FINDING ECM-FRIENDLY CURVES THROUGH A STUDY OF GALOIS PROPERTIES

RAZVAN BARBULESCU, JOPPE W. BOS, CYRIL BOUVIER, THORSTEN KLEINJUNG, AND PETER L. MONTGOMERY

Abstract. In this paper we prove some divisibility properties of the cardinality of elliptic curves modulo primes. These proofs explain the good behavior of certain parameters when using Montgomery or Edwards curves in the setting of the elliptic curve method (ECM) for integer factorization. The ideas of the proofs help us to find new families of elliptic curves with good division properties which increase the success probability of ECM.

1. Introduction

The elliptic curve method (ECM) for integer factorization [16] is the asymptotically fastest method for finding relatively small factors p of large integers N. In practice, ECM is used, on the one hand, to factor large integers. For instance, the current ECM-record is a 241-bit factor of $2^{1181} - 1$ [9]. On the other hand, ECM is used to factor many small (100 to 200 bits) integers as part of the number field sieve [19, 15, 2], the most efficient general purpose integer factorization method.

Traditionally, the elliptic curve arithmetic used in ECM is implemented using Montgomery curves [17] (e.g., in the widely-used GMP-ECM software [25]). Generalizing the work of Euler and Gauss, Edwards introduced a new normal form for elliptic curves [12] which results in a fast realization of the elliptic curve group operation in practice. These Edwards curves have been generalized by Bernstein and Lange [7] for usage in cryptography. Bernstein et al. explored the possibility to use these curves in the ECM setting [6]. After Hisil et al. [13] published a coordinate system which results in the fastest known realization of curve arithmetic, a follow-up paper by Bernstein et al. discusses the usage of the so-called "$a = -1$" twisted Edwards curves [5] in ECM.

It is common to construct or search for curves which have favorable properties. The success of ECM depends on the smoothness of the cardinality of the curve considered modulo the unknown prime divisor p of N. This usually means constructing curves with large torsion group over $\mathbb{Q}$ or finding curves such that the order of the elliptic curve, when considered modulo a family of primes, is always divisible by an additional factor. Examples are the Suyama construction [23], the curves proposed by Atkin and Morain [1], a translation of these techniques to Edwards curves [6, 5], and a family of curves suitable for Cunningham numbers [10].

Key words and phrases. Elliptic Curve Method (ECM), Edwards curves, Montgomery curves, torsion properties, Galois groups.

This work was supported by the Swiss National Science Foundation under grant number 200020-132160 and by a PHC Germaine de Staël grant.

In this paper we study and prove divisibility properties of the cardinality of elliptic curves over prime fields. We do this by studying properties of Galois groups of torsion points using Chebotarëv's theorem [18]. Furthermore, we investigate some elliptic curve parameters for which ECM finds exceptionally many primes in practice, but which do not fit in any of the known cases of good torsion properties. We prove this behavior and provide parametrizations for families of elliptic curves with these properties.

2. Galois properties of torsion points of elliptic curves

In this section we give a systematic way to compute the probability that the order of a given elliptic curve reduced by an arbitrary prime is divisible by a certain prime power.

2.1. Torsion Properties of Elliptic Curves.

Definition 2.1. Let K be a finite Galois extension of $\mathbb{Q}$, p a prime and $\mathfrak{p}$ a prime ideal above p with residue field $k_\mathfrak{p}$. The decomposition group $\mathrm{Dec}(\mathfrak{p})$ of $\mathfrak{p}$ is the subgroup of $\mathrm{Gal}(K)$ which stabilizes $\mathfrak{p}$. Call $\alpha^{(\mathfrak{p})}$ the canonical morphism from $\mathrm{Dec}(\mathfrak{p})$ to $\mathrm{Gal}(k_\mathfrak{p}/\mathbb{F}_p)$ and let $\phi_\mathfrak{p}$ be the Frobenius automorphism on the field $k_\mathfrak{p}$. We define $\mathrm{Frobenius}(p) = \bigcup_{\mathfrak{p}|p}(\alpha^{(\mathfrak{p})})^{-1}(\phi_\mathfrak{p})$.

In order to state Chebotarëv's theorem we say that a set S of primes admits a natural density equal to δ and write $\mathbb{P}(S) = \delta$ if $\lim_{N\to\infty} \frac{\#(S \bigcap \Pi(N))}{\#\Pi(N)}$ exists and equals δ, where $\Pi(N)$ is the set of primes up to N. If $\mathrm{event}(p)$ is a property which can be defined for all primes except a finite set (thus of null density), when we note $\mathbb{P}(\mathrm{event}(p))$ we tacitly exclude the primes where $\mathrm{event}(p)$ cannot be defined.

Theorem 2.2 (Chebotarëv, [18])**.** *Let K be a finite Galois extension of $\mathbb{Q}$. Let $H \subset \mathrm{Gal}(K)$ be a conjugacy class. Then*

$$\mathbb{P}(\mathrm{Frobenius}(p) = H) = \frac{\#H}{\#\,\mathrm{Gal}(K)}.$$

Before applying Chebotarëv's theorem to the case of elliptic curves, we introduce some notation. For every elliptic curve E over a field F and all $m \in \mathbb{N}$, $m \geq 2$, we consider the field $F(E[m])$ which is the smallest extension of F containing all the m-torsion of E. The next result is classical, but we present its proof for the intuition it brings.

Proposition 2.3. *For every integer $m \geq 2$ and any elliptic curve E over some field F, the following holds:*

(1) $F(E[m])/F$ is a Galois extension;
(2) there is an injective morphism $\iota_m : \mathrm{Gal}(F(E[m])/F) \hookrightarrow \mathrm{Aut}(E(\overline{F})[m])$.

Proof. (1) Since the addition law of E can be expressed by rational functions over F, there exist polynomials $f_m, g_m \in F[X, Y]$ such that the coordinates of the points in $E(\overline{F})[m]$ are the solutions of the system $(f_m = 0, g_m = 0)$. Therefore $F(E[m])$ is the splitting field of $\mathrm{Res}_X(f_m, g_m)$ and $\mathrm{Res}_Y(f_m, g_m)$ and in particular is Galois. (2) For each $\sigma \in \mathrm{Gal}(F(E[m])/F)$ we call $\iota_m(\sigma)$ the application which sends $(x, y) \in E(\overline{F})[m]$ into $(\sigma(x), \sigma(y))$. Thanks to the discussion above, $\iota_m(\sigma)$ sends points of $E(\overline{F})[m]$ in $E(\overline{F})[m]$. Since the addition law can be expressed by rational functions over F, for each σ, $\iota_m(\sigma) \in \mathrm{Aut}(E(\overline{F})[m])$. One easily checks that ι_m is a group morphism and its kernel is the identity. □

Notation 2.4. We fix generators for $E(\overline{\mathbb{Q}})[m]$, thereby inducing an isomorphism $\psi_m : \mathrm{Aut}(E(\overline{\mathbb{Q}})[m]) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let ι_m be the injection given by Proposition 2.3. We call $\rho_m : \mathrm{Gal}(F(E[m])/F) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ the injective morphism $\psi_m \circ \iota_m$.

Let p be a prime such that E has good reduction at p and $p \nmid m$. Let $\iota_m^{(p)}$ be the injection of $\mathrm{Gal}(\mathbb{F}_p(E[m])/\mathbb{F}_p)$ into $\mathrm{Aut}(E(\overline{\mathbb{F}_p})[m])$ given by Proposition 2.3. By [21, Prop. VII.3.1] there is a canonical isomorphism $r_m^{(\mathfrak{p})}$ from $\mathrm{Aut}(E(\overline{\mathbb{Q}})[m])$ to $\mathrm{Aut}(E(\overline{\mathbb{F}_p})[m])$ for each prime ideal $\mathfrak{p}$ over p.

Remark 2.5. Note that $\#\,\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is bounded by $\#\,\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For every prime π, we have $\#\,\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z}) = (\pi-1)^2(\pi+1)\pi$, and for every integer $k \geq 1$, $\#\,\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z}) = \pi^4 \#\,\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z})$.

