A complete classification of ECM-friendly families using modular curves

Razvan Barbulescu, Sudarshan Shinde

A COMPLETE CLASSIFICATION OF ECM-FRIENDLY FAMILIES USING MODULAR CURVES -PRELIMINARY VERSION-

RAZVAN BARBULESCU AND SUDARSHAN SHINDE

Abstract. The number field sieve, an algorithm with major applications in cryptography, uses the elliptic curve method of factorization (ECM) as a building block. It is a motivation to search parameterizations of infinite families of elliptic curves defined over a given number field K with exceptional image of ℓ-adic Galois representation. This boils down to making the complete list of finite indexed subgroups H of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ of genus 0 and 1 and computing K-rational points on the modular curve X_H. Fast algorithms for this latter step are proposed in [SZ17] and [RZB15]. We measure the consequences on ECM of the newly found families using a heuristic of Montgomery.

1. Introduction

Integer factorization is an important problem in algorithmic number theory and cryptology. The factoring algorithms are naturally split into two classes : on the one hand these whose cost depends 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 cost depends on the size of the factors we search, except for 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 $N = pq$ where p and q are two primes of equal bit size. However, ECM is used as a subroutine by NFS and, in computations of cryptologic relevance, ECM takes an important fraction of the cost of NFS. A second important problem in cryptology is that of computing discrete logarithms, i.e. in a cyclic group G of generator g given g^x find x, for which 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 uses elliptic curves E with rational coefficients and a point $\mathrm{P} \in E(\mathbb{Q})$ with denominators relatively prime to N and computes $P_M := [M]\cdot \mathrm{P}$, while keeping the coordinates modulo N, for some integer M with many prime factors; if $\#\,\mathrm{E}(\mathbb{F}_p)$ divides M, P_M is the neutral element of $E(\mathrm{F}_p)$, which allows us to find p.

The choice of M varies from one implementation to another, but as a first approximation we take $M = \mathrm{B}!^{\log_2 B}$ for some integer B. The condition for success is then that $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth i.e. all its prime factors are less than B. By Hasse's theorem [Has36], 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 less than p to be B-smooth. In the original variant of ECM, as proposed by Lenstra [LJ87], one selects at random uniformly integers x, y and a in $[0, p-1]$ and sets $b = y^2 - x^3 - ax$ so that $(x, y) \in E(\mathrm{F}_p)$. 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 $\frac{1}{\mathcal{O}(\log p)}$ the proportion of integer in $[p-\sqrt{p}, p+\sqrt{p}]$ which are B-smooth.

In cryptologic applications, ECM is used in its variant where the elliptic curves E are selected from families of curves with rational coefficients. Soon after ECM was published, Montgomery [Mon87] introduced a parametrization, $By^2 = x^3+Ax^2+x$, which speeds up the point addition and doubling. Montgomery also suggested to use infinite families of elliptic curves in the Montgomery parametrization in order to guarantee that $\#\,\mathrm{E}(\mathbb{F}_p)$ has known smaller factors. Indeed, by [Sil08, Prop. 3.1 (ch 7)], when E has good reduction modulo p, $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$ embeds in $\mathrm{E}(\mathbb{F}_p)$, so $\#E_{\mathrm{tors}}$ divides $\#E(\mathrm{F}_p)$. Experimentally, this increases the proportion of primes p where $\#E(\mathrm{F}_p)$ is B-smooth.

An important direction of improvements for ECM was to select families of elliptic curves over $\mathbb{Q}$. Since the number of curves used to factor a given integer is not known in advance, we restrict the research to infinite families.

Montgomery gave infinite families of elliptic curves in Mongomery form having 12 and respectively 16 rational torsion points. Suyama [Suy85] proposed an infinite family of curves E in Montgomery form having 6 torsion points such that, for any prime p, 12 divides $\#\,\mathrm{E}(\mathrm{F}_p)$. Later, Atkin and Morain [AM93] proposed infinite families for each other possible torsion groups over $\mathbb{Q}$. In 2010, Brier and Clavier [BC10] found families of curves defined over $\mathbb{Q}$ which have large torsion subgroups over $\mathbb{Q}(i)$. In 2010 and 2011, Bernstein, Birkner, Lange [BBL10], and the same group and Peters [BBLP13] proposed infinite families of Edwards curves, i.e. of the form $x^2 + y^2 = 1 + dx^2y^2$, which have a faster point addition. The families they proposed have 6, 8 and respectively 16 torsion points over $\mathbb{Q}$ and are isomorphic over $\mathbb{Q}$ to known families of Montgomery curves. In 2016 Heer, McGuire and Robinson [HMR16] present families defined over number fieds K which have large torsion subgroups over K.

In 2012, Barbulescu, Bos, Bouvier, Kleinjung and Montgomery [BBB$^+$13] found better infinite subfamilies of the Suyama family which have the same number of torsion points over any fixed number field and infinite families of elliptic curves having a torsion subgroup $\mathbb{Z}/2\times\mathbb{Z}/4$ and yet better smoothness properties than the general curves with this torsion. For this, they related the study of ECM-friendly curves to the study of a particular Galois group. For a rational elliptic curve E and an integer m, the m-torsion field $\mathbb{Q}(\mathrm{E}[m])$ is the number field generated by $\mathrm{E}(\bar{\mathbb{Q}})[m]$. This field is an extension of $\mathbb{Q}$ (Prop. 2.3 in [BBB$^+$13]). As $\mathrm{E}(\bar{\mathbb{Q}})[m] \simeq \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$, there exists an injective map

$$\rho_{\mathrm{E},m} : \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

By Serre's work [Ser71] we know that the index of $\Im(\rho_{E,m})$ is bounded independently of m. Shimura's work [Shi71] implies that, for a given m, the Galois image is surjective for all elliptic curve except a subset verifying algebraic equations. Barbulescu et al. proved a formula which relates the smoothness properties to the Galois groups of torsion fields : it is impossible to change the smoothness properties of $\#\,\mathrm{E}(\mathbb{F}_p)$ without changing the Galois group of $\mathbb{Q}(E[m])$ for some m.

Recently, Sutherland and Zwyina [SZ17] and Rouse and Zureick-Brown [RZB15] studied all the infinite families of rational elliptic curves whose Galois group of $\mathbb{Q}(E[m])$, for a prime power m, is isomorphic to some subgroup H of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

They obtained the complete classification when m is a power of 2 and when H contains $-I$.

Roadmap:

(1) Elliptic curve method
(2) Looking for ECM-friendly curves using computer algebra systems
(3) ECM-friendly curves using modular curves
(4) Tools to compare different families of curves

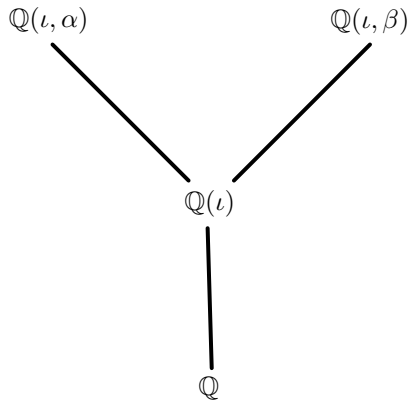
2. Cryptologic utilization of ECM

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 $\mathbb{Z}/N\mathbb{Z}$ and we used the L notation

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

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 proportio of those ϕ such that $N_{\mathbb{Q}(\alpha)}(\phi(\alpha))$ and $N_{\mathbb{Q}(\beta)}(\phi(\beta))$ are B-smooth for $B = L_N(1/3, \sqrt[3]{8/9})$. 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 F_{p^n} for a prime p, the best asymptotic complexity is obtained by the extended tower number field sieve (exTNFS) [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 $\mathrm{F}_p[t]/\langle h\rangle$, the polynomial $f(\omega, x)$ and $g(\omega, x)$ have a common irreducible factor $\varphi \in \mathrm{F}_p(\omega)[x]$ 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 $B = L_{p^n}(1/3, \sqrt[3]{8/9})$. 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 $h = h_0+h_1t+h_2x^t$ for $h_0, h_1, h_2 \in \mathbb{Z}$, $N_{\mathbb{Q}(\iota,\alpha)}(a(\iota) - \alpha b(\iota)) = N_{\mathbb{Q}(\iota)}(a' - \iota b') = h_0v^2 + h_1uv + h_2u^2$, 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 $h_2u^2 + h_1uv + h_0v^2$ 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.

