightarrow{T} & E \\
\downarrow & & \downarrow{\scriptstyle \pi} \\
B\mu_2 & \longrightarrow & [E/\mu_2] \\
\downarrow & & \downarrow \\
\operatorname{Spec} k & \xrightarrow{x(T)} & E/\mu_2
\end{array}$$

Appendix B. Modular curves

In Section 5.2, we used the construction of modular curves over $\mathbb{Q}$ from [Zyw15], using the Galois theory of the étale fundamental group.

In this section we briefly describe modular curves as stacks, and refer to [DR73] for more details. First we start with the modular curves $X(n)$ as the fine moduli space (Deligne-Mumford stack) parametrizing elliptic curves with a level-n structure. There are two definition in the

literature: the first one is that of a basis (P_1, P_2) of $E[n]$ such that the Weil pairing $e_{W,n}(P_1, P_2) = \zeta$ for $\zeta \in \mu_n$ a fixed primitive n-root of unity. The corresponding curve is then defined (and smooth) over $\mathbb{Z}^{1/n}(\mu_n)$.

The second definition, more general, is to instead ask for an isomorphism $E[n] \to \mathbb{Z}/n\mathbb{Z} \times \mu_n$. The resulting curve $X(n)$ is this time defined (and smooth) over $\mathbb{Z}^{1/n}$, but it is not geometrically connected: each choice of primitive n-th root gives a connected geometric component.

Now, if $\Gamma \subset \Gamma(1)$ is some level subgroup of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, let n such that $\Gamma(n) \subset \Gamma$, and define $X(\Gamma)$ as the stacky quotient $[X(n)/(\Gamma/\Gamma(n))]$. It is not hard to see that $X(\Gamma)$ is independent of the choice of n.

In particular, this gives a construction, valid over $\mathbb{Z}[1/2]$, of $X(\Gamma^0(4))$, $X(\Gamma^0(4) \cap \Gamma(2))$ and $X(\Gamma(2,4))$ as used in Section 5.

Since our moduli curves are now fine moduli space, we have a universal elliptic curve (stack) with Γ-level structure over $X(\Gamma)$. Its automorphism group (preserving the level structure) is either μ_2 if $-1 \notin \Gamma$, or trivial if $-1 \in \Gamma$. In the later case, the generic inertia of $X(\Gamma)$ is then trivial, hence $X(\Gamma)$ is a scheme, étale locally at all points that do not admit extra automorphisms, so concretely for all elliptic curves (with level structure) with j-invariant different from $0, 1728$. If we require furthermore that $\det(\Gamma/\Gamma(n)) = (\mathbb{Z}/N\mathbb{Z})^\times$, then $X(\Gamma)$ is geometrically connected. We recover the conditions from Theorem 5.6.

It remains to tackle the question of fields of moduli vs field of definition. In general, if X is a fine Deligne-Mumford moduli stack parametrizing a class of objects, then by definition to give such an object C/k is the same as giving a point $\operatorname{Spec} k \to X$. We say that k is a field of definition of C. The fine space X also admit a coarse space X_0 (an algebraic space in general, but for our modular curves their coarse spaces are schemes), and the point $\operatorname{Spec} k \to X$ induces a point x_0 on X_0; we call the field of moduli the residual field k_0 of x_0. For instance for an elliptic curve E/k, its field of moduli is given by its j-invariant $j(E)$.

In general, the field of moduli is not a field of definition. Assume that we have two models C_1/k_1, C_2/k_2 that become isomorphic over a common algebraic closure of k_1, k_2 (so gives points on X above the same point x_0 on X_0). Let's call $C/\overline{k}$ a representative of the isomorphism class of C_1, C_2 over $\overline{k}$, then by descent theory (assuming all our fields are perfect and our inertia tame to avoid complications with inseparability) C_1/k_1 is given by a descent data from $C/\overline{k}$. But the two descent data defining C_1, C_2 may not be compatible with each other, hence may not "glue" to define a curve over $k_1 \cap k_2$.

From the stack point of view the way to understand the situation is as follows: we have a residual gerbe G_{x_0} above x_0; informally this gerbe is the category of all models C_i/k_i that are isomorphic to C over $\overline{k}$. If $C_1, C_1'/k_1$ correspond to two elements of the gerbe above the same field, then by definition they are twist of each others. So étale locally around our field of definition k_1, our category is equivalent to the category of $\mathrm{Aut}(C_1)$-torsors ($\mathrm{Aut}(C_1)$ is precisely the inertia of the corresponding point $\operatorname{Spec} k_1 \to X$): indeed the category of twists of C_1 is equivalent to the category of $\mathrm{Aut}(C_1)$-torsors. But our gerbe G_{x_0} itself may not be equivalent to a category of torsor (i.e. neutral), unless k_0 is also a field of definition, not only a field of moduli.

Now, a very nice feature of modular curves, is that all their residual gerbes are neutral:

Proposition B.1. *Let $X(\Gamma)$ be as above the modular stack of elliptic curves with a Γ-level structure, and $x : \operatorname{Spec} k \to X(\Gamma)$ a point. Then the residual gerbe at x is trivial: the field of moduli is a field of definition.*

Proof. This is [DR73, Proposition 3.2 p. 274]. For the convenience of the reader we summarize the proof. First the result is well known for $\Gamma = \{\mathrm{Id}\}$: we have explicit formulas that give an equation of an elliptic curve from its j-invariant (over the same field).

Now if we add a level structure, then x corresponds to a curve with level structure, (E, G), and we distinguish several cases. If $\mathrm{Aut}(E, G) = \mathrm{Aut}(E)$, then the obstruction for the residual gerbe at (E, G) being neutral, which lives in $H^2(k, \mathrm{Aut}(E, G))$ is the same (via the isomorphism above) to the obstruction for the residual gerbe at E to be neutral, which lives in $H^2(k, \mathrm{Aut}(E))$. But the latter is trivial by the first point, so the former too.

Otherwise, we at least have an injection $\mathrm{Aut}(E, G) \subset \mathrm{Aut}(E)$, and a map $H^2(k, \mathrm{Aut}(E, G)) \to H^2(k, \mathrm{Aut}(E))$. The image of the obstruction related to (E, G) in $H^2(k, \mathrm{Aut}(E))$ is zero by the first point. But a difficulty is that the map on the H^2 need not be injective.

If $\mathrm{Aut}(E) = \mu_n$ is isomorphic to a group of roots of unity, then it is easy to see using the long exact sequence of cohomology and Hilbert's 90 that $H^2(k, \mathrm{Aut}(E, G)) \to H^2(k, \mathrm{Aut}(E))$ is injective in that case.

The other cases are all induced by $j(E) = 0, 1728$ and the characteristic is $p = 2, 3$, in which case E is defined over $\mathbb{F}_p$, hence (E, G) is defined over a finite field $\mathbb{F}_q$. But finite fields have cohomological dimension 1, hence do not admit non trivial gerbes. □

This finishes the generalisation of Theorem 5.6. We stress that this feature is specific to the dimension 1 case, in [BL24] it is shown that moduli space of abelian varieties can have arbitrary bad obstruction: any gerbe (over one point) lives in the moduli stack $\mathcal{A}_g$ of principally polarised abelian variety of dimension g for g large enough.

We conclude this section about a discussion on twists. If $E \to X(1)$ is the universal elliptic curve, then $\mathrm{Aut}(E) = \mu_2$: the generic inertia of a point $\operatorname{Spec} k \to X(1)$ is μ_2. One can then form (using the construction from [AOV08, Appendix A]) the quotient $E/\mu_2 \to X(1)/\mu_2$ to obtain the universal Kummer line; we remark that $X(1)$ and $X(1)/\mu_2$ have the same coarse moduli space (which is isomorphic to $\mathbb{P}^1$ via the j-invariant). A similar construction holds for the universal elliptic curve with level structure over $X(\Gamma)$ when $-1 \notin \Gamma$.

So for a generic Kummer line $E/\pm 1$, $\mathrm{Aut}(E/\pm 1) = \mathrm{Aut}(E)/\pm 1$ is trivial (this also holds in higher dimension). So a (generic) Kummer line does not have twists: if we have two models of Kummer lines defined over k and isomorphic over $\overline{k}$, then this isomorphism is automatically rational.

The exceptions are as always the Kummer lines associated to the elliptic curves of j-invariant $0, 1728$.

Example B.2 (Twists of Kummer lines)**.** *We first look at the twists of the Kummer line of $E : y^2 = x^3 - x$ of j-invariant 1728; we will assume that k is not of characteristic 2 for simplicity. Its ramification is given by, along the point at infinity, $x = -1, 0, 1$. The map $x \mapsto -x$ is a non trivial automorphism of $E/\pm 1$, so the Kummer line admits quadratic twists.*

Explicitly, the curves $E_a : y^2 = x^3 + ax$ are all isomorphic to E over $\overline{k}$. The corresponding Kummer line has ramification given by $x = 0, a^{1/2}, -a^{1/2}$ (and the point at infinity).

If $\xi = (a_2/a_1)^{1/2}$, then the map $x \mapsto \xi x$ is an isomorphism between the Kummer line of E_{a_1} and the Kummer line of E_{a_2}. But this isomorphism is rational if and only if ξ is rational. So each element in $k^*/k^{*,2} \simeq H^1(k, \mu_2)$ gives a different quadratic twist.

$E/\pm 1$ has a Legendre form with $\lambda = -1$, the other Legendre invariants are $\lambda = 2, 1/2$ (we only have 3 invariants because of the extra automorphism). The other quadratic twists of this Kummer line do not have rational 2-torsion, hence no Legendre form (nor theta form). It also have a theta model (possibly over an extension) with theta constants $(\zeta_8 : 1)$, where ζ_8 is a primitive 8-root of unity. The other theta constants are: $(\zeta_8^3 : 1), (\zeta_8^5 : 1), (\zeta_8^7 : 1), (\zeta_8 + 1 : \zeta_8 - 1), (\zeta_8^3 + 1 : \zeta_8^3 - 1), (\zeta_8^5 + 1 : \zeta_8^5 - 1), (\zeta_8^7 + 1 : \zeta_8^7 - 1), (\zeta_8(1 + \zeta_8) : \zeta_8(1 - \zeta_8)), (\zeta_8^3(1 + \zeta_8^3) : \zeta_8^3(1 - \zeta_8^3)), (\zeta_8^5(1 + \zeta_8^5) : \zeta_8^5(1 - \zeta_8^5)), (\zeta_8^7(1 + \zeta_8^7) : \zeta_8^7(1 - \zeta_8^7))$.

We can recover possible Montgomery models (possibly over an extension) associated to these three Legendre models of $E/\pm 1$ by letting $\alpha = \sqrt{\lambda}$ and $A = -\alpha - 1/\alpha$. For $\lambda = -1$, we find

$\alpha = i$ and $A = 0$. For $\lambda = 2$, we find $\alpha = \sqrt{2}$ and $A = -3\sqrt{2}/2$, or $\alpha = -\sqrt{2}$ and $A = 3\sqrt{2}/2$. But $E/\pm 1$ can be isomorphic to the first Montgomery model over the base field only if -1 is a square in k, and to the second and third only when 2 is a square in k.

Now we look at the twists of the Kummer line of $E : y^2 = x^3 - 1$ of j-invariant 0; we will assume that k is not of characteristic 3 for simplicity. The ramification is given by the point at infinity and $x = 1, j, j^2$ where j is a third root of unity.

If $\mu_3 \subset k$, then $x \mapsto jx$ is an automorphism of the Kummer line, so it admits cubic twists. The curves $E_b : y^2 = x^3 + b$ are all isomorphic to E over $\overline{k}$. The corresponding Kummer line has ramification given by $b^{1/3}, jb^{1/3}, j^2b^{1/3}$ (and the point at infinity). If $\xi = (b_2/b_1)^{1/3}$, then the map $x \mapsto \xi x$ is an isomorphism between the Kummer line of E_{b_1} and the Kummer line of E_{b_2}. But this isomorphism is rational if and only if ξ is rational. So each element in $k^*/k^{*,3} \simeq H^1(k, \mu_3)$ gives a different cubic twist.

If $\mu_3 \not\subset k$, then over k the Kummer line does not have automorphisms and do not admit twists over k; but it will admit twists over $k(j)$.

$E/\pm 1$ has a Legendre form with $\lambda = \zeta_6$, where $\zeta_6^6 = 1$ is a primitive 6th root of unity. The other Legendre invariant is ζ_6^5 (the automorphism is of order 3 so there are only 2 Legendre invariants).

Appendix C. Graph of the subgroups of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$

Let $f : \mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ be the reduction map modulo 4. For $M, N \geqslant 1$ two integers, we will deal with the following groups:

- $\Gamma(N) = \{g \in \mathrm{SL}_2(\mathbb{Z}) \mid g \equiv I \bmod N\}$
- $\Gamma_1(N) = \{g \in \mathrm{SL}_2(\mathbb{Z}) \mid g \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod N\}$
- $\Gamma_0(N) = \{g \in \mathrm{SL}_2(\mathbb{Z}) \mid g \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod N\}$
- $\Gamma(M, MN) = \{g \in \mathrm{SL}_2(\mathbb{Z}) \mid g \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod MN, g \equiv I \bmod M\} = \Gamma(M) \cap \Gamma_0(MN)$

Column on the left list the order of the groups. The notations on the Fig. 6 are as follows for a group ${}_cG_{\texttt{idx}}$:

- The relevant G will be of the form $f(H)$ where H is a subgroup of $\Gamma(4)$.
- For the groups that are not of this form, they are written G_a where a is the index in Magma when listing subgroups of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$.
- c is the number of conjugacy classes of G in $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$.
- If present, `idx` is the label of the corresponding modular curve on the LMFDB (beta feature as of writing).

Remark C.1. *Note that, aside from level 2 groups which can be seen as subgroups of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ (and therefore trivially verifies $-I \in G$ and $\det G = (\mathbb{Z}/2\mathbb{Z})^*$), none of these respect the conditions of Theorem 5.6 (indeed, $\det G = \{1\} \neq (\mathbb{Z}/4\mathbb{Z})^*$, and some of them doesn't have $-I \in G$, like $\Gamma_1(4)$). It is then implicit that we consider the smallest subgroup H in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ that contains G, $-I$ and such that $\det H = (\mathbb{Z}/4\mathbb{Z})^*$.*

This amounts to looking at the following representation $\widetilde{\rho}_{E,4} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_4)) \to \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ rather than $\rho_{E,4} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ as defined in Definition 5.5.

$\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ is labelled `48.30` on LMFDB and $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ is `96.195` (beta feature as of writing).

Red nodes correspond to the models studied in this paper, which are from top to bottom: Montgomery, Theta twisted, Theta.

We also have:

- $G_{18} = \langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right) \rangle$.
- $G_{16} = \langle \left(\begin{smallmatrix} 1 & 3 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle$.

- $G_{15} = \langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right) \rangle$.
- $G_{13} = \langle \left(\begin{smallmatrix} 1 & 3 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right) \rangle$.
- $G_{11} = \langle \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle$.
- $G_9 = \langle \left(\begin{smallmatrix} 1 & 3 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right) \rangle$.
- $G_8 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right) \rangle$.
- $G_6 = \langle \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right) \rangle$.
- $G_5 = \langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle$.
- $G_4 = \langle \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right) \rangle$.

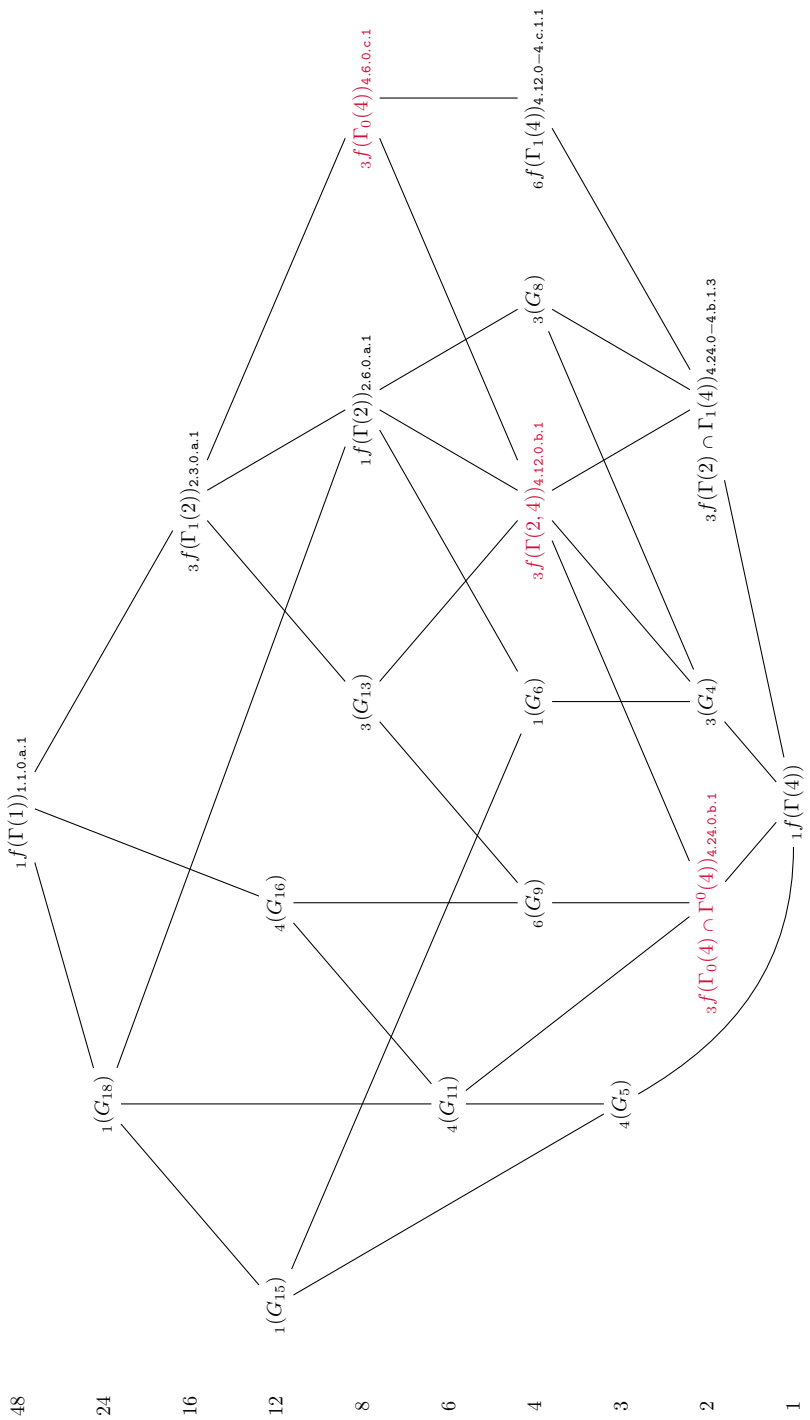


FIGURE 6. Subgroups of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$

Institut de mathématiques de Bordeaux (Univ. Bordeaux, CNRS, Bordeaux INP) and Inria Bordeaux, France

Email address: razvan.barbulescu@u-bordeaux.fr

Email address: damien.robert@inria.fr

Email address: nicolas.sarkis@math.u-bordeaux.fr