Notation 2.6. For all $g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ we put $\mathrm{Fix}(g) = \{v \in (\mathbb{Z}/m\mathbb{Z})^2 \mid g(v) = v\}$. Conjugation of g gives an isomorphic group of fixed elements. If we are interested only in the isomorphism class we use the notation $\mathrm{Fix}(C)$ where C is a set of conjugated elements. We use analogous notations for $\mathrm{Aut}(E(\overline{\mathbb{Q}})[m])$ and $\mathrm{Aut}(E(\overline{\mathbb{F}_p})[m])$.

Theorem 2.7. *Let E be an elliptic curve over $\mathbb{Q}$ and $m \geq 2$ be an integer. Put $K = \mathbb{Q}(E[m])$. Let T be a subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Then,*

(1) $$\mathbb{P}(E(\mathbb{F}_p)[m] \simeq T) = \frac{\#\{g \in \rho_m(\mathrm{Gal}(K/\mathbb{Q})) \mid \mathrm{Fix}(g) \simeq T\}}{\#\,\mathrm{Gal}(K/\mathbb{Q})}.$$

(2) Let $a, n \in \mathbb{N}$ such that $a \leq n$ and $\gcd(a,n) = 1$ and let ζ_n be a primitive nth root of unity. Put $G_a = \{\sigma \in \mathrm{Gal}(K(\zeta_n)/\mathbb{Q}) \mid \sigma(\zeta_n) = \zeta_n^a\}$. Then:

$$\mathbb{P}(E(\mathbb{F}_p)[m] \simeq T \mid p \equiv a \bmod n) = \frac{\#\{\sigma \in G_a \mid \mathrm{Fix}(\rho_m(\sigma_{|K})) \simeq T\}}{\#G_a}.$$

Proof. (1) Let $p \nmid m$ be a prime for which E has good reduction and let $\mathfrak{p}$ be a prime ideal of K over p. We abbreviate $H = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \mathrm{Fix}(\iota_m(\sigma)) \simeq T\}$. First note that $E(\mathbb{F}_p)[m] = \mathrm{Fix}(\iota_m^{(p)}(\phi_p))$ where ϕ_p is the Frobenius in $\mathrm{Gal}(\mathbb{F}_p(E[m])/\mathbb{F}_p)$. Since the diagram

$$\begin{array}{ccccc}
\mathrm{Dec}\,\mathfrak{p} & \hookrightarrow & \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) & \xhookrightarrow{\iota_m} & \mathrm{Aut}(E(\overline{\mathbb{Q}})[m]) \\
\downarrow{\scriptstyle \alpha^{(\mathfrak{p})}} & & & & \downarrow{\scriptstyle r_m^{(\mathfrak{p})}} \\
\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_p(E[m])/\mathbb{F}_p) & \xhookrightarrow{\iota_m^{(p)}} & \mathrm{Aut}(E(\overline{\mathbb{F}_p})[m])
\end{array}$$

is commutative and since $\mathrm{Frobenius}(p) \subset \mathrm{Gal}(K/\mathbb{Q})$ is the conjugacy class generated by $(\alpha^{(\mathfrak{p})})^{-1}(\phi_{\mathfrak{p}})$ we have $E(\mathbb{F}_p)[m] \simeq \mathrm{Fix}(\iota_m(\mathrm{Frobenius}(p)))$.

Decompose H into a disjoint union of conjugacy classes $C_1, \ldots, C_N$. Then $\mathrm{Fix}(\iota_m(\mathrm{Frobenius}(p))) \simeq T$ is equivalent to $\mathrm{Frobenius}(p)$ being one of the C_i. Thanks to Theorem 2.2 we obtain:

$$\mathbb{P}(E(\mathbb{F}_p)[m] \simeq T) = \sum_{i=1}^{N} \mathbb{P}(\mathrm{Frobenius}(p) = C_i) = \sum_{i=1}^{N} \frac{\#C_i}{\#\,\mathrm{Gal}(K/\mathbb{Q})} = \frac{\#H}{\#\,\mathrm{Gal}(K/\mathbb{Q})}.$$

(2) Using similar arguments as in (1) we have to evaluate

$$\frac{\mathbb{P}(\mathrm{Frobenius}(p) \in \{C_1, \ldots, C_N\}, p \equiv a \bmod n)}{\mathbb{P}(p \equiv a \bmod n)}.$$

Let p be a prime and $\mathfrak{p}$ a prime ideal as in the first part of the proof, and let $\mathfrak{P}$ be a prime ideal of $K(\zeta_n)$ lying over $\mathfrak{p}$. Furthermore let $\tilde{C}_1, \ldots, \tilde{C}_{\tilde{N}}$ be the

conjugacy classes of $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ that are in the pre-images of $C_1, \ldots, C_N$ and whose elements σ satisfy $\sigma(\zeta_n) = \zeta_n^a$. Since $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ maps ζ_n to primitive nth roots of unity we have for $\sigma \in (\alpha^{(\mathfrak{P})})^{-1}(\phi_{\mathfrak{P}})$ that $\sigma(\zeta_n) = \zeta_n^b$ holds for some b. Together with $\sigma(x) \equiv x^p \bmod \mathfrak{P}$ we get $\zeta_n^b \equiv \zeta_n^p \bmod \mathfrak{P}$. If we exclude the finitely many primes dividing the norms of $\zeta_n^c - 1$ for $c = 1, \ldots, n-1$ we obtain $b \equiv p \bmod n$. Since Frobenius$(K(\zeta_n), p)$, the Frobenius conjugacy class for $K(\zeta_n)$, is the pre-image of Frobenius(p), we get with the argument above $\mathbb{P}(\text{Frobenius}(p) \in \{C_1, \ldots, C_N\}, p \equiv a \bmod n) = \mathbb{P}(\text{Frobenius}(K(\zeta_n), p) \in \{\tilde{C}_1, \ldots, \tilde{C}_{\tilde{N}}\})$. A similar consideration for the denominator $\mathbb{P}(p \equiv a \bmod n)$ completes the proof. □

Remark 2.8. Put $K = \mathbb{Q}(E[m])$. If $[K(\zeta_n) : \mathbb{Q}(\zeta_n)] = [K : \mathbb{Q}]$, then one has $\mathbb{P}(E(\mathbb{F}_p)[m] \simeq T \mid p \equiv a \bmod n) = \mathbb{P}(E(\mathbb{F}_p)[m] \simeq T)$ for a coprime to n. Indeed, according to Galois theory, $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})/\mathrm{Gal}(K(\zeta_n)/K) \simeq \mathrm{Gal}(K/\mathbb{Q})$ through $\overline{\sigma} \mapsto \sigma_{|K}$. Since $[K(\zeta_n) : \mathbb{Q}(\zeta_n)] = [K : \mathbb{Q}]$, we have $[K(\zeta_n) : K] = \varphi(n)$ and therefore each element σ of $\mathrm{Gal}(K/\mathbb{Q})$ extends in exactly one way to an element of $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ which satisfies $\sigma(\zeta_n) = \zeta_n^a$. Note that for $n \in \{3, 4\}$ the condition is equivalent to $\zeta_n \notin K$.

The families constructed by Brier and Clavier [10], which are dedicated to integers N such that the nth cyclotomic polynomial has roots modulo N, modify $[K(\zeta_n) : \mathbb{Q}(\zeta_n)]$ by imposing a large torsion subgroup over $\mathbb{Q}(\zeta_n)$.