3. A research of families using computer algebra

The numerous families of ECM-friendly curves in the literature were found by methods which are not guaranteed to produce the exhaustive list of families. In this section we discuss a computer algebra algorithm which allows us to find all the families in the literature in a unified manner.

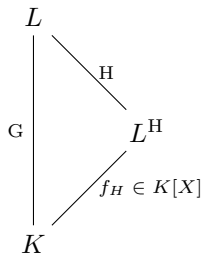


FIGURE 1

From a computer algebra point of view, the problem we are tackling is a particular case of the inverse Galois problem: given an algebraic extension K of $\mathbb{Q}(a_1, \ldots, a_t)$, the field of rational fractions in t variables, and a finite Galois extension L of K defined by a polynomial $f \in K[x]$, compute for each subgroup H of $G := \mathrm{Gal}(L/K)$ a parametrization of the coefficients of f so that $\mathrm{Gal}(f)$ is conjugated in $\mathrm{Gal}(L/K)$ to a subgroup of H.

In general, this version of the inverse Galois problem can be solved algorithmically as follows. First, one factors f in $L[x]$ and obtains the list of automorphisms of L/K. Then one computes the list of subgroups H of G. Thirdly, for each H, one solves a linear system to obtain L^H. Finally, one computes a primitive element θ of L^H together with its minimal polynomial F_H over K and obtains the equivalence:

$$\mathrm{Gal}(f) \subset H \text{ if and only if } \exists\ \theta \in K, f_H(\theta) = 0,$$

which is illustrated in Figure 1.

The algebraic conditions hence obtained can then be used to create parametrizations. Although the problem of parametrizing an algebraic set is open in the general case, in this article we will need to treat solely plane curves. Let $\mathcal{C}$ be a plane curve and K a number field for which we search a parametrization of the K-rational points of $\mathcal{C}$. One starts by computing the genus g of $\mathcal{C}$. If $g \geq 2$, Faltings' theorem implies that there is no parametrization of the solutions of f_H over K (the set of solutions is finite). If $g = 1$ and we can find a K-rational point, $\mathcal{C}$ is an elliptic curve and, if we can find a non-torsion K-rational point then we have an infinite parametrization. If $g = 0$ and we are able to find a K-rational point, then $\mathcal{C}$ is a conic and we have a K-rational parametrization of the family. Let us take a first example.

Exemple 3.1 (Sec 3.4.1 in [BBB+13])**.** We consider the twisted Edwards curves, $\mathcal{E}_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$. We are given the family $a = -1$ and $d = -e^4$ for which $\mathrm{Gal}(\mathcal{E}_{-1,-e^4}[8]/\mathbb{Q}(e))$ is of order 32, and we look for an equation satisfied by the rational values of e such that, for the elliptic curve E corresponding to e, $\mathrm{Gal}(\mathrm{E}/\mathbb{Q})$ is contained in a proper subgroup of $\mathrm{Gal}(\mathcal{E}_{-1,-e^4}[8]/\mathbb{Q}(e))$. For a generic value of d, we consider the irreducible factors of the exact quotient of 8-division polynomial Ψ_8 by the 4-division polynomial Ψ_4. As Ψ_4 divides Ψ_8, this quotient Ψ_8^{exact} is a polynomial in $\mathbb{Q}(d)[X]$. The roots of Ψ_8^{exact} correspond to the points of order 8. We notice that Ψ_8^{exact} has 2 irreducible quartic factors and a factor of degree 16. Let us denote by these factors by $P_{8,0}$, $P_{8,1}$, $P_{8,2}$.

We solve the Galois inverse problem for $K = \mathbb{Q}(e)$ and L is the function field of one of the factors of Ψ_8.

- For $P_{8,0}$, there are exactly 3 non-trivial subfields which are all quadratic. These fields are defined by x^2+2e, $x^2-(e^2+1)$ and x^2+2e^3+2e. The last equation is an elliptic curve of rank 0 over $\mathbb{Q}$ thus the familly is finite. As the first two are the conics with rational points, we parametrize them to get the following equations to be satisfied by the rational values of e: $e=-\frac{g^2}{2}$ or $e=\frac{g^2-1}{2g}$. This ensures that $\mathrm{Gal}(\mathcal{E}_{-1,e(g)}[8]/\mathbb{Q}(e))$ is a proper subgroup of $\mathrm{Gal}(\mathcal{E}_{-1,-e^4}[8]/\mathbb{Q}(e))$.
- For $P_{8,1}$, there are once again exactly 3 non-trivial subfields which are all quadratic. These fields are defined by x^2-2e, $x^2-(e^2+1)$ and x^2-2e^3-2e. As in the previous case, the last equation is an elliptic curve of rank 0 over $\mathbb{Q}$ thus it does not (for now!) interest us (cf Section [***]). Here one can choose $e=\frac{g^2}{2}$ or $e=-\frac{g^2-1}{2g}$ to get the necessary equations.
- Finally for $P_{8,2}$, we obtain 14 proper non-trivial subfields of which 7 are quadratic and 7 are quartic. The 7 quadratic subfields are defined by $x^2\pm e(e+1)(e-1)$, $x^2\pm e$, $x^2\pm(e+1)(e-1)$ and x^2+1. Here too, as the first equation is an elliptic curve of rank 0 over $\mathbb{Q}$ and the last one can not be satisfied over $\mathbb{Q}$, thus these equations do not interest us. Whereas the second and the third one give us $e=-x^2$ or $e=\frac{2g^2+2+1}{2g+1}$ respectively. Among the 7 equations defining the quartic subfields, 5 are elliptic curves of rank 0 over $\mathbb{Q}$ and 2 are reducible into two genus 0 components over a quadratic extension and over this extension these components admit only finitely many points.

As $d=-e^4$, it would suffice to consider the families up to sign. We thus conclude that the subfamilies presented in [BBB+13, Table 3] are exhaustive.

For more details about the computation of subfields of algebraic function fields we refer to Hess' work [Hes04]. Since it is slow to obtain the exhaustive list of subfields, we present two types of subfields for which the computation is faster.

3.1. **Computing a list of maximal subfamilies.** Les us consider the case in which the ℓ-adic image of Galois is surjective for a pair (E,ℓ) and we want to certify this. In this case it suffices to have a finite set of families which are maximal with respect to inclusion and each of which satisfies an equation describing a negligible set of points in the space of parameters. This also justifies that we call generic for ℓ the elliptic curves whose ℓ-adic Galois image is surjective.

Let ℓ^k be a prime power and $\mathrm{E}: y^2=x^3+ax+b$ be an elliptic curve over $\mathbb{Q}(a,b)$. We put $K_0=\mathbb{Q}(a,b)$ and, for $i=1,2,\ldots,k$, we construct $K_i:=\mathbb{Q}(a,b)(\mathrm{E}[\ell^i])$ as an extension of $K_{i-1}:=\mathbb{Q}(a,b)(\mathrm{E}[\ell^{i-1}])$. Since the group of ℓ^i torsion is isomorphic to $(\mathbb{Z}/\ell^i\mathbb{Z})^2$, we can construct K_i/K_{i-1} using four extensions, which correspond to two x and two y coordinates. Indeed, we make the first extension by an irreducible factor $f_{i,1}$ of $\Psi_{\ell^i}^{\mathrm{exact}}$ and call x_1 one of its roots. The second extension is by an irreducible factor $f_{i,2}$ of $y^2-(x_1^3+ax_1+b)$, which can be linear, and call y_1 one of its roots. Note that $P_1(x_1,y_1)$ belongs to $E[\ell^i]$. Thirdly, we compute the set S of x coordinates of the points $\{[a]P_1+Q \mid Q\in E[\ell^{i-1}] \text{ and} a\ (\mathbb{Z}/\ell^i\mathbb{Z})^*\}$ and we make an extension by an irreducible factor $f_{i,3}$ of $\Psi_{\ell^i}^{\mathrm{exact}}/\prod_{s\in S}(x-s)$ and call x_2 one of its roots. Finally we make an extension by an irreducible factor $f_{i,4}$ of $y^2-(x_2^3+ax_2+b)$, which can be linear, and call y_2 one of its roots. Note that $P_2(x_2,y_2)$ belongs to $E[\ell^i]$ and, because $f_{i,3}$ is relatively prime to $\prod_{s\in S}(x-s)$, the pair (P_1,P_2) is a basis of $E[\ell^i]$, so K_i is the ℓ^i-torsion field.

When we instantiate a and b elements a_0 and b_0 of the number field K, some of the polynomials $f_{i,j}$ with $1 \leq i \leq k$ and $1 \leq j \leq 4$ can be reducible. If all of them remain irreducible, then $\mathrm{Gal}(E_{a_0,b_0}[\ell^i]/K)$ has the same cardinality as $\mathrm{Gal}(E_{a,b}[\ell^i]/K)$, so E_{a_0,b_0} is generic.

By writing necessary conditions for the polynomials $f_{i,j}$ to factor we obtain a list of maximal families. If $k = 1$ we drop the i index and in the general case we renumber the polynomials so that we have a tower of function fields defined by the polynomials $f_1, f_2, \ldots, f_t$ for some t. Algorithm 1 obtains a list of equations so that, if none is satisfied, then the ℓ-adic Galois image is surjective.

Algorithm 1 Finding necessary polynomial conditions

Input: A prime power ℓ^k and a number field K

Output: A list of necessary polynomial conditions in a and b over an extension of $\mathbb{Q}(a, b)$ such that $\mathrm{Gal}(K(a, b)(\mathrm{E}[\ell^k]))$ is exceptional for the elliptic curve $\mathrm{E} : y^2 = x^3 + ax + b$.

1: Compute a list of extensions $K(a, b) = L_0 \subset L_1 \subset L_2 \subset \cdots \subset K_t = K(a, b)(E[\ell^k])$ and call f_j an irreducible polynomial which defines L_j/L_{j-1}.
2: For each j compute a primitive element of $L_j/K(a, b)$ and call F_j its minimal polynomial over $K(a, b)$.
3: **for** $j = 1, 2, \ldots, t$ **do**
4: **for** $d = 1, \ldots, \lfloor \deg f_j \rfloor$ **do**
5: **for** $r \in$ maximal partitions of $\deg(f_j)$ **do**
6: $\mathrm{S}_{i,r} \leftarrow$ System of polynomial equations in a, b and a root of f_i arising from equating coefficients
7: $\mathrm{C}_{i,r} \leftarrow$ Triangulation of $\mathrm{S}_{i,r}$ (Resultant)
8: ▷ Necessary for a certain factorization pattern of f_j.
9: **end for**
10: **end for**
11: **end for**
12: **return** Set of $\mathrm{C}_{i,r}$

Exemple 3.2. Let $\mathrm{E} : y^2 = x^3 + ax + b$ be a rational elliptic curve. Let $\Psi_3 = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$ be its 3-division polynomial and $\Delta = 4a^3 + 27b^2$ its discriminant. We apply the above algorithm in this case in order to obtain a system of necessary equations for $\mathrm{Gal}(\mathbb{Q}(a, b)(\mathrm{E}[3])/\mathbb{Q}(a, b))$ to be exceptional. Considering the construction of torsion fields discussed above, we see that one does not need more than 4 extension to construct $\mathbb{Q}(a, b)(\mathrm{E}[3])$: The first one by an irreducible factor of Ψ_3 to get the field $\mathbb{Q}(a, b)(x_1)$, where x-coordinate of a point P_1 of order 3. The second one is by the quadratic polynomial $x^2 - \Psi_2(x_1)$, if it is irreducible, in order to get the field $\mathbb{Q}(a, b)(x_1, y_1)$. This extension gives the necessary y-coordinate y_1 of the point P_1. Similarly, to create another point P_2, we make a third extension by an irreducible factor of Ψ_3 over $\mathbb{Q}(a, b)(x_1, y_1)$. This extension gives us the x-coordinate x_2 of point P_2 and the field $\mathbb{Q}(a, b)(x_1, y_1, x_2)$. Finally we make a quadratic extension to obtain the y-coordinate y_2 of P_2. These four extensions construct $\mathbb{Q}(a, b)(\mathrm{E}[3])$. In a generic case, the total degree is $4 \times 2 \times 3 \times 2 = 48$. If $\mathrm{Gal}(\mathbb{Q}(a, b)(\mathrm{E}[3])/\mathbb{Q}(a, b))$ is exceptional, one of the above extensions is is not of its generic degree. We consider the maximal partitions of degree of each extension.

- Ψ_3 has 2 quadratic factors or one linear factor. This we note as $[(2,2)]$ or $[(1,3)]$.
- Ψ_3 is irreducible and the second polynomial $x^2 - \Psi_2(x_1)$ factors into two linear factor. This we note as $[(4),(1,1)]$.
- If the first two polynomials are irreducible and the third one has a linear factor, we note it as $[(4),(2),(1,2)]$.
- Finally we have one possibility: $[(4),(2),(3),(1,1)]$.

Thus there are at most 5 maximal families of elliptic curves with exception Galois image.

We apply the above algorithm in each case. For $(1,3)$ we obtain a simple condition that Ψ_3 has a root. For $(2,2)$, the algorithm considers the following system,

$$\begin{cases} e_2 + f_2 = 0 \\ e_2 f_2 + e_1 + f_1 = 2a \\ e_1 f_2 + e_2 f_1 = 4b \\ e_1 f_1 = -1/3\, a^2 \end{cases} \Rightarrow \begin{cases} f_2 = -e_2 \\ f_1 = 2a + e_2 f_2 - e_1 \\ e_1 \left({e_2}^2 + 2\,a - e_1\right) + \frac{1}{3}\, a^2 = 0. \\ {e_2}^6 + 4\, a {e_2}^4 + \frac{16}{3}\, {e_2}^2 a^2 - 16\, b^2 = 0 \end{cases}$$

This system arises from equating the coefficients of the equation $x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2 = (x^2 + e_2 x + e_1)(x^2 + f_2 x + f_1)$. This enables us to determine for any curve whether the factorization pattern of Ψ_3 is $(2,2)$. Finally we have the following,

Case	Condition
$[(1,3)]$	$\exists x \in \mathbb{Q}(a,b)$ such that $3x^4 + 6ax^2 + 12bx - a^2 = 0$
$[(2,2)]$	$\exists x \in \mathbb{Q}(a,b)$ such that $3x^6 + 12ax^4 + 16a^2x^2 - 48b^2 = 0$
$[(4),(1,1)]$	$\exists x \in \mathbb{Q}(a,b)(x_1)$ such that $27\,x^8 + 216\,bx^6 + 18\,\Delta x^4 - \Delta^2 = 0$
$[(4),(2),(1,2)]$	$\exists x \in \mathbb{Q}(a,b)(x_1,y_1)$ such that $C_1 = 0$
$[(4),(2),(3),(1,1)]$	–

Here, $C_1 = 27\,x^{12} + 432\,ax^{10} + 2304\,a^2x^8 + 288\left(20\,a^3 + 39\,b^2\right)x^6 + 1536a\Delta x^4 - 256\Delta^2$.

We emphasize that the list of families is exhaustive in the sense that all the families of elliptic curves with exceptional mod 3 Galois image are subfamilies of the ones presented.

Remark 3.1. Out of possible 5 maximal equations in the above example, we notice that there are in fact only two maximal equations. The first one being that Ψ_3 has a root and the second one being that the polynomial C_1 has a root in $\mathbb{Q}(a,b)(x_1,y_1)$. The later condition is equivalent to j-invariant being a cube as the polynomial $x^3 - j$ has a root in the extension field defined by C_1 over $\mathbb{Q}(a,b)$. Thus in order to test an elliptic curve E is generic for 3, we check whether its 3-division polynomial has a root and whether its j-invariant is a cube.

3.2. **Computing quadratic subfields.**

Let us start with a simple remark: quadratic fields are uniquely determined by their discriminant. Rouse and Zureick-Brown noted that one can factor the discriminant of L and then, for each squarefree factor D of $\mathrm{Disc}(L/\mathbb{Q})$, test if $\mathrm{K}(\sqrt{D})$ is a subfield of L. Let is take an example.

Exemple 3.3 (Sec 3.5.1 and Sec 3.5.3 in [BBB+13])**.** Let us consider the case of the Suyama family, which is the set of Montgomery curves, $\mathcal{M}_{A,B} : By^2 = x^3 + Ax^2 + x$.

