Finding ECM-friendly curves through a study of Galois properties

10th Algorithmic Number Theory Symposium

Razvan Barbulescu[1] Joppe W. Bos[3] **Cyril Bouvier**[1]
Thorsten Kleinjung[2] Peter L. Montgomery[3]

1. Université de Lorraine, CNRS, INRIA, France
2. Laboratory for Cryptologic Algorithms, EPFL, Lausanne, Switzerland
3. Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA

July 9-13, 2012

Motivations

D. Bernstein, P. Birkner, T. Lange, *Starfish on Strike*.

> *This improvement is not merely a matter of luck: in particular, the interesting curve* $-x^2 + y^2 = 1 - (\frac{77}{36})^4 x^2 y^2$*, with torsion group* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*, easily outperforms the other 999 curves.*

A. Kruppa, *Speeding up Integer Multiplication and Factorization*.

> *...the choice* $\sigma = 11$*, which surprisingly leads to a higher average exponent of* 2 *in the group order.*

D. Bernstein, P. Birkner, T. Lange, C. Peters, *ECM using Edwards curves*.

> *We performed an analogous computation using Edwards curves with torsion group* $\mathbb{Z}/12\mathbb{Z}$ *and found an even closer match to* $\frac{11}{3}$ *and* $\frac{5}{3}$ *[for the average exponents of* 2 *and* 3*]. For Suyama curves with torsion group* $\mathbb{Z}/6\mathbb{Z}$ *the averages were only* $\frac{10}{3}$ *and* $\frac{5}{3}$*, except for a few unusual curves such as* $\sigma = 11$*.*

Goals

- Having theoretical tools to study the torsion properties of every elliptic curve.
- Being able to compare the theoretical torsion properties of two given elliptic curves and explaining the behaviour of exceptionally good curves.
- Finding good families of elliptic curves for the Elliptic Curve Method (ECM) for integer factorization.

Forms of Elliptic Curves and Subfamilies

In this talk, elliptic curves will mainly be in one of these two forms:

- Twisted Edwards curves: for $a, d \in \mathbb{Q}$ such that $ad(a-d) \neq 0$,

$$ax^2 + y^2 = 1 + dx^2y^2$$

- Montgomery curves: for $A, B \in \mathbb{Q}$ such that $B(A^2 - 4) \neq 0$,

$$By^2 = x^3 + Ax^2 + x$$

Among these curves, we will focus on three subfamilies:

- Suyama family: rational parametrization of Montgomery curves with a 3-torsion point. The parameter is called σ.
- "$a = -1$" twisted Edwards curves with rational torsion $\mathbb{Z}/6\mathbb{Z}$: it a translation of Suyama family with the additional condition $a = -1$.
- "$a = -1$" twisted Edwards curves with rational torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$: these curves are exactly the ones with $d = -e^4$ and $a = -1$.

Plan

1. Torsion properties of elliptic curves
   - Probability and torsion subgroup
   - Probability, cardinality and average valuation
2. Application
   - Twisted Edwards curves with rational torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
   - Montgomery curves with Suyama parametrization

Some notations

Let E be an elliptic curve over $\mathbb{Q}$, K be a field, and let m be a positive integer.

Definition

- $E(K)[m]$ is the group of m-torsion points of E defined over K.
- $E(\overline{\mathbb{Q}})[m]$ is often denoted by $E[m]$.
- $\mathbb{Q}(E[m])$ is the smallest extension of $\mathbb{Q}$ containing all the m-torsion of E.

Properties

- $\mathbb{Q}(E[m])/\mathbb{Q}$ *is a Galois extension*
- *There exists an* ***injective*** *morphism, denoted by* ρ_m, *from* $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ *to* $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

ρ_m is unique up to a choice of generators of $E[m]$.

Probability and Torsion Subgroup

Definition

$$\mathbb{P}(\mathcal{A}(p)) = \lim_{B\to\infty} \frac{\#\{p \leq B \text{ prime such that } \mathcal{A} \text{ is true}\}}{\#\{p \leq B \text{ prime}\}}$$

Theorem (Part 1)

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,

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

Proof: use Chebotarev's theorem.

Example 1

$$E_1 : y^2 = x^3 + 5x + 7 \qquad E_2 : y^2 = x^3 - 11x + 14$$

		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.	$\frac{1}{48} \approx 0.02083$	$\frac{1}{16} = 0.06250$
	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

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

Probability and Torsion Subgroup

Theorem (Part 2)

Previously: E is an elliptic curve over $\mathbb{Q}$ and $m \geq 2$ is an integer. T is a subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. $K = \mathbb{Q}(E[m])$.
Let a and n be coprime positive integers, 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:

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

Remark: If $[K(\zeta_n) : \mathbb{Q}(\zeta_n)] = [K : \mathbb{Q}]$, then,

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

Note that for $n \in \{3, 4\}$ the condition is equivalent to $\zeta_n \notin K$.

Example 2

	$\sigma = 10$	$\sigma = 11$
$\# \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$	96	
$\# \mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$	16	8
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/4\mathbb{Z})$	$\frac{1}{2}$	$\frac{1}{2}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$	$\frac{1}{8}$	0
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$	$\frac{5}{16}$	$\frac{3}{8}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$	$\frac{1}{16}$	$\frac{1}{8}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/4\mathbb{Z} \mid p \equiv 3 \bmod 4)$	$\frac{1}{2}$	$\frac{1}{2}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \mid p \equiv 3 \bmod 4)$	$\frac{1}{2}$	$\frac{1}{2}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/4\mathbb{Z} \mid p \equiv 1 \bmod 4)$	$\frac{1}{2}$	$\frac{1}{2}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \mid p \equiv 1 \bmod 4)$	$\frac{1}{4}$	0
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \mid p \equiv 1 \bmod 4)$	$\frac{1}{8}$	$\frac{1}{4}$
$\mathbb{P}(E(\mathbb{F}_p)[4] \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \mid p \equiv 1 \bmod 4)$	$\frac{1}{8}$	$\frac{1}{4}$

When checked against experimental values (with all primes below 2^{25}) the relative difference never exceeds 0.2%.

Probability, Cardinality and Average Valuation

Let π be a prime, E an elliptic curve over $\mathbb{Q}$.

Definition

Let i, j, k be non-negative integers such that $i \leq j$. Define:

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

Theorem

Let n be a positive integer such that everything is "generic" for the π^i-torsion, for $i > n$.
Then, for any $k \geq 1$, $\mathbb{P}(\pi^k \mid \#E(\mathbb{F}_p))$ can be expressed as ***polynomials*** *in $p_{\pi,j}(i,j)$, for $0 \leq i \leq j \leq n$.*
The average valuation of π can also be expressed as a polynomial in $p_{\pi,j}(i,j)$, for $0 \leq i \leq j \leq n$,

Cf. article for detailed hypothesis and exact formulae.

Example 3

$E_1 : y^2 = x^3 + 5x + 7 \qquad E_2 : y^2 = x^3 - 11x + 14$

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

Comparison of the theoretical values (Th.) of previous Theorem to the experimental results for all primes below 2^{25} (Exp.).

*320 hours of computation with