A CLASSIFICATION OF ECM-FRIENDLY FAMILIES USING MODULAR CURVES

RAZVAN BARBULESCU AND SUDARSHAN SHINDE

Abstract. In this work, we establish a link between the classification of ECM-friendly curves and Mazur's program B, which consists in parameterizing all the families of elliptic curves with exceptional Galois image. Building upon two recent works which treated the case of congruence subgroups of prime-power level which occur for infinitely many j-invariants, we prove that there are exactly 1525 families of rational elliptic curves with distinct Galois images which are cartesian products of subgroups of prime-power level. This makes a complete list of rational families of ECM-friendly elliptic curves, out of which less than 25 were known in the literature. We furthermore refine a heuristic of Montgomery to compare these families and conclude that the best 4 families which can be put in $a = -1$ twisted Edwards' form are new.

1. Introduction

Integer factorization is an important problem in algorithmic number theory and cryptology. The factoring algorithms split into two classes: on the one hand those whose costs depend only on the size of the integer N to factor, like the quadratic sieve and the number field sieve (NFS) [Pol93,LLJMP93] and on the other hand those whose costs depend on the size of the factors we are looking for, up to a polynomial factor in the bit size of N, as it is the case for the trial division and the elliptic curve method of factorization (ECM) [LJ87]. At the first sight, only the first class is relevant in cryptology because the numbers to factor in the RSA system are of the form $\mathrm{N} = pq$ where p and q are two primes of equal bit size. However, ECM is used in NFS and, in computations of cryptologic relevance, ECM takes an important part of the cost of NFS. Another important problem in cryptology is that of computing discrete logarithms, i.e. in a cyclic group G with generator g, given g^x, find x. For this problem as well, the best known algorithm is a variant of NFS.

In brief, ECM works as follows: given an integer N with an unknown prime factor p, one first chooses a rational elliptic curve E and a point $\mathrm{P} \in \mathrm{E}(\mathbb{Q})$ with denominators relatively prime to N. One then computes $\mathrm{P_M} := [\mathrm{M}] \cdot \mathrm{P}$, while keeping the coordinates modulo N. If $\#\,\mathrm{E}(\mathbb{F}_p)$ divides M, then $\mathrm{P_M}$ is the neutral element of $\mathrm{E}(\mathbb{F}_p)$ or it is congruent to $(0:0:0)$ mod p. The z-coordinate of P_M in the Weierstrass equation being divisible by p, one finds a multiple of p by computing $\gcd(z, \mathrm{N})$.

The choice of M varies from one implementation to another, but as a first approximation, we take $\mathrm{M} = \mathrm{B}!^{\lceil \log_2 \mathrm{B} \rceil}$ for some integer B. The algorithm succeeds if $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth i.e. all its prime factors are less than B. By Hasse's theorem, we have $\#\,\mathrm{E}(\mathbb{F}_p) \approx p$. It is then natural to compare the chances of $\#\,\mathrm{E}(\mathbb{F}_p)$ being B-smooth with the chances of an integer of the same size as p being B-smooth.

In the version of ECM proposed by Lenstra [LJ87], one selects uniformly random integers x, y and a in $[0, p-1]$ and sets $\mathrm{E} : y^2 = x^3 + ax + b$ such that $(x, y) \in \mathrm{E}(\mathbb{F}_p)$. Lenstra [LJ87, Prop 2.7]

proved that the proportion of elliptic curves selected in this manner for which $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth equals, up to a factor $1/\mathcal{O}(\log p)$, the proportion of B-smooth integers in $[p-\sqrt{p}, p+\sqrt{p}]$.

In cryptologic applications of ECM, one uses elliptic curves from parameterized sets. We shall refer to these parameterized sets as families of elliptic curves. Soon after ECM was published, Montgomery [Mon87] introduced a parameterization, $\mathrm{B}y^2 = x^3 + \mathrm{A}x^2 + x$, which speeds up the point addition and doubling. Montgomery also suggested to use elliptic curves with 12 and 16 rational torsion points. Indeed, if an elliptic curve E has good reduction modulo p for a prime p coprime to cardinality of the torsion subgroup $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$, then $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$ embeds in $\mathrm{E}(\mathbb{F}_p)$. So, the torsion order $\#\,\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$ divides $\#\,\mathrm{E}(\mathbb{F}_p)$ for $p > 7$. Experimentally, this increases the proportion of primes p where $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth.

Mazur's theorem states that there are 15 possible torsion structures over $\mathbb{Q}$ and the families corresponding to them have been considered for ECM [AM93, BBLP13, BBL10]. However, the torsion subgroup is not the complete story because two families can have the same torsion subgroup yet different proportions of primes modulo which the cardinality is B-smooth. Indeed, the Suyama family [Mon87, p. 262] has 6 rational torsion points but has better performance in ECM than a generic curve with the same torsion. Also note that, if E is a Suyama curve, then 12 divides $\#\,\mathrm{E}(\mathbb{F}_p)$ for all primes p of good reduction, whereas only the divisibility by 6 is guaranteed for an arbitrary curve with the same torsion.

Brier and Clavier [BC10] found families defined over $\mathbb{Q}$ with large torsion over $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unity and $n = 3, 4, 5$. Heer, McGuire and Robinson [HMR16] presented more rational families with large torsion over $\mathbb{Q}(\zeta_3)$ and noted experimentally that they are better in ECM than elliptic curves having the same torsion over $\mathbb{Q}$.

Barbulescu, Bos, Bouvier, Kleinjung and Montgomery [BBB+13] noted that the torsion subgroup over number fields do not explain the behaviour of curves in ECM. Indeed, they proposed subfamilies of the Suyama family which have the same torsion as the Suyama family over any fixed number field and yet they have better smoothness properties. Similarly, they found families of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ having better properties than the generic curves having the same torsion. They proved that this difference is due to the Galois group of m-torsion field, $\mathbb{Q}(\mathrm{E}[m])$, which is generated by the coordinates of the m-torsion points of E over $\overline{\mathbb{Q}}$.

We use the notations of Serre [Ser71]. Let P_1 and P_2 be such that $\mathrm{E}(\overline{\mathbb{Q}})[m] = \frac{\mathbb{Z}}{m\mathbb{Z}}\mathrm{P}_1 + \frac{\mathbb{Z}}{m\mathbb{Z}}\mathrm{P}_2$. We call the mod m Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of E the map:

$$\begin{array}{rccc} \rho_{\mathrm{E},m}: & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \to & \mathrm{Aut}(\mathrm{E}[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ & \rho & \mapsto & \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right), \end{array}$$

where $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ such that $\sigma(\mathrm{P}_1) = a\mathrm{P}_1 + b\mathrm{P}_2$ and $\sigma(\mathrm{P}_2) = c\mathrm{P}_1 + d\mathrm{P}_2$. We refer to $\mathrm{Im}\rho_{\mathrm{E},m}$ as mod m Galois image and the integer m as the level of $\mathrm{Im}\rho_{\mathrm{E},m}$. Furthermore, if $\rho_{\mathrm{E},m}$ is non-surjective, we say mod m Galois image is exceptional.

In a similar manner, for a prime ℓ, we define $\rho_{\mathrm{E},\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\mathrm{E}[\ell^\infty]) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\rho_{\mathrm{E}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\mathrm{E}_{\mathrm{torsion}}) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$. Serre's open image theorem [Ser71] states that, for an elliptic curve E without complex multiplication, $\rho_{\mathrm{E},\ell}$ is surjective for all but finitely many primes ℓ and there exists an integer m such that $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Im}\rho_{\mathrm{E}}] = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{Im}\rho_{\mathrm{E},m}]$.

Given a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, Mazur's program B [SZ06, page 109] consists in classifying all elliptic curves E such that $\mathrm{Im}\rho_{\mathrm{E}} \subset \mathrm{H}$, up to conjugacy. Shimura's theory [Shi71] states that the set of these elliptic curves can be parameterized by the modular curve X_{H}.

Sutherland and Zwyina [SZ17] computed the equations of modular curves X_H for $H \subset GL_2(\mathbb{Z}/m\mathbb{Z})$ when $-I \in H$ and m is a prime-power. Rouse and Zureick-Brown [RZB15] obtained the complete classification when m is a power of 2.

In this work, we are interested in methods which, given an integer m, find all the possible images of $\rho_{E,m}$ and furthermore obtain families of curves E for these images. We present two methods. The first one in Section 2 is based on the computations of all the subfields of a function field. And, the second one in Section 3 is based on the theory of modular curves. In the same section, we recall the recent results on Mazur's program B and complete the work of Sutherland and Zywina by giving parameterizations of the families associated to subgroups of prime-power level which do not contain $-I$.

Then, in Section 4, we consider the subgroups H of $GL_2(\mathbb{Z}/m\mathbb{Z})$ for any interger m which are isomorphic to the cartesian product of their projections modulo prime-power divisors of m (see Def. 4.1). We solve Mazur's program B for cartesian prodcuts which occur as Galois images for infinitely many elliptic curves with distinct j-invariants:

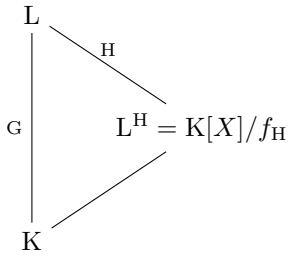
Theorem 4.1 *There are exactly* 1525 *subgroups of* $GL_2(\widehat{\mathbb{Z}})$ *which are cartesian and occur as Galois images for infinitely many* j*-invariants.*

Surprisingly, we obtain that the ECM-friendly families from the literature are in this list (see Section 4.3). In Section 5, we give a new point of view on a heuristic of Montgomery to rank ECM-friendly curves and conclude that the best 4 families which can be put in $a = -1$ twisted Edwards' form are new.

2. The subfields approach

Given an integer m, we want to parameterize, for each subgroup H of $GL_2(\mathbb{Z}/m\mathbb{Z})$, the set of rational pairs (a, b) such that, for $E : y^2 = x^3 + ax + b$, we have $\mathrm{Im}\rho_{E,m} \subset H$, up to conjugacy in $GL_2(\mathbb{Z}/m\mathbb{Z})$. More generally, given a rational parameterization $a = a(e)$ and $b = b(e)$ of Galois group G, we want to further parameterize $e = e(t)$ such that $\mathrm{Im}\rho_{E,m} \subset H$ for a subgroup of G. In this section, we give a solution based on the computation of the subfields of a function field. It is simple and feasible (For example, level 8 of Montgomery curves).

Let L be the m-torsion field of E. One computes a defining polynomial of L over $K = \mathbb{Q}(a, b)$ (resp. $\mathbb{Q}(e)$) [BBB+13, Section 2.2]. One then computes $G = \mathrm{Gal}(L/K)$. For each subgroup H of G, one computes a defining polynomial f_H of the fixed subfield L^H.



The pairs $(a, b) \in K^2$ for which $G \subset H$ are such that $\exists\, t \in K,\ f_H(a, b, t) = 0$. (resp. the parameters $e \in K$ for which $G \subset H$ are such that $\exists\, t \in K,\ f_H(a(e), b(e), t) = 0$.)

Let $\mathcal{C}$ be a plane curve and K a number field and let g be its genus. If $g \geq 2$, Faltings' theorem implies that there is no parameterization of the K-rational points of $\mathcal{C}$, that is to say, the set of points is finite. If $g = 1$, we use an algorithm from [vH95] (implemented in u MAPLE's "algcurves"

package) to put it in Weierstrass form. Note that if this algorithm fails to find a rational point on $\mathcal{C}$, the user must provide such a point; we succeed in doing so in all the computations in this work.

Cremona's algorithm [Cre01] (implemented in SAGE) enables one to compute the rank of an elliptic curves and generators. Note that the search bounds of the algorithm can make the computations impractical; in this work, we succeed in either certifying that the rank is 0 or in finding generators of the Mordell-Weil group.

If $g = 0$, we use an algorithm from [vH97] (implemented in using MAPLE's "algcurves" package) to parameterize it. Note that this algorithm too is not proven to find a rational point but in all the examples treated in this work, the algorithm succeeds.

Let us illustrate this method with the following example.

2.1. **The case of twisted Edwards' curves.** [Section 3.4.1 in [BBB+13]] We consider a subfamily of twisted Edwards' curves $\mathcal{E}_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ given by $a = -1$ and $d = -e^4$. We set $\mathrm{L} = \mathbb{Q}(e)(\mathcal{E}_{-1,-e^4}[8])$. Using MAPLE, we obtain that $[\mathrm{L} : \mathbb{Q}(e)] = 32$. We are interested in finding all the subfamilies of $\mathcal{E}_{-1,-e^4}$ i.e. all the parameterizations $e = e(t)$ for which the degree of L is less than 32. We note that the existence of Weil pairing implies that $\mathbb{Q}(\zeta_8) \subset \mathrm{L}$ [Sil08, III.8]. Thus to simplify the computations, we proceed in two steps: first we compute equations for the subfields containing $\mathrm{K} := \mathbb{Q}(\zeta_8) = \mathbb{Q}(e)(\sqrt{-1}, \sqrt{2})$.

Using MAPLE's implementation of an algorithm in [VHKN13], we compute the quadratic subfields between K and L as shown in the following diagram.

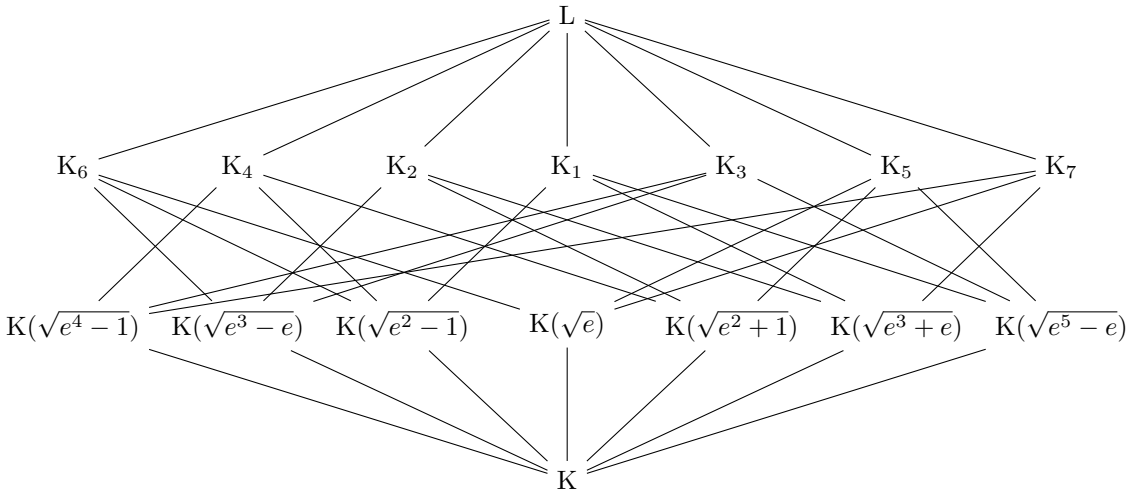


FIGURE 1. Subfields of $\mathrm{L} = \mathbb{Q}(e)(\mathrm{E}_e[8])$ over $\mathrm{K} = \mathbb{Q}(\zeta_8)(e)$ where $\mathrm{E}_e : y^2 - x^2 = 1 - e^4x^2y^2$. The fields $\mathrm{K}_1, \ldots \mathrm{K}_7$ are the compositums of pairs of quadratic fields.

We then consider the curves $\mathcal{C}$ that define these quadratic subfields. For each of them, we note the genus of the associated plane curve. One of the curves has genus 2 so there are only finitely many points. For the curves with genus 1, we compute their Weierstrass forms using MAPLE's "algcurves" package based on [VH94]. However, using MAGMA, we see that all the genus 1 curves have rank 0 so the corresponding families are finite. We summarize it in the table below.

defining polynomial of $\mathcal{C}$	genus	$\#\mathcal{C}(\mathbb{Q}(\zeta_8))$ is infinite ?
$x^2 - e$	0	yes
$x^2 - (e^2 + 1)$	0	yes
$x^2 - (e^2 - 1)$	0	yes
$x^2 - (e^4 - 1)$	1	no
$x^2 - (e^3 + e)$	1	no
$x^2 - (e^3 - e)$	1	no
$x^2 - (e^5 - e)$	2	no

We are thus left with the three curves of genus 0. For each curve, we start by finding a parameterization, then by computing the subfamilies.

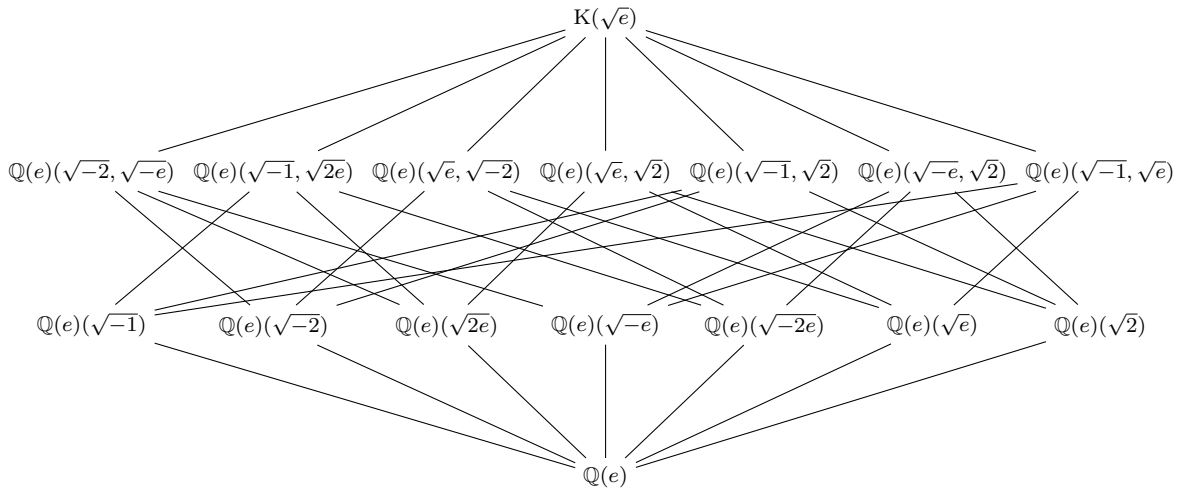
(1) We parameterize the curve of equation $x^2 - e = 0$ by $e(t) = t^2$. The fields of above $\mathbb{Q}(\sqrt{e})$ are defined by the relative polynomials $x^2 - (t^4 + 1)$, $x^2 - (t^4 - 1)$ and $x^2 - (t^8 - 1)$. The first two define elliptic curves with rank 0 and the last one has genus 3.

(2) We parameterize the curve of equation $x^2 - (e^2 + 1) = 0$ by $e(t) = \frac{t^2-1}{2t}$. The fields of above $\mathbb{Q}(\sqrt{e^2 + 1})$ are defined by the relative polynomials $x^2 - t(t^2 + 1)$, $x^2 - (t^4 + 6t^2 + 1)$ and $x^2 - t(t^2 + 1)(t^4 + 6t^2 + 1)$. Once again, the first two define elliptic curves of rank 0 and the last one has genus 3.

(3) We parameterize the curve of equation $x^2 - (e^2 - 1) = 0$ by $e(t) = \frac{t^2+1}{2t}$. The fields of above $\mathbb{Q}(\sqrt{e^2 - 1})$ are defined by the relative polynomials $x^2 - t(t^2 - 1)$, $x^2 - (t^4 - 6t^2 + 1)$ and $x^2 - t(t^2 - 1)(t^4 - 6t^2 + 1)$. Here too, the first two define elliptic curves of rank 0 and the last one has genus 3.

We deduce that the only fields between K and L corresponding to families are $\mathrm{K}(\sqrt{e})$, $\mathrm{K}(\sqrt{e^2 + 1})$ and $\mathrm{K}(\sqrt{e^2 - 1})$.

Thus if a field F between $\mathbb{Q}(e)$ and L correspond to a rational family then the field $\langle \mathrm{F}, \mathrm{K} \rangle$ also correspond to a rational family. So, in order to compute the families defined over $\mathbb{Q}(e)$, we consider the subfields of $\mathrm{K}(\sqrt{e})$, $\mathrm{K}(\sqrt{e^2 + 1})$ and $\mathrm{K}(\sqrt{e^2 - 1})$. For the first one, we consider the subfield between $\mathbb{Q}(e)$ and $\mathrm{K}(\sqrt{e})$), as represented in the following subfields diagram.



Three of the defining polynomials of the quadratic subfields in the diagram correspond to curves with no rational points and the others are parameterized by $e = t^2$, $e = -t^2$, $e = 2t^2$ and $e = -2t^2$. As the degree of e in $\mathcal{E}_{-1,-e^4}$ is even, there is only one family for $e = t^2$ and $e = -t^2$. Thus in this case, we have 2 distinct subfamilies. We need not consider the fields of degree 4 because they contain at least one of $\sqrt{-1}$, $\sqrt{-2}$ and $\sqrt{2}$ which lead to polynomials systems without rational solutions.

Similarly, for the fields $\mathrm{K}(\sqrt{e^2+1})$ and $\mathrm{K}(\sqrt{e^2-1})$, each gives 2 subfamilies given by $e^2+1 = t^2$, $e^2+1 = 2t^2$ and $e^2-1 = t^2$, $e^2-1 = 2t^2$. We have proven the following result.

Proposition 2.1. *There are exactly* 6 *rational subfamilies of the family* $\mathrm{E}_{-1,-e^4}$.

Out of these families, four were presented in [BBB+13] and the two described by $2(e^2 \pm 1) = t^2$ are new.

3. The Modular curves approach

An alternative approach to the one with subfields is due to the following theorem from Shimura's theory.

Theorem 3.1 ([Shi71])**.** *Let* E *be an elliptic curve such that* $j(\mathrm{E}) \notin \{0, 1728\}$, N *a positive integer and* H *a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ *such that* $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right) \in \mathrm{H}$ *and* $\det(\mathrm{H}) = (\mathbb{Z}/\mathrm{N}\mathbb{Z})^*$. *Then there exists a polynomial* $X_{\mathrm{H}}(j,t)$ *such that* $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\mathrm{N}])/\mathbb{Q})$ *is conjugated to a subgroup of* H *if and only if* $\exists\, t_0 \in \mathbb{Q}$ *such that* $X_{\mathrm{H}}(j(\mathrm{E}), t_0) = 0$.

In this section, the matrix $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$ plays an important role and we denote it by $-\mathrm{I}$.

For a modern description of the theory, we refer to [Zyw15, Sec 3]. The main ingredient of the computations is the field of modular functions of level N which we will discuss briefly.

Let $\mathbb{H}$ be the upper half complex plane i.e. the set of complex numbers with positive imaginary parts. Let $\mathcal{F}_{\mathrm{N}}$ be the set of meromorphic functions f on $\mathbb{H}$ which are invariant by linear fractional action of the principal congruence subgroup of level N such that the coefficients of q-expansion of f are in $\mathbb{Q}(\zeta_{\mathrm{N}})$. Let j be the modular j-invariant. Then $\mathcal{F}_{\mathrm{N}}$ is a Galois extension of $\mathbb{Q}(j)$ with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})/\{\pm 1\}$ [Shi71, Ch. 6, Sec. B], [Zyw15, Prop. 3.1]. Let $\mathcal{F}_{\mathrm{N}}^{\mathrm{H}}$ be the fixed field under the action of $\mathrm{H} \subset \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})/\{\pm 1\}$. Finally, the modular curve of H is the plane curve associated with the defining polynomial of the function field extension $\mathcal{F}_{\mathrm{N}}^{\mathrm{H}}$. The computation of X_{H} is done in two steps:

(1) We compute a system of modular functions which generate the field $\mathcal{F}_N$; this allows us to find a primitive element h of the extension $\mathcal{F}_{\mathrm{N}}^{\mathrm{H}}/\mathbb{Q}(\zeta_{\mathrm{N}}, j)$. (it is called hauptmodul when H has genus 0).
(2) We compute the minimal polynomial of h which defines the curve X_{H}.

We refer to [SZ17, Sec 2] for a complete description of the method for prime-power level. Rouse and Zureick-Brown [RZB15] computed all the subgroups $\mathrm{H} \subset \mathrm{GL}_2(\mathbb{Z}_2)$ which can occur as mod 2^∞ Galois image for at least one elliptic curve $\mathrm{E}/\mathbb{Q}$ without complex multiplication. They proved that there are 1208 groups which can occur as $\mathrm{Im}\rho_{\mathrm{E},2^\infty}$. Out of them, 1200 groups occur for infinitely many elliptic curves with distinct j-invariants and 8 for finitely many j-invariants. For this, they first deal (in Sec. 4) with 727 subgroups such that $-\mathrm{I} \in \mathrm{H}$ and prove that for 194 of them $\mathrm{X}_{\mathrm{H}}(\mathbb{Q})$ is infinite. Then, (in Sec. 5) they compute parameterizations for the 1006 subgroups H that do not contain $-\mathrm{I}$.

Sutherland and Zywina [SZ17] computed the complete list of subgroups $H \subset GL_2(\mathbb{Z}_\ell)$, for all primes ℓ, such that $-I \in H$, which can occur as mod ℓ^∞ Galois images for infinitely many elliptic curves with distinct j-invariants. A list of parameterizations of the corresponding modular curves X_H is given in the online complement of their article. For each subgroup H containing $-I$, they found the list of subgroups H', up to conjugacy, with surjective determinant such that $-I \notin H$ and $H = \langle -I, H' \rangle$. An argument that we will see below guarantees that, for each j-invariant whose curves have the Galois image contained in H, there exists exactly one elliptic curve (up to isomorphism over $\mathbb{Q}$) whose Galois image is contained in H', up to conjugacy in H. Hence, without computing parameterizations of the elliptic curves whose Galois images do not contain $-I$, Sutherland and Zywina concluded that there are exactly 47 (resp. 23, 15, 2, 11) proper subgroups of $GL_2(\mathbb{Z}_\ell)$ for $\ell = 3$ (resp. $5, 7, 11, 13$) which can occur as Galois images for infinitely many elliptic curves with distinct j-invariants, and none for other odd primes.

Remark: Theorem 3.3 of [SZ17] is applicable to all totally real number fields and generalizes to arbitrary number fields with a uniform bound on subgroups of genus 0 and 1. Thus, over any number field, one can make a similar classification.

3.1. **Parameterizations when $-I \notin H$.** Two curves with the same j-invariant can have different Galois images. For example, an elliptic curve has a rational point P of order 3 if, and only if, its mod 3 Galois image is contained, up to conjugacy, in the group of matrices $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Indeed, one can choose a basis of $E[m]$ containing P. Then, as P is rational, it is fixed by every automorphism. This ensures that the first column of the image of any automorphism is $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Consider the set of pairs $(a, b) \in \mathbb{Q}^2$ such that for $E : y^2 = x^3 + ax + b$, there exists a rational x_3 such that $\Psi_3(x_3) = 0$, where Ψ_3 is the third division polynomial of E. Then, among the set of curves $dy^2 = x^3 + ax + b$, which have the same j-invariant, only those such that $(x_3^3 + ax_3 + b)/d$ is a rational square, have a rational point of order 3. Hence, when $-I \notin H$, we have to parameterize the pairs (a, b) rather than the j-invariants.

The following result gives a method to parameterize the set of curves whose Galois image is in a subgroup H which does not contain $-I$. We put $\tilde{H} = \langle -I, H \rangle$. If $X_{\tilde{H}}$ is a conic with a rational point then we parameterize it as $j = j(t)$ and apply the following lemma for $K = \mathbb{Q}(t)$, $a = -3j(j - 1728) \in K$ and $b = -2j(j - 1728)^2 \in K$.

Lemma 3.1 ([RZB15] Sec. 5)**.** *Let $K = \mathbb{Q}(t)$ (resp. $\mathbb{Q}$). Let $\tilde{H} \subset GL_2(\mathbb{Z}/N\mathbb{Z})$ such that $-I \in \tilde{H}$. Let $H \subset \tilde{H}$ such that $-I \notin H$ and $\tilde{H} = \langle -I, H \rangle$. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over K such that $\mathrm{Im}\rho_{E,N} = \tilde{H}$. Then there exists a unique squarefree d in $\mathbb{Z}[x]$ (resp. in $\mathbb{Z}$) such that $\mathrm{Gal}(K(E_d[N])/K) \subset H$, where $E_d : dy^2 = x^3 + ax + b$. Furthermore, the value of d is in the finite set of squarefree elements of $\mathbb{Z}[t]$ (resp. $\mathbb{Z}$) whose prime factors divide either the numerator or the denominator of $N \cdot (4a^3 + 27b^2)$.*

In the light of the above lemma, we have a method, presented in [RZB15], which allows us to parameterize the curves corresponding to the subgroups of a group $\tilde{H}$ containing $-I$ whose modular curve is a conic. Once we parameterize the pairs $(a = a(t), b = b(t))$ such that $y^2 = x^3 + ax + b$ has the Galois image in $\tilde{H}$, we proceed in two steps:

(1) We compute the list of prime factors $p_1, \ldots, p_k$ of $N \cdot (4a^3 + 27b^2)$ and enumerate the products $d = (-1)^{e_0} \prod_{i=1}^{k} p_i^{e_i}$ where $e_0, \ldots, e_k \in \{0, 1\}$. Test if the field $K(E[N])$ contains a root of $x^2 - d$ to obtain the list of its quadratic subfields.
(2) We make the list of subgroups H of $GL_2(\mathbb{Z}/N\mathbb{Z})$ such that $\langle H, -I \rangle = \tilde{H}$ and $\det H = (\mathbb{Z}/N\mathbb{Z})^*$ and $-I \notin H$. For each $d(t)$ corresponding to quadratic subfields, we eliminate

all but one subgroup H by giving numerical values to t and computing the Galois image of $d(t)y^2 = x^3 + ax + b$.

Example 3.1. Consider the case of $\mathrm{H} = \langle \left(\begin{smallmatrix} 0 & 1 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 2 \end{smallmatrix}\right) \rangle \subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. According to [SZ17, Tab. 1], the set of rational triples (d, a, b) such that for $\mathrm{E} : dy^2 = x^3 + ax + b$, $\mathrm{Im}\rho_{\mathrm{E},3}$ contained in H are such that there exist rationals t and λ such that $a = -3\lambda^2(t+27)(t+3)$ and $b = -2\lambda^3(t^2+18t-27)(t+27)$. The prime factors of $3(4a^3+27b^2)$ are 2, 3, t and $(t+27)$. Out of the 32 squarefree possible values of d, the only squares in $\mathbb{Q}(t)(\mathrm{E}[3])$ are $d = (t+27)$, $d = -3(t+27)$ and $d = -3$.

There are three subgroups of H of index 2, out of which two have surjective determinant and do not contain $-\mathrm{I}$: $\mathrm{H}_1 = \langle \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 2 \end{smallmatrix}\right) \rangle$ and $\mathrm{H}_2 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 2 \end{smallmatrix}\right) \rangle$.

For numerical values t_0 of t (e.g. $t_0 = 5$), we compute the image of $\rho_{\mathrm{E}_{d_1(t=t_0)},3}$ and $\rho_{\mathrm{E}_{d_2(t=t_0)},3}$ using the scripts in the online complement [BS19] and obtain that $d_1 = t + 27$ corresponds H_1 and $d_2 = -3(t+27)$ to H_2. Lemma 3.1 allows to conclude that, if the Galois image of E_{d_1} is not contained in H_2 for one numerical value it is not contained for any $t \in \mathbb{Q}$.

The work of Zywina [Zyw15] presents parameterizations corresponding to the groups which do not contain $-\mathrm{I}$, but only for prime levels. We completed the classification for the remaining prime-power cases ℓ^k where ℓ is odd. It is summarized in the following theorem. Note that two subgroups of H, corresponding to different quadratic subfields, can be conjugated.

Theorem 3.2. *Let ℓ be an odd prime. The set of subgroups $\mathrm{H} \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ which occur as Galois image for infinitely many j-invariants such that $-\mathrm{I} \in \mathrm{H}$ are the ones given in Tables 2 and 3, p. 23.*

It is remarkable that, for any prime-power, the subgroups that do not contain $-\mathrm{I}$ which occur for infinitely many j-invariants have genus 0 and have rational parameterizations so one can apply Lemma 3.1 to $\mathrm{K} = \mathbb{Q}(t)$. The method in this section applies to subgroups of arbitrary genera and levels using Lemma 3.1 for $\mathrm{K} = \mathbb{Q}$.

4. Finding families corresponding to subgroups of arbitrary level

A theorem of Cox and Parry [CP84] gives an explicit upper bound on the level of a subgroup in terms of its genus. This allowed Cummins and Pauli [CP03] to obtain the complete list of subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ of genus $g \leq 24$.

For each such subgroup Γ, one can compute the list of subgroups Γ' of $\mathrm{GL}_2(\mathbb{Z})$ such that $\Gamma' \cap \mathrm{PSL}_2(\mathbb{Z}) = \Gamma$. (see the proof of [Sut15, Prop. 3.6].) The method in [RZB15] permits to compute X_H for any H. In this section, we propose an elementary method which is restricted to a certain class of subgroups which plays an important role in ECM (see Section 5.5).

Definition 4.1. Given a tuple of matrices $(\mathrm{M}_i)_{i\in\mathrm{I}}$ of $\prod_{i\in I}\mathrm{GL}_2(\mathbb{Z}/\ell_i^{k_i}\mathbb{Z})$, we define their cartesian product $\times_{i\in\mathrm{I}}\mathrm{M}_i$ as the matrix M of $\mathrm{GL}_2(\mathbb{Z}/\prod_{i\in\mathrm{I}}\ell_i^{k_i}\mathbb{Z})$ whose coefficients are the lifts of corresponding coefficients of M_i. A subgroup H of $\mathrm{GL}_2(\mathbb{Z}/\prod_{i\in\mathrm{I}}\ell_i^{k_i}\mathbb{Z})$ is called cartesian if it is equal to $\times_{i\in\mathrm{I}}\mathrm{H}_i = \{\times_{i\in\mathrm{I}}\mathrm{M}_i | \mathrm{M}_i \in \mathrm{H}_i\}$, where H_i is the projection of H modulo $\ell_i^{k_i}$.

An example of a non-cartesian subgroup is $\{\mathrm{I}, -\mathrm{I}\} \subset \mathrm{GL}_2(\mathbb{Z}/15\mathbb{Z})$.

4.1. The case $\mathrm{H}_1 \times \mathrm{H}_2$.

We consider three cases depending on whether $-\mathrm{I}$ belongs to both or either or neither of H_1 and H_2.

The case where $-\mathrm{I} \in \mathrm{H}_1$ and $-\mathrm{I} \in \mathrm{H}_2$. We start with the 17 maximal subgroups of $1\mathrm{A}^0$-$1a$ (See the scripts in [Sut15]): 16 groups of genus 0 and a group of genus 1, all of which contain $-\mathrm{I}$. For any pair of maximal subgroups H_1 and H_2 of levels ℓ_1^n and ℓ_2^m, at least one of them has genus 0, say H_1. Let $j = j_1(t_1)$ be a parameterization of $\mathrm{X}_{\mathrm{H}_1}$. Then $\mathrm{X}_{\mathrm{H}_2}(j_1(t_1), t_2)$ is a plane curve which characterizes elliptic curves with Galois image in $\mathrm{H}_1 \times \mathrm{H}_2$. To parameterize it, we proceed as in Section 2.

Example 4.1. Let $\mathrm{H}_1 = 2\mathrm{B}^0$-$2a$ and $\mathrm{H}_2 = 3\mathrm{A}^0$-$3a$ with $j_1(t) = \frac{(t-256)^3}{t^2}$ and $j_2(t) = t^3$. We consider the curve $X_{\mathrm{H}_1 \times \mathrm{H}_2}$ defined by the numerator of $j_1(x) - j_2(y)$ which is $-x^2y^3 - x^3 + 768\,x^2 - 196608\,x + 16777216$. Using the "algcurves" package of MAPLE, we obtain that this curve is of genus 0 and it can be parameterized by choosing $x = t^3, y = -\frac{t^3-256}{t^2}$. Thus, if j-invariant of an elliptic curve E is of the form $\frac{-\left(t^3-256\right)^3}{t^6}$, we have $\mathrm{Im}\rho_{\mathrm{E},2} \subset \mathrm{H}_1$ and $\mathrm{Im}\rho_{\mathrm{E},3} \subset \mathrm{H}_2$.

For the 16 maximal subgroups, there are 112 possible cartesian products $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2}$ such that H_1 and H_2 have relatively prime levels. Out of them, 20 have genus 0, 28 have genus 1. If for some H_1 and H_2, we succeed in parameterizing the curve $X_{\mathrm{H}_1 \times \mathrm{H}_2}$, then we proceed in the similar manner, by taking the maximal subgroups of H_1 and H_2. We obtain 163 products of genus 1 and 46 products of genus 0. Out of them, all the products of genus 0 have infinitely many rational points whereas 35 products of genus 1 have positive rank.

Given a product $\mathrm{H}_1 \times \mathrm{H}_2$ of genus 1, let us assume that there are infinitely many elliptic curves with distinct j-invariants with Galois image contained in $\mathrm{H}_1 \times \mathrm{H}_2$. One can then ask whether the Galois image is actually *equal* to $\mathrm{H}_1 \times \mathrm{H}_2$ for infinitely many of those curves. In the prime-power case, this is not necessarily true [RZB15, Remark 6.3]. We find 8 similar cases when the level is composite:

$$\begin{array}{llll} \mathrm{X}_5\text{-}3\mathrm{A}^0\text{-}3a, & \mathrm{X}_5\text{-}3\mathrm{C}^0\text{-}3a, & \mathrm{X}_5\text{-}3\mathrm{D}^0\text{-}3a, & \mathrm{X}_5\text{-}3\mathrm{D}^0\text{-}3a\mathrm{T}1 \\ 3\mathrm{A}^0\text{-}3a\text{-}5\mathrm{A}^0\text{-}5a, & \mathrm{X}_5\text{-}9\mathrm{B}^0\text{-}9a, & \mathrm{X}_5\text{-}9\mathrm{B}^0\text{-}9a\mathrm{T}1, & \mathrm{X}_5\text{-}9\mathrm{B}^0\text{-}9a\mathrm{T}2. \end{array}$$

This gives us $81 - 8 = 73$ distinct families of elliptic curves with distinct exceptional Galois images for two coprime prime-power levels such that their associated Galois images contain $-\mathrm{I}$.

The case where $-\mathrm{I} \in \mathrm{H}_1$ and $-\mathrm{I} \notin \mathrm{H}_2$. We first consider the group $\mathrm{H}_2' = \langle \mathrm{H}_2, -\mathrm{I} \rangle$ and compute $X_{\mathrm{H}_1 \times \mathrm{H}_2'}$. As above, we consider the genus of this curve and parameterize it to get a model $\mathrm{E}_{\mathrm{H}_1 \times \tilde{\mathrm{H}}_2}$. By Lemma 3.1, there exists a quadratic twist of $\mathrm{E}_{\mathrm{H}_1 \times \mathrm{H}_2'}$ such that its mod ℓ_2^m Galois image is contained in H_2. For 81 infinite families, we find 110 such families. Out of them, 85 are of genus 0 and 25 are of genus 1.

The case where $-\mathrm{I} \notin \mathrm{H}_1$ and $-\mathrm{I} \notin \mathrm{H}_2$. Let $\mathrm{H}_1' = \langle \mathrm{H}_1, -\mathrm{I} \rangle$ and $y^2 = x^3 + a(t)x + b(t)$ be its model of j-invariant $j_1(t)$. Also let $d_1(t)y^2 = x^3 + a(t)x + b(t)$ be a model for H_1. We define H_2', $d_2(t)$ in a similar manner. For a given rational t_1, Lemma 3.1 applied to a curve of j-inavariant $j_1(t_1)$ and $\mathrm{K} = \mathbb{Q}$ states the existence of a unique elliptic curve up to isomorphism over $\mathbb{Q}$ whose Galois image is contained in H_1. Equivalently, there exists a unique rational δ_1 up to a square such that the curve $\delta_1 y^2 = x^3 + a(j)x + b(j)$ has Galois image contained in H_1. By the unicity of δ_1, we have $d_1(t_1) = \delta_1$ up to a square. This shows that

$$\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2} := \{(t_1, t_2) \in \mathrm{X}_{\mathrm{H}_1' \times \mathrm{H}_2'} \mid \frac{d_1(t_1)}{d_2(t_2)} = \square\},$$

corresponds to the pair $\mathrm{H}_1 \times \mathrm{H}_2$.

We thus consider the equation $d_1(t)/d_2(t) = x^2$. If the plane curve defined by this equation has infinitely many points then we obtain a required model. Out of 60 pairs, there are 48 curves of genus 0, none of genus 1 and 12 curves of genus greater than 1. Let us illustrate it with an example.

Example 4.2. Let $\mathrm{H}_1 = 2\mathrm{A}^0\text{-}4a$ and $\mathrm{H}_2 = 7\mathrm{B}^0\text{-}7a$. Let $\mathrm{H}_1' = \langle \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 3 \end{pmatrix} \rangle \subset \mathrm{H}_1 \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\mathrm{H}_2' = \langle \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix} \rangle \subset \mathrm{H}_2 \subset \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. Let us note that neither H_1' nor H_2 contains $-\mathrm{I}'$. We first compute a model for $\mathrm{E}_{\mathrm{H}_1 \times \mathrm{H}_2}$ using the case where $-\mathrm{I}$ is in both the groups. As both of them contain $-\mathrm{I}$, only j-invariant suffices to parameterize these curves. We get the following parameterization for the j-invariant.

$$j(t) = \frac{-\left(1494501t^4 + 1198050t^3 + 359905t^2 + 48020t + 2401\right)^3 \left(30301t^4 + 24370t^3 + 7337t^2 + 980t + 49\right)}{(5t+1)^2 t^{14}}.$$

We then fix a model E_t with this j-invariant and then compute $d_1(t)$ and $d_2(t)$ by the method as explained in Example 3.1. We obtain $d_1(t) = 2t(5t+1)$ and $d_2(t) = -1$. Note that, these twists are not unique and they depend on the model E_t. In order to compute a model for $\mathrm{E}_{\mathrm{H}_1' \times \mathrm{H}_2'}$, we cannot twist E_t by $d_1(t)$ and $d_2(t)$, as the ratio of $d_1(t)$ and $d_2(t)$ is not a square. So, we consider the curve $2t(5t+1) + x^2$ defined by the equation $d_1(t)/d_2(t) = x^2$. This is a genus 0 curve which we parameterize by $t(s) = -\frac{s^2}{5\,s^2+50}$. Finally, we specialize E_t at $t = -\frac{s^2}{5\,s^2+50}$ and then twist it by -1 to obtain the model.

4.2. **The case $\mathrm{H}_1 \times \mathrm{H}_2 \times \mathrm{H}_3$.** According to the results in the tables of Cummins and Pauli [CP03], we must have $\{\ell_1, \ell_2, \ell_3\} = \{2, 3, 5\}$ or $\{2, 3, 7\}$. Since we consider first the case of maximal subgroups, we have to test only the case where the levels of $\mathrm{H}_1, \mathrm{H}_2$ and H_3 are equal to 2, 3, 5 respectively or 2, 3, 7 respectively. In each case, we consider only those triples of groups $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ where the genus of $\mathrm{X}_{\mathrm{H}_i \times \mathrm{H}_j}$ is either 0 or 1.

- The case of levels 2, 3 and 5: We start with triples $\mathrm{H}_1, \mathrm{H}_2$ and H_3 of levels 2, 3 and 5 respectively such that each $\mathrm{H_i}$ is maximal and all three curves defined by $\mathrm{X}_{\mathrm{H}_i \times \mathrm{H}_j}$ for all distinct i, j have infinitely many rational points. There are precisely 3 such triples: $(2\mathrm{B}^0\text{-}2a, 3\mathrm{A}^0\text{-}3a, 5\mathrm{B}^0\text{-}5a)$, $(2\mathrm{A}^0\text{-}8b, 3\mathrm{A}^0\text{-}3a, 5\mathrm{A}^0\text{-}5a)$ and $(2\mathrm{A}^0\text{-}8b, 3\mathrm{A}^0\text{-}3a, 5\mathrm{C}^0\text{-}5a)$.
  - The first two cases are simple to treat as there is at least a pair with genus 0, say $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2}$. In this case, let $j = j_{1,2}(t)$ be its parameterization and $j_3(s)$ be a parameterization of $\mathrm{X}_{\mathrm{H}_3}$. We consider the curve defined by $j_{1,2}(t) - j_3(s) = 0$ and verify that it is of genus higher than 1.
  - In the case $\mathrm{H}_1 = 2\mathrm{A}^0\text{-}8b, \mathrm{H}_2 = 3\mathrm{A}^0\text{-}3a, \mathrm{H}_3 = 5\mathrm{C}^0\text{-}5a$, all the curves $\mathrm{X}_{\mathrm{H}_i \times \mathrm{H}_j}$, with $1 \leq i \neq j \leq 3$ have genus 1 and rank 1. We consider the j-invariant associated with $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_3}$ which is $j_{1,3}(x, y) = -\frac{8000\left(40\,x^2 - 10\,xy + y^2\right)^3 (2\,x+y) y^3}{\left(20\,x^2 - y^2\right)^5}$, where (x, y) are points on the elliptic curve $\mathrm{E} : y^2 - 5xy + \frac{125}{4}y = x^3 + \frac{15}{2}x^2 + \frac{2625}{16}x$. On the other hand, $\mathrm{X}_{\mathrm{H}_2}$ is also of genus 0 and its j-invariant can be parameterized by $j_3(s) = s^3$.
    If there are infinitely many points on $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2 \times \mathrm{H}_3}$ then $j_{1,3}(x, y)$ must be a cube infinitely many often. It is equivalent to saying $\left(20\,x^2 - y^2\right)(2\,x + y)$ must be a cube infinitely often. We thus consider $\mathrm{Res}_x\left(t^3 - \left(20\,x^2 - y^2\right)(2\,x+y), \mathrm{E}\right)$. This curve is of genus 5.

  Thus in all these case, we have the resulting curves of higher genus. Thus there are no new families, and we do not need to consider non-maximal subgroups.
- In the case of levels 2, 3 and 7, for each triple of maximal subgroups, at least two fa : There is no trimilies intersect in a finite number of points, hence the intersection of three families is always finite.

The above computations and the scripts in the online complement [BS19] prove the following results.

Theorem 4.1. *There are exactly* 1525 *subgroups of* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *which are cartesian and occur as Galois images for infinitely many* j*-invariants.*

The list of these models is in online complement [BS19].

4.3. **Discussion on the families in the literature.** To our knowledge, there are 23 families of elliptic curves which were reported to be used in ECM computations. In this section, we compare the list of families Theorem 4.1 with the previously known ones.

In short, the families used in ECM are motivated by the torsion properties and by the average number of full multiplications needed for doubling-and-adding on the elliptic curve. A recent study [BI19] makes a state-of-the-art presentation of the implementation techniques and concludes that it is important that 1) the elliptic curve can be put on a particular form (Montgomery, Edwards, Hessian) and that 2) one can generate many curves of the family which have a rational point of coordinates of less than 32 bits. Of course any family can be put in short Weierstrass form. To have a better cost, one uses either the twisted Edwards form or the twisted Hessian form which is not possible for all elliptic curves.

The twisted Edwards' curves are birationally equivalent to Montgomery curves [BBJ+08, Theorem 3.2] and have two subfamilies which have an even better cost: the case $a = -\square$, which is abusively also called twisted Edwards and has the best arithmetic cost, and the case $a = \square$ which is simply called Edwards form. A direct computation (Appendix B) shows that an elliptic curve can be put in twisted Edwards/ Montgomery form if and only if it belongs to the family X_{13} using [RZB15] notations. The corresponding group contains $-\mathrm{I}$ and has index 2 subgroups not containing $-\mathrm{I}$ of the same level which also correspond to infinite families: we identify these families with the cases $a = \square$ and $a = -\square$ (see row 2 and row 3 of Table 4).

Bernstein et al. [BCKL15] proved that an elliptic curve can be put in twisted Hessian form if and only if it is isogenous to a curve having a rational point of order 3. Hence, in order to parameterize twisted Hessian curves, we parameterize curves with mod 3 Galois image contained in the group of upper triangular matrices (see row 4 in Table 4).

We distinguish the case of families having a point of infinite order, i.e. given a family of rational parameterization $\mathrm{E} : y^2 = x^3 + a(t)x + b(t)$ we call subfamily a subset of the family where t is parameterized by a plane curve of genus 0 or 1 so that there exists a point of E which does not have order ≤ 16 except for a finite explicit set. For example, Montgomery [Mon87] attributes to Suyama a family as well as a subfamily having a point of infinite order, the subfamily being much more known than the family. (see row 5 and row 18 in Table 4). more Also, Gélin et al. [GKL17] proposed subfamilies with points of infinite order on the families of [BBB+13]. We do not discuss further the case of subfamilies with points of infinite order because they are not known to modify the behaviour of ECM and because they produce curves of large coefficients. Instead, several authors make lists of elliptic curves from families which have small coefficients and compute directly a rational point [BI19, HMR16, BBL10].

Table 4 makes a list of the families in the literature and identifies their [RZB15] and [Sut15] labels. To prove the equivalence, one tests by direct computations that the curves of one family are birationally equivalent to a curve of the other (verification scripts are provided in the Appendix B).

5. A criterion to compare families of ECM-friendly curves

As discussed in Appendix A, an important application of ECM consists in using the same elliptic curve to test smoothness of many integers. In this context, several articles [BBL10], [HMR16], [GKL17], [Mon87] measure the quality of a curve E for the ECM algorithm as the proportion of

B \ $\log_2 n$	25	29	33	37	40
1000	-2.03	-1.37	-1.81	-1.79	-1.73
2000	-1.94	-1.65	-1.75	-1.6	-1.68
3000	-1.94	-1.51	-1.62	-1.61	-1.63
4000	-1.82	-1.45	-1.55	-1.53	-1.59
5000	-1.8	-1.41	-1.57	-1.45	-1.61

TABLE 1. Values of $\beta(\mathrm{E}, n, \mathrm{B})$ for $\mathrm{E} : y^2 = x^3 + 3x + 5$ and various values of $\log n$ and B.

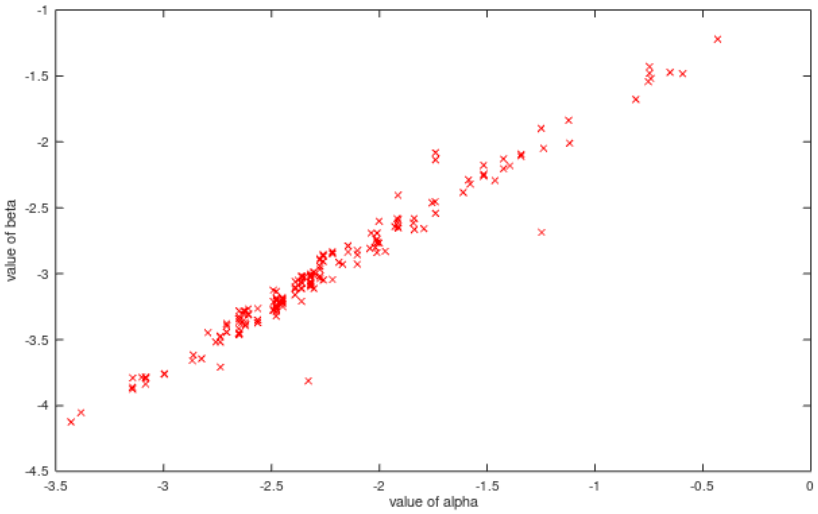
primes p less than a bound X for which $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth, where X and B are given parameters. In the rest of this section we study if one can compare this proportion for two elliptic curves, regardless of the two parameters X and B.

Given an elliptic curve E and two integers n and B, let $\beta(\mathrm{E}, n, \mathrm{B})$ be a real number such that

$$\frac{\#\{p \sim n \,|\, \#\,\mathrm{E}(\mathbb{F}_p) \text{ is B-smooth}\}}{\#\{p \,|\, p \sim n\}} \approx \frac{\#\{x \sim ne^{\beta(\mathrm{E},n,\mathrm{B})} \,|\, x \text{ is B-smooth}\}}{\#\{x \,|\, x \sim ne^{\beta(\mathrm{E},n,\mathrm{B})}\}},$$

where the expression $p \sim n$ denotes that $p \in [n - 2\sqrt{n}, n + 2\sqrt{n}]$ and the sign $\approx$ denotes the equality up to a difference of $1/\#\{x \mid x \sim ne^{\beta(\mathrm{E},n,\mathrm{B})}\}$. This notation comes to correct the common heuristic which states that a cardinality of $\mathrm{E}(\mathbb{F}_p)$ is as smooth as a random integer of the same size.

Table 1 below shows the values of β for the curve E of equation $y^2 = x^3 + 3x + 5$ and various values of $\log_2 n$ and B. We did a similar experiment for a curve from 200 random families of Theorem 4.1, which suggests that $\beta_{\mathrm{E},n,\mathrm{B}}$ converges uniformly when n and B go to infinity.



The graph also indicates that $\beta = \lim \beta(\mathrm{E}, n, B)$ and $\alpha(\mathrm{E})$ have a linear relationship.

Open question 5.1. *Let* E *be an elliptic curve without complex multiplication. Decide whether there exists a real number* $\beta(\mathrm{E})$ *such that*

$$\mathrm{Prob}(\#\,\mathrm{E}(\mathbb{F}_p) \textit{ is B-smooth} \mid p \sim n) \sim_n \mathrm{Prob}(m \textit{ is B-smooth} \mid m \sim ne^{\beta(\mathrm{E})}),$$

where $\sim_n$ *denotes the asymptotic equivalence,* $p \sim n$ *denotes that* $p \in [n - 2\sqrt{n}, n + 2\sqrt{n}]$, Prob *on the left side denotes the Chebotarev density and* Prob *on the right side denotes the proportion of* B*-smooth integers in the interval.*

Answering the above question goes beyond the scope of this article. Nevertheless, this offers a new point of view on a tool that Peter Montgomery used in experiments to compare elliptic curves. Indeed, Montgomery [Mon92, pages 75-76] considered the value

$$\log(2) \cdot \overline{\mathrm{val}_2}(\mathrm{E}) + \log(3) \cdot \overline{\mathrm{val}_3}(\mathrm{E}),$$

where $\overline{\mathrm{val}_2}$ and $\overline{\mathrm{val}_3}$ denote the average value of $\mathrm{val}_2(\#\,\mathrm{E}(\mathbb{F}_p))$ and $\mathrm{val}_3(\#\,\mathrm{E}(\mathbb{F}_p))$ when p runs through all the primes of good reduction up to a bound n. These are similar to the first terms of a numeric series that rigorously defines α, as we explain in the next subsection.

Murphy [Mur99] introduced a tool α which answers the above question for the values taken by polynomials:

$$\alpha = \sum_{\ell \text{ prime}} \log(\ell) \cdot \left(\frac{1}{\ell - 1} - \overline{\mathrm{val}_\ell}\right),$$

where $\overline{\mathrm{val}_\ell}$ is the average value of the valuation in ℓ of the set of integers that we study, the average being defined rigorously in the sequel of this section.

Indeed, Barbulescu and Lachand in Theorem 1.1 of [BL17] proved that $\beta(\mathrm{F}) = \alpha(\mathrm{F})$ for any quadratic polynomial F of primitive fundamental negative discriminant.

5.1. **Formal definition of α.** We say that a set S of primes admits a Chebotarev density δ, and we write $\mathrm{Prob}(\mathrm{S}) = \delta$, if $\lim_{n\to\infty} \frac{\#(\mathrm{S}\cap\Pi(n))}{\#\Pi(n)}$ exists and is equal to δ. Here $\Pi(n)$ denotes the set of primes less than n. For an elliptic curve E and a prime ℓ, we define the average valuation at ℓ of $\#\,\mathrm{E}(\mathbb{F}_p)$, where p is a random prime by

$$\overline{\mathrm{val}_\ell}(\mathrm{E}) = \sum_{n\geq 1} n \cdot \mathrm{Prob}(\{p \text{ prime } \mid \mathrm{val}_\ell(\#\,\mathrm{E}(\mathbb{F}_p) = n)\}).$$

The convergence of the series defining $\overline{\mathrm{val}_\ell}(\mathrm{E})$ is proven in [BBB+13, Th 2.16], the proof allowing to compute it explicitly using $\mathrm{Im}\rho_{\mathrm{E},\ell^\infty}$.

Definition 5.1. Given an elliptic curve E and a prime ℓ, we put

$$\alpha_\ell(\mathrm{E}) = \log(\ell)(\overline{\mathrm{val}_\ell}(n) - \overline{\mathrm{val}_\ell}(\mathrm{E}))$$

and

$$\alpha(\mathrm{E}) = \sum_{\ell \text{ prime}} \alpha_\ell(\mathrm{E}).$$

Let us prove the convergence of this series.

Theorem 5.1. *For any elliptic curve* $\mathrm{E}/\mathbb{Q}$ *without complex multiplication, the series* $\sum_l \alpha_l(\mathrm{E})$ *converges.*

Proof. By Serre's open image theorem, any elliptic curve without complex multiplication has a finite set of primes ℓ such that the mod ℓ^∞ Galois image is not surjective in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Hence, the series which defines α has the same nature of convergence as the series corresponding to a curve which would have a surjective Galois image at all primes. From [BBB+13, Th 2.16], applied for $n = 1$, we have $\overline{\mathrm{val}_\ell}(\mathrm{E}) = \frac{\ell}{\ell-1}\mathrm{Prob}(\mathrm{E}(\mathbb{F}_p)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}) + \frac{\ell((2\ell+1))}{(\ell-1)(\ell+1)}\mathrm{Prob}(\mathrm{E}(\mathbb{F}_p)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z})$. If

a matrix other than I has a non-trivial fixed subspace, it is of the form $\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}$ or $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ where a is non-zero. By counting stabilizers, we obtain that in $\mathrm{GL}_2(\mathbb{F}_\ell)$ there are $\ell(\ell+1)(\ell-2)$ matrices conjugated to $\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}$, ℓ^2-1 conjugated to $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ and, by [BBB+13, Prop 2.3], we obtain then $\overline{\mathrm{val}_\ell}(\mathrm{E}) = \frac{\ell(\ell^3+\ell^2-2\ell-1)}{(\ell+1)^2(\ell-1)^3}$. Hence, $\alpha_\ell(\mathrm{E}) = \log(\ell)(\frac{1}{\ell-1} - \overline{\mathrm{val}_\ell}(\mathrm{E})) = \mathcal{O}(\frac{\log(\ell)}{\ell^2})$, which is the term of a convergent series. □

Note that, if a curve E has surjective Galois image at all primes, which is the case for all curves except a finite set of families described by curves, $\alpha(\mathrm{E}) \approx -0.8119977339443$, which is negative and suggests that the cardinality of an elliptic curve has slightly more chances of being smooth than a random integer of the same size.

5.2. **Computation of α.** For each family of Theorem 4.1, we compute the value of α.

Example 5.1. (1) Let us consider the family X_{193n} of [RZB15] which has $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ (row 13 of Table 4). We see that the index of mod 2^i Galois image in $\mathrm{GL}_2(\mathbb{Z}/2^i\mathbb{Z})$ is constant for all $i \geq 3$. We describe it by saying Serre's exponent is 3 and by [BBB+13, Th 2.16], we find that $\overline{\mathrm{val}_2}$ changes from the value when $\rho_{\mathrm{E},2^\infty}$ is surjective, i.e. $\frac{14}{9}$, to its new value $\frac{16}{3}$. Furthermore, for any generic curve in this family, for all primes different than 2, the corresponding Galois image is surjective. Thus,

$$\alpha_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}} = \alpha_{generic} + \left(\frac{14}{9} - \frac{16}{3}\right)\log 2 \approx -3.4355.$$

(2) Let us consider the Suyama-11 family, which is parameterized in [BBB+13, Sec. 3.5.1]. For these curves, $\overline{\mathrm{val}_2}$ changes from $\frac{14}{9}$ to $\frac{11}{3}$ and $\overline{\mathrm{val}_3}$ changes from $\frac{87}{128}$ to $\frac{27}{16}$. And, for any generic curve in this family, for all primes different than 2 and 3, the corresponding Galois image is surjective. Thus,

$$\alpha_{\mathrm{Suyama-11}} = \alpha_{generic} + \left(\frac{14}{9} - \frac{11}{3}\right)\log 2 + \left(\frac{87}{128} - \frac{27}{16}\right)\log 3 \approx -3.3825.$$

Given an elliptic curve without complex multiplication, one can use the modular curves to determine it Galois image. Then $\alpha(\mathrm{E})$ is equal to the pre-computed value of the family of E. We can now test the efficiency of α by comparing the smoothness probabilities of $\#\,\mathrm{E}(\mathbb{F}_p)$ when p is a random prime of a given size n and that of a random integer of size $ne^{\alpha(\mathrm{E})}$.

Example 5.2. In the following tables, the first two columns give the proportions of B-smooth integers of size n, ne^α. We compare them with the proportion of primes $p \sim n$ such that $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth. The last two columns indicate relative errors. Where the relative error of a with respect to b is $\frac{|a-b|}{|b|}$.

The followings averages are taken over several randomly chosen curves in each family with 2 different values of B and $n = 2^{25}$.

(1) Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

	n	ne^α	$\#\,\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^\alpha}$
$\mathrm{B}_1 = 30$	0.000518	0.005753	0.005126	889 %	10.89 %
$\mathrm{B}_2 = 100$	0.008892	0.03883	0.042573	378.8 %	9.63 %

(2) Suyama-11

	n	ne^α	$\#\,\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^\alpha}$
$\mathrm{B}_1 = 30$	0.000518	0.005133	0.005743	1008 %	11.89 %
$\mathrm{B}_2 = 100$	0.008892	0.04013	0.04101	361%,	2.19%

5.3. **ECM-friendly families with the best values of α.** Often in ECM, one uses curves with better arithmetic i.e. the curves for which the point addition and multiplication are less time consuming, for example, Montgomery curves or twisted Edwards' curves with $a = -1$. We consider intersecting the families with better values of α with the ones with better arithmetic.

Example 5.3 (A new family)**.** It is known that the family of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the family of twisted Edwards' curves with $a = -1$ do not intersect. There are however four families which have the same value of α as the one with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ and which are also of the form twisted Edwards' with $a = -1$. One of them is X_{192i} in [RZB15] and can be transformed into twisted Edwards' form by choosing

$$a = -1, \qquad d = -\frac{\left(t^2+4\right)^4}{64\left(t^2-4\right)^2 t^2}.$$

The other familes are X_{189d}, X_{207n} and X_{211m}.

5.4. $\alpha(\mathrm{E})$ **over number fields.** So far, we have considered rational elliptic curves E and their values of $\alpha(\mathrm{E})$. These curves fare better when we try to factor a random integer N. However, if more information is available about N, one might want to use it in order to factor N. For example, if we know by some oracle that -3 is a square modulo N, we consider families with better values of α over $\mathbb{Q}(\sqrt{-3})$. Indeed these family can be defined over $\mathbb{Q}(\sqrt{-3})$, however we restrict ourselves to the families defined over $\mathbb{Q}$. In this case, one must modify the definition of α from its original version of Section 5.1.

Let K be a number field, E, a rational elliptic curve and ℓ, a prime. We define the average valuation at ℓ of $\#\,\mathrm{E}(\mathbb{F}_p)$ when p is a random prime which splits completely in K by

$$\overline{\mathrm{val}_{\ell,\mathrm{K}}}(\mathrm{E}) = \sum_{n\geq 1} n\mathrm{Prob}(\{p \text{ prime which splits completely in K} \mid \mathrm{val}_\ell(\#\,\mathrm{E}(\mathbb{F}_p) = n)\}).$$

The existence and the computation of $\overline{\mathrm{val}_{\ell,\mathrm{K}}}(\mathrm{E})$ follows from Theorem [BBB+13, Th 2.16]. We now define α relative to K.

Definition 5.2. Given an elliptic curve $\mathrm{E}/\mathbb{Q}$, a prime ℓ and a number field K, we put

$$\alpha_{\ell,\mathrm{K}}(\mathrm{E}) = \log(\ell)(\overline{\mathrm{val}_{\ell,\mathrm{K}}}(n) - \overline{\mathrm{val}_\ell}(\mathrm{E}))$$

and

$$\alpha_{\mathrm{K}}(\mathrm{E}) = \sum_{\ell \text{ prime}} \alpha_\ell(\mathrm{E}).$$

Example 5.4. Let $\mathrm{E} : y^2 + xy + y = x^3 + 9481x + 89898842$ and $\mathrm{K} = \mathbb{Q}(\zeta_3)$, the cyclotomic field of degree 3. For E, the mod 2 and mod 3 images of Galois are X_6 and $3\mathrm{D}^0$-$3a$T1 in Table 2. On the other hand, p splits completely in K if, and only if, $p \equiv 1 \bmod 3$.

For E, $\overline{\mathrm{val}_{2,\mathrm{K}}}$ changes from $\frac{14}{9}$ (generic value) to $\frac{8}{3}$ and $\overline{\mathrm{val}_{3,\mathrm{K}}}$ changes from $\frac{87}{128}$ (generic value) to $\frac{21}{8}$. Thus,

$$\alpha_{\mathrm{K}}(\mathrm{E}) = \alpha_{generic} + \left(\frac{14}{9} - \frac{8}{3}\right)\log 2 + \left(\frac{87}{128} - \frac{21}{8}\right)\log 3 \approx -3.7193.$$

Proposition 5.1. *The best 50 values of α over $\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)$ for $n = 3, 4, 5$, where ζ_n is a primitive n-th root of unity, for the rational families correspond to the families given in Tables 5, 6, 7 and 8 respectively.*

There are families of curves with α larger than -0.81 (e.g. X_{2b}-$5A^0$-$5a$). This implies that any random elliptic curve performs better than the curves from these families. The complete list of 1525 families and the corresponding values of α is available at [BS19].

5.5. **Going beyond α.** Although α is very easy to compute, one can define more precise tools, e.g.

$$\mathbb{E}(\mathrm{E}) = \sum_{m \text{ B-smooth integer} \leq n} \mathrm{Prob}(m \text{ divides} \#\,\mathrm{E}(\mathbb{F}_p) \cdot \mathrm{Prob}(x \mid m \text{ is B-smooth}),$$

where x denotes a random integer of the size of n. A key difference between α and $\mathbb{E}$ is that α depends on the probabilities of $\#\,\mathrm{E}(\mathbb{F}_p)$ being divisible by prime-powers but not on that of being divisible by composite numbers. This difference is due to the fact that we have families with Galois images which are cartesian products. The question remains to solve Mazur's program B for the subgroups which are non-cartesian. When mod m Galois image is non-cartesian, divisibility properties can change. For example, two curves can have the same mod 2 and mod 3 Galois images and thus the same value of α yet have different probabilities that 6 divides $\#\,\mathrm{E}(\mathbb{F}_p)$ as illustrated in the example below.

Example 5.5. Let us consider the curves $\mathrm{E}_1 : y^2 = x^3 - 75x - 2950$ and $\mathrm{E}_2 : y^2 = x^3 + 45x - 366$ which have the mod 2 and mod 3 Galois images. The following table gives compares probabilities of divisibility by 2, 3 and 6 for E_1 and E_2. These probabilities are computed using mod 6 Galois images for E_1 and E_2 and then using Theorem 2.7 of [BBB+13].

Curve	$\mathbb{P}(2 \mid \#(\mathrm{E}(\mathbb{F}_p))$	$\mathbb{P}(3 \mid \#(\mathrm{E}(\mathbb{F}_p))$	$\mathbb{P}(6 \mid \#(\mathrm{E}(\mathbb{F}_p))$	α
E_1	2/3	3/4	1/2	-1.39
E_2	2/3	3/4	**7/12> 2/3· 3/4**	-1.39

If the Chebotarev density were a probability, one would say that the fact of being divisible by 2 and that of being divisible by 3 are correlated.

6. Conclusion and future work

The goal of this work was to classify infinite families of ECM-friendly elliptic curves. The exhaustive method of finding these families and the experimental tool α enables us to conclude that there do not exist other ECM-friendly curves over $\mathbb{Q}$ than 1525 families provided and several new families are better.

One can obtain the complete list of genus 0 and genus 1 modular curves of prime-power level. This list is independent of the number fields over which the elliptic curves are defined. Hence the list of ECM-friendly families is contained in a finite set independent of the number field.

One can also consider modular curves of higher genus and finitely many elliptic curves arising from them for ECM as a natural extension of this work. This can be interesting for implementation of ECM. This raises the question of efficiently computing X_H for subgroups H of higher level.

A different question is that of a rigorous analysis of the smoothness properties of $\#\,\mathrm{E}(\mathbb{F}_p)$ which make use of α.

References

[AM93] A Oliver L Atkin and Francois Morain. Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60(201):399–405, 1993. 2, 21, 25

[BBB+13] Razvan Barbulescu, Joppe Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter Montgomery. Finding ecm-friendly curves through a study of galois properties. *The Open Book Series*, 1(1):63–86, 2013. 2, 3, 4, 6, 11, 13, 14, 15, 16, 22, 25

[BBJ+08] Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Progress in Cryptology – AFRICACRYPT*, pages 389–405, 2008. 11, 20

[BBL10] Daniel J Bernstein, Peter Birkner, and Tanja Lange. Starfish on strike. In *International Conference on Cryptology and Information Security in Latin America*, pages 61–80. Springer, 2010. 2, 11, 21, 25

[BBLP13] Daniel Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. Ecm using edwards curves. *Mathematics of Computation*, 82(282):1139–1179, 2013. 2, 21, 25

[BC10] Éric Brier and Christophe Clavier. New families of ecm curves for cunningham numbers. In *International Algorithmic Number Theory Symposium*, pages 96–109. Springer, 2010. 2, 21, 25

[BCKL15] Daniel J Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted Hessian curves. In *Progress in cryptology – LATINCRYPT 2015*, volume 9230 of *Lecture notes in computer science*, pages 269–294. Springer, 2015. 11, 20, 25

[BGGM14] R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain. Discrete logarithms in GF(p^2) — 160 digits, 2014. Announcement available at the NMBRTHRY archives, item 004706. 19

[BGGM15] R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *Lecture notes in computer science*, pages 129–155, 2015. 19

[BGK+] Shi Bai, Pierrick Gaudry, Alexander Kruppa, François Morain, Emmanuel Thomé, and Paul Zimmermann. Crible algébrique: Distribution, optimisation—number field sieve (cado-nfs). 18

[BI19] Cyril Bouvier and Laurent Imbert. Faster cofactorization with ECM using mixed representations. working paper or preprint, January 2019. 11

[BL17] Razvan Barbulescu and Armand Lachand. Some mathematical remarks on the polynomial selection in nfs. *Mathematics of Computation*, 86(303):397–418, 2017. 13

[BS19] Razvan Barbulescu and Sudarshan Shinde. Online complement for "A classification of ECM-friendly families using modular curves", 2019. available at https://webusers.imj-prg.fr/~razvan.barbaud/ECMfriendly/ECMfriendly.html. 8, 10, 11, 16

[CP84] David A Cox and Walter R Parry. Genera of congruence subgroups in q-quaternion algebras. *J. Reine Angew. Math*, 351(66):112, 1984. 8

[CP03] C.J. Cummins and S. Pauli. Congruence subgroups of $psl(2,\mathbb{Z})$ of genus less than or equal to 24. *Experimental Mathematics*, 12(2):243–255, 2003. 8, 10

[Cre01] JE Cremona. Classical invariants and 2-descent on elliptic curves. *Journal of Symbolic Computation*, 31(1-2):71–87, 2001. 4

[Cro07] Ernie Croot. Smooth numbers in short intervals. *International Journal of Number Theory*, 3(01):159–169, 2007. 18

[GKL17] Alexandre Gélin, Thorsten Kleinjung, and Arjen K Lenstra. Parametrizations for families of ecm-friendly curves. In *International Symposium on Symbolic and Algebraic Computation – ISSAC 2017*, pages 165–171, 2017. 11

[HMR16] Henriette Heer, Gary McGuire, and Oisin Robinson. JKL-ECM: an implementation of ECM using hessian curves. *LMS Journal of Computation and Mathematics*, 19(A):83–99, 2016. 2, 11, 21, 22, 25

[JL03] A. Joux and R. Lercier. Improvements to the general number field for discrete logarithms in prime fields. *Mathematics of Computation*, 72(242):953–967, 2003. 19

[KB16] T. Kim and R. Barbulescu. The extended tower number field sieve: A new complexity for the medium prime case. In *Advances in Cryptology – CRYPTO 2016*, volume 9814 of *Lecture notes in computer science*, pages 543–571, 2016. 19

[Kub76] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society*, 3(2):193–237, 1976. 25

[LJ87] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987. 1

[LLJMP93] Arjen K Lenstra, Hendrik W Lenstra Jr, Mark S Manasse, and John M Pollard. The number field sieve. In *The development of the number field sieve*, pages 11–42. Springer, 1993. 1

[Mon87] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987. 2, 11, 20, 25

[Mon92] Peter Lawrence Montgomery. *An FFT extension of the elliptic curve method of factorization*. PhD thesis, University of California, Los Angeles, 1992. 13, 21, 25

[Mur99] Brian Antony Murphy. *Polynomial selection for the number field sieve integer factorisation algorithm*. PhD thesis, The Australian National University, 1999. 13

[Pol93] John M Pollard. The lattice sieve. In *The development of the number field sieve*, pages 43–49. Springer, 1993. 1

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of galois. *Research in Number Theory*, 1(1):1–34, 2015. 3, 6, 7, 8, 9, 11, 14, 15, 21

[Ser71] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1971. 2

[Shi71] Gorō Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1. Princeton university press, 1971. 2, 6

[Sil08] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, 2008. 4

[Sut15] Andrew V Sutherland. Computing images of galois representations attached to elliptic curves. *arXiv preprint arXiv:1504.07618*, 2015. 8, 9, 11, 21

[Suy85] Hiromi Suyama. Informal preliminary report (8), 1985. Letter to Richard P. Brent. 25

[SZ06] Jean-Pierre Serre and Don Bernard Zagier. *Modular functions of one variable V: proceedings international conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976*, volume 601. Springer, 2006. 2

[SZ17] Andrew V Sutherland and David Zywina. Modular curves of prime-power level with infinitely many rational points. *Algebra & Number Theory*, 11(5):1199–1229, 2017. 3, 6, 7, 8

[VH94] Mark Van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation*, 18(4):353–363, 1994. 4

[vH95] Mark van Hoeij. An algorithm for computing the weierstrass normal form. In *Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 90–95. ACM, 1995. 3

[vH97] Mark van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *Journal of Symbolic Computation*, 23(2-3):209–227, 1997. 4

[VHKN13] Mark Van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *Journal of Symbolic computation*, 52:17–34, 2013. 4

[Zyw15] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015. 6, 8

Appendix A: Cryptologic utilization of ECM

In cryptology, ECM is used as an algorithm to test B-smoothness : given an integer N, find all its prime factors less than B. Under a conjecture about the existence of smooth integers in short intervals [Cro07, Conj 1], H. Lenstra Jr. proved that, if N has a prime factor less than B, ECM will find it with probability at least $1/2$ in time $M(N)L_B(1/2, \sqrt{2})^{1+o(1)}$, where $M(N) = \mathcal{O}((\log N)^2)$ is the cost of the arithmetic operations in $\mathbb{Z}/N\mathbb{Z}$ where the L notation is as follows:

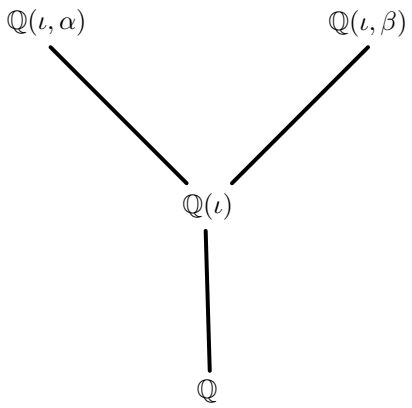
$$L_B(\alpha, c) = \exp(c(\log N)^\alpha (\log\log N)^{1-\alpha}).$$

Smoothness tests play a key role in cryptology. Indeed, when factoring integers with NFS, one selects two distinct number fields $\mathbb{Q}[x]/f(x)$ and $\mathbb{Q}[x]/g(x)$ such that f and g have a common root m modulo N; we call α (resp. β) a root of f (resp. g) in its number field. The next stage of NFS consists of enumerating polynomials $\phi(x) \in \mathbb{Z}[x]$ and collecting all but a negligible proportion of those ϕ such that $N_{\mathbb{Q}(\alpha)}(\phi(\alpha))$ and $N_{\mathbb{Q}(\beta)}(\phi(\beta))$ are B-smooth for $\mathrm{B} = L_N(1/3, \sqrt[3]{8/9})$.

The textbook implementation of NFS is without ECM as a subroutine. However in practice we use a hybrid version The smoothness tests are done using ECM both in the complexity analysis and in practice, e.g. in the open source implementation CADO-NFS [BGK+].

The next stage of NFS consists in solving a linear system to find a tuple $(u_\phi)_{\phi \text{ collected}}$ such that $x_1 := \prod_\phi \phi(\alpha)^{u_\phi}$ and $x_2 := \prod_\phi \phi(\beta)^{u_\phi}$ are squares. Finally, one computes two polynomials r_1 and r_2 in $\mathbb{Z}[x]$ such that $r_1(\alpha)^2 = x_1$ and $r_2(\beta)^2 = x_2$ and obtain the solution $y_1^2 \equiv y_2^2 \pmod N$ where $y_1 = r_1(m) \bmod N$ and $y_2 = r_2(m) \bmod N$, where m id the common root of f and g modulo N. If $\gcd(y_1 - y_2, N) \notin \{1, N\}$, one finds a factor, otherwise one goes back to the beginning of the algorithm (in practice one computes many solutions (y_1, y_2) simultaneously).

When computing discrete logarithms in the multiplicative group of $\mathbb{F}_{p^n}$ for a prime p, the best asymptotic complexity is obtained by the extended tower number field sieve [KB16], which is a variant of NFS. The first step is to select a factor η of n and a polynomial $h(t) \in \mathbb{Z}[t]$ of degree η which is irreducible modulo p. Let ι be a root of H in its number field. Then one selects two polynomials f and g in $\mathbb{Z}[t, x]$ such that, if ω is a root of H in $\mathbb{F}_p[t]/\langle h \rangle$, the polynomial $f(\omega, x)$ and $g(\omega, x)$ have a common irreducible factor $\varphi \in \mathbb{F}_p(\omega)[x]$ of degree $\kappa := n/\eta$. If we call α and β roots of f and g respectively in their number fields, we obtain the following diagram:



Once H, f and g have been selected, the algorithm continues by enumerating a large number of pairs $a(t), b(t) \in \mathbb{Z}[t]$ and collecting all but a negligible proportion of the pairs a and b for which $N_{\mathbb{Q}(\iota,\alpha)}(a(\iota) - \alpha b(\iota))$ and $N_{\mathbb{Q}(\iota,\beta)}(a(\iota) - \beta b(\iota))$ are B-smooth for $\mathrm{B} = L_{p^n}(1/3, \sqrt[3]{8/9})$. In the next step, one factors $a(\iota) - \alpha b(\iota)$ and respectively $a(\iota) - \beta b(\iota)$ into prime ideals and writes a linear system whose coefficients are the valuations of prime ideals and the unknowns are in bijection with the prime ideals of norm less than B. The solution allows us to obtain the discrete logarithm of any element in a time which is negligible with respect to the cost of collecting the pairs $a(t)$ and $b(t)$.

As in the factoring variant of NFS, the smoothness tests are done with ECM. We note that in the case of discrete logarithm we have a larger number of methods to select the polynomials f and g. For example, in the case of the generalized Joux and Lercier method [JL03, BGGM15], one can set f to be any irreducible polynomial in $\mathbb{Z}[x]$ having an irreducible factor φ of degree κ. For example, in [BGGM14], the authors used $f(x) = \phi_8(x)$ so that for any pair (a, b), $N_{\mathbb{Q}(\alpha)}(a - \alpha b) = a^4 + b^4$, so half of the integers to factor in NFS can be tackled with elliptic curves defined over $\mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive 8th root of unity. Moreover, when $h = h_0 + h_1 t + h_2 x^t$ for $h_0, h_1, h_2 \in \mathbb{Z}$, $N_{\mathbb{Q}(\iota,\alpha)}(a(\iota) - \alpha b(\iota)) = N_{\mathbb{Q}(\iota)}(a' - \iota b') = h_0 v^2 + h_1 uv + h_2 u^2$, where $u - \iota v = N_{\mathbb{Q}(\iota,\alpha)/\mathbb{Q}(\iota)}(a(\iota) - \alpha b(\iota))$.

To sum up, an improvement of ECM adapted to integers of the form $h_2 u^2 + h_1 uv + h_0 v^2$ would translate in an improvement of the relation collection of NFS and this can change the systems based on discrete logarithm in fields $F_{p^{2n}}$. An improvement on ECM in the general case would

have consequences on the system based on factoring and discrete logarithm. Hence, for cryptologic applications, it is then important to find all the infinite families of elliptic curves defined over given number fields which have exceptional Galois images for some torsion, and to verify experimentally if they can bring a speed-up of ECM.

Appendix B: identifying families of ECM-friendly families

In this appendix, we give the scripts of verifications of Table 4.

row 1. The Montgomery and the twisted Edwards form are birationally equivalent due to Theorem 3.2 in [BBJ+08].

```
def MontgomeryToWeierstrass(A, B):
    return EllipticCurve([0, A/B,0 1/B^2,0])
def X13(t):
    j = (t^6 + 48*t^5 + 816*t^4 + 5632*t^3 + 13056*t^2 + 12288*t + 4096)/(t^2 + 16*t)
    a = (-3)*(j-1728)*j
    b = (-2)*j*(j-1728)^2
    return EllipticCurve([a,b])
Q.<t> = QQ[]
X13(t).is_isomorphic(MontgomeryToWeierstrass(-1/4*t - 2, 3*(t^2 + 16*t)/(t^5 + 40*t^4 +
    520*t^3 + 2240*t^2 + 896*t - 1024)))
```

row 2. One can directly compute the function field of 4-division points as an extension of $\mathbb{Q}(d)$ and obtain the the Galois image is contained in that of X_{13f}. Conversely, any curve of X_{13f} can be put in twisted Edwards form with $a = -1$, as checked by the following script.

```
def X13f(t):
    a = -27*t^4 + 432*t^3 - 432*t^2 - 20736*t + 82944
    b = -54*t^6 + 1296*t^5 - 6480*t^4 - 65664*t^3 + 746496*t^2 - 1990656*t
    return EllipticCurve([a,b])
def twistedEdwardsToWeierstrass(a, d):
    return MontgomeryToWeierstrass(2*(a+d)/(a-d), 4/(a-d))
Q.<t> = QQ[]; K = Q.fraction_field(); t= K(t)
X13f(t).is_isomorphic(twistedEdwardsToWeierstrass(-1,(-1/4*t^2 + 16)*4/(t-8)^2))
```

row 3. The group corresonding to X_{13h} is $\{\begin{pmatrix}1 & *\\ 0 & *\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})\}$, which corresponds to the elliptic curves having a rational point of order 4. Theorem 3.3 of [BBJ+08] states that an elliptic curve can be put in twisted Edwards' form such that $a = \square$ if and only if it has a rational point of order 4. X_{13h} does have a point of order 4 and can be put in twisted Edwards' form with $a = \square$.

row 4. Theorem 5.4 of [BCKL15] ensures that a curve is isogenous to a twisted Hessian curve if and only if it is isogenous to a curve having a point of order 3. The family $3\mathrm{B}^0$-$3a$ corresponds to the group $\{\begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})\}$, which characterizes the curves which are isogenous to curve with a point of order 3.

row 5. On page 262 of [Mon87] we read the description of the Suyama family as the Montgomery curves $\mathcal{M}_{A,B}$ for which there exist $x_3, y_3 \in \mathbb{Q}$ such that $A = (-x_3^3 - 6x_3^3 + 1)/(4x_3^3)$ and $B = (x_3 - 1)^2/(4x_3y_3^2)$. These equations are equivalent to $\Psi_{\mathcal{M}_{A,B}}, 3(x_3) = 0$ and $By_3^2 = x_3^3 + Ax_3^2 + x_3$ and are further equivalent to the fact that $\mathcal{M}_{A,B}$ has a torsion point of order 3. Hence, the SUyama family is equivalent to the intersection of X_{13} (Montgomery form) and $3\mathrm{B}^0$-$3a$T2 (point of order 3). On page 263 of the same article, one has a parameterization of a subset of the Suyama family which has a point of infinite order, this family also being called Suyama.

rows 6. to 11. These rows consider families which parameterize the elliptic curves having a point of order n for $n = 5, 7, 8, 9, 1011, 12$. The correspondence with the parameterizations of [RZB15] and [Sut15] is done to the matrix groups which are $\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})\}$.

row 12. To our knowledge, this family is not reported to be used in ECM computations, it is listed here for reference in the following rows.

row 13. Montgomery noted that every elliptic curve with torsion $\mathbb{Z}/2 \times \mathbb{Z}/8$ can be put in Montgomery form, and it can therefore be put in twisted Edwards form. This shows that the parameterizations of [AM93], [Mon92] and [BBLP13] describe the same set of elliptic curves. The following script checks that the family of Section 2.3.2 in [HMR16] is the same family in disguise.

```
def Kubert(b,c):
    return EllipticCurve([(1-c),-b,-b,00])
def AtkinMorain_8_2(alpha):
     d = alpha*(8*alpha+2)/(8*alpha^2-1)
     b = (2*d-1)*(d-1)
     c = (2*d-1)*(d-1)/d
     return Kubert(b,c)
def HeerMcGuireRobinson_2_3_2(t):
    nu = (t^4-6*t^2+1)/(4*(t^2+1)^2)
    b = nu^2-1/16
    return Kubert(b,0)
Q.<t> = QQ[]; K = Q.fraction_field(); t = K(t)
assert AtkinMorain_8_2(t).is_isomorphic(HeerMcGuireRobinson_2_5_1(4*t+1))
```

rows 14. In Sections 3.1, 3.5 and 3.7 of [BC10] we have respectively parameterizations of the curves such that $\mathrm{E}[n](\mathbb{Q}(\zeta_3)) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $n = 3$, 4 and respectively 5. The Galois image in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ has order $\varphi(n)$ and surjective determinant, so the corresponding group is $\{\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/n\mathbb{Z})^*\}$. We identify these groups as corresponding to $3\mathrm{D}^0$-$3a$T1, X_{58i} and respectively $5\mathrm{H}^0$-$5a$T1.

row 15. In the previous paragraph, we explained how to identify the Galois image. The following script checks that the family in Section 3.2 of [BC10] an the family in Section 3.5.1 of [HMR16] coincide.

```
def HeerMcGuireRobinson_2_3_1(t):
    mu = (2*t^3+1)/(3*t^2)
    a = -27*mu*(mu^3+8)
    b = 54*(mu^6-20*mu^3-8)
    return EllipticCurve([a,b])
def BrierClavier_3_2(lam,tau):
    a = (-3)*lam^4*(tau^12-8*tau^9+240*tau^6-464*tau^3+16)
    b = (-2)*lam^6*(tau^18-12*tau^15-480*tau^12+3080*tau^9-12072*tau^6+4128*tau^3+64)
    return a,b
def twisted_BrierClavier(tau):
    Qt = tau.parent();  Q3.<s3> = QuadraticField(-3);  Qt3.<t> = Q3[]; tau = Qt3(tau)
    a,b = BrierClavier_3_2(s3/(3*tau),tau)
    Kt = Qt.fraction_field(); a = Kt(a); b = Kt(b)
    return EllipticCurve([a,b])
Q.<t> = QQ[]
assert twisted_BrierClavier(t).is_isomorphic(HeerMcGuireRobinson_2_3_1(-1/t))
```

row 16. The following script checks that the family of Section 3.5 of [BC10] and Section 3 of [BBL10]. It is interesting to note that this family is not equal to that of row 12. Indeed, the condition $a = -\square$ which was imposed in order to improve the arithmetic cost, also improved the torsion properties.

```
def BrierClavier_3_5(t):
    a = -27*(t^8+14*t^4+1)
    b = 54*(t^12-33*t^8-33*t^4+1)
```

```
    return EllipticCurve([a,b])
def BernsteinBirknerLange_3(e):
    def MontgomeryToWeierstrass(A, B):
        return EllipticCurve([0A/B,0 1/B^2,0])
    def twistedEdwardsToWeierstrass(a, d):
        return MontgomeryToWeierstrass(2*(a+d)/(a-d), 4/(a-d))
    return twistedEdwardsToWeierstrass(-1,-e^4).short_weierstrass_model()
Q.<t>=QQ[]; K = Q.fraction_field(); t = K(t)
BrierClavier_3_5(t).is_isomorphic(BernsteinBirknerLange_3(t))
```

row 17. Section 3.7 of [HMR16] and Table 3 give the same parameterization of the pairs $a(t), b(t)$: $a = -27t^{20} - 6156t^{15} - 13338t^{10} + 6156t^5 - 27$ and $b = 54t^{30} - 28188t^{25} - 540270t^{20} - 540270t^{10} + 28188t^5 + 54$.

row 18. and 19. The families Suyama-11 and Suyama-9/4 are obtained from Suyama by imposing additional conditions. For Suyama-11 the condition on a Montgomery curve $\mathcal{M}_{\mathrm{A,B}}$ is $(\mathrm{A}+2)/\mathrm{B} = -\square$, which in Edwards coordinates $\mathcal{E}_{a,d}$ is $a = -\square$. Hence, Suyama-11 is the intersection of X_{13f} and $3\mathrm{B}^0$-3aT2. Similarly, the family Suyama-9/4 is obtained from Suyama by the additional condition on $\mathcal{M}_{\mathrm{A,B}}$ is $\mathrm{B} = \square$, or equivalently in Edwards coordinates $\mathcal{E}_{a,d}$ the condition is $a - d = \square$. The unique twist of X_{13} such that $a - d$ is a square for all elements of the parameterization is X_{13d}. Hence, Suyama-9/4 is the intersection of X_{13d} and $3\mathrm{B}^0$-3aT2.

rows 20. to 23. Section 2.1 identified the families of these rows as corresponding to parameterizations of some subgroups H. to identify the label we tested several numerical curves in the families of [BBB+13] and computed the Galois group of $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[8])/\mathbb{Q})$.

IMJ-PRG, (Sorbonne Univ., Univ. Paris Diderot, CNRS), Inria, Paris
E-mail address: razvan.barbulescu@imj-prg.fr sudarshan.shinde@imj-prg.fr

label	parameterization
3B0-3aT1 3B0-3aT2	$a = -3(t+3)(t-27)^3$, $b = -2(t^2+18t-27)(t-27)^4$
3D0-3aT1	$a = -3(t^2-6t+36)(t+6)t$, $b = -2(t^2-6t-18)(t^4+6t^3+54t^2-108t+324)$
9B0-9aT1 9B0-9aT2	$a = -3(t^3+9t^2+27t+3)(t+3)$, $b = (-2t^6-36t^5-270t^4-1008t^3-1782t^2-972t+54)$
9C0-9aT1 9C0-9aT2	$a = -3(t^3+3)(t^2-3t+9)^3(t+3)^3$, $b = -2(t^6+18t^3-27)(t^2-3t+9)^4(t+3)^4$
9H0-9aT1	$a = -3(t^3+9)(t^3+3)(t^2+3t+3)(t^2-3t+3)(t^2+3)$, $b = -2(t^{12}+18t^9+162t^6+486t^3+729)(t^4+3t^2+9)(t^2-3)$
9H0-9bT1 9H0-9bT2	$a = -3(t^6-18t^5+171t^4+180t^3-297t^2-162t+189)(t^3+9t^2-9t-9)(t^3-3t^2-9t+3)$, $b = -2(t^{12}+126t^{10}-1944t^9+6723t^8+23328t^7-21708t^6-58320t^5+34263t^4+54432t^3$ $-24786t^2-17496t+9477)(t^6-18t^5-45t^4+180t^3+135t^2-162t-27)$
9H0-9cT1	$a = 144(t^6+9t^5+9t^4-90t^3+27t^2+81t+27)(t+3)(t+1)(t-1)(t-3)t$, $b = 16(t^{12}+18t^{11}+126t^{10}-18t^9-2025t^8-972t^7+13284t^6-2916t^5-18225$ $t^4-486t^3+10206t^2+4374t+729)(t^2+6t-3)(t^2-6\,t-3)(t^2-3)$
9I0-9aT1 9I0-9aT2	$a = -3(17t^9+9t^8-144t^6-918t^5+810t^4-3672t^3-648t^2-4131t-27)(t^3+3t^2-9t-3)$, $b = 142t^{18}+684t^{17}-162t^{16}-10944t^{15}-10152t^{14}+24624t^{13}$ $-131976t^{12}+393984t^{11}+834948t^{10}-1128600t^9+1628100t^8-7978176t^7+$ $12435768t^6-4210704t^5+14154264t^4+12410496t^3+8314974t^2+498636t-1458$
9I0-9bT1 9I0-9bT2	$a = -144(t^3+9t^2-9t+15)(t^3+9t+6)(t^3-3)(t+1)(t-1)$, $b = 16(t^6+12t^5+27t^4+48t^3-9t^2-108t-99)$ $(t^6+12t^5-9t^4+12t^3-9t^2+9)(t^6-6t^5+63t^4-132t^3+207t^2-54t-207)$
9I0-9cT1 9I0-9cT2	$a = -3(t^9-9t^8+27t^7-48t^6+54t^5-45t^4+27t^3-9t^2+1)(t^3-3t^2+1)$, $b = -2t^{18}+36t^{17}-270t^{16}+1140t^{15}-3114t^{14}+5940t^{13}-8256t^{12}+8460t^{11}$ $-6480t^{10}+4064t^9-2718t^8+2160t^7-1470t^6+612t^5-54t^4-84t^3+36t^2-2$
9J0-9aT1 9J0-9aT2	$a = -3(t^9-9t^7+6t^6+18t^5-9t^4-27t^3+27t^2-9t+1)(t^3+3t^2-6t+1)^3(t^2-t+1)$, $b = -2(t^{18}-18t^{16}+24t^{15}+81t^{14}-198t^{13}-30t^{12}+540t^{11}-828t^{10}+884t^9-729t^8$ $-180t^7+1491t^6-1944t^5+1341t^4-552t^3+135t^2-18t+1)(t^3+3t^2-6t+1)^4$
9J0-9bT1 9J0-9bT2	$a = -3(t^9-9t^8-1800t^6-54t^5+5022t^4-216t^3-5184t^2-243t+1971)$ $(t^3-9t^2-9t+9)^3(t^2+3)$, $b = -2(t^{18}-18t^{17}+81t^{16}+4176t^{15}-37692t^{14}-12312t^{13}-559980t^{12}-208656t^{11}$ $+2381886t^{10}-184140t^9-4348242t^8+1154736t^7+6764148t^6+635688t^5-8021916t^4$ $-2321136t^3+5447817t^2+931662t-1363959)(t^3-9t^2-9t+9)^4$
9J0-9cT1 9J0-9cT2	$a = -3(5t^3-9t^2-9t-3)(t^3+9t^2+27t+3)(t^3-9t+12)(t^2+3)(t+3)^3(t-3)^3t^3$, $b = 2(11t^6-6t^5-63t^4+156t^3-99t^2-54t-9)(t^6+6t^5-9t^4-12t^3-225t^2+486t+9)$ $(t^6+6t^5-48t^3-63t^2-54t-18)(t+3)^4(t-3)^4t^4$
27A0-27aT1 27A0-27aT2	$a = -3(t^9+9t^6+27t^3+3)(t^3+3)$, $b = -2t^{18}-36t^{15}-270t^{12}-1008t^9-1782t^6-972t^3+54$

??

TABLE 2. Curves with exceptional Galois images in $\mathrm{GL}_2(\mathbb{Z}_3)$ associated to groups which do not contain $-\mathrm{I}$. For each subgroup H containing $-\mathrm{I}$ we call ⟨label H⟩T1, ⟨label H⟩T2, ... the subgroups of H of index 2, up to conjugacy, which do not contain $-\mathrm{I}$. The parameterization (a,b) corresponds to T1 and the parameterization $(9a, -27b)$ corresponds to T2. If H has a unique index two subgroup, up to conjugacy, then the parameterization $(9a, -27b)$ is a second family of Galois group T1.

label	parameterization
5D0-5aT1 5D0-5aT2	$a = -27t^4 - 6156t^3 - 13338t^2 + 6156t - 27,$ $b = 54(t^4 - 522t^3 - 10006t^2 + 522t + 1)(t^2 + 1)$
5D0-5bT1 5D0-5bT2	$a = -27t^4 + 324t^3 - 378t^2 - 324t - 27,$ $b = 54(t^4 - 18t^3 + 74t^2 + 18t + 1)(t^2 + 1)$
5H0-5aT1 5H0-5aT2	$a = -27(t^8 + t^7 + 7t^6 - 7t^5 + 7t^3 + 7t^2 - t + 1)$ $(t^8 - 4t^7 + 7t^6 - 2t^5 + 15t^4 + 2t^3 + 7t^2 + 4t + 1)(t^4 + 3t^3 - t^2 - 3t + 1),$ $b = 54(t^8 + 6t^7 + 17t^6 + 18t^5 + 25t^4 - 18t^3 + 17t^2 - 6t + 1)$ $(t^8 - 4t^7 + 17t^6 - 22t^5 + 5t^4 + 22t^3 + 17t^2 + 4t + 1)$ $(t^8 - t^6 + t^4 - t^2 + 1)(t^4 - 2t^3 - 6t^2 + 2t + 1)(t^2 + 1)$
25B0-25aT1 25B0-25aT2	$a = -27t^{20} - 324t^{15} - 378t^{10} + 324t^5 - 27,$ $b = 54(t^{20} + 18t^{15} + 74t^{10} - 18t^5 + 1)(t^8 - t^6 + t^4 - t^2 + 1)(t^2 + 1)$
25B0-25bT1 25B0-25bT2	$a = -27t^{20} - 6480t^{19} - 58320t^{18} - 181440t^{17} - 473040t^{16} - 816156t^{15} - 1561680t^{14}$ $-1645920t^{13} - 2157840t^{12} - 1121040t^{11} - 1633338t^{10} + 1121040t^9 - 2157840t^8$ $+1645920t^7 - 1561680t^6 + 816156t^5 - 473040t^4 + 181440t^3 - 58320t^2 + 6480t - 27,$ $b = -54(t^{20} - 510t^{19} - 13590t^{18} - 32280t^{17} - 82230t^{16} - 153522t^{15}$ $-302910t^{14} - 273540t^{13} - 412830t^{12} - 268230t^{11} - 262006t^{10} + 268230t^9$ $-412830t^8 + 273540t^7 - 302910t^6 + 153522t^5 - 82230t^4 + 32280t^3 - 13590t^2 + 510t + 1)$ $(t^8 + 6t^7 + 17t^6 + 18t^5 + 25t^4 - 18t^3 + 17t^2 - 6t + 1)(t^2 + 1)$
7B0-7aT1 7B0-7aT2	$a = -27(t^2 + 13t + 49)^3(t^2 + 5t + 1),$ $b = 54(t^4 + 14t^3 + 63t^2 + 70t - 7)(t^2 + 13t + 49)^4$
7E0-7aT1 7E0-7aT2	$a = -27(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1)(t^2 - t + 1),$ $b = 54t^{12} - 28188t^{11} - 483570t^{10} + 2049300t^9 - 3833892t^8 + 7104348t^7$ $-13674906t^6 + 17079660t^5 - 11775132t^4 + 4324860t^3 - 790074t^2 + 27540t + 54$
7E0-7bT1 7E0-7bT2	$a = -432(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)(t^2 - t + 1),$ $b = 3456t^{12} - 62208t^{11} + 404352t^{10} - 1223424t^9 + 1969920t^8 - 1679616t^7$ $+943488t^6 - 767232t^5 + 601344t^4 - 158976t^3 - 51840t^2 + 20736t + 3456$
7E0-7cT1 7E0-7cT2	$a = -189(5t^2 - t - 1)(3t^2 - 9t + 5)(t^2 - t + 1)(t^2 - 3t - 3),$ $b = -2646(9t^4 - 12t^3 - t^2 + 8t - 3)(3t^4 - 4t^3 - 5t^2 - 2t - 1)(t^4 - 6t^3 + 17t^2 - 24t + 9)$
13B0-13aT1 13B0-13aT2	$a = -3(t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1)$ $(t^4 - t^3 + 5t^2 + t + 1)^3,$ $b = -2(t^{12} - 512t^{11} - 13079t^{10} - 32300t^9 - 104792t^8 - 111870t^7$ $-419368t^6 + 111870t^5 - 104792t^4 + 32300t^3 - 13079t^2$ $+512t + 1)(t^4 - t^3 + 5t^2 + t + 1)^4(t^2 + 1)$
13B0-13bT1 13B0-13bT2	$a = -27(t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1)(t^4 - t^3 + 5t^2 + t + 1)^3,$ $b = 54(t^{12} - 8t^{11} + 25t^{10} - 44t^9 + 40t^8 + 18t^7 - 40t^6 - 18t^5 + 40t^4 + 44t^3 + 25t^2 + 8t + 1)$ $(t^4 - t^3 + 5t^2 + t + 1)^4(t^2 + 1)$

TABLE 3. Curves with exceptional Galois image in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell = 5, 7, 13$ corresponding to groups which do not contain $-\mathrm{I}$. For each subgroup H containing $-\mathrm{I}$ we call ⟨label H⟩T1, ⟨label H⟩T2, ... the subgroups of H of index 2, up to conjugacy, which do not contain $-\mathrm{I}$. Set $\epsilon = 1$ if -1 is a square mod ℓ, -1 otherwise. The parameterization (a,b) corresponds to T1 and the parameterization $(\ell^2 a, \epsilon\ell^3 b)$ corresponds to T2. If H has a unique index two subgroup, up to conjugacy, then the parameterization $(\ell^2 a, \epsilon\ell^3 b)$ is a second family of Galois group T1.

#	Family	label in our tables	comment	$\subset$
1	Section 10.3.1 of [Mon87] Section 2.1 of [BBLP13]	X_{13}	Montgomery form twisted Edwards	1
2	Section 1.1 of [BBL10]	X_{13f}	$a = -\square$ twisted Edwards	1
3	Section 2.1 of [BBLP13]	X_{13h}	$E(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ Edwards curves $a = \square$ twisted Edwards	1
4	Section 2 of [BCKL15]	$3B^0$-$3a$	isogenous to a curve with a point of order 3	
5	Section 10.3.2 of [Mon87] and [Suy85]	X_{13}, $3B^0$-$3a$T2	Suyama	1,4
6	Section 3.2 of [AM93]	$5D^0$-$5b$T1	$E(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$	
7	Section 3.3 of [AM93]	$7E^0$-$7b$T1	$E(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z}$	
8	Section 4. of [BBL10]	X_{195l}	$E(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$	3
9	Section 3.4 of [AM93]	$9I^0$-$9c$T2	$E(\mathbb{Q}) \simeq \mathbb{Z}/9\mathbb{Z}$	4
10	Section 3.5 of [AM93]	X_6, $5D^0$-$5b$T1	$E(\mathbb{Q}) \simeq \mathbb{Z}/10\mathbb{Z}$	6
11	Section 6.1 of [Mon92] Section 6.1 of [BBLP13]	X_{13h}, $3B^0$-$3a$T2	$E(\mathbb{Q}) \simeq \mathbb{Z}/12\mathbb{Z}$	3,4
12	page 217 of [Kub76]	X_{25n}	$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1,3
13	Section 6.2 of [Mon92] Section 3.1 of [AM93] Section 6.5 of [BBLP13] Section 3.5.2 of [HMR16]	X_{193n}	$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1,3,8,12
14	Section 3.1 of [BC10]	$3D^0$-$3a$T1	$E(\mathbb{Q}(\zeta_3)) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	4
15	Section 3.2 of [BC10] Section 3.5.1 of [HMR16]	X_6, $3D^0$-$3a$T1	$E(\mathbb{Q}(\zeta_3)) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	4,14
16	Section 3.5 of [BC10] Section 3 of [BBL10]	X_{58i}	$E(\mathbb{Q}(i)) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1,3,12
17	Section 3.7 of [BC10]	$5H^0$-$5a$T1	$E(\mathbb{Q}(\zeta_5)) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	6
18	Section 5 of [BBL10] Section 3.5.1 of [BBB+13]	X_{13f}, $3B^0$-$3a$T2	Suyama-11 exceptional Galois	1,2,4,5
19	Section 3.5.3 of [BBB+13]	X_{13d}, $3B^0$-$3a$T2	Suyama-9/4 exceptional Galois	1,4,5
20	Section 3.4.1 of [BBB+13], $e = g^2$	X_{183d}	exceptional Galois	1,3,12,16
21	Section 3.4.1 of [BBB+13], $e = \frac{2g^2+2g+1}{2g+1}$	X_{183i}	exceptional Galois	1,3,12,16
22	Section 3.4.1 of [BBB+13], $e = \frac{g^2}{2}$	X_{187d}	exceptional Galois	1,3,12,16
23	Section 3.4.1 of [BBB+13], $e = \frac{g^2-1}{2g}$	X_{189d}	exceptional Galois	1,3,12,16

TABLE 4. Correspondence between ECM-friendly families in the literature and the families in Theorem 4.1.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
X189d	-3.4305	✓	✓	✓	✗
X192i	-3.4305	✓	✗	✓	✗
X193n	-3.4305	✓	✓	✗	✗
X207n	-3.4305	✓	✓	✓	✗
X211m	-3.4305	✓	✗	✓	✗
X235l	-3.4305	✓	✓	✗	✗
X13d-3B0-3aT1	-3.3825	✓	✗	✗	✓
X13d-3B0-3aT2	-3.3825	✓	✗	✗	✓
X13f-3B0-3aT1	-3.3825	✓	✗	✓	✓
X13f-3B0-3aT2	-3.3825	✓	✗	✓	✓
X13h-3B0-3aT1	-3.3825	✓	✓	✗	✓
X13h-3B0-3aT2	-3.3825	✓	✓	✗	✓
X8d-3B0-3aT1	-3.3825	✗	✗	✗	✓
X8d-3B0-3aT2	-3.3825	✗	✗	✗	✓
X6-5D0-5aT1	-3.1922	✗	✗	✗	✗
X6-5D0-5bT1	-3.1922	✗	✗	✗	✗
X15-5D0-5aT1	-3.1886	✗	✗	✗	✗
X15-5D0-5bT1	-3.1886	✗	✗	✗	✗
X19-5D0-5aT1	-3.1886	✗	✗	✗	✗
X19-5D0-5bT1	-3.1886	✗	✗	✗	✗
X13-3B0-3aT1	-3.1514	✓	✗	✗	✓
X13-3B0-3aT2	-3.1514	✓	✗	✗	✓
X8-3B0-3aT1	-3.1514	✗	✗	✗	✓
X8-3B0-3aT2	-3.1514	✗	✗	✗	✓
X13c-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13c-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT2	-3.1442	✓	✗	✗	✓
X8c-3B0-3aT1	-3.1442	✗	✗	✗	✓
X8c-3B0-3aT2	-3.1442	✗	✗	✗	✓
X6-3D0-3aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT2	-3.1013	✗	✗	✗	✓
X16-3D0-3aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT2	-3.0977	✗	✗	✗	✓
X17-3D0-3aT1	-3.0977	✗	✗	✗	✓
X17-9B0-9aT1	-3.0977	✗	✗	✗	✓
X17-9B0-9aT2	-3.0977	✗	✗	✗	✓
X183d	-3.0839	✓	✓	✓	✗
X183i	-3.0839	✓	✓	✓	✗
X185g	-3.0839	✓	✓	✗	✗
X185h	-3.0839	✓	✗	✓	✗
X187d	-3.0839	✓	✓	✓	✗
X187k	-3.0839	✓	✓	✓	✗
X189e	-3.0839	✓	✓	✓	✗
X192g	-3.0839	✓	✓	✗	✗
X193i	-3.0839	✓	✗	✓	✗

TABLE 5. Best 50 families characterized by α(E) over $\mathbb{Q}$.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
X6-3D0-3aT1	-3.7193	✗	✗	✗	✓
X6-9B0-9aT1	-3.7193	✗	✗	✗	✓
X6-9B0-9aT2	-3.7193	✗	✗	✗	✓
X16-3D0-3aT1	-3.7156	✗	✗	✗	✓
X16-9B0-9aT1	-3.7156	✗	✗	✗	✓
X16-9B0-9aT2	-3.7156	✗	✗	✗	✓
X17-3D0-3aT1	-3.7156	✗	✗	✗	✓
X17-9B0-9aT1	-3.7156	✗	✗	✗	✓
X17-9B0-9aT2	-3.7156	✗	✗	✗	✓
X13d-3B0-3aT1	-3.5884	✓	✗	✗	✓
X13d-3B0-3aT2	-3.5884	✓	✗	✗	✓
X13f-3B0-3aT1	-3.5884	✓	✗	✓	✓
X13f-3B0-3aT2	-3.5884	✓	✗	✓	✓
X13h-3B0-3aT1	-3.5884	✓	✓	✗	✓
X13h-3B0-3aT2	-3.5884	✓	✓	✗	✓
X8d-3B0-3aT1	-3.5884	✗	✗	✗	✓
X8d-3B0-3aT2	-3.5884	✗	✗	✗	✓
X189d	-3.4305	✓	✓	✓	✗
X192i	-3.4305	✓	✗	✓	✗
X193n	-3.4305	✓	✓	✗	✗
X207n	-3.4305	✓	✓	✓	✗
X211m	-3.4305	✓	✗	✓	✗
X235l	-3.4305	✓	✓	✗	✗
X13-3B0-3aT1	-3.3574	✓	✗	✗	✓
X13-3B0-3aT2	-3.3574	✓	✗	✗	✓
X8-3B0-3aT1	-3.3574	✗	✗	✗	✓
X8-3B0-3aT2	-3.3574	✗	✗	✗	✓
X13c-3B0-3aT1	-3.3502	✓	✗	✗	✓
X13c-3B0-3aT2	-3.3502	✓	✗	✗	✓
X13e-3B0-3aT1	-3.3502	✓	✗	✗	✓
X13e-3B0-3aT2	-3.3502	✓	✗	✗	✓
X13g-3B0-3aT1	-3.3502	✓	✗	✗	✓
X13g-3B0-3aT2	-3.3502	✓	✗	✗	✓
X8c-3B0-3aT1	-3.3502	✗	✗	✗	✓
X8c-3B0-3aT2	-3.3502	✗	✗	✗	✓
9H0-9bT1	-3.2237	✗	✗	✗	✓
9H0-9bT2	-3.2237	✗	✗	✗	✓
9I0-9aT1	-3.2237	✗	✗	✗	✓
9I0-9aT2	-3.2237	✗	✗	✗	✓
9I0-9cT1	-3.2237	✗	✗	✗	✓
9I0-9cT2	-3.2237	✗	✗	✗	✓
X6-5D0-5aT1	-3.1922	✗	✗	✗	✗
X6-5D0-5bT1	-3.1922	✗	✗	✗	✗
X15-5D0-5aT1	-3.1886	✗	✗	✗	✗
X15-5D0-5bT1	-3.1886	✗	✗	✗	✗
X19-5D0-5aT1	-3.1886	✗	✗	✗	✗
X19-5D0-5bT1	-3.1886	✗	✗	✗	✗
X183d	-3.0839	✓	✓	✓	✗
X183i	-3.0839	✓	✓	✓	✗
X185g	-3.0839	✓	✓	✗	✗

TABLE 6. Best 50 families characterized by α(E) over $\mathbb{Q}(\zeta_3)$.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
X183d	-3.6616	✓	✓	✓	✗
X183i	-3.6616	✓	✓	✓	✗
X185g	-3.6616	✓	✓	✗	✗
X185h	-3.6616	✓	✗	✓	✗
X187d	-3.6616	✓	✓	✓	✗
X187k	-3.6616	✓	✓	✓	✗
X189d	-3.6616	✓	✓	✓	✗
X189e	-3.6616	✓	✓	✓	✗
X192g	-3.6616	✓	✓	✗	✗
X192i	-3.6616	✓	✗	✓	✗
X193i	-3.6616	✓	✗	✓	✗
X193n	-3.6616	✓	✓	✗	✗
X194k	-3.6616	✓	✗	✓	✗
X194l	-3.6616	✓	✓	✗	✗
X195h	-3.6616	✓	✓	✓	✗
X195l	-3.6616	✓	✓	✓	✗
X205h	-3.6616	✓	✓	✓	✗
X205i	-3.6616	✓	✓	✓	✗
X207l	-3.6616	✓	✓	✓	✗
X207n	-3.6616	✓	✓	✓	✗
X208a	-3.6616	✓	✗	✓	✗
X208c	-3.6616	✓	✓	✗	✗
X211m	-3.6616	✓	✗	✓	✗
X211s	-3.6616	✓	✓	✗	✗
X212h	-3.6616	✓	✗	✓	✗
X212i	-3.6616	✓	✓	✗	✗
X213h	-3.6616	✓	✗	✓	✗
X213i	-3.6616	✓	✓	✗	✗
X215c	-3.6616	✓	✓	✗	✗
X215l	-3.6616	✓	✗	✓	✗
X225g	-3.6616	✓	✗	✓	✗
X225h	-3.6616	✓	✓	✗	✗
X227i	-3.6616	✓	✓	✗	✗
X227k	-3.6616	✓	✗	✓	✗
X235i	-3.6616	✓	✗	✓	✗
X235l	-3.6616	✓	✓	✗	✗
X240h	-3.6616	✓	✗	✓	✗
X240l	-3.6616	✓	✓	✗	✗
X243d	-3.6616	✓	✓	✗	✗
X243g	-3.6616	✓	✗	✓	✗
X10d-3B0-3aT1	-3.4980	✗	✗	✗	✓
X10d-3B0-3aT2	-3.4980	✗	✗	✗	✓
X13d-3B0-3aT1	-3.4980	✓	✗	✗	✓
X13d-3B0-3aT2	-3.4980	✓	✗	✗	✓
X13f-3B0-3aT1	-3.4980	✓	✗	✓	✓
X13f-3B0-3aT2	-3.4980	✓	✗	✓	✓
X13h-3B0-3aT1	-3.4980	✓	✓	✗	✓
X13h-3B0-3aT2	-3.4980	✓	✓	✗	✓
X8d-3B0-3aT1	-3.4980	✗	✗	✗	✓
X8d-3B0-3aT2	-3.4980	✗	✗	✗	✓

TABLE 7. Best 50 families characterized by α(E) over $\mathbb{Q}(i)$.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
25B0-25aT1	-4.0148	✗	✗	✗	✗
25B0-25aT2	-4.0148	✗	✗	✗	✗
25B0-25bT1	-4.0148	✗	✗	✗	✗
25B0-25bT2	-4.0148	✗	✗	✗	✗
5H0-5aT1	-4.0148	✗	✗	✗	✗
5H0-5aT2	-4.0148	✗	✗	✗	✗
X6-5D0-5aT1	-3.4437	✗	✗	✗	✗
X6-5D0-5aT2	-3.4437	✗	✗	✗	✗
X6-5D0-5bT1	-3.4437	✗	✗	✗	✗
X6-5D0-5bT2	-3.4437	✗	✗	✗	✗
X15-5D0-5aT1	-3.4401	✗	✗	✗	✗
X15-5D0-5aT2	-3.4401	✗	✗	✗	✗
X15-5D0-5bT1	-3.4401	✗	✗	✗	✗
X15-5D0-5bT2	-3.4401	✗	✗	✗	✗
X19-5D0-5aT1	-3.4401	✗	✗	✗	✗
X19-5D0-5aT2	-3.4401	✗	✗	✗	✗
X19-5D0-5bT1	-3.4401	✗	✗	✗	✗
X19-5D0-5bT2	-3.4401	✗	✗	✗	✗
X189d	-3.4305	✓	✓	✓	✗
X192i	-3.4305	✓	✗	✓	✗
X193n	-3.4305	✓	✓	✗	✗
X207n	-3.4305	✓	✓	✓	✗
X211m	-3.4305	✓	✗	✓	✗
X235l	-3.4305	✓	✓	✗	✗
X13d-3B0-3aT1	-3.3825	✓	✗	✗	✓
X13d-3B0-3aT2	-3.3825	✓	✗	✗	✓
X13f-3B0-3aT1	-3.3825	✓	✗	✓	✓
X13f-3B0-3aT2	-3.3825	✓	✗	✓	✓
X13h-3B0-3aT1	-3.3825	✓	✓	✗	✓
X13h-3B0-3aT2	-3.3825	✓	✓	✗	✓
X8d-3B0-3aT1	-3.3825	✗	✗	✗	✓
X8d-3B0-3aT2	-3.3825	✗	✗	✗	✓
X13-3B0-3aT1	-3.1514	✓	✗	✗	✓
X13-3B0-3aT2	-3.1514	✓	✗	✗	✓
X8-3B0-3aT1	-3.1514	✗	✗	✗	✓
X8-3B0-3aT2	-3.1514	✗	✗	✗	✓
X13c-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13c-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT2	-3.1442	✓	✗	✗	✓
X8c-3B0-3aT1	-3.1442	✗	✗	✗	✓
X8c-3B0-3aT2	-3.1442	✗	✗	✗	✓
X6-3D0-3aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT2	-3.1013	✗	✗	✗	✓
X16-3D0-3aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT2	-3.0977	✗	✗	✗	✓

TABLE 8. Best 50 families characterized by α(E) over $\mathbb{Q}(\zeta_5)$.