The group $\mathrm{Gal}(\mathbb{Q}(\mathcal{M}_{A,B})[8]/\mathbb{Q}(\sigma))$ is isomorphic to D_8 which has two subgroups of index 2 : the group of rotations C_8 and the group D_4. The irreducible factors of $\mathrm{Disc}(Q(\mathcal{M}_{A,B})[8])$ are -1,2,B,$A-2$ and $A+2$. We test all the 32 function fields $\mathbb{Q}(\sigma,\sqrt{f})$ with f product of a subset of these irreducible factors. We obtain that the subgroup D_4 corresponds to the condition $(A+2)/B = -\square$, which corresponds to the family Suyama-11 (Sec 3.5.1) and $(A^2-4) = \square$, which corresponds to the family Suyama-9/4 (Sec 3.5.3). Note that the method applied allow to conclude that the list of quadratic subfamilies is exhaustive.

In the next section we present a method which is faster thanks to the theory of modular curves.

4. Modular curves approach

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

Theorem 4.1 ([Shi71] and Prop 3.3 [Zyw15a])**.** *Let* E *be an elliptic curve such that* $j(E) \notin \{0, 1728\}$*, N a positive integer and* H *a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *such that* $-I_2 \in \mathrm{H}$ *and* $\det(\mathrm{H}) = (\mathbb{Z}/N\mathbb{Z})^*$*. Then there exists a polynomial* $X_{\mathrm{H}}(j,t)$ *such that* $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[N])/\mathbb{Q})$ *is conjugated to a subgroup of* H *if and only if* $\exists t_0 \in \mathbb{Q}$ *such that* $X_{\mathrm{H}}(j(\mathrm{E}), t_0) = 0$*.*

Contrary to the previous section, where the equations made use of the coefficients a and b of the elliptic curves, here they contain the j-invariant. On the one hand equations using j have the advantage that they correspond to plane curves. On the other hand, the use of the j-invariant can only correspond to a subset of the possible subgroups H. Indeed, two elliptic curves (resp. families of curves) can have the same j-invariant yet have different Galois images and therefore different behavior in the ECM algorithm. For example, for the curve $\mathrm{E} : y^2 = x^3 - 336x + 448$, $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[3])/\mathbb{Q})$ is of order 12 and if we twist E by 7, we reduce the order to 6. These curves have the same j-invariant however their performance in the ECM algorithm is different. The twist fares better.

Note that, as stated by the Rademacher-Thompson theorem, the list of subgroups of $\mathrm{PSL}_2(\mathbb{Z})$, and therefore of subgroups of $\mathrm{GL}_2(\mathbb{Z})$ of surjective determinant and containing $-I_2$, which have genus 0 or 1 is finite. The explicit list was computed by Cummmins and Pauli [CP03]. One can then apply Theorem 4.1 to obtain a complete classification of infinite families.

The computation of X_H is done in three steps. First one computes a system of generators of X_N^H, then one computes a primitive element h of the extension $X_N^H/\mathbb{Q}(\zeta_N, j)$ (called hauptmodule when H has genus 0) and finally one obtains X_H as the minimal polynomial of h. For a complete description we refer to the works of Rouse and Zureick-Brown [RZB15] and respectively Sutherland and Zywina [Sut15], who computed the explicit equations for all cingruence subgroups of genus 0 and 1 having surjective determinant and containing $-I_2$.

In order to obtain the complete list of ECM-friendly infinite families one has to extend this list to subgroups which don't contain $-I_2$.

4.1. **Modular curves when $-I_2 \notin H$.** A simple remark is that any congruence subgroup H of $\mathrm{GL}_2(\mathbb{Z})$ either contains $-I_2$ or is contained in a subgroup

$\tilde{H} := \langle H, -I_2 \rangle$ which contains $-I_2$. Rouse and Zureick-Brown noted that, X_H is a quadratic subfield of $X_N^{\tilde{H}}/\mathbb{Q}(\zeta_N, j)$, which can be computed as in Section 3.2.

To our knowledge, the list of subgroups H not containing $-I_2$ is not complete because the case of subgroups of level ℓ^k with $\ell > 2$ and $k > 1$ is not treated in [RZB15] and [Zyw15a].

Lemme 4.1. *Let* E *be a non-CM elliptic curve over a field* K, $m > 1$ *a an integer. Let* $\widetilde{H} \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ *containing* -1 *such that* $\rho_{\mathrm{E},m}(\mathrm{Gal}(K(\mathrm{E}[m])/K)) = \widetilde{H}$. *Let* H *be an index 2 subgroup of* $\widetilde{\mathrm{H}}$ *such that* $-1 \notin \mathrm{H}$ *and* $\widetilde{\mathrm{H}} = \langle \mathrm{H}, -1 \rangle$. *Then there exists a quadratic twist* E_d *of* E *such that*

$$\rho_{\mathrm{E}_d,m}(\mathrm{Gal}(K(\mathrm{E}_d[m])/K)) = \mathrm{H}.$$

Proof. Let us consider the fixed subfield L of $K(\mathrm{E}[m])$ by H. As H is of index 2 in $\widetilde{H}$, L is a quadratic extension of K. Let $d \in K$ such that $L = K(\sqrt{d})$. Let E_d denote the quadratic twist of E by d. Clearly any basis $(x_1, y_1), (x_2, y_2) \in K(\mathrm{E}[m])^2$ of $\mathrm{E}[m]$ can be transformed into a basis $(x_1, y_1/\sqrt{d}), (x_2, y_2/\sqrt{d})$ of $\mathrm{E}_d[m]$. We thus have $K(\mathrm{E}_d[m]) \subset K(\mathrm{E}[m])$. Let ψ be the restriction map from $\mathrm{Gal}(K(\mathrm{E}[m])/K))$ to $\mathrm{Gal}(K(\mathrm{E}_d[m])/K))$. Let $\sigma \in \mathrm{Gal}(K(\mathrm{E}[m])/K))$ such tha $\rho_{\mathrm{E},m}(\sigma) = -1$. We then have either $\rho(\sqrt{d}) = \sqrt{d}$ or $\rho(\sqrt{d}) = -\sqrt{d}$. As $\rho_{\mathrm{E},m}(\sigma) = -1 \notin H$, $\sigma(\sqrt{d}) = -\sqrt{d}$. Then clearly as σ fixes the basis $(x_1, y_1/\sqrt{d}), (x_2, y_2/\sqrt{d})$ of $\mathrm{E}_d[m]$, it fixes $K(\mathrm{E}_d[m])$. So we have $\sigma \in \ker(\psi)$. On the other hand for any $1 \neq \tau \in \ker(\psi)$, we have $\tau(\sqrt{d}) = -\sqrt{d}$. Then clearly if $(x_3, y_3), (x_4, y_4) \in K(\mathrm{E}_d[m])^2$ is a basis of $\mathrm{E}_d[m]$ then $(x_3, y_3\sqrt{d}), (x_4, y_4\sqrt{d}) \in K(\mathrm{E}[m])^2$ is a basis of $\mathrm{E}[m]$ and as $\tau(\sqrt{d}) = -\sqrt{d}$, $\rho_{\mathrm{E},m}(\tau) = -1$. So we have $\ker(\psi) = \{\pm 1\}$. Thus we conclude $\rho_{\mathrm{E}_d,m}(\mathrm{Gal}(K(\mathrm{E}_d[m])/K)) = \widetilde{H}/\{\pm 1\} = \mathrm{H}$. □

In the light of the above lemma, we look for quadratic subfields of torsion points fields when -1 is in Galois image. In practice, as the discriminant of a subfield divides that of a superfield, we check twists by possible factors of discriminant of $K(\mathrm{E}[m])$.

Exemple 4.1. Let $\mathrm{E}_t : y^2 = x^3 - 3\,(t+27)(t+3)x - 2\left(t^2 + 18\,t - 27\right)(t+27)$ with $j(\mathrm{E}_t) = \frac{(t+27)(t+3)^3}{t}$ and $\mathrm{Disc}(\mathrm{E}_t) = 2^{12}3^6t(t+27)^2$. By Table 1 of [SZ17], for infinitely many values of t, $\rho_{\mathrm{E}_t,3}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_t[3])/\mathbb{Q})) \simeq \widetilde{H} = \langle \left(\begin{smallmatrix} 0 & 1 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 2 \end{smallmatrix}\right) \rangle$. $\widetilde{H}$ has two subgroups H_1 and H_2 of index 2 not containing -1. By Lemma 4.1, there exist quadratic twists E_{H_1} and E_{H_2} of E_t such that $\rho_{E_{H_i},3} \simeq H_i$. By specializing at several values of t, we obtain their models. These are the twists by $t + 27$ and $-3(t + 27)$.

Table 1, 2 and 3 give models of curves with exceptional mod l^n-Galois images for $l^n \in \{3, 9, 27, 5, 25, 7, 13\}$.

Remark 4.1. The families for $\ell \in \{2, 3, 5, 7, 13\}$ are previously computed in [Zyw15a].

Theorem 4.2. *Let* ℓ *be an odd prime different than 11 and* $\ell^n < 28$ *be a prime-power and* $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ *such that* $-1 \notin H$ *and* H *arises as a mod -* ℓ^n *Galois image for infinitely many rational elliptic curves. Let* E *be one such curve. Then* E *is isomorphic to a specialization of one of the curves in the families give in Table 2, 3 ,4 or 5.*

In order to certify the correctness of families given in the above theorem, we shall need an easy lemma.

Lemme 4.2. *Let ℓ be an odd prime. Then if $-1 \in \rho_{E,\ell^n}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q}))$ then $-1 \in \rho_{E,\ell}(\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}))$.*

Proof. This is straightforward. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q})$ such that $\rho_{E,\ell^n}(\sigma) = -1$. Let P, Q be a basis of $\mathrm{E}[\ell^n]$ in $\mathbb{Q}(\mathrm{E}[\ell^n])$ then $P' = [\ell^{n-1}]P, Q' = [\ell^{n-1}]Q$ is a basis of $\mathrm{E}[\ell]$ which is in $\mathbb{Q}(\mathrm{E}[\ell])$. Let σ' be the restriction of σ to $\mathbb{Q}(\mathrm{E}[\ell])$. One can verify that $\sigma'(P') = -P'$ and $\sigma'(Q') = -Q'$ and thus $\rho_{\mathrm{E},\ell}(\sigma') = -1$. □

Now we prove Theorem 4.2.

Proof. (Of Theorem 4.2) Let $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ such that $-1 \notin H$. Let $\widetilde{H} = \langle H, -1\rangle$. Let $j(t)$ be j-invariant classifying the elliptic curves whose mod $-\ \ell^n$ Galois image lie in $\widetilde{H}$. Let E_H be a model corresponding to H. By the above lemma, it suffices to verify that the image of $\rho_{\mathrm{E}_H,\ell}$ does not contain -1. □

4.2. **Families over number fields.** In [RZB15], the authors computed equations for 10 pointless conics and 25 elliptic curves with rank 0 (c.f. Figure 3 in [RZB15]). The 10 pointless conics correspond to the genus 0 subgroups which do not contain an element corresponding to complex conjugation. Such an element is required in order to have infinitely many rational elliptic curves whose associated Galois image is contained in those subgroups ([Zyw15b, Prop. 3.5]). However these genus 0 and genus 1 curves can admit infinitely many points over number fields. Table * * give such families over $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$.

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

5.1. **Motivation.** Let us recall that ECM succeeds if $\#\,\mathrm{E}(\mathbb{F}_p)$ is B-smooth for a bound $B > 0$. Since $\#\,\mathrm{E}(\mathbb{F}_p)$ belongs to Hasse's interval, $[p - 2\sqrt{p}, p + 2\sqrt{p}]$, one can ask for a bound B if the chances of $\#\,\mathrm{E}(\mathbb{F}_p)$ being B-smooth are the same as the proportion of B-smooth integers in an interval centered in p of length $c\sqrt{p}$ for a constant c.

Theorem 5.1 (Lenstra [LJ87])**.** *Let p be a prime and* B *an integer. Then,*

$$\mathrm{Prob}(\#\,\mathrm{E}(\mathbb{F}_p) \text{ is } B\text{-smooth}) = \frac{1}{\mathcal{O}(\log p)}\mathrm{Prob}(n \in [p - \sqrt{p}, p + \sqrt{p}] \text{ is } B\text{-smooth}),$$

where the sign Prob *in the right side denotes the proportion of B-smooth integers in the interval and the sign* Prob *in the left side denotes for a fixed prime p the proportion of triplets $(x_0, y_0, a) \in \mathrm{F}_p^3$ such that, when putting $b = y_0^2 - x_0^3 - ax$ and $E_{a,b} : y^2 = x^3 + ax + b$ having the point (x_0, y_0), the order $\#E_{a,b}(\mathrm{F}_p)$ is B-smooth.*

On the one hand, the theorem is precise because the factor $\mathcal{O}(\log p)$ is hidden in the $o(1)$-term in the complexity of ECM. On the other hand, the theorem is not precise enough because the experiments show that if one restricts to elliptic curves E from some families, e;g. Montgomery curves $M_{a,b} : by^2 = x^3 + ax^2 + x$, then the proportion of smooth cardinalities can be improved. This is a motivation to consider the factor $\frac{1}{\mathcal{O}(\log p)}$ as all the good properties are hidden in this factor.

As discussed in Section 2, an important application of ECM consists in using the same elliptic curve to test smoothness of many integers. In this context, several papers measure the quality of a curve E for ECM as the proportion of primes p

B \ $\log_2 n$	24	25	26	27	28
400	-0.62	-0.81	-0.97	-0.75	-1.17
600	-0.62	-1.16	-0.87	-0.90	-1.15
800	-0.66	-1.2	-0.76	-0.82	-0.93
1000	-0.68	-1.21	-0.82	-0.78	-0.88

TABLE 1. Values of $\alpha(\mathrm{E}, n, B)$ for $\mathrm{E} : y^2 = x^3 + 3x + 5$ and various values of $\log_2 n$ and B.

less than a bound X for which $\#E(\mathrm{F}_p)$ 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 $\alpha(\mathrm{E}, n, \mathrm{B})$ be a real number such that

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

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 $1/\{x \mid x \sim ne^{\alpha(E,n,B)}\}$. This notation comes to correct the common heuristic which states that a cardinality is as smooth as a random integer of the same size and to replace it by the statement that a cardinality of a reduction of E to a prime of the same size as n is B-smooth for the same proportion of primes p as a random integer of logarithm $\log n + \alpha(E, n, B)$.

Table 1 shows the values of α for the curve $\mathrm{E} : y^2 = x^3 + 3x + 5$ and various values of $\log_2 n$ and B. As suggested by the above example, perhaps we can render $\alpha(\mathrm{E}, n, \mathrm{B})$ independent of n and B. We assume further heuristically that for a fixed curve E and varying primes p in the neighbourhood of n,

Table 1 determines us to ask whether $\alpha(E, n, B)$ converges when n and B go to infinity.

Open question 5.1. *Let E be an elliptic curve without CM. Find, if it exists, a real number $\alpha(E)$ such that*

$$\mathrm{Prob}(\#\,\mathrm{E}(\mathbb{F}_p) \text{ is } B\text{-smooth} \mid p \sim n) \sim_n \mathrm{Prob}(\text{random integer} \sim ne^{\alpha(\mathrm{E})} \text{ is } B\text{-smooth}),$$

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

A positive answer was by Barbulescu and Lachand to an analoguous question in Theorem 1.1 of [BL17], where the definition is

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

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

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

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

5.2. **Formal definition of α.** We say that a set S of primes admits a Chebotarev density δ, and we write $\mathrm{Prob}(S) = \delta$, if $\lim_{n\to\infty} \frac{\#(S\cap\Pi(n))}{\#\Pi(n)}$ 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 $\#E(\mathrm{F}_p)$ when p is a random prime by

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

The good definition of val_ℓ is proven in [BBB+13, Th 2.16], the proof allowing to compute it explicitely.

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

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

and

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

The good definition of α is due to the fact that we substracted the average valuation of a random integer (which is a constant with respect to the formula of Montgomery).

Theorem 5.2. *For any elliptic curve $E/\mathbb{Q}$ without CM, the series $\sum_l \alpha_l(\mathrm{E})$ converges.*

Proof. By Serre's open image theorem, any elliptic curve has a finite set of primes ℓ such that the image of Galois 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 $\overline{\mathrm{val}_\ell}(E) = \frac{\ell}{\ell-1}\mathrm{Prob}(E(\mathrm{F}_p)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}) + \frac{\ell((2\ell+1))}{(\ell-1)(\ell+1)}\mathrm{Prob}(E(\mathrm{F}_p)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z})$. By counting stabilizers, we obtain that in $\mathrm{GL}_2(\mathrm{F}_\ell)$ there are $\ell(\ell+1)(\ell-2)$ matrices conjugated to $\begin{pmatrix}1 & 0\\ 0 & \alpha\end{pmatrix}$, ℓ^2-1 conjugated to $\begin{pmatrix}1 & 0\\ 0 & \alpha\end{pmatrix}$ and, by [BBB+13, Prop 2.3], we obtain then $\overline{\mathrm{val}_\ell}(E) = \frac{\ell(\ell^3+\ell^2-2\ell-1)}{(\ell+1)^2(\ell-1)^3}$. Hence, $\alpha_\ell(E) = \log(\ell)(\frac{1}{\ell-1} - \overline{\mathrm{val}_\ell}(E)) = \mathcal{O}(\frac{\log(\ell)}{\ell^2})$, which is the term of a convergent series. □

Note that, if a curve E has surjective Galois at all primes, which is the case for all curves except a finite set of families described by curves, $\alpha(E) \approx -0.8119977339443$, 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.

5.3. **Properties of α.** Given an elliptic curve α we start by upper bounding the primes where the Galois image can be non-surjective using e.g. [**?**, Th 1] or directly use Zywina's algorithm [Zyw11].

Exemple 5.1. (1) Let us consider a curve E such that $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. The family of curves with this torsion has been parametrized by Kubert [Kub76], and corresponds to an index 2 subgroup of H_{193} of [RZB15]. These curves are parametrized by the modular curve X_{193n} in [RZB15]. We see that Serre's exponent is 2 and by [BBB+13, Th 2.16] we find that $\overline{\text{val}_2}$ changes from the value whe the Galois is surjective, i.e. $\frac{14}{9}$, to its new value $\frac{16}{3}$. 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 a curve from the Suyama-11 family, which is parametrized in [BBB+13, Sec.]. For these curves, $\overline{\text{val}_2}$ changes from $\frac{14}{9}$ (generic value) to $\frac{11}{3}$ and $\overline{\text{val}_3}$ changes from $\frac{87}{128}$ (generic value) to $\frac{27}{16}$. Thus,

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

We can now test the efficiency of α by comparing the smoothness probabilities of $\#E(\mathrm{F}_p)$ when p is a random prime of a given size n and that of a random integer of size $ne^{\alpha(E)}$.

Exemple 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.

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	$\text{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	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	$\text{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005133	0.005743	1008 %	11.89 %
$\mathrm{B}_2 = 100$	0.008892	0.04013	0.04101	361%,	2.19%

5.4. **ECM-friendly families with the best values of α.** Table 6 lists first 8 families for ECM with respect to their values of $\alpha(E)$. We remark that the first best two values of α are associated with the above two families.

Even the curves with better arithmetic in the sense that the point addition and multiplication are less expensive can be used in ECM in order to improve its time consumption. One might thus hope to intersect the families of better values of α and the families with better arithmetic e.g. twisted Edward's curves with $a = -1$ in order to obtain even better curves. However one can see that the family of elliptic

curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the family of twisted Edward's curves with a=-1 do not intersect.

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

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

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 $\#E(\mathrm{F}_p)$ being divisible by prime powers but not on that of being divisible by composite numbers. Hence, two curves can have the same value of α yet have different probabilities that 6 divides $\#E(\mathrm{F}_p)$.

Exemple 5.3. Let us consider the following family $\mathcal{F}_6$ defined in [BJ16, Theorem 1.4],

$$j(t) = 2^{10}3^3t^3(1 - 4t^3).$$

For an elliptic curve E in this family we have, $\mathbb{Q}(\mathrm{E}[2]) \subset \mathbb{Q}(\mathrm{E}[3])$. These curves arise from the entanglement fields [Mor17]. Let us consider the following numerical comparison between $\mathcal{F}_6$ and a generic family $\mathcal{F}_3$ with the same Galois image in $\mathrm{GL}_2(\mathbb{Z}_3)$ as that of $\mathcal{F}_6$.

Family	$\mathbb{P}(2\|\#(\mathrm{E}(\mathbb{F}_p))$	$\mathbb{P}(3\|\#(\mathrm{E}(\mathbb{F}_p))$	$\mathbb{P}(6\|\#(\mathrm{E}(\mathbb{F}_p))$	α
$\mathcal{F}_3$	2/3	3/4	1/2	-1.39
$\mathcal{F}_6$	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 make a complete classification of infinite families of ECM-friendly curves. The families given in this paper and the experimental tool α, even though it does not take into account the correlation, enables us to conclude that there do not exist other ECM friendly curves over $\mathbb{Q}$ than the ones provided. The question of the same classification over the number fields and the usefulness of the curves coming from the entanglement fields is yet to be resolved completely.

One might even consider the modular curves of higher genus and finitely many elliptic curves arising from them for ECM as a natural extension of this work. A different question is that of proving the smoothness properties of $\#E(\mathrm{F}_p)$ 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.

[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.

[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.

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

[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.

[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.

[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.

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

[BJ16] Julio Brau and Nathan Jones. Elliptic curves with 2-torsion contained in the 3-torsion field. *Proceedings of the American Mathematical Society*, 144(3):925–936, 2016.

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

[CP03] C.J. Cummins and S. Pauli. Congruence subgroups of psl(2,z) of genus less than or equal to 24. *Experimental Mathematics*, 12(2):243–255, 2003.

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

[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper i. die struktur der gruppe der divisorenklassen endlicher ordnung. *Journal für die reine und angewandte Mathematik*, 175:55–62, 1936.

[Hes04] Florian Hess. An algorithm for computing isomorphisms of algebraic function fields. In *Algorithmic Number Theory – ANTS VI*, volume 3076 of *Lecture notes in computer science*, pages 263–271, 2004.

[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.

[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.

[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.

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

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

[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.

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

[Mon92] Peter Lawrence Montgomery. *An FFT extension of the elliptic curve method of factorization*. PhD thesis, UNIVERSITY OF CALIFORNIA Los Angeles, 1992.

[Mor17] J. S. Morrow. Composite images of galois for elliptic curves over $\mathbf{Q}$ & entanglement fields. *ArXiv e-prints*, jul 2017.

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

[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.

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

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

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

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

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

[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.

[Zyw11] David Zywina. On the surjectivity of mod l representations associated to elliptic curves, 2011. preprint, available at http://pi.math.cornell.edu/ zywina/papers/EffectiveModl.pdf.

[Zyw15a] David Zywina. On the possible images of the mod ell representations associated to elliptic curves over q. *arXiv preprint arXiv:1508.07660*, 2015.

[Zyw15b] David Zywina. Possible indices for the galois image of elliptic curves over q. *arXiv preprint arXiv:1508.07663*, 2015.

TABLE 2. Curves with exceptional Galois images for 3,9,27.

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

TABLE 3. Curves with exceptional Galois images for 5,25.

label	# of subgroups	First model
5D0-5a	2	$a = -27t^4 - 6156t^3 - 13338t^2 + 6156t - 27,$ $b = 54(t^4 - 522t^3 - 10006t^2 + 522t + 1)(t^2 + 1)$
5D0-5b	2	$a = -27t^4 + 324t^3 - 378t^2 - 324t - 27,$ $b = 54(t^4 - 18t^3 + 74t^2 + 18t + 1)(t^2 + 1)$
5H0-5a	2	$a = -27(t^8 + t^7 + 7t^6 - 7t^5 + 7t^3 + 7t^2 - t + 1)$ $(t^8 - 4t^7 + 7t^6 - 2t^5 + 15t^4 + 2t^3 + 7t^2 + 4t + 1)(t^4 + 3t^3 - t^2 - 3t + 1),$ $b = 54(t^8 + 6t^7 + 17t^6 + 18t^5 + 25t^4 - 18t^3 + 17t^2 - 6t + 1)$ $(t^8 - 4t^7 + 17t^6 - 22t^5 + 5t^4 + 22t^3 + 17t^2 + 4t + 1)$ $(t^8 - t^6 + t^4 - t^2 + 1)(t^4 - 2t^3 - 6t^2 + 2t + 1)(t^2 + 1)$
25B0-25a	2	$a = -27t^{20} - 324t^{15} - 378t^{10} + 324t^5 - 27,$ $b = 54(t^{20} + 18t^{15} + 74t^{10} - 18t^5 + 1)(t^8 - t^6 + t^4 - t^2 + 1)(t^2 + 1)$
25B0-25b	2	$a = -27t^{20} - 6480t^{19} - 58320t^{18} - 181440t^{17} - 473040t^{16} - 816156t^{15} - 1561680t^{14}$ $-1645920t^{13} - 2157840t^{12} - 1121040t^{11} - 1633338t^{10} + 1121040t^9 - 2157840t^8$ $+1645920t^7 - 1561680t^6 + 816156t^5 - 473040t^4 + 181440t^3 - 58320t^2 + 6480t - 27,$ $b = -54(t^{20} - 510t^{19} - 13590t^{18} - 32280t^{17} - 82230t^{16} - 153522t^{15}$ $-302910t^{14} - 273540t^{13} - 412830t^{12} - 268230t^{11} - 262006t^{10} + 268230t^9$ $-412830t^8 + 273540t^7 - 302910t^6 + 153522t^5 - 82230t^4 + 32280t^3 - 13590t^2 + 510t + 1)$ $(t^8 + 6t^7 + 17t^6 + 18t^5 + 25t^4 - 18t^3 + 17t^2 - 6t + 1)(t^2 + 1)$

TABLE 4. Curves with exceptional Galois images for 7.

label	# of subgroups	First model
7B0-7a	2	$a = -27(t^2 + 13t + 49)^3(t^2 + 5t + 1),$ $b = 54(t^4 + 14t^3 + 63t^2 + 70t - 7)(t^2 + 13t + 49)^4$
7E0-7a	2	$a = -27(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1)(t^2 - t + 1),$ $b = 54t^{12} - 28188t^{11} - 483570t^{10} + 2049300t^9 - 3833892t^8 + 7104348t^7$ $-13674906t^6 + 17079660t^5 - 11775132t^4 + 4324860t^3 - 790074t^2 + 27540t + 54$
7E0-7b	2	$a = -432(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)(t^2 - t + 1),$ $b = 3456t^{12} - 62208t^{11} + 404352t^{10} - 1223424t^9 + 1969920t^8 - 1679616t^7$ $+943488t^6 - 767232t^5 + 601344t^4 - 158976t^3 - 51840t^2 + 20736t + 3456$
7E0-7c	2	$a = -189(5t^2 - t - 1)(3t^2 - 9t + 5)(t^2 - t + 1)(t^2 - 3t - 3),$ $b = -2646(9t^4 - 12t^3 - t^2 + 8t - 3)(3t^4 - 4t^3 - 5t^2 - 2t - 1)(t^4 - 6t^3 + 17t^2 - 24t + 9)$

TABLE 5. Curves with exceptional Galois images for 13.

label	# of subgroups	First model
13B0-13a	2	$a = -3(t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1)$ $(t^4 - t^3 + 5t^2 + t + 1)^3,$ $b = -2(t^{12} - 512t^{11} - 13079t^{10} - 32300t^9 - 104792t^8 - 111870t^7$ $-419368t^6 + 111870t^5 - 104792t^4 + 32300t^3 - 13079t^2$ $+512t + 1)(t^4 - t^3 + 5t^2 + t + 1)^4(t^2 + 1)$
13B0-13b	2	$a = -27(t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1)(t^4 - t^3 + 5t^2 + t + 1)^3,$ $b = 54(t^{12} - 8t^{11} + 25t^{10} - 44t^9 + 40t^8 + 18t^7 - 40t^6 - 18t^5 + 40t^4 + 44t^3 + 25t^2 + 8t + 1)$ $(t^4 - t^3 + 5t^2 + t + 1)^4(t^2 + 1)$

$X_2 52 = \left(t^8 - 70\,t^6 + 107\,t^4 - 38\,t^2 + 1\right)^4 (t-1)^8 (1+t)^8 \left(t^2 + 3\,t + 1\right)^8 \left(t^2 - 3\,t + 1\right)^8 j^4 -$
$4\,\left(t^{76} - 480\,t^{74} + 93576\,t^{72} - 9722250\,t^{70} + 588106804\,t^{68} - 21308406240\,t^{66} + 460441048449\,t^{64} - 568147722839\right.$
$\left(6\,t^{88} + 224\,t^{86} + 58096\,t^{84} - 84763480\,t^{82} + 14742175064\,t^{80} - 1116040805536\,t^{78} + 43275826141572\,t^{76} - 86153\right.$

TABLE 6. Best 8 families characterized by α(E)

family E : $y^2 = x^3 + a(t)x + b(t)$	α(E)	remarks
$a(t) = -1769472\,t^{16} + 3538944\,t^{14} - 1327104\,t^{12} - 221184\,t^{10}$ $-1589760\,t^8 - 13824\,t^6 - 5184\,t^4 + 864\,t^2 - 27$ $b(t) = 905969664\,t^{24} - 2717908992\,t^{22} + 2378170368\,t^{20} - 396361728\,t^{18}$ $-1985347584\,t^{16} + 1847328768\,t^{14} + 229146624\,t^{12} + 115458048\,t^{10}$ $-7755264\,t^8 - 96768\,t^6 + 36288\,t^4 - 2592\,t^2 + 54$	-3.43	**torsion** : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ **level:8**
$a(t) = -27t^{16} - 864t^{15} - 12096t^{14} - 96768t^{13} - 580608t^{12}$ $-3870720t^{11} - 27095040t^{10} - 142884864t^9 - 500539392t^8 - 1143078912t^7$ $-1734082560t^6 - 1981808640t^5 - 2378170368t^4$ $-3170893824t^3 - 3170893824t^2 - 1811939328t - 452984832$ $b(t) = 54t^{24} + 2592t^{23} + 57024t^{22} + 760320t^{21} + 6386688t^{20}$ $+25546752t^{19} - 127733760t^{18} - 2934226944t^{17} - 24999321600t^{16}$ $-138195763200t^{15} - 5638387138856t^{14} - 1862107398144t^{13}$ $-5461864611840t^{12} - 14896859185152t^{11} - 36085677686784t^{10}$ $-70756230758400t^9 - 102397221273600t^8 - 96148748500992t^7 - 33484638781440t^6$ $+53575422050304t^5 + 107150844100608t^4 + 102048422952960t^3$ $+61229053771776t^2 + 22265110462464t + 3710851743744$	-3.43	**torsion** : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ **level: 8**
$a(t) = -27t^{16} - 25056t^{14} - 316224t^{12} + 2059776t^{10}$ $-4907520t^8 + 32956416t^6 - 80953344t^4 - 102629376t^2 - 1769472$ $b(t) = 54t^{24} - 111456t^{22} - 9979200t^{20} - 8805888t^{18}$ $+75852288t^{16} + 3849928704t^{14} - 25856409600t^{12} + 61598859264t^{10}$ $+19418185728t^8 - 36068917248t^6 - 653996851200t^4 - 116870086656t^2 + 905969664$	-3.43	**torsion** : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ **level: 8**
$a(t) = -27t^{16} + 216t^{14} - 324t^{12} - 216t^{10} + 270t^8 - 216t^6 - 324t^4 + 216t^2 - 27$ $b(t) = 54t^{24} - 648t^{22} + 2268t^{20} - 1512t^{18} - 3078t^{16} + 3888t^{14}$ $+1512t^{12} + 3888t^{10} - 3078t^8 - 1512t^6 + 2268t^4 - 648t^2 + 54$	-3.43	**torsion** : $\mathbb{Z}/8\mathbb{Z}$ **level:16**
$a(t) = -27t^{16} - 864t^{15} + 13824t^{14} + 628992t^{13}$ $+7402752t^{12} + 36771840t^{11} + 30965760t^{10}$ $-514473984t^9 - 2477924352t^8 - 4115791872t^7$ $+1981808640t^6 + 18827182080t^5 + 30321672192t^4$ $+20610809856t^3 + 3623878656t^2 - 1811939328t - 452984832$ $b(t) = 54t^{24} + 2592t^{23} + 165888t^{22} + 5550336t^{21} +$ $88687872t^{20} + 635185152t^{19} - 371589120t^{18}$ $-45072433152t^{17} - 383285551104t^{16} - 1506238267392t^{15} - 1640258076672t^{14}$ $+114473230663 68t^{13} + 571898446479 36t^{12} + 915785845309 44t^{11}$ $-104976516907008t^{10} - 771193992904704t^9 - 1569937617321984t^8$ $-1476933489524736t^7 - 974098582732 80t^6$ $+13320798118871 04t^5 + 1487935585124352t^4 + 744953487556608t^3$ $+178120883699712t^2 + 22265110462464t + 3710851743744$	-3.43	**torsion** : $\mathbb{Z}/4\mathbb{Z}$ **level:16**
$a(t) = -27t^{16} - 12960t^{15} - 232416t^{14} - 1088640t^{13} - 1975104t^{12}$ $+1451520t^{11} + 5377536t^{10} + 22394880t^9 + 48176640t^8 - 89579520t^7 + 86040576t^6$ $-92897280t^5 - 5056266 24t^4 + 1114767360t^3 - 951975936t^2 + 212336640t - 1769472$ $b(t) = 54t^{24} - 54432t^{23} - 3595104t^{22} - 50730624t^{21}$ $-316540224t^{20} - 838688256t^{19} - 733404672t^{18}$ $+2414168064t^{17} + 12561246720t^{16} + 20149420032t^{15}$ $+16335323136t^{14} + 1226244096t^{13} - 268429787136t^{12}$ $-4904976384t^{11} + 261365170176t^{10} - 12895628820 48t^9$ $+3215679160320t^8 - 2472108097536t^7$ $-3004025536512t^6 + 137410683863 04t^5 - 207447801200 64t^4$ $+132987286978 56t^3 - 376973977190 4t^2 + 228304355328t + 905969664$	-3.43	**torsion** $\mathbb{Z}/2\mathbb{Z}$ **16**
Suyama-11 from [BBB$^+$13]	-3.39	**torsion** $\mathbb{Z}/6\mathbb{Z}$ **Serre's exponent for $\ell = 2$ is 1**
Suyama from [BBB$^+$13]	-3.15	**torsion** $\mathbb{Z}/6\mathbb{Z}$ **Serre's exponent for $\ell = 2$ is 2**

TABLE 7. Further genus 0 families on $\mathbb{Q}(i)$

Curve	j-map	some j invariants
X_{21}	$(-\frac{12\,it^2-i-4\,t}{12\,t^2+1}) \circ (\frac{4\,(8\,t-1)}{t^4})$	
X_{72}	$(-\frac{8\left(9\,it-4\,t^2+2\right)}{7\,(2\,t^2+1)}) \circ (-t^2) \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	
X_{59}	$(-\frac{it^2+i}{2\,t}) \circ (-2t^2-1) \circ (\frac{8\left(t^2+3\right)}{t-1}) \circ (\frac{t^3}{t+16})$	
X_{88}	$(-\frac{4\left(5\,it-2\,t^2+2\right)}{3\,(t^2+1)}) \circ (-t^2) \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	
X_{182}	$(-\frac{2\,it^2+i}{2\,t}) \circ (-2\,t^2-1) \circ (-2\,t^2+1) \circ (\frac{8\left(t^2+3\right)}{t-1})$	
X_{184}	$(-\frac{it^2+4\,i}{2\,t}) \circ (-\frac{8}{t^2+2}) \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	
X_{186}	$(-\frac{4\,it}{2\,t^2+1}) \circ (\frac{t^2+2\,t-1}{t^2+1}) \circ (\frac{8}{t^2-1}) \circ (t^2-16) \circ (\frac{t^3}{t+16})$	
X_{198}	$(-\frac{2\left(it^2-2\,i\right)}{t^2+2}) \circ (\frac{t^2+2}{t^2-2}) \circ (-2\,t^2-1) \circ (-2\,t^2+1) \circ (\frac{8\left(t^2+3\right)}{t-1})$	
X_{201}	$(-\frac{2\left(it^2-2\,i\right)}{t^2+2}) \circ (\frac{8\,t}{t^2-2}) \circ (-2t^2-8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	
X_{206}	$(-\frac{it^2+2\,i}{2\,t}) \circ (-\frac{4}{t^2+1}) \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	

$$4\,\left(t^{68}+1286\,t^{66}-341143\,t^{64}+21784456\,t^{62}+1211381828\,t^{60}-243163011896\,t^{58}+13430782409076\,t^{56}-40925\right.$$
$$\left.\left(t^8-278\,t^6+315\,t^4-86\,t^2+1\right)^3\left(t^8-22\,t^6+2411\,t^4-2150\,t^2+625\right)^3\left(t^4+5\,t^2+1\right)^6\left(t^4-27\,t^2+9\right)^6\right.$$

IMJ-PRG, (SORBONNE UNIV., UNIV. PARIS DIDEROT, CNRS), INRIA, PARIS
E-mail address: razvan.barbulescu@imj-prg.fr sudarshan.shinde@imj-prg.fr

TABLE 8. Further genus 1 families on $\mathbb{Q}(i)$

X_n	j-map	some j invariants
X_{51}	$-4x \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{52}	$8x \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{53}	$-4x \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{54}	$-8x \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{149}	$x+1 \circ (-t^2+8) \circ (t^2-16) \circ (\frac{t^3}{t+16})$	$6112i-15616, \frac{3375}{31}$
X_{151}	$2(x-1) \circ (-t^2+8) \circ (t^2-16) \circ (\frac{t^3}{t+16})$	$\frac{9869198625}{614656}, \frac{-4987112077182710979766592}{154766099193094612161}$
X_{152}	$2x \circ t^2 \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{154}	$-x \circ t^2 \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{157}	$4x \circ (-t^2-8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{158}	$2x \circ (-t^2-8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{159}	$2x \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{160}	$x+1 \circ -\frac{64}{t^2-8} \circ (t^2-16) \circ (\frac{t^3}{t+16})$	$-1408i-256, 16581375$
X_{161}	$2(x-1) \circ -\frac{64}{t^2-8} \circ (t^2-16) \circ (\frac{t^3}{t+16})$	$\frac{4869777375}{92236816}, \frac{3262481399665767653245001408}{300283484326400961}$
X_{162}	$x-1 \circ -t^2 \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{163}	$2-2x \circ -t^2 \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	$78608, \frac{16974593}{256}$
X_{164}	$-x-1 \circ -t^2 \circ (-t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{168}	$4x \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{252}	$\frac{x+y-1}{x-1} \circ (\frac{t^2+2}{t^2-2}) \circ (\frac{8}{t^2-1}) \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{253}	$-\frac{2(2x-y)}{x} \circ \frac{t^2-8}{t^2+8t+8} \circ \frac{8}{t^2+1} \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{285}	$-\frac{2x}{2x-y} \circ \frac{2(t^2-2)}{t^2+4t+2} \circ -2t^2-8 \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{300}	$-\frac{x-y-1}{x-1} \circ \frac{t^2+2}{t} \circ (-\frac{64}{t^2-8}) \circ (t^2-16) \circ (\frac{t^3}{t+16})$	-
X_{353}	$2x \circ (-t^2) \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{354}	$-x \circ (-t^2) \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{355}	$x \circ (-t^2) \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-
X_{356}	$2x \circ (-t^2) \circ (-t^2+8) \circ (-t^2+48) \circ (\frac{t^3}{t+16})$	-

TABLE 9. Further genus 1 families on $\mathbb{Q}(i)$

n	X_H
X_{51}	
X_{52}	
X_{53}	
X_{54}	
X_{149}	
X_{151}	$\left(t^4+84\,t^2+1564\right)^2 j^3+\left(-34560\,t^{12}+770560\,t^{10}+675235072\,t^8+44\right.$
X_{152}	
X_{154}	
X_{157}	
X_{158}	
X_{159}	
X_{160}	$\left(t^4+42\,t^2-527\right)^4 j^3+\left(28\,t^{18}+2755\,t^{16}-90104\,t^{14}+15405172\,t^{12}+2980114928\,t^{10}-\right.$
X_{161}	$\left(t^4+84\,t^2+1564\right)^4 j^3+\left(-224\,t^{18}-66512\,t^{16}-7943936\,t^{14}-452927744\,t^{12}-7950874624\,t^{10}+504612\right.$
X_{162}	$\left(t^2-13\right)^4 j^3-$
X_{163}	$\left(t^2+10\right)^4 j^3+\left(768\,t^{12}+6400\right.$
X_{164}	
X_{168}	
X_{252}	
X_{253}	
X_{285}	
X_{300}	
X_{353}	$t^8\left(t^4+100\right)\left(t^2+6\right)\left(t^2-6\right)j^3+\left(-2596864\,t^{24}-921796608\,t^{20}-46565165312\,t^{16}+2236588867\right.$
X_{354}	
$X_{\cdots}$	