An important particular case of Theorem 2.7 is as follows:

Corollary 2.9. *Let E be an elliptic curve and π be a prime number. Then,*

$$\mathbb{P}(E(\mathbb{F}_p)[\pi] \simeq \mathbb{Z}/\pi\mathbb{Z}) = \frac{\#\{g \in \rho_\pi(\mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})) \mid \det(g - \mathrm{Id}) = 0, g \neq \mathrm{Id}\}}{\#\,\mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})},$$

$$\mathbb{P}(E(\mathbb{F}_p)[\pi] \simeq \mathbb{Z}/\pi\mathbb{Z} \times \mathbb{Z}/\pi\mathbb{Z}) = \frac{1}{\#\,\mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})}.$$

Example 2.10. Let us compute these probabilities for the curves $E_1 : y^2 = x^3 + 5x + 7$ and $E_2 : y^2 = x^3 - 11x + 14$ and the primes $\pi = 3$ and $\pi = 5$. Here E_1 illustrates the generic case, whereas E_2 has special Galois groups. One checks with Sage [22] that $[\mathbb{Q}(E_1[3]) : \mathbb{Q}] = 48$ and $\#\,\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) = 48$. By Proposition 2.3 we deduce that $\rho_3(\mathrm{Gal}(\mathbb{Q}(E_1[3])/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. A simple computation shows that $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ contains 21 elements having 1 as eigenvalue, one of which is Id. Corollary 2.9 gives the following probabilities: $\mathbb{P}(E(\mathbb{F}_p)[3] \simeq \mathbb{Z}/3\mathbb{Z}) = \frac{20}{48}$ and $\mathbb{P}(E(\mathbb{F}_p)[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = \frac{1}{48}$. We used the same method for all the probabilities of Table 1, where we compare them to experimental values.

Note that the relative difference between theoretical and experimental values never exceeds 0.4%. It is interesting to observe that reducing the Galois group does not necessarily increase the probabilities, as it is shown for $\pi = 3$.

2.2. **Effective Computations of $\mathbb{Q}(E[m])$ and $\rho_m(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}))$.** The main tools are the division polynomials as defined below.

Definition 2.11. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ and $m \geq 2$ an integer. The m-division polynomial P_m is defined as the monic polynomial whose roots are the x-coordinates of all the m-torsion affine points. P_m^{new} is defined as the monic polynomial whose roots are the x-coordinates of the affine points of order exactly m.

Proposition 2.12. *For all $m \geq 2$ we have:*

		E_1	E_2
$\#\,\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$		48	
$\#\,\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$		48	16
$\mathbb{P}(E(\mathbb{F}_p)[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$	Th.	$\frac{1}{48} \approx 0.02083$	$\frac{1}{16} = 0.0625$
	Exp.	0.02082	0.06245
$\mathbb{P}(E(\mathbb{F}_p)[3] \simeq \mathbb{Z}/3\mathbb{Z})$	Th.	$\frac{20}{48} \approx 0.4167$	$\frac{4}{16} = 0.2500$
	Exp	0.4165	0.2501
$\#\,\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$		480	
$\#\,\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q})$		480	32
$\mathbb{P}(E(\mathbb{F}_p)[5] \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$	Th.	$\frac{1}{480} \approx 0.002083$	$\frac{1}{32} = 0.03125$
	Exp.	0.002091	0.03123
$\mathbb{P}(E(\mathbb{F}_p)[5] \simeq \mathbb{Z}/5\mathbb{Z})$	Th.	$\frac{114}{480} = 0.2375$	$\frac{10}{32} = 0.3125$
	Exp.	0.2373	0.3125

TABLE 1. Comparison of the theoretical values (Th) of Corollary 2.9 to the experimental results of all primes below 2^{25} (Exp).

(1) $P_m, P_m^{\mathrm{new}} \in \mathbb{Q}[X]$*;*
(2) $\deg(P_m) = \frac{(m^2+2-3\eta)}{2}$*, where* η *is the remainder of* m *modulo* 2.

Proof. For a proof we refer to [8]. □

Note that one obtains different division polynomials for other shapes of elliptic curves (Weierstrass, Montgomery, Edwards, etc.). Nevertheless, the Galois group $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is model independent and can be computed with the division polynomials of Definition 2.11 as, in characteristic different from 2 and 3, every curve can be written in short Weierstrass form.

One can compute $\mathbb{Q}(E[\pi])$ for any prime $\pi \geq 3$ using the following method:

1. Make a first extension of $\mathbb{Q}$ through an irreducible factor of P_π and obtain a number field F_1 where P_π has a root α_1.
2. Let $f_2(y) = y^2 - (\alpha_1^3 + a\alpha_1 + b) \in F_1[y]$ and F_2 be the extension of F_1 through f_2. F_2 contains a π-torsion point M_1. In F_2, P_π has $\frac{\pi-1}{2}$ trivial roots representing the x coordinates of the multiples of M_1.
3. Call F_3 the extension of F_2 through an irreducible factor of $P_\pi \in F_2[x]$ other than those corresponding to the trivial roots.
4. Let α_2 be the new root of P_π in F_3. Let $f_4(y) = y^2 - (\alpha_2^3 + a\alpha_2 + b) \in F_3[y]$ and F_4 be the extension of F_3 through f_4. F_4 contains all the π-torsion.

In practice we observe that in general $P_\pi, f_2, P_\pi^{(F_2)}$ and f_4 are irreducible, where $P_\pi^{(F_2)}$ is P_π divided by the factors corresponding to the trivial roots. If this is the case, as $\deg(P_\pi) = \frac{\pi^2-1}{2}$ (Proposition 2.12), the absolute degree of F_4 is $\frac{\pi^2-1}{2} \cdot 2 \cdot \frac{\pi^2-\pi}{2} \cdot 2 = (\pi-1)^2(\pi+1)\pi$. According to Remark 2.5, $\#\,\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z}) = (\pi-1)^2(\pi+1)\pi$, thus $\rho_\pi(\mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$. The case of composite m can be handled in a similar way by replacing P_π by P_m^{new} in the method above, and experiments show that in general $\rho_m(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Serre [20] proved that the observation above is almost always true. The next theorem is a restatement of items (1) and (6) in the introduction of [20].

Theorem 2.13 (Serre). *Let E be an elliptic curve without complex multiplication.*

(1) For all primes π and $k \geq 1$ the index $[\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z}) : \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q}))]$ is non-decreasing and bounded by a constant depending on E and π.

(2) For all primes π outside a finite set depending on E and for all $k \geq 1$, $\rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z})$.

Definition 2.14. Put $I(E, \pi, k) = [\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z}) : \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q}))]$. If E does not admit complex multiplication, we call Serre's exponent the integer $n(E, \pi) = \min\{n \in \mathbb{N}^* \mid \forall k \geq n, I(E, \pi, k+1) = I(E, \pi, k)\}$.

The method described above allows us to compute $\mathbb{Q}(E[m])$ as an extension tower. Then it is easy to obtain its absolute degree and a primitive element. Identifying $\rho_\pi(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}))$ (up to conjugacy) is easy when there is only one subgroup (up to conjugacy) of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ with the right order. In the other case we check for each $g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ using the fixed generators of $E(\overline{\mathbb{Q}})[m]$ whether g gives rise to an automorphism on $\mathbb{Q}(E[m])$. In practice, the bottleneck of this method is the factorization of polynomials with coefficients over number fields.

2.3. **Divisibility by a prime power.** It is a common fact that, for a given prime π, the cardinality of an arbitrary elliptic curve over $\mathbb{F}_p$ has a larger probability to be divisible by π than an arbitrary integer of size p. In this subsection we shall rigorously compute those probabilities under some hypothesis of generality.

Notation 2.15. Let π be a prime and $i, j, k \in \mathbb{N}$ such that $i \leq j$. We put:

$$p_{\pi,k}(i, j) = \mathbb{P}(E(\mathbb{F}_p)[\pi^k] \simeq \mathbb{Z}/\pi^i\mathbb{Z} \times \mathbb{Z}/\pi^j\mathbb{Z}).$$

Let $\ell \leq m$ be integers. When it is defined we denote:

$$p_{\pi,k}(\ell, m|i, j) = \mathbb{P}(E(\mathbb{F}_p)[\pi^{k+1}] \simeq \mathbb{Z}/\pi^\ell\mathbb{Z} \times \mathbb{Z}/\pi^m\mathbb{Z} \mid E_p[\pi^k] \simeq \mathbb{Z}/\pi^i\mathbb{Z} \times \mathbb{Z}/\pi^j\mathbb{Z}).$$

When it is clear from the context, π is omitted.

Remark 2.16. Since for every natural number m and every prime p coprime to m, $E(\mathbb{F}_p)[m] \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, we have $p_{\pi,k}(i, j) = 0$ for $j > k$. In the case $j < k$, if $p_{\pi,k}(\ell, m \mid i, j)$ is defined, it equals 1 if $(\ell, m) = (i, j)$ and equals 0 if $(\ell, m) \neq (i, j)$. Finally, for $j = k$, there are only three conditional probabilities which can be non-zero: $p_{\pi,k}(i, k \mid i, k)$, $p_{\pi,k}(i, k+1 \mid i, k)$, and $p_{\pi,k}(k+1, k+1 \mid k, k)$.

Theorem 2.17. *Let π be a prime and E an elliptic curve over $\mathbb{Q}$. If k is an integer such that $I(E, \pi, k+1) = I(E, \pi, k)$, in particular if E has no complex multiplication and $k \geq n(E, \pi)$, then for all $0 \leq i < k$ we have:*

(1) $p_{\pi,k}(k+1, k+1 \mid k, k) = \frac{1}{\pi^4}$;

(2) $p_{\pi,k}(k, k+1 \mid k, k) = \frac{(\pi-1)(\pi+1)^2}{\pi^4}$;

(3) $p_{\pi,k}(i, k+1 \mid i, k) = \frac{1}{\pi}$.

Proof. Let $M = (\mathbb{Z}/\pi^k\mathbb{Z})^2$. For all $g \in \mathrm{GL}_2(\pi M)$, we consider the set $\mathrm{Lift}(g) = \{h \in \mathrm{GL}_2(M) \mid h_{|\pi M} = g\} = \{g + \pi^{k-1} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z}/\pi\mathbb{Z}\}$, whose cardinality is π^4. Since $I(E, \pi, k+1) = I(E, \pi, k)$, we have $\frac{\#\,\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q})}{\#\,\mathrm{Gal}(\mathbb{Q}(E[\pi^{k+1}])/\mathbb{Q})} = \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z})}{\#\,\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z})}$, which equals $\frac{1}{\pi^4}$ by Remark 2.5. So for all $g \in \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q}))$, $\mathrm{Lift}(g) \subset \rho_{\pi^{k+1}}(\mathrm{Gal}(\mathbb{Q}(E[\pi^{k+1}])/\mathbb{Q}))$. Thanks to Theorem 2.7, the proof will follow if we count for each g the number of extensions with a given fixed group.

(1) For $g = \mathrm{Id} \in \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q})$, there is only one element of $\mathrm{Lift}(g)$ fixing $(\mathbb{Z}/\pi^{k+1}\mathbb{Z})^2$, so $p_{\pi,k}(k+1, k+1 \mid k, k) = \frac{1}{\pi^4}$.
(2) The element $g = \mathrm{Id} \in \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q})$, can be extended in exactly $\pi^4 - 1 - \#\,\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$ ways to elements in $\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z})$ which fix the π^k-torsion, a point of order π^{k+1}, but not all the π^{k+1}-torsion. So $p_{\pi,k}(k, k+1 \mid k, k) = \frac{(\pi-1)(\pi+1)^2}{\pi^4}$.
(3) Every element of $\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z})$ which fixes a line, but is not the identity, can be extended in exactly π^3 ways to an element of $\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z})$ which fixes a line of $(\mathbb{Z}/\pi^{k+1}\mathbb{Z})^2$. So $p_{\pi,k}(i, k+1 \mid i, k) = \frac{\pi^3}{\pi^4} = \frac{1}{\pi}$.

□

The theorem below uses the information on $\mathrm{Gal}(\mathbb{Q}(E[\pi^{n(E,\pi)}])/\mathbb{Q})$ for a given prime π in order to compute the probabilities of divisibility by any power of π.

Notation 2.18. Let π be a prime and $\gamma_n(h) = \pi^n \sum_{\ell=0}^{h} \pi^\ell p_n(\ell, n)$. We also define

$$\delta(k) = \begin{cases} p_{i+1}(i+1, i+1) & \text{if } k = 2i+1 \\ 0 & \text{otherwise} \end{cases}, \; S_k(h) = \pi^k \left(\sum_{\ell=h}^{\lfloor \frac{k}{2} \rfloor} p_{k-\ell}(\ell, k-\ell) + \delta(k) \right).$$

Theorem 2.19. *Let π be a prime, E an elliptic curve over $\mathbb{Q}$ without complex multiplication and $n \geq n(E, \pi)$. Then, for any $k \geq 1$,*

$$\mathbb{P}(\pi^k \mid \#E(\mathbb{F}_p)) = \begin{cases} \frac{S_k(0)}{\pi^k} & \text{if } 1 \leq k \leq n, \\ \frac{1}{\pi^k}(\gamma_n(k-n-1) + S_k(k-n)) & \text{if } n < k \leq 2n, \\ \frac{1}{\pi^k}(\gamma_n(n) + p_n(n,n)\pi^{2n-1} - \frac{\pi^{4n-1} p_n(n,n)}{\pi^k}) & \text{if } k > 2n. \end{cases}$$

Let $\overline{v_\pi}$ be the average valuation of π of $\#E(\mathbb{F}_p)$ for an arbitrary prime p. Then,

$$\overline{v_\pi} = 2\sum_{\ell=1}^{n-1} p_\ell(\ell, \ell) + \frac{\pi}{\pi - 1} \sum_{\ell=0}^{n-1} p_n(\ell, n) + \sum_{\ell=0}^{n-2} \sum_{i=\ell+1}^{n-1} p_i(\ell, i) + \frac{\pi(2\pi+1)}{(\pi-1)(\pi+1)} p_n(n, n).$$

Proof. Let k be a positive integer. Using Figure 1, one checks that

$$\mathbb{P}(\pi^k \mid \#E(\mathbb{F}_p)) = \sum_{\ell=0}^{\lfloor \frac{k}{2} \rfloor} p_{k-\ell}(\ell, k-\ell) + \delta(k). \tag{1}$$

Let $c_1 = \frac{1}{\pi^4}$, $c_2 = \frac{(\pi-1)(\pi+1)^2}{\pi^4}$, and $c_3 = \frac{1}{\pi}$. With these notations, the hypothesis can be illustrated by Figure 1. For $j > n$ and $\ell < n$, the probability $p_j(\ell, j)$ is the product of the conditional probabilities of the unique path from (ℓ, j) to (ℓ, n) in the graph of Figure 1 times the probability $p_n(\ell, n)$. For $j > n$ and $\ell \geq n$, the probability $p_j(\ell, j)$ is the product of the conditional probabilities of the unique path from (ℓ, j) to (n, n) in the graph of Figure 1 times the probability $p_n(n, n)$.

There are 3 cases that have to be treated separately: $1 \leq k \leq n$, $n < k \leq 2n$ and $k > 2n$. For $1 \leq k \leq n$, the result follows from Equation (1). Let us explain

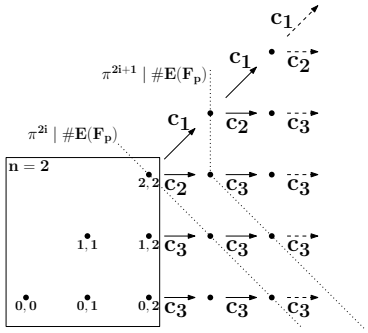

FIGURE 1. Each node of coordinates (i, j) represents the event $\left(E_p[\pi^j] \simeq \mathbb{Z}/\pi^i\mathbb{Z} \times \mathbb{Z}/\pi^j\mathbb{Z}\right)$. The arrows represent the conditional probabilities of Theorem 2.17.

the case for $k > 2n$, with $k = 2i$:

$$\begin{aligned}\mathbb{P}(\pi^{2i} \mid \#E(\mathbb{F}_p)) &= \sum_{\ell=0}^{i} p_{2i-\ell}(\ell, 2i-\ell) + \delta(2i) = \sum_{\ell=0}^{i} p_{2i-\ell}(\ell, 2i-\ell) \\ &= \sum_{\ell=0}^{n-1} p_{2i-\ell}(\ell, 2i-\ell) + \sum_{\ell=n}^{i-1} p_{2i-\ell}(\ell, 2i-\ell) + p_i(i,i) \\ &= \sum_{\ell=0}^{n-1} c_3^{2i-l-n} p_n(\ell, n) + \sum_{\ell=n}^{i-1} c_3^{2i-2l-1} c_2 c_1^{l-n} p_n(n,n) + c_1^{i-n} p_n(n,n).\end{aligned}$$

After computations, one obtains the desired formula. The cases $k > 2n$ odd, and $n < k \leq 2n$ are treated similarly. The formula for $\overline{v_\pi}$ is obtained using $\overline{v_\pi} = \sum_{k \geq 1} \mathbb{P}(\pi^k \mid \#E_p)$.

□

Remark 2.20. The theorem proves in particular that there exists a bound B such that for primes $\pi > B$, $\mathbb{P}(\pi^2 \mid \#E(\mathbb{F}_p)) < \frac{2}{\pi^2}$, so the probability that the cardinality is divisible by the square of a prime greater than B is at most $\frac{2}{B}$. This confirms the experimental result that an elliptic curve is close to a cyclic group when reduced modulo an arbitrary prime, regardless on its rank over $\mathbb{Q}$.

Example 2.21. Let us compare the theoretical and experimental average valuation of $\pi = 2$, $\pi = 3$ and $\pi = 5$ for the curves $E_1 : y^2 = x^3 + 5x + 7$ and $E_2 : y^2 = x^3 - 11x + 14$. For E_1, we apply Theorem 2.19 with $n = 1$ and compute the necessary probabilities with Corollary 2.9 knowing that the Galois groups are isomorphic to $\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$. For E_2, we apply Theorem 2.19 with $n = 5$ for $\pi = 2$, $n = 2$ for $\pi = 3$ and $n = 1$ for $\pi = 5$ and compute the necessary probabilities with Corollary 2.9 (when $n = 1$) and Theorem 2.7 when $n \geq 2$. The results are shown in Table 2.

In order to apply Theorem 2.19, we need $n \geq n(E, \pi)$. But since we do not know any algorithm to compute $n(E, \pi)$, we have to assume that our guesses for $n(E_i, \pi)$, $i = 1, 2$, are true. The relative error for E_2 and $\pi = 5$ is large compared to others cases, which can be explained by the fact that we were unable to compute $\mathrm{Gal}(\mathbb{Q}(E_2[25])/\mathbb{Q})$ and cannot be sure that $n(E_2, 5) = 1$.

	Average valuation of 2			Average valuation of 3			Average valuation of 5		
	n	Th.	Exp.	n	Th.	Exp.	n	Th.	Exp.
E_1	1	$\frac{14}{9} \approx 1.556$	1.555	1	$\frac{87}{128} \approx 0.680$	0.679	1	$\frac{695}{2304} \approx 0.302$	0.301
E_2	5	$\frac{1351}{384} \approx 3.518$	3.499	2	$\frac{199}{384} \approx 0.518$	0.516	1	$\frac{355}{768} \approx 0.462$	0.469

TABLE 2. Experimental values (Exp.) are obtained with all primes below 2^{25}. Theoretical values (Th.) come from Theorem 2.19.

3. Applications to some Families of Elliptic Curves

As shown in the preceding section, changing the torsion properties is equivalent to modifying the Galois group. One can see the fact of imposing rational torsion points as a way of modifying the Galois group. In this section we change the Galois group either by splitting the division polynomials or by imposing some equations that directly modify the Galois group. With these ideas, we find new infinite ECM-friendly families and we explain the properties of some known curves.

3.1. Preliminaries on Montgomery and Twisted Edwards Curves.

Let K be a field whose characteristic is neither 2 nor 3.

3.1.1. *Edwards curves.* For $a, d \in K$, with $ad(a-d) \neq 0$, the twisted Edwards curve $ax^2 + y^2 = 1 + dx^2y^2$ is denoted by $E_{a,d}$. The "$a = -1$" twisted Edwards curves are denoted by E_d. In [6] completed twisted Edwards curves are defined by

$$\overline{E}_{a,d} = \{((X:Z),(Y:T)) \in \mathbb{P}^1 \times \mathbb{P}^1 \mid aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2\}.$$

The completed points are the affine (x, y) embedded into $\mathbb{P}^1 \times \mathbb{P}^1$ by $(x, y) \mapsto ((x : 1), (y : 1))$ (see [6] for more information). We denote $(1 : 0)$ by ∞.

We give an overview of all the 2- and 4-torsion and some 8-torsion points on $\overline{E}_{a,d}$, as specified in [6], in Figure 2.

3.1.2. *Montgomery curves and Suyama family.* Let $A, B \in K$ be such that $B(A^2 - 4) \neq 0$. The Montgomery curve $By^2 = x^3 + Ax^2 + x$ associated to (A, B) is denoted by $M_{A,B}$ (see [17]) and its completion in $\mathbb{P}^2$ by $\overline{M}_{A,B}$.

Remark 3.1. If $a, d, A, B \in K$ are such that $d = \frac{A-2}{B}$ and $a = \frac{A+2}{B}$, then there is a birational map between $\overline{E}_{a,d}$ and $\overline{M}_{A,B}$ given by $((x : z), (y : t)) \mapsto ((t + y)x : (t+y)z : (t-y)x)$ (see [4]). Therefore $\overline{M}_{A,B}$ and $\overline{E}_{a,d}$ have the same group structure over any field where defined and in particular the same torsion properties. Any statement in twisted Edwards language can be easily translated into Montgomery coordinates and vice versa.

A Montgomery curve for which there exist $x_3, y_3, k, x_\infty, y_\infty \in \mathbb{Q}$ such that

$$\begin{cases} P_3(x_3) = 0, \qquad By_3^2 = x_3^3 + Ax_3^2 + x_3 & \text{(3-torsion point)} \\ k = \dfrac{y_3}{y_\infty}, \qquad k^2 = \dfrac{x_3^3 + Ax_3^2 + x_3}{x_\infty^3 + Ax_\infty^2 + x_\infty} & \text{(non-torsion point)} \\ x_\infty = x_3^3. & \text{(Suyama equation)} \end{cases} \tag{2}$$

is called a Suyama curve. As described in [23, 24], the solutions of (2) can be parametrized by a rational value denoted σ. For all $\sigma \in \mathbb{Q}\backslash\{0, \pm 1, \pm 3, \pm 5, \pm\frac{5}{3}\}$, the associated Suyama curve has positive rank and a rational point of order 3.

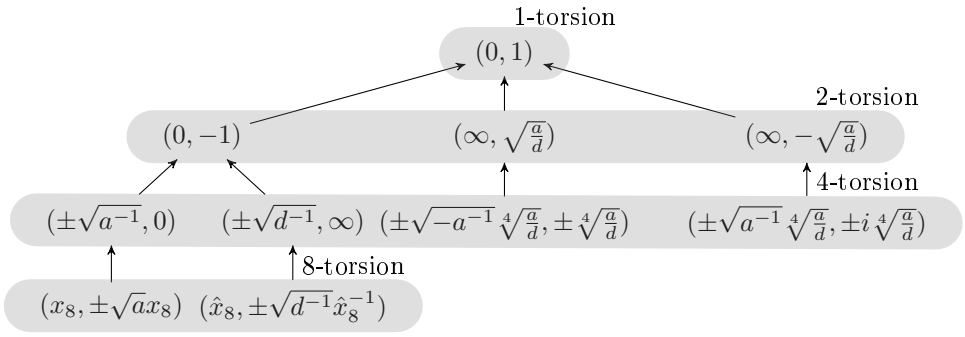

FIGURE 2. An overview of all 1-, 2- and 4-torsion and some 8-torsion points on twisted Edwards curves. The x_8 and $\hat{x}_8$ in the 8-torsion points are such that $adx_8^4 - 2ax_8^2 + 1 = 0$ and $ad\hat{x}_8^4 - 2d\hat{x}_8^2 + 1 = 0$.

Remark 3.2. In the following, when we say that an elliptic curve $E_{a,d}$ has good reduction modulo a prime p, we also suppose that we have $v_p(a) = v_p(d) = v_p(a - d) = 0$ (resp. $v_p(A - 2) = v_p(A + 2) = v_p(B) = 0$ for a Montgomery curve). In this case the reduction map is simply given by reducing the coefficients modulo p. The results below are also true for primes of good reduction which do not satisfy these conditions, by slightly modifying the statements and the proofs. Moreover, in ECM, if the conditions are not satisfied, we immediately find the factor p.

3.2. **Study of the 2^k-Torsion of Montgomery/Twisted Edwards Curves.** The rational torsion of a Montgomery/twisted Edwards curve is $\mathbb{Z}/2\mathbb{Z}$ but it is known that 4 divides the order of the curve when reduced modulo any prime p [23]. The following theorem gives more detail on the 2^k-torsion.

Theorem 3.3. *Let $E = E_{a,d}$ be a twisted Edwards curve (resp. a Montgomery curve $M_{A,B}$) over $\mathbb{Q}$. Let p be a prime such that E has good reduction at p.*

1. *If $p \equiv 3 \pmod 4$ and $\frac{a}{d}$ (resp. $A^2 - 4$) is a quadratic residue modulo p, then $E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$;*
2. *If $p \equiv 1 \pmod 4$, a (resp. $\frac{A+2}{B}$) is a quadratic residue modulo p (in particular $a = \pm 1$) and $\frac{a}{d}$ (resp. $A^2 - 4$) is a quadratic residue modulo p, then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subset E(\mathbb{F}_p)[4]$;*
3. *If $p \equiv 1 \pmod 4$, $\frac{a}{d}$ (resp. $A^2 - 4$) is a quadratic non-residue modulo p and $a - d$ (resp. B) is a quadratic residue modulo p, then $E(\mathbb{F}_p)[8] \simeq \mathbb{Z}/8\mathbb{Z}$.*

Proof. Using Remark 3.1, it is enough to prove the results in the Edwards language, which follow by some calculations using Figure 2. □

Theorem 3.3 suggests that by imposing equations on the parameters a and d we can improve the torsion properties. The case where $\frac{a}{d}$ is a square has been studied in [6] and [5] for the family of Edwards curves having $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ (when $a = 1$) respectively $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (when $a = -1$) rational torsion. Here we focus on two

other equations:

(3) $\exists c \in \mathbb{Q}$, $a = -c^2$ ($A + 2 = -Bc^2$ for Montgomery curves),

(4) $\exists c \in \mathbb{Q}$, $a - d = c^2$ ($B = c^2$ for Montgomery curves).

We were not able to compute the generic Galois group of the m-torsion for a family of curves, i.e., a group that is isomorphic to the Galois group for "most" of the curves of the family (here "most" is meant in the sense that most polynomials of degree d have Galois group $\mathcal{S}_d$). But we can compute this Galois group for every elliptic curve. So when we talk about the Galois group of a family of curves, we mean that we computed the Galois group for some curves of this family and that the Galois group was always the same (up to conjugacy), so the curves have the same probabilities.

The cardinality of the Galois group of the 4-torsion for generic Montgomery curves is 16 and this is reduced to 8 for the family of curves satisfying (3). Using Theorem 2.7, we can compute the changes of probabilities due to this new Galois group. For all curves satisfying (3) and all primes $p \equiv 1 \pmod 4$, the probability of having $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as the 4-torsion group becomes 0 (instead of $\frac{1}{4}$); the probabilities of having $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ as the 4-torsion group become $\frac{1}{4}$ (instead of $\frac{1}{8}$).

The Galois group of the 8-torsion of the family of curves satisfying (4) has cardinality 128 instead of 256 for generic Montgomery curves. Using Theorem 2.7, one can see that the probabilities of having an 8-torsion point are improved.

Using Theorem 2.19, one can show that both families of curves, the family satisfying (3) and the one satisfying (4), increase the probability of having the cardinality divisible by 8 from 62.5% to 75% and the average valuation of 2 from $\frac{10}{3}$ to $\frac{11}{3}$.

3.3. **Better Twisted Edwards Curves with Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ using Division Polynomials.** In this section we search for curves such that some of the factors of the division polynomials split and by doing so we try to change the Galois groups. As an example we consider the family of $a = -1$ twisted Edwards curves E_d with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$-torsion, these curves are exactly the ones with $d = -e^4$ (see [5]). The technique might be used in any context.

3.3.1. *Looking for subfamilies.* For a generic d, P_8^{new} splits into three irreducible factors: two of degree 4 and one of degree 16. If one takes $d = -e^4$, the polynomial of degree 16 splits into three factors: two of degree 4, called $P_{8,0}$ and $P_{8,1}$, and one of degree 8, called $P_{8,2}$. By trying to force one of these three polynomials to split, we found four families, as shown in Table 3.

$d = -e^4$	generic e	$e = g^2$	$e = \frac{2g^2+2g+1}{2g+1}$	$e = \frac{g^2}{2}$	$e = \frac{g-\frac{1}{g}}{2}$
$P_{8,0}$	4	4	4	2, 2	2, 2
$P_{8,1}$	4	4	4	4	2, 2
$P_{8,2}$	8	4, 4	4, 4	8	8

TABLE 3. Subfamilies of twisted Edwards curves with torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the degrees of the irreducible factors of $P_{8,0}$, $P_{8,1}$ and $P_{8,2}$.

In all these families the generic average valuation of 2 is increased by $\frac{1}{6}$ ($\frac{29}{6}$ instead of $\frac{14}{3}$), except the family $e = \frac{g-\frac{1}{g}}{2}$ for which it is increased by $\frac{2}{3}$, bringing it to the same valuation as for the family of twisted Edwards curves with $a = 1$ and torsion isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Note that these four families cover all the curves presented in the first three columns of [5, Table 3.1], except the two curves with $e = \frac{26}{7}$ and $e = \frac{19}{8}$, which have a generic Galois group for the 8-torsion.

3.3.2. *The family* $e = \frac{g-\frac{1}{g}}{2}$. In this section, we study in more details the family $e = \frac{g-\frac{1}{g}}{2}$. Theorem 2.7 proofs that the group order modulo all primes is divisible by 16. In order to gain more intuition, we give an alternative proof. We need the following theorem which computes the 8-torsion points that double to the 4-torsion points $(\pm\sqrt[4]{-d^{-1}}, \pm\sqrt[4]{-d^{-1}})$.

Theorem 3.4. *Let E_d be a twisted Edwards curve over $\mathbb{Q}$ with $d = -e^4$, $e = \frac{g-\frac{1}{g}}{2}$ and $g \in \mathbb{Q} \setminus \{-1, 0, 1\}$. Let $p > 3$ be a prime of good reduction. If $t \in \{1, -1\}$ such that $tg(g-1)(g+1)$ is a quadratic residue modulo p then the points $(x, y) \in E_d(\mathbb{F}_p)$, with $w \in \{1, -1\}$, and*

$$x = \pm g^w y, \qquad y = \pm\sqrt{\frac{4tg^{2-w}}{(g - tw)^3(g + tw)}} \tag{5}$$

have order eight and double to $(\pm e^{-1}, te^{-1})$.

Proof. Note that all points (x, y) of order eight satisfy $\infty \neq x \neq 0 \neq y \neq \infty$. Following [6, Theorem 2.10] a point (x, y) doubles to $((2xy : 1 + dx^2y^2), (x^2 + y^2 : 1 - dx^2y^2)) = ((2xy : -x^2 + y^2), (x^2 + y^2 : 2 - (-x^2 + y^2)))$. Let $s, t \in \{1, -1\}$ such that (x, y) doubles to (se^{-1}, te^{-1}), hence

$$\frac{2xy}{-x^2 + y^2} = \frac{s}{e} \quad \text{and} \quad \frac{x^2 + y^2}{2 - (-x^2 + y^2)} = \frac{t}{e}.$$

From the terms in the first equation we obtain $\left(\frac{x}{y}\right)^2 + \frac{2exs}{y} + e^2 = 1 + e^2$. Write $e = \frac{g-\frac{1}{g}}{2}$ such that $\left(\frac{x}{y} + se\right)^2 = \left(\frac{g+\frac{1}{g}}{2}\right)^2$. Hence $\frac{x}{y} \in \left\{\pm g, \pm\frac{1}{g}\right\}$ depending on the sign s and the sign after taking the square root. This gives $x^2 = G^2y^2$ with $G^2 \in \{g^2, g^{-2}\}$.

From the second equation we obtain $(e - t)x^2 + (e + t)y^2 = 2t$ and substituting x^2 results in $\left((e - t)G^2 + (e + t)\right) y^2 = 2t$. This can be solved for y when $2t\left((e - t)G^2 + (e + t)\right)$ is a quadratic residue modulo p. This is equivalent to checking if any of

$$2t\left((e - 1)g^2 + (e + 1)\right) = \frac{t(g - 1)^3(g + 1)}{g}, \tag{6}$$

$$2t\left((e - 1) + (e + 1)g^2\right) = \frac{t(g - 1)(g + 1)^3}{g} \tag{7}$$

is a quadratic residue modulo p. By assumption $tg(g - 1)(g + 1)$ is a quadratic residue modulo p. Hence, both expression (6) and (7) are quadratic residues modulo p. Solving for y and keeping track of all the signs results in the formulae in (5). □

A direct consequence of this theorem is as follows.

Corollary 3.5. *Let $E = E_d$ be a twisted Edwards curve over $\mathbb{Q}$ with $d = -\left(\frac{g-\frac{1}{g}}{2}\right)^4$, $g \in \mathbb{Q} \setminus \{-1, 0, 1\}$ and $p > 3$ a prime of good reduction. Then $E(\mathbb{Q})$ has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the group order of $E(\mathbb{F}_p)$ is divisible by 16.*

Proof. We consider two cases.
(1) If $p \equiv 1 \pmod 4$ then -1 is a quadratic residue modulo p. Hence, the 4-torsion points $(\pm i, 0)$ exist (see Figure 2) and $16 \mid \#E(\mathbb{F}_p)$.
(2) If $p \equiv 3 \pmod 4$ then -1 is a quadratic non-residue modulo p. Then exactly one of $\{g(g-1)(g+1), -g(g-1)(g+1)\}$ is a quadratic residue modulo p. Using Thm. 3.4 it follows that the curve $E(\mathbb{F}_p)$ has eight 8-torsion points and hence $16 \mid \#E(\mathbb{F}_p)$. □

Corollary 3.5 explains the good behavior of the curve with $d = -(\frac{77}{36})^4$ and torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ found in [5]. This parameter can be expressed as $d = -(\frac{77}{36})^4 = -\left(\frac{g-\frac{1}{g}}{2}\right)^4$ for $g = \frac{9}{2}$ and, therefore, the group order is divisible by an additional factor two.

Corollary 3.6. *Let $g \in \mathbb{Q} \setminus \{-1, 0, 1\}$, $d = -\left(\frac{g-\frac{1}{g}}{2}\right)^4$ and $p \equiv 1 \pmod 4$ be a prime of good reduction. If $g(g-1)(g+1)$ is a quadratic residue modulo p then the group order of $E_d(\mathbb{F}_p)$ is divisible by 32.*

Proof. All 16 4-torsion points are in $E_d(\mathbb{F}_p)$ (see Figure 2). By Thm. 3.4 we have at least one 8-torsion point. Hence, $32 \mid \#E_d(\mathbb{F}_p)$. □

We generated different values $g \in \mathbb{Q}$ by setting $g = \frac{i}{j}$ with $1 \leq i < j \leq 200$ such that $\gcd(i, j) = 1$. This resulted in 12 231 possible values for g and Sage [22] found 614 non-torsion points. As expected, we observed that they behave similarly as the good curve found in [5].

3.3.3. *Parametrization.* In [5] a "generating curve" is specified which parametrizes d and the coordinates of the non-torsion points. Arithmetic on this curve can be used to generate an infinite family of twisted Edwards curves with torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and a non-torsion point. Using ideas from [10] we found a parametrization which does not involve a generating curve and hence no curve arithmetic.

Theorem 3.7. *Let $t \in \mathbb{Q} \setminus \{0, \pm 1\}$ and $d = -e^4$, $e = \frac{3(t^2-1)}{8t}$, $x_\infty = (4e^3 + 3e)^{-1}$ and $y_\infty = \frac{9t^4-2t^2+9}{9t^4-9}$. Then the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and (x_∞, y_∞) is a non-torsion point.*

Proof. The twisted Edwards curve has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ because $d = -e^4$ and e is not equal to 0 and ± 1. The point (x_∞, y_∞) is on the curve and since $x_\infty \notin \{0, \infty, e^{-1}, -e^{-1}\}$ this is a non-torsion point. □

This rational parametrization allowed us to impose additional conditions on the parameter e. For the four families, except $e = g^2$ which is treated below, the parameter e is given by an elliptic curve of rank 0 over $\mathbb{Q}$.

Corollary 3.8. *Let $P = (x, y)$ be a non-torsion point on the elliptic curve $y^2 = x^3 - 36x$ having rank 1. Let $t = \frac{x+6}{x-6}$, using notations of Theorem 3.7, the curve E_{-e^4} belongs to the family $e = g^2$ and has positive rank over $\mathbb{Q}$.*

3.4. **Better Suyama Curves by a Direct Change of the Galois Group.** In this section we will present two families that change the Galois group of the 4- and 8-torsion without modifying the factorization pattern of the 4- and 8-division polynomial.

3.4.1. *Suyama*-11. Kruppa observed in [14] that among the Suyama curves, the one corresponding to $\sigma = 11$ finds exceptionally many primes. Barbulescu [3] extended it to an infinite family that we present in detail here.

Experiments show that the $\sigma = 11$ curve differs from other Suyama curves only by its probabilities to have a given 2^k-torsion when reduced modulo primes $p \equiv 1 \pmod 4$. The reason is that the $\sigma = 11$ curve satisfies Equation (3). Section 3.2 illustrates the changes in probabilities of the $\sigma = 11$ curve when compared to curves which do not satisfy Equation (3) and shows that Equation (3) improves the average valuation of 2 from $\frac{10}{3}$ to $\frac{11}{3}$.

Let us call Suyama-11 the set of Suyama curves which satisfy Equation (3). When solving the system formed by Suyama's system plus Equation (3), we obtain an elliptic parametrization for σ. Given a point (u, v) on $E_{\sigma_{11}} : v^2 = u^3 - u^2 - 120u + 432$, σ is obtained as $\sigma = \frac{120}{u-24} + 5$. The group $E_{\sigma_{11}}(\mathbb{Q})$ is generated by the points $P_\infty = (-6, 30)$, $P_2 = (-12, 0)$ and $Q_2 = (4, 0)$ of orders ∞, 2 and 2 respectively. We exclude $0, \pm P_\infty$, P_2, Q_2, $P_2 + Q_2$, and $Q_2 \pm P_\infty$, which are the points producing non-valid values of σ. The points $\pm R, Q_2 \pm R$ lead to isomorphic curves. Note that the $\sigma = 11$ curve corresponds to the point $(44, 280) = P_\infty + P_2$.

3.4.2. *Edwards $\mathbb{Z}/6\mathbb{Z}$: Suyama-11 in disguise.* In [5, Sec. 5] it is shown that the $a = -1$ twisted Edwards curves with $\mathbb{Z}/6\mathbb{Z}$-torsion over $\mathbb{Q}$ are precisely the curves E_d with $d = \frac{-16u^3(u^2-u+1)}{(u-1)^6(u+1)^2}$ where u is a rational parameter.[1] In particular, according to [5, Sec. 5.3] one can translate any Suyama curve in Edwards language and then impose the condition that $-a$ is a square to obtain curves of the $a = -1$ type. Finally, [5, Sec. 5.5] points out that this family has exceptional torsion properties.

In order to understand the properties of this family, we translate it back to Montgomery language using Remark 3.1. Thus, we are interested in Suyama curves which satisfy equation $A + 2 = -Bc^2$ (the Montgomery equivalent for $-a$ being a square). This is the Suyama-11 family, so its torsion properties were explained in Section 3.4.1. These two families have been discovered independently in [3] and [5].

3.4.3. *Suyama-$\frac{9}{4}$*. In experiments by Zimmermann, new Suyama curves with exceptional torsion properties were discovered, such as $\sigma = \frac{9}{4}$. Further experiments show that their special properties are related to the 2^k-torsion and concern exclusively primes $p \equiv 1 \pmod 4$. Indeed, the $\sigma = \frac{9}{4}$ curve satisfies Equation (4). Section 3.2 illustrates the changes in probabilities of the $\sigma = \frac{9}{4}$ curve when compared to curves which do not satisfy Equation (4) and shows that Equation (4) improves the average valuation of 2 from $\frac{10}{3}$ to $\frac{11}{3}$.

Let us call Suyama-$\frac{9}{4}$ the set of Suyama curves which satisfy Equation (4). When solving the system formed by Suyama's system plus Equation (4), we obtain an elliptic parametrization for σ. Given a point (u, v) on $E_{\sigma_{94}} : v^2 = u^3 - 5u$, σ is obtained as $\sigma = u$. The group $E_{\sigma_{94}}(\mathbb{Q})$ is generated by the points $P_\infty = (-1, 2)$ and $P_2 = (0, 0)$ of orders ∞ and 2 respectively. We exclude the points $0, \pm P_\infty$, P_2

[1] There is a typo in the proof of [5, Thm. 5.1]; the $\frac{16u^3(u^2-u+1)}{(u-1)^6(u+1)^2}$ misses a minus sign.

Families	Curves	Average valuation of 2			Average valuation of 3		
		n	Th.	Exp.	n	Th.	Exp.
Suyama	$\sigma = 12$	2	$\frac{10}{3} \approx 3.333$	3.331	1	$\frac{27}{16} \approx 1.688$	1.689
Suyama-11	$\sigma = 11$	2	$\frac{11}{3} \approx 3.667$	3.669	1	$\frac{27}{16} \approx 1.688$	1.687
Suyama-$\frac{9}{4}$	$\sigma = \frac{9}{4}$	3	$\frac{11}{3} \approx 3.667$	3.664	1	$\frac{27}{16} \approx 1.688$	1.687
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	E_{-11^4}	3	$\frac{14}{3} \approx 4.667$	4.666	1^*	$\frac{87}{128} \approx 0.680$	0.679
$e = \frac{g-\frac{1}{g}}{2}$	$E_{-\left(\frac{77}{36}\right)^4}$	3	$\frac{16}{3} \approx 5.333$	5.332	1^*	$\frac{87}{128} \approx 0.680$	0.679
$e = g^2$	E_{-9^4}	3	$\frac{29}{6} \approx 4.833$	4.833	1^*	$\frac{87}{128} \approx 0.680$	0.680
$e = \frac{g^2}{2}$	$E_{-\left(\frac{81}{8}\right)^4}$	3	$\frac{29}{6} \approx 4.833$	4.831	1^*	$\frac{87}{128} \approx 0.680$	0.679
$e = \frac{2g^2+2g+1}{2g+1}$	$E_{-\left(\frac{5}{3}\right)^4}$	3	$\frac{29}{6} \approx 4.833$	4.833	1^*	$\frac{87}{128} \approx 0.680$	0.679

TABLE 4. Experimental values (Exp.) are obtained with all primes below 2^{25}. The case $n = 1^*$ means that the Galois group is isomorphic to $GL_2(\mathbb{Z}/\pi\mathbb{Z})$.

and $P_2 \pm P_\infty$ which produce non-valid values of σ. If two points in $E_{\sigma_{94}}(\mathbb{Q})$ differ by P_2 they correspond to isomorphic curves. We recognize the curve associated to $\sigma = \frac{9}{4}$ when considering the point $(\frac{9}{4}, -\frac{3}{8}) = [2]P_\infty$.

3.5. **Comparison.** Table 4 gives a summary of all the families found in this article. The theoretical average valuations were computed with Theorem 2.19, Theorem 2.7 and Corollary 2.9 under some assumptions on Serre's exponent (see Example 2.21 for more information).

Note that, when we impose torsion points over $\mathbb{Q}$, the average valuation does not simply increase by 1, as can be seen in Table 4 for the average valuation of 3.

4. Conclusion and further work

We have used Galois theory in order to analyze the torsion properties of elliptic curves. We have determined the behavior of generic elliptic curves and explained the exceptional properties of some known curves (Edwards curves of torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$). The new techniques suggested by the theoretical study have helped us to find infinite families of curves having exceptional torsion properties. We list below some questions which were not addressed in this work:

- Can one effectively compute Serre's exponent?
- How does Serre's work relate to the independence of the m- and m'-torsion probabilities for coprime numbers m and m'?
- Is there a model predicting the success probability of ECM from the probabilities given in Theorem 2.19?
- Is it possible to effectively use the Resolvent Method [11] in order to compute equations which improve the torsion properties?

References

[1] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60(201):399–405, 1993.

[2] S. Bai, P. Gaudry, A. Kruppa, F. Morain, E. Thomé, and P. Zimmermann. Crible algébrique: distribution, optimisation (CADO-NFS). `http://cado-nfs.gforge.inria.fr/`.

[3] R. Barbulescu. Familles de courbes adaptées à la factorisation des entiers. Research report, `http://hal.inria.fr/inria-00419218/en/`, 2009.

[4] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In S. Vaudenay, editor, *Africacrypt*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer, Heidelberg, 2008.

[5] D. J. Bernstein, P. Birkner, and T. Lange. Starfish on strike. In M. Abdalla and P. S. L. M. Barreto, editors, *Latincrypt*, volume 6212 of *Lecture Notes in Computer Science*, pages 61–80. Springer, Heidelberg, 2010.

[6] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters. ECM using Edwards curves. Cryptology ePrint Archive, Report 2008/016, 2008. `http://eprint.iacr.org/`.

[7] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *Asiacrypt*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, Heidelberg, 2007.

[8] I. Blake, G. Seroussi, and N. Smart. *Elliptic curves in cryptography*, volume 265. Cambridge Univ Pr, 1999.

[9] J. W. Bos, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery. Efficient SIMD arithmetic modulo a Mersenne number. In *IEEE Symposium on Computer Arithmetic – ARITH-20*, pages 213–221. IEEE Computer Society, 2011.

[10] E. Brier and C. Clavier. New families of ECM curves for Cunningham numbers. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory – ANTS-IX*, volume 6197 of *Lecture Notes in Computer Science*, pages 96–109. Springer, 2010.

[11] H. Cohen. *A course in computational algebraic number theory*, volume 138. Springer Verlag, 1993.

[12] H. M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, July 2007.

[13] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson. Twisted Edwards curves revisited. In J. Pieprzyk, editor, *Asiacrypt 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 326–343. Springer, Heidelberg, 2008.

[14] A. Kruppa. *Speeding up Integer Multiplication and Factorization*. PhD thesis, Université Henri Poincaré - Nancy I, January 2010.

[15] A. K. Lenstra and H. W. Lenstra, Jr. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verslag, 1993.

[16] H. W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987.

[17] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[18] J. Neukirch. *Class field theory*, volume 280. Springer-Verlag, 1986.

[19] J. M. Pollard. The lattice sieve. pages 43–49 in [15].

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

[21] J. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Verlag, 2009.

[22] W. Stein et al. *Sage Mathematics Software (Version 4.7)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[23] H. Suyama. Informal preliminary report (8), October 1985.

[24] P. Zimmermann and B. Dodson. 20 years of ECM. In F. Hess, S. Pauli, and M. E. Pohst, editors, *Algorithmic Number Theory – ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 525–542. Springer, Heidelberg, 2006.

[25] P. Zimmermann et al. GMP-ECM (elliptic curve method for integer factorization). `https://gforge.inria.fr/projects/ecm/`, 2010.

Université de Lorraine, CNRS, INRIA, France

Laboratory for Cryptologic Algorithms, EPFL, Lausanne, Switzerland

ENS Paris, Université de Lorraine, CNRS, INRIA, France

Laboratory for Cryptologic Algorithms, EPFL, Lausanne, Switzerland

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA