THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Finding ECM-friendly curves through a study of Galois properties

Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery

msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.63

Finding ECM-friendly curves through a study of Galois properties

Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery

We prove some divisibility properties of the cardinality of elliptic curve groups 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 behind the proofs help us to find new infinite families of elliptic curves with good division properties increasing the success probability of ECM.

1. Introduction

The elliptic curve method (ECM) for integer factorization [22] is the asymptotically fastest known 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 2011 ECM record is a 241-bit factor of $2^{1181} - 1$ [12]. On the other hand, ECM is used to factor many small (100- to 200-bit) integers as part of the number field sieve [26; 21; 4], the most efficient general purpose integer factorization method.

Traditionally, the elliptic curve arithmetic used in ECM is implemented using Montgomery curves [23] (for example, in the widely used GMP-ECM software [35]). Generalizing the work of Euler and Gauss, Edwards [15] introduced a new normal form for elliptic curves which results in a fast realization of the elliptic curve group operation in practice. These "Edwards curves" have been generalized by Bernstein and Lange [9] for use in cryptography. Bernstein et al. [8] explored the possibility of using these curves in the ECM setting. After Hisil et al. [18] published a coordinate system which results in the fastest known realization of

MSC2010: primary 14H52; secondary 11Y05.
Keywords: elliptic curve method (ECM), Edwards curves, Montgomery curves, torsion properties, Galois groups.

curve arithmetic, a follow-up paper by Bernstein et al. [7] discusses the use of the so-called "$a = -1$" twisted Edwards curves 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 [32], the curves proposed by Atkin and Morain [3], a translation of these techniques to Edwards curves [8; 7], and a family of curves suitable for Cunningham numbers [13].

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 Chebotarev's theorem [24]. 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 infinite 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.

2A. *Torsion properties of elliptic curves.*

Definition 2.1. Let K be a finite Galois extension of $\mathbb{Q}$, let p be a prime, and let $\mathfrak{p}$ be a prime ideal of K above p with residue field $k_\mathfrak{p}$. The decomposition group $\mathrm{Dec}(\mathfrak{p})$ of $\mathfrak{p}$ is the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ that stabilizes $\mathfrak{p}$. Denote by $\alpha^{(\mathfrak{p})}$ 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

$$\mathrm{Frobenius}(p) = \bigcup_{\mathfrak{p}\mid p} (\alpha^{(\mathfrak{p})})^{-1}(\phi_\mathfrak{p}).$$

We say that a set S of primes *admits a natural density equal to* δ, and we write $\mathsf{P}(S) = \delta$, if

$$\lim_{N\to\infty} \frac{\#(S \cap \Pi(N))}{\#\Pi(N)}$$

exists and equals δ, where $\Pi(N)$ is the set of primes up to N. If event(p) is a property which can be defined for all primes except a finite set, when we write $\mathsf{P}(\text{event}(p))$ we tacitly exclude the primes where event(p) cannot be defined.

Theorem 2.2 (Chebotarev, [24]). *Let K be a finite Galois extension of $\mathbb{Q}$. Let $H \subset \mathrm{Gal}(K/\mathbb{Q})$ be a conjugacy class. Then*

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

Before applying Chebotarev's theorem to the case of elliptic curves we introduce some notation. For every elliptic curve E over a field F and for all integers $m \geq 2$, we let $F(E[m])$ denote the smallest extension of F over which all of the geometric m-torsion points of E are rational. 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 elliptic curve E over a perfect field F, the following hold*:

(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. 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. This proves statement (1).

For each $\sigma \in \mathrm{Gal}(F(E[m])/F)$ we denote by $\iota_m(\sigma)$ the function that sends $(x, y) \in E(\overline{F})[m]$ to $(\sigma(x), \sigma(y))$. Thanks to the discussion above, $\iota_m(\sigma)$ sends points of $E(\overline{F})[m]$ to $E(\overline{F})[m]$. Since the addition law can be expressed by rational functions over F, for each σ we have $\iota_m(\sigma) \in \mathrm{Aut}(E(\overline{F})[m])$. One easily checks that ι_m is a group morphism and its kernel is the identity, proving statement (2). □

Notation. Let E be an elliptic curve over $\mathbb{Q}$ and let $m \geq 2$ be an integer. 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, and let $\rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ be the injective morphism $\psi_m \circ \iota_m$.

Let p be a prime such that E has good reduction at p and $p \nmid m$. If k is an extension field of $\mathbb{F}_p$, we write $E(k)$ for the group of k-rational points on the reduction of E modulo p. 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 [29, Proposition 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 2.4. 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 $k \geq 1$ we have $\#\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z}) = \pi^4 \#\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z})$.

Notation. For all $g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ we put $\mathrm{Fix}(g) = \{v \in (\mathbb{Z}/m\mathbb{Z})^2 \mid g(v) = v\}$. If C is a conjugacy class of elements of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we let $\mathrm{Fix}(C)$ denote the isomorphism class of the group $\mathrm{Fix}(g)$, for some $g \in C$; this isomorphism class does not depend on the choice of g. We use analogous notations for the fixed groups of elements of, and conjugacy classes in, the groups $\mathrm{Aut}(E(\overline{\mathbb{Q}})[m])$ and $\mathrm{Aut}(E(\overline{\mathbb{F}}_p)[m])$.

Theorem 2.5. *Let E be an elliptic curve over $\mathbb{Q}$ and let $m \geq 2$ 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) $$\mathsf{P}\big(E(\mathbb{F}_p)[m] \simeq T\big) = \frac{\#\{g \in \rho_m(\mathrm{Gal}(K/\mathbb{Q})) \mid \mathrm{Fix}(g) \simeq T\}}{\#\,\mathrm{Gal}(K/\mathbb{Q})}.$$

(2) *Let a and n be positive integers such that $a \leq n$ and $\gcd(a, n) = 1$, and let ζ_n be a primitive n-th root of unity. Put*

$$G_a = \{\sigma \in \mathrm{Gal}(K(\zeta_n)/\mathbb{Q}) \mid \sigma(\zeta_n) = \zeta_n^a\}.$$

Then

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

Proof. 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. Let H denote the set $\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \mathrm{Fix}(\iota_m(\sigma)) \simeq T\}$. 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 $\mathrm{Fix}(\iota_m(\mathrm{Frobenius}(p))) \simeq T$ if and only if $\mathrm{Frobenius}(p)$ is one of the C_i. Thanks to Theorem 2.2 we obtain

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

This proves statement (1).

Using similar arguments, we see that to prove statement (2) we have to evaluate

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

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 $\widetilde{C}_1, \ldots, \widetilde{C}_{\widetilde{N}}$ be the conjugacy classes of $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ that are in the preimages 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 n-th roots of unity we have for $\sigma \in (\alpha^{(\mathfrak{P})})^{-1}(\phi_{\mathfrak{P}})$ that $\sigma(\zeta_n) = \zeta_n^b$ for some b. Together with $\sigma(x) \equiv x^p \bmod \mathfrak{P}$ this gives $\zeta_n^b \equiv \zeta_n^p \bmod \mathfrak{P}$. 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 $\text{Frobenius}(K(\zeta_n), p)$, the Frobenius conjugacy class for $K(\zeta_n)$, is the preimage of $\text{Frobenius}(p)$, the argument above gives

$$\mathsf{P}\big(\text{Frobenius}(p) \in \{C_1, \ldots, C_N\},\, p \equiv a \bmod n\big) = \mathsf{P}\big(\text{Frobenius}(K(\zeta_n), p) \in \{\widetilde{C}_1, \ldots, \widetilde{C}_{\widetilde{N}}\}\big).$$

Considering the denominator $\mathsf{P}(p \equiv a \bmod n)$ similarly completes the proof. □

Remark 2.6. Put $K = \mathbb{Q}(E[m])$. If $[K(\zeta_n) : \mathbb{Q}(\zeta_n)] = [K : \mathbb{Q}]$, then one has

$$\mathsf{P}\big(E(\mathbb{F}_p)[m] \simeq T \mid p \equiv a \bmod n\big) = \mathsf{P}\big(E(\mathbb{F}_p)[m] \simeq T\big)$$

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 [13], which were developed to help factor integers N such that the n-th cyclotomic polynomial has roots modulo all prime factors of N, modify $[K(\zeta_n) : \mathbb{Q}(\zeta_n)]$ by imposing a large torsion subgroup over $\mathbb{Q}(\zeta_n)$.

The following corollary is an important particular case of Theorem 2.5.

Corollary 2.7. *Let E be an elliptic curve over $\mathbb{Q}$ and let π be a prime number. Put $K = \mathbb{Q}(E[\pi])$. Then*

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

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

π	T	d_1	$\mathsf{P}_{\text{theor}}(E_1,\pi,T)$ $\mathsf{P}_{\text{exper}}(E_1,\pi,T)$	d_2	$\mathsf{P}_{\text{theor}}(E_2,\pi,T)$ $\mathsf{P}_{\text{exper}}(E_2,\pi,T)$
3	$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$	48	$\frac{1}{48}\approx 0.02083$ 0.02082	16	$\frac{1}{16}=0.06250$ 0.06245
3	$\mathbb{Z}/3\mathbb{Z}$	48	$\frac{20}{48}\approx 0.4167$ 0.4165	16	$\frac{4}{16}=0.2500$ 0.2501
5	$\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$	480	$\frac{1}{480}\approx 0.002083$ 0.002091	32	$\frac{1}{32}=0.03125$ 0.03123
5	$\mathbb{Z}/5\mathbb{Z}$	480	$\frac{114}{480}\approx 0.2375$ 0.2373	32	$\frac{10}{32}=0.3125$ 0.3125

Table 1. Theoretical and experimental values of $\mathsf{P}(E,\pi,T):=\mathsf{P}\big(E(\mathbb{F}_p)[\pi]\simeq T\big)$ for the elliptic curves E_1 and E_2, for several primes π and groups T. The theoretical values were obtained from Corollary 2.7, and the experimental values were computed using all primes less than 2^{25}. The columns labeled d_1 and d_2 give the degrees of the number fields $\mathbb{Q}(E_1[\pi])$ and $\mathbb{Q}(E_2[\pi])$, respectively.

Example 2.8. We 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 [30] that $[\mathbb{Q}(E_1[3]):\mathbb{Q}]=48$. Since $\#\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})=48$, Proposition 2.3 tells us that $\rho_3(\mathrm{Gal}(\mathbb{Q}(E_1[3])/\mathbb{Q}))=\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. The group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ contains 20 nonidentity elements having 1 as an eigenvalue. From Corollary 2.7 we find

$$\mathsf{P}\big(E_1(\mathbb{F}_p)[3]\simeq\mathbb{Z}/3\mathbb{Z}\big)=\tfrac{20}{48},\quad \mathsf{P}\big(E_1(\mathbb{F}_p)[3]\simeq\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\big)=\tfrac{1}{48}.$$

We used the same method for all the probabilities displayed in 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 $\pi=3$.

2B. ***Effective computations of*** $\mathbb{Q}(E[m])$ ***and*** $\rho_m(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}))$ ***for prime powers.*** The main tools we use to compute $\mathbb{Q}(E[m])$ and its Galois group are the division polynomials, as defined below.

Definition 2.9. 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 the monic polynomial whose roots are the x-coordinates of all the affine m-torsion points of E. We also define P_m^{new} to be the monic polynomial whose roots are the x-coordinates of the affine points of order exactly m.

Proposition 2.10. *For all $m \geq 2$ the polynomials P_m and P_m^{new} lie in $\mathbb{Q}[X]$. Furthermore, $\deg(P_m) = (m^2 + 2 - 3\eta)/2$, where η is the remainder of m modulo 2.*

Proof. For a proof we refer to [29, Exercise III.3.7, pp. 105–106]. □

Note that one obtains different division polynomials for other shapes of elliptic curves (Weierstrass, Montgomery, Edwards, and so on). Nevertheless, the Galois group $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is independent of the model of E, and can be computed with the division polynomials of Definition 2.9 because, 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 to 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 splitting field of f_2. There is a π-torsion point M_1 of E defined over F_2. In F_2, P_π has $(\pi - 1)/2$ trivial roots representing the x coordinates of the multiples of M_1.
3. Let F_3 be the extension of F_2 defined by an irreducible factor of $P_\pi \in F_2[x]$ other than those corresponding to the trivial roots.
4. Let α_2 be a 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 let F_4 be the splitting field of f_4. Then F_4 contains all the π-torsion of E.

The case of prime powers π^k with $k \geq 2$ is handled recursively. Having computed $\mathbb{Q}(E[\pi^{k-1}])$, we obtain $\mathbb{Q}(E[\pi^k])$ by repeating the four steps above with $P_{\pi^k}^{\text{new}}$ instead of P_π and by defining trivial roots to be the x-coordinates of the points $\{P + M_1 \mid P \in E[\pi^{k-1}]\}$.

In practice, we observe that in general P_π, 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, then using the formula $\deg(P_\pi) = (\pi^2 - 1)/2$ from Proposition 2.10, we find that the absolute degree of F_4 is

$$\frac{\pi^2 - 1}{2} \cdot 2 \cdot \frac{\pi^2 - \pi}{2} \cdot 2 = (\pi - 1)^2(\pi + 1)\pi.$$

By Remark 2.4, $\#\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$ is also equal to $(\pi - 1)^2(\pi + 1)\pi$, so in general we expect $\rho_\pi(\mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$. Also, we observed that in general the degree of the extension $\mathbb{Q}(E[\pi^k])/\mathbb{Q}(E[\pi^{k-1}])$ is π^4.

The next theorem shows that the observations above are almost always true. It is a restatement of items (1) and (6) from the introduction of [27].

Theorem 2.11 (Serre). *Let E be an elliptic curve without complex multiplication.*

(1) *For all primes π the sequence of indices*

$$[\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z}) : \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q}))] \quad \textit{for } k \geq 1$$

is nondecreasing 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 2.12. 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 define *Serre's exponent* to be the integer

$$n(E,\pi) = \min\{n \in \mathbb{Z}_{>0} \mid \forall k \geq n : I(E,\pi,k+1) = I(E,\pi,k)\}.$$

In [28] Serre showed that in some cases one can prove that $I(E,\pi,k) = 1$ for all positive integers k. Indeed, Serre proved that the surjectivity of ρ_{π^k} (or the equivalent equality $I(E,\pi,k) = 1$) follows from the surjectivity of ρ_π (or the equivalent equality $I(E,\pi,1) = 1$) for all rational elliptic curves E without complex multiplication and for all primes $\pi \geq 5$. In order to have the same kind of results for $\pi = 2$ (respectively, $\pi = 3$) one has to suppose that ρ_2, ρ_4 and ρ_8 are surjective (respectively, ρ_3 and ρ_9 are surjective).

Serre also conjectured that only a finite number of primes, not depending on the curve E, can occur in the second point of Theorem 2.11. The current conjecture is that for all rational elliptic curves without complex multiplication and all primes $\pi \geq 37$, ρ_π is surjective. Zywina [36] describes an algorithm that computes, for a given E, the primes π for which ρ_π is not surjective; Zywina has checked the conjecture for all elliptic curves in Magma's database (currently this covers curves with conductor at most 140,000). For other recent progress on this conjecture of Serre, see [11] and [10].

Remark 2.13. One application of Serre's results is as follows. Experiments show that if E is an elliptic curve over $\mathbb{Q}$ without complex multiplication, then $E(\mathbb{F}_p)$ is close to a cyclic group for almost all primes p, regardless of the rank of E over $\mathbb{Q}$. For a given bound B, computing

$$\mathsf{P}(\exists \pi > B \mid \mathbb{Z}/\pi\mathbb{Z} \times \mathbb{Z}/\pi\mathbb{Z} \subset E(\mathbb{F}_p)) \tag{1}$$

goes beyond the scope of this paper. However, if π is a prime such that ρ_π is surjective, then Corollary 2.7 shows that

$$\mathsf{P}(\mathbb{Z}/\pi\mathbb{Z} \times \mathbb{Z}/\pi\mathbb{Z} \subset E(\mathbb{F}_p)) = \frac{1}{\pi(\pi+1)(\pi-1)^2}.$$

This suggests that the probability in expression (1) should be $O(1/B^3)$.

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. When this is not the case

we use fixed generators for $E(\overline{\mathbb{Q}})[m]$ to check for each $g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ 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.

A faster probabilistic algorithm for computing $\mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})$ was proposed by Sutherland [31]. This algorithm was not known by the authors at the time of writing and would have helped to accelerate the computation of the examples.

2C. ***Divisibility by a prime power.*** It is well-known that, for a given prime π, the cardinality of a randomly chosen elliptic curve over $\mathbb{F}_p$ has a larger probability of being divisible by π than a randomly chosen integer of size p (see [22, Proposition 1.14, p. 660]). In this subsection we shall consider the analogous problem, where instead of fixing p and varying E, we fix an $E/\mathbb{Q}$ and vary p.

Notation. Let π be a prime and let i, j, and k be nonnegative integers such that $i \le j$. We put

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

Let $\ell \le m$ be integers. When it is defined we write

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

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

Remark 2.14. Since for every integer $m > 0$ and every prime p coprime to m we have $E(\mathbb{F}_p)[m] \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, it follows that $p_{\pi,k}(i,j) = 0$ 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 $(\ell,m) \ne (i,j)$. Finally, for $j = k$, there are only three conditional probabilities which can be nonzero: $p_{\pi,k}(i,k \mid i,k)$, $p_{\pi,k}(i,k+1 \mid i,k)$, and $p_{\pi,k}(k+1,k+1 \mid k,k)$.

Theorem 2.15. *Let π be a prime and E an elliptic curve over $\mathbb{Q}$. If k is an integer such that $I(E,\pi,k+1) = I(E,\pi,k)$ (for example, if E has no complex multiplication and $k \ge n(E,\pi)$), then we have*

$$p_{\pi,k}(k+1,k+1 \mid k,k) = 1/\pi^4,$$
$$p_{\pi,k}(k,k+1 \mid k,k) = (\pi-1)(\pi+1)^2/\pi^4, \quad \textit{and}$$
$$p_{\pi,k}(i,k+1 \mid i,k) = 1/\pi \quad \textit{for } 0 \le i < k.$$

Proof. Let $M = (\mathbb{Z}/\pi^k\mathbb{Z})^2$. For all $g \in \mathrm{GL}_2(\pi M)$, we consider the set

$$\mathrm{Lift}(g) = \big\{h \in \mathrm{GL}_2(M) \;\big|\; h|_{\pi M} = g\big\} = \big\{g + \pi^{k-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \;\big|\; a,b,c,d \in \mathbb{Z}/\pi\mathbb{Z}\big\},$$

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 $1/\pi^4$ by Remark 2.4. So for all $g \in \rho_{\pi^k}(\mathrm{Gal}(\mathbb{Q}(E[\pi^k])/\mathbb{Q}))$, we have $\mathrm{Lift}(g) \subset \rho_{\pi^{k+1}}(\mathrm{Gal}(\mathbb{Q}(E[\pi^{k+1}])/\mathbb{Q}))$. Thanks to Theorem 2.5, the proof will follow if we count for each g the number of lifts with a given fixed group.

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

The element $g = \mathrm{Id}$ can be lifted in exactly $\pi^4 - 1 - \#\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$ ways to an element in $\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z})$ that fixes the π^k-torsion and a point of order π^{k+1}, but not all the π^{k+1}-torsion. Therefore $p_{\pi,k}(k,k+1 \mid k,k) = (\pi-1)(\pi+1)^2/\pi^4$.

Every element of $\mathrm{GL}_2(\mathbb{Z}/\pi^k\mathbb{Z})$ that fixes a line, but is not the identity, can be lifted in exactly π^3 ways to an element of $\mathrm{GL}_2(\mathbb{Z}/\pi^{k+1}\mathbb{Z})$ that fixes a line of $(\mathbb{Z}/\pi^{k+1}\mathbb{Z})^2$. This shows that $p_{\pi,k}(i,k+1 \mid i,k) = \pi^3/\pi^4 = 1/\pi$. □

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. It also gives a formula for the average π-adic valuation $\bar{v}_\pi$ of $\#E(\mathbb{F}_p)$, which we define as

$$\bar{v}_\pi = \sum_{k\geq 1} k\,\mathsf{P}\big(v_\pi(\#E(\mathbb{F}_p)) = k\big),$$

where v_π denotes π-adic valuation. We do not claim that $\bar{v}_\pi$ is equal to

$$\lim_{x\to\infty} \frac{1}{\#\Pi(x)} \sum_{p\leq x} v_\pi(\#E(\mathbb{F}_p)),$$

although we expect this to be true.

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

$$\delta(k) = \begin{cases} p_{i+1}(i+1,i+1) & \text{if } k = 2i+1, \\ 0 & \text{otherwise} \end{cases}$$

and

$$S_k(h) = \pi^k\left(\delta(k) + \sum_{\ell=h}^{\lfloor k/2\rfloor} p_{k-\ell}(\ell,k-\ell)\right).$$

Theorem 2.16. *Let π be a prime, let E an elliptic curve over $\mathbb{Q}$, and let n be a positive integer such that $I(E,\pi,k) = I(E,\pi,n)$ for all $k \geq n$ (for example, a curve without complex multiplication and $n \geq n(E,\pi)$). Then, for every $k \geq 1$,*

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

Furthermore, $\bar{v}_\pi$ is finite, and we have

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

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

$$\mathsf{P}\big(\#E(\mathbb{F}_p) \equiv 0 \bmod \pi^k\big) = \sum_{\ell=0}^{\lfloor k/2 \rfloor} p_{k-\ell}(\ell, k-\ell) + \delta(k). \tag{2}$$

Let $c_1 = 1/\pi^4$, $c_2 = (\pi-1)(\pi+1)^2/\pi^4$, and $c_3 = 1/\pi$. With these notations, the situation 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 $\ell \ge n$, 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 three cases that are to be treated separately: $1 \le k \le n$, $n < k \le 2n$ and $k > 2n$. For $1 \le k \le n$, the result follows from (2). Let us give the computation

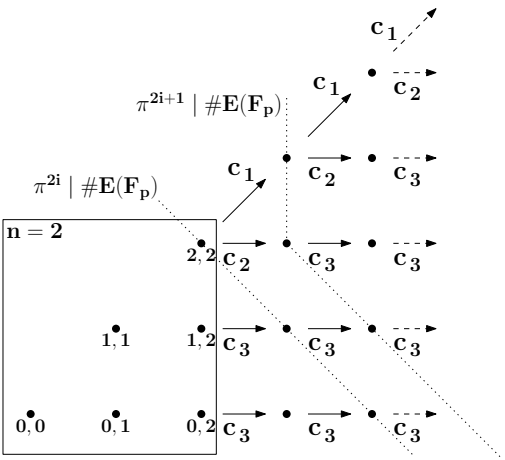

Figure 1. The node with coordinates (i, j) represents the event $\big(E(\mathbb{F}_p)[\pi^j] \simeq \mathbb{Z}/\pi^i\mathbb{Z} \times \mathbb{Z}/\pi^j\mathbb{Z}\big)$. The arrows represent the conditional probabilities of Theorem 2.15.

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

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

This leads to the desired formula. The case $k > 2n$ odd and the case $n < k \le 2n$ are treated similarly.

To prove the statements about $\bar{v}_\pi$, we note that $\mathsf{P}(\#E(\mathbb{F}_p) \equiv 0 \bmod \pi^k)$ is $O(1/\pi^k)$ as $k \to \infty$. Thus, the sum defining $\bar{v}_\pi$ is absolutely convergent, and we are justified in rearranging terms to find

$$\bar{v}_\pi = \sum_{k \ge 1} k\, \mathsf{P}\big(v_\pi(\#E(\mathbb{F}_p)) = k\big) = \sum_{k \ge 1} \mathsf{P}\big(\#E(\mathbb{F}_p) \equiv 0 \bmod \pi^k\big).$$

Substituting in our formulas for the summands in the last expression, we obtain the formula for $\bar{v}_\pi$ given in the theorem. □

Example 2.17. Let us compare the theoretical and experimental average valuation of $\pi = 2$, $\pi = 3$ and $\pi = 5$ for the curves

$$E_1 : \ y^2 = x^3 + 5x + 7 \quad \text{and} \quad E_3 : \ y^2 = x^3 - 10875x + 526250,$$

which do not admit complex multiplication. (We exclude E_2 in this example because it does have complex multiplication.) For E_1, we apply Theorem 2.16 with $n = 1$ and compute the necessary probabilities with Corollary 2.7 knowing that the Galois groups are isomorphic to $\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$. For E_3, we apply Theorem 2.16 with $n = 3$ for $\pi = 2$ and $n = 1$ for $\pi = 3$ and $\pi = 5$, and compute the necessary probabilities with Theorem 2.5 (when $n = 3$) and Corollary 2.7 (when $n = 1$). The results are shown in Table 2.

In order to apply Theorem 2.16, one has to show that $I(E, \pi, k) = I(E, \pi, n)$ for all $k \ge n$ (or $n \ge n(E, \pi)$ since E_1 and E_3 do not have complex multiplication). For E_1, we were able to prove that $n(E, \pi) = 1$ for $\pi = 2$, $\pi = 3$, and $\pi = 5$ by using the remarks at the end of Section 2B. For E_3, Andrew Sutherland computed for us the Galois groups up to the 2^5-, 3^3-, and 5^2-torsion. These computations lead us to believe that $n(E_3, 2) = 3$, $n(E_3, 3) = 1$, and $n(E_3, 5) = 1$, but we have been unable to prove that these values are correct; in particular, this means that the theoretical probabilities for E_3 given in Table 2 are conjectural.

π	$n(E_1,\pi)$	$\overline{v}_{\pi,\text{theor}}$ $\overline{v}_{\pi,\text{exper}}$	$n(E_3,\pi)$	$\overline{v}_{\pi,\text{theor}}$ $\overline{v}_{\pi,\text{exper}}$
2	1	$\frac{14}{9} \approx 1.556$ 1.555	3	$\frac{895}{576} \approx 1.554$ 1.554
3	1	$\frac{87}{128} \approx 0.680$ 0.679	1	$\frac{39}{32} \approx 1.219$ 1.218
5	1	$\frac{695}{2304} \approx 0.302$ 0.301	1	$\frac{155}{192} \approx 0.807$ 0.807

Table 2. Theoretical and experimental values of the average π-adic valuation of $\#E_1(\mathbb{F}_p)$ and $\#E_3(\mathbb{F}_p)$, for $\pi = 2, 3, 5$. The theoretical values come from Theorem 2.16, and the experimental values were computed using all primes less than 2^{25}. The values of $n(E_3,\pi)$ and those of $\overline{v}_{\pi,\text{theor}}$ for E_3 are conjectural.

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 view the imposition of 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.

3A. ***Preliminaries on Montgomery and twisted Edwards curves.*** Let K be a field whose characteristic is neither 2 nor 3.

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 [8] completed twisted Edwards curves are defined by

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

The completed points are the affine (x, y) embedded into $\mathbb{P}^1 \times \mathbb{P}^1$ by the map $(x, y) \mapsto ((x:1),(y:1))$; see [8] for more information. We denote $(1:0)$ by ∞.

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

Montgomery curves and the Suyama family. Take $A, B \in K$ with $B(A^2-4) \neq 0$. The Montgomery curve $By^2 = x^3 + Ax^2 + x$ associated to (A, B) is denoted by $M_{A,B}$ (see [23]) 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 $d = (A-2)/B$ and $a = (A+2)/B$, then there is a birational map between $\overline{E}_{a,d}$ and $\overline{M}_{A,B}$ given by

$$\big((x:z),(y:t)\big) \mapsto \big((t+y)x : (t+y)z : (t-y)x\big)$$

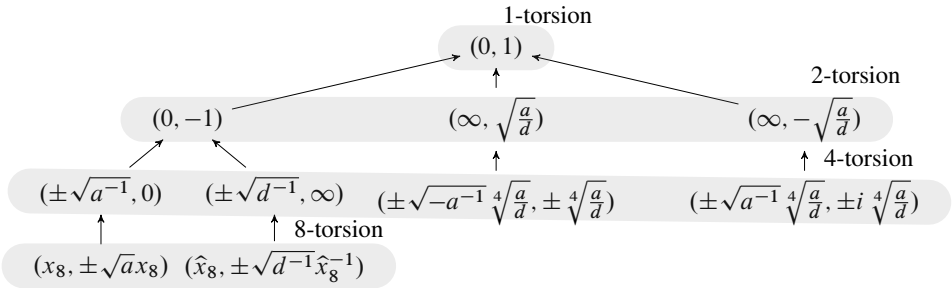

Figure 2. An overview of all 1-, 2-, and 4-torsion and some 8-torsion points on twisted Edwards curves. The x_8 and $\hat{x}_8$ in the 8-torsion points are such that $adx_8^4 - 2ax_8^2 + 1 = 0$ and $ad\hat{x}_8^4 - 2d\hat{x}_8^2 + 1 = 0$.

(see [6]). Therefore $\overline{M}_{A,B}$ and $\overline{E}_{a,d}$ have the same group structure over any field where they are both defined, and in particular they have 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

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

is called a Suyama curve. As described in [32; 34], the solutions of (3) can be parametrized by a rational value denoted σ. For all $\sigma \in \mathbb{Q}\setminus\{0, \pm 1, \pm 3, \pm 5, \pm\frac{5}{3}\}$, the associated Suyama curve has positive rank and a rational point of order 3.

Remark 3.2. In the following, when we say that a twisted Edwards curve $E_{a,d}$ (or a Montgomery curve $M_{A,B}$) has good reduction modulo a prime p, we also suppose that we have $v_p(a) = v_p(d) = v_p(a-d) = 0$ (respectively, $v_p(A-2) = v_p(A+2) = v_p(B) = 0$ 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.

3B. ***The generic Galois group of a family of curves.*** In the following, when we talk about the *Galois group of the m-torsion of a family of curves*, we mean a group isomorphic to the Galois group of the m-torsion for all curves of the family except for a sparse set of curves (which can have a smaller Galois group).

For example, let us consider the Galois group of the 2-torsion for the family $\{\mathscr{E}_r : y^2 = x^3 + rx^2 + x \mid r \in \mathbb{Q} \setminus \{\pm 2\}\}$. The Galois group of the 2-torsion of the curve $\mathscr{E} : y^2 = x^3 + Ax^2 + x$ over $\mathbb{Q}(A)$ is $\mathbb{Z}/2\mathbb{Z}$. Hence, for most values of r the Galois group is $\mathbb{Z}/2\mathbb{Z}$ and for a sparse set of values the Galois group is the trivial group. So, we say that the Galois group of the 2-torsion of this family is $\mathbb{Z}/2\mathbb{Z}$.

To our best knowledge, there is no implementation of an algorithm computing Galois groups of polynomials with coefficients in a function field. Instead we can compute the Galois group for every curve of the family, so we can guess the Galois group of the family from a finite number of instantiations. In practice, we took a dozen random curves in the family; if the Galois groups of the m-torsion for these curves were all the same, we guessed that it was the Galois group of the m-torsion of the family of curves.

3C. ***Study of the 2^k-torsion of Montgomery and 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 [32]. The following theorem gives more detail on the 2^k-torsion.

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

(1) *Suppose $p \equiv 3 \pmod 4$. If a/d (respectively, $A^2 - 4$) 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) *Suppose $p \equiv 1 \pmod 4$. If a (respectively, $(A+2)/B$) is a quadratic residue modulo p (in particular, if $a = \pm 1$) and a/d (respectively, $A^2 - 4$) 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) *Suppose $p \equiv 1 \pmod 4$. If a/d (respectively, $A^2 - 4$) is a quadratic nonresidue modulo p and $a - d$ (respectively, 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 a/d is a square has been studied in [8] for the family of Edwards curves with $a = 1$ and rational torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, and in [7] for the family with $a = -1$ and rational torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Here we focus on two other equations:

$$\exists c \in \mathbb{Q},\ a = -c^2 \qquad (A + 2 = -Bc^2 \text{ for Montgomery curves}), \tag{4}$$

$$\exists c \in \mathbb{Q},\ a - d = c^2 \qquad (B = c^2 \text{ for Montgomery curves}). \tag{5}$$

The cardinality of the Galois group of the 4-torsion for generic Montgomery curves is 16; this is reduced to 8 for the family of curves satisfying (4). Using Theorem 2.5, we can compute the changes of probabilities due to this new Galois group. For all curves satisfying (4) 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 (5) has cardinality 128, instead of 256 for generic Montgomery curves. Using Theorem 2.5, one can see that the probabilities of having an 8-torsion point are improved.

Using Theorem 2.16, one can show that for both families of curves — the family satisfying (4) and the one satisfying (5) — the probability that the cardinality is divisible by 8 increases from $\frac{5}{8}$ to $\frac{3}{4}$, and the average valuation of 2 increase from $\frac{10}{3}$ to $\frac{11}{3}$.

3D. ***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; by doing so, we hope 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 [7]). The technique might be used in any context.

Looking for subfamilies. For a generic d, the polynomial 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.

In all these families the generic average valuation of 2 is increased by $\frac{1}{6}$ — rising from $\frac{14}{3}$ up to $\frac{29}{6}$ — except for the family $e = (g - g^{-1})/2$, 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 [7, 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.

The family $e = (g - g^{-1})/2$. In this section, we study in more detail the family $e = (g - g^{-1})/2$. Using Theorem 2.5 one can prove that the group order modulo all primes is divisible by 16. However, we give an alternative proof which is also of independent interest. We need the following theorem which computes the 8-torsion points that double to the 4-torsion points $(\pm\sqrt[4]{-d^{-1}}, \pm\sqrt[4]{-d^{-1}})$.

Special form of e	Degrees of factors of $P_{8,0}$	$P_{8,1}$	$P_{8,2}$	Avg. 2-adic val. over p that are 1 mod 4	3 mod 4	all p
none	4	4	8	16/3	4	14/3
g^2	4	4	4, 4	17/3	4	29/6
$(2g^2+2g+1)/(2g+1)$	4	4	4, 4	17/3	4	29/6
$g^2/2$	2, 2	4	8	17/3	4	29/6
$(g-g^{-1})/2$	2, 2	2, 2	8	17/3	5	16/3

Table 3. Averages, over different subsets of primes, of the 2-adic valuation of $\#E(\mathbb{F}_p)$, for E in one of several subfamilies of twisted Edwards curves E_d with torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The subfamilies all have $d = -e^4$, where e is further specialized according to the entries in the first column. The second through fourth columns give the degrees of the factors of the polynomials $P_{8,i}$ defined in the article. The fifth through seventh columns give the average 2-adic valuation of $\#E(\mathbb{F}_p)$ as p ranges through primes that are 1 modulo 4, primes that are 3 modulo 4, and all primes, respectively.

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

$$y = \pm\sqrt{\frac{4tg^{2-w}}{(g-tw)^3(g+tw)}} \quad \text{and} \quad x = \pm g^w y \tag{6}$$

have order 8, and double to $(\pm e^{-1}, te^{-1})$.

Proof. For all points (x, y) of order 8, neither x nor y is equal to 0 or ∞. Following Theorem 2.10 of [8] we find that a point (x, y) doubles to

$$\begin{aligned}\big((2xy : 1+dx^2y^2), (x^2+y^2 : 1-dx^2y^2)\big)\\ = \big((2xy : -x^2+y^2), (x^2+y^2 : 2-(-x^2+y^2))\big).\end{aligned}$$

Let $s, t \in \{1, -1\}$ be such that (x, y) doubles to (se^{-1}, te^{-1}). Then

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

From the first equality we obtain $(x/y)^2 + 2esx/y + e^2 = 1 + e^2$. Write $e = (g - g^{-1})/2$, so that we obtain $(x/y + se)^2 = ((g + g^{-1})/2)^2$. It follows that $x/y \in \{\pm g, \pm 1/g\}$, 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 equality we obtain $(e-t)x^2 + (e+t)y^2 = 2t$, and substituting $x^2 = G^2y^2$ results in $((e-t)G^2 + (e+t))y^2 = 2t$. This can be solved for y

when $2t((e-t)G^2+(e+t))$ is a quadratic residue modulo p. This is equivalent to checking if either of

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

$$2t\big((e-1)+(e+1)g^2\big) = \frac{t(g-1)(g+1)^3}{g} \tag{8}$$

is a quadratic residue modulo p. By assumption, $tg(g-1)(g+1)$ is a quadratic residue modulo p. Hence, expressions (7) and (8) are both quadratic residues modulo p. Solving for y and keeping track of all the signs results in the formulas in (6). □

Corollary 3.5. *Let $E = E_d$ be a twisted Edwards curve over $\mathbb{Q}$ such that $d = -((g-g^{-1})/2)^4$ for some $g \in \mathbb{Q} \setminus \{-1,0,1\}$, and let $p > 3$ be 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. The proof depends on the congruence class of p modulo 4.

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 $16 \mid \#E(\mathbb{F}_p)$.

If $p \equiv 3 \pmod 4$ then -1 is a quadratic nonresidue modulo p. Then exactly one of $\{g(g-1)(g+1), -g(g-1)(g+1)\}$ is a quadratic residue modulo p. Using Theorem 3.4 it follows that the curve $E(\mathbb{F}_p)$ has rational points of order 8, and hence $16 \mid \#E(\mathbb{F}_p)$. □

Corollary 3.5 explains the good behavior of the curve with $d = -\left(\frac{77}{36}\right)^4$ and torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ found in [7]. This parameter can be expressed as $d = -\left(\frac{77}{36}\right)^4 = -((g-g^{-1})/2)^4$ for $g = \frac{9}{2}$ and, therefore, the group order is divisible by an additional factor of 2.

Corollary 3.6. *Let $g \in \mathbb{Q} \setminus \{-1,0,1\}$, let $d = -((g-g^{-1})/2)^4$, and let $p \equiv 1 \pmod 4$ be a prime of good reduction for the curve E_d. 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 of the 4-torsion points are in $E_d(\mathbb{F}_p)$ (see Figure 2). By Theorem 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 $1 \le i < j \le 200$ such that $\gcd(i,j) = 1$. This resulted in 12,231 possible values for g, and Sage [30] found 614 nontorsion points. As expected, we observed that they behave similarly to the good curve found in [7].

Parametrization. In [7] a "generating curve" is specified which parametrizes d and the coordinates of the nontorsion points. Arithmetic on this generating 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 with a nontorsion point. Using ideas from [13] we found a parametrization that does not involve a generating curve, and hence requires no curve arithmetic.

Theorem 3.7. *Let $t \in \mathbb{Q} \setminus \{0, \pm 1, \pm 3, \pm 1/3\}$ and set*

$$e = \frac{3(t^2-1)}{8t}, \quad d = -e^4, \quad x_\infty = \frac{1}{4e^3+3e}, \quad y_\infty = \frac{9t^4-2t^2+9}{9t^4-9}.$$

Then the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and (x_∞, y_∞) is a nontorsion point.

Proof. Since $t \neq 0$ and $t \neq \pm 1$, we see that e, d, x_∞ and y_∞ are nonzero rationals; further, $e \neq \pm 1$ because $t \neq \pm 3$ and $t \neq \pm 1/3$, so $d \neq -1$. Thus, the twisted Edwards curves E_d is nonsingular, and its torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ because $d = -e^4$. A calculation shows that the point (x_∞, y_∞) is on the curve; it is a nontorsion point because $x_\infty \notin \{0, \infty, e^{-1}, -e^{-1}\}$. □

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 nontorsion point on the rank-1 elliptic curve $y^2 = x^3 - 36x$ over $\mathbb{Q}$. Let $t = (x+6)/(x-6)$ and let e be as in Theorem 3.7. Then the curve E_{-e^4} belongs to the family $e = g^2$ and has positive rank over $\mathbb{Q}$.*

3E. ***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.

Suyama-11. Kruppa observed in [19] that among the Suyama curves, the one corresponding to $\sigma = 11$ finds exceptionally many primes. Barbulescu [5] extended this single example to an infinite family which 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 group when reduced modulo primes $p \equiv 1 \pmod 4$. The reason is that the $\sigma = 11$ curve satisfies (4). Section 3C illustrates the changes in probabilities of the $\sigma = 11$ curve when compared to curves which do not satisfy (4) and shows that (4) improves the average valuation of 2 from $\frac{10}{3}$ to $\frac{11}{3}$.

We will refer to the set of Suyama curves that satisfy (4) as *Suyama*-11. When solving the system formed by Suyama's system plus (4), we obtain an elliptic

parametrization for σ. Given a point (u, v) on the curve

$$E_{\sigma_{11}}: \ v^2 = u^3 - u^2 - 120u + 432,$$

the associated σ is obtained as $\sigma = 5 + 120/(u - 24)$. 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 invalid 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 $(44, 280) = P_\infty + P_2$.

Edwards $\mathbb{Z}/6\mathbb{Z}$: Suyama-11 in disguise. In [7, §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

$$d = -\frac{16u^3(u^2 - u + 1)}{(u - 1)^6(u + 1)^2} \tag{9}$$

where u is a rational parameter.[1] In particular, according to [7, §5.3] one can translate any Suyama curve into Edwards language and then impose the condition that $-a$ is a square to obtain curves of the $a = -1$ type. Finally, [7, §5.5] points out that this family has exceptional torsion properties.

In order to understand the properties of this family, we translate it back into Montgomery language using Remark 3.1. Thus, we are interested in Suyama curves that satisfy the 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 on page 81. These two families have been discovered independently in [5] and [7].

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 exclusively concern primes $p \equiv 1 \pmod 4$. Indeed, the $\sigma = \frac{9}{4}$ curve with satisfies (5). Section 3C illustrates the changes in probabilities of that curve when compared to curves which do not satisfy (5), and shows that (5) improves the average valuation of 2 from $\frac{10}{3}$ to $\frac{11}{3}$.

We refer to the set of Suyama curves satisfying (5) as *Suyama-$\frac{9}{4}$*. When solving the system formed by Suyama's system together with (5), we obtain an elliptic parametrization for σ. Given a point (u, v) on the curve

$$E_{\sigma_{9/4}}: \ v^2 = u^3 - 5u,$$

the associated σ is obtained as $\sigma = u$. The group $E_{\sigma_{9/4}}(\mathbb{Q})$ is generated by the points $P_\infty = (-1, 2)$ and $P_2 = (0, 0)$ of orders ∞ and 2, respectively. We exclude

[1] In the proof of [7, Theorem 5.1], the fraction corresponding to (9) is missing a minus sign.

the points $0, \pm P_\infty$, P_2, and $P_2 \pm P_\infty$, which produce invalid values of σ. If two points in $E_{\sigma_{9/4}}(\mathbb{Q})$ differ by P_2 they correspond to isomorphic curves. The curve associated to $\sigma = \frac{9}{4}$ is obtained from the point $\left(\frac{9}{4}, -\frac{3}{8}\right) = [2]P_\infty$.

3F. ***Comparison.*** Table 4 gives a summary of all the families discussed in this article. The theoretical average valuations were computed with Theorem 2.16, Theorem 2.5, and Corollary 2.7, under some assumptions on Serre's exponent (see Example 2.17 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.

Family	Curve	n_2	$\overline{v}_{2,\text{theor}}$ $\overline{v}_{2,\text{exper}}$	n_3	$\overline{v}_{3,\text{theor}}$ $\overline{v}_{3,\text{exper}}$
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	$\frac{11}{3} \approx 3.667$ 3.369	1	$\frac{27}{16} \approx 1.688$ 1.687
Suyama-$\frac{9}{4}$	$\sigma = \frac{9}{4}$	3	$\frac{11}{3} \approx 3.667$ 3.364	1	$\frac{27}{16} \approx 1.688$ 1.687
$\mathbb{Z}/2 \times \mathbb{Z}/4\mathbb{Z}$ (Twisted Edwards E_{-e^4})	$e = 11$	3	$\frac{14}{3} \approx 4.667$ 4.666	1*	$\frac{87}{128} \approx 0.680$ 0.679
$e = (g - g^{-1})/2$	$g = \frac{9}{2}$	3	$\frac{16}{3} \approx 5.333$ 5.332	1*	$\frac{87}{128} \approx 0.680$ 0.679
$e = g^2$	$g = 3$	3	$\frac{29}{6} \approx 4.833$ 4.833	1*	$\frac{87}{128} \approx 0.680$ 0.680
$e = g^2/2$	$g = \frac{9}{2}$	3	$\frac{29}{6} \approx 4.833$ 4.831	1*	$\frac{87}{128} \approx 0.680$ 0.679
$e = \frac{2g^2+2g+1}{2g+1}$	$g = 1$	3	$\frac{29}{6} \approx 4.833$ 4.833	1*	$\frac{87}{128} \approx 0.680$ 0.679

Table 4. Theoretical and experimental values of $\overline{v}_2$ and $\overline{v}_3$ for sample curves from the families discussed in this paper. The theoretical values come from Theorem 2.16, and the experimental values were computed using all primes less than 2^{25}. The columns labeled n_2 and n_3 give the values of $n(E, 2)$ and $n(E, 3)$. The notation $n = 1^*$ means that the Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/\pi\mathbb{Z})$.

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 some questions which were not addressed in this work:

- How does Serre's work relate to the independence of the m- and m'-torsion probabilities for coprime integers m and m'?
- Is there a model predicting the success probability of ECM from the probabilities given in Theorem 2.16?
- Is it possible to effectively use the resolvent method [14] in order to compute equations which improve the torsion properties?

Acknowledgments

We thank Andrew Sutherland for bringing the article of Zywina [36] to our attention. We are also indebted to Everett Howe and Kiran Kedlaya for their editing effort and for the corrections they brought to this paper. This work was supported by the Swiss National Science Foundation under grant number 200020-132160 and by a PHC Germaine de Staël grant.

References

[1] Michel Abdalla and Paulo S. L. M. Barreto (eds.), *Progress in cryptology — LATINCRYPT 2010: Proceedings of the 1st International Conference on Cryptology and Information Security in Latin America held in Puebla, August 8–11, 2010*, Lecture Notes in Computer Science, no. 6212, Berlin, Springer, 2010.

[2] Elisardo Antelo, David Hough, and Paolo Ienne (eds.), *Proceedings of the 20th IEEE Symposium on Computer Arithmetic: ARITH-20*, Los Alamitos, CA, Institute of Electrical and Electronics Engineers, IEEE Computer Society, 2011.

[3] A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), no. 201, 399–405. MR 93k:11115

[4] Shi Bai, Pierrick Gaudry, Alexander Kruppa, François Morain, Emmanuel Thomé, and Paul Zimmermann, *Crible algébrique: Distribution, optimisation — number field sieve (CADO-NFS)*. http://cado-nfs.gforge.inria.fr/

[5] Razvan Barbulescu, *Familles de courbes adaptées à la factorisation des entiers*, research report 00419218, version 2, INRIA, 2009. http://hal.inria.fr/inria-00419218/en/

[6] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards curves*, in Vaudenay [33], 2008, pp. 389–405. MR 2010e:11057

[7] Daniel J. Bernstein, Peter Birkner, and Tanja Lange, *Starfish on strike*, in Abdalla and Barreto [1], 2010, pp. 61–80.

[8] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *ECM using Edwards curves*, Cryptology ePrint Archive, report 2008/016, 2008. http://eprint.iacr.org/2008/016

[9] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, in Kurosawa [20], 2007, pp. 29–50. MR 2011d:11125

[10] Yu. Bilu, P. Parent, and M. Rebolledo, *Rational points on* $X_0^+(p^r)$, 2011. arXiv 1104.4641 [math.NT]

[11] Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584. MR 2012a:11077

[12] J. W. Bos, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery, *Efficient SIMD arithmetic modulo a Mersenne number*, in Antelo et al. [2], 2011, pp. 213–221.

[13] Éric Brier and Christophe Clavier, *New families of ECM curves for Cunningham numbers*, in Hanrot et al. [16], 2010, pp. 96–109. MR 2011m:11243

[14] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, Berlin, 1993. MR 94i:11105

[15] Harold M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 3, 393–422. MR 2008b:14052

[16] Guillaume Hanrot, François Morain, and Emmanuel Thomé (eds.), *Algorithmic number theory: Proceedings of the 9th Biennial International Symposium (ANTS-IX) held in Nancy, July 19–23, 2010*, Lecture Notes in Computer Science, no. 6197, Berlin, Springer, 2010. MR 2011g:11002

[17] Florian Hess, Sebastian Pauli, and Michael Pohst (eds.), *Algorithmic number theory: Proceedings of the 7th International Symposium (ANTS-VII) held at the Technische Universität Berlin, Berlin, July 23–28, 2006*, Lecture Notes in Computer Science, no. 4076, Berlin, Springer, 2006. MR 2007h:11001

[18] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson, *Twisted Edwards curves revisited*, in Pieprzyk [25], 2008, pp. 326–343. MR 2546103

[19] Alexander Kruppa, *Speeding up integer multiplication and factorization*, Ph.D. thesis, Université Henri Poincaré — Nancy I, 2010. http://tel.archives-ouvertes.fr/tel-00477005/en/

[20] Kaoru Kurosawa (ed.), *Advances in cryptology — ASIACRYPT 2007: Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security held in Kuching, December 2–6, 2007*, Lecture Notes in Computer Science, no. 4833, Berlin, Springer, 2007. MR 2010i:94001

[21] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The development of the number field sieve*, Lecture Notes in Mathematics, no. 1554, Springer, Berlin, 1993. MR 96m:11116

[22] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673. MR 89g:11125

[23] Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243–264. MR 88e:11130

[24] Jürgen Neukirch, *Class field theory*, Grundlehren der mathematischen Wissenschaften, no. 280, Springer, Berlin, 1986. MR 87i:11005

[25] Josef Pieprzyk (ed.), *Advances in cryptology — ASIACRYPT 2008: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security held in Melbourne, December 7–11, 2008*, Lecture Notes in Computer Science, no. 5350, Berlin, Springer, 2008. MR 2010j:94005

[26] J. M. Pollard, *The lattice sieve*, in Lenstra and Lenstra [21], 1993, pp. 43–49. MR 1321220

[27] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 52 #8126

[28] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 83k:12011

[29] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, no. 106, Springer, Dordrecht, 2009. MR 2010i:11005

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

[31] Andrew Sutherland, *Computing the image of Galois*, presentation at the 12th meeting of the Canadian Number Theory Association held in Lethbridge, June 17–22, 2012. http://math.mit.edu/~drew/CNTA12.pdf

[32] Hiromi Suyama, *Informal preliminary report* (8), personal communication to Richard Brent, 1985.

[33] Serge Vaudenay (ed.), *Progress in cryptology—AFRICACRYPT 2008: Proceedings of the 1st International Conference on Cryptology in Africa held in Casablanca, June 11–14, 2008*, Lecture Notes in Computer Science, no. 5023, Berlin, Springer, 2008. MR 2009m:94064

[34] Paul Zimmermann and Bruce Dodson, *20 years of ECM*, in Hess et al. [17], 2006, pp. 525–542. MR 2007j:11172

[35] Paul Zimmermann et al., *GMP-ECM (Elliptic curve method for integer factorization)*, 2010. https://gforge.inria.fr/projects/ecm/

[36] David Zywina, *On the surjectivity of mod ℓ representations associated to elliptic curves*, preprint, 2011. http://www.mast.queensu.ca/~zywina/papers/EffectiveModl.pdf

RAZVAN BARBULESCU: razvan.barbulescu@inria.fr
Université de Lorraine, LORIA - Bât. A, Équipe CARAMEL, Campus Scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy, France

JOPPE W. BOS: jbos@microsoft.com
Microsoft Research, One Microsoft Way, Redmond, WA 98052, United States

CYRIL BOUVIER: cyril.bouvier@inria.fr
ENS Paris and Université de Lorraine, LORIA - Bât. A, Équipe CARAMEL, Campus Scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy, France

THORSTEN KLEINJUNG: thorsten.kleinjung@epfl.ch
EPFL, Laboratory for Cryptologic Algorithms, CH-1015 Lausanne, Switzerland

PETER L. MONTGOMERY: pmontgom@math.ucla.edu
Microsoft Research, One Microsoft Way, Redmond, WA 98052, United States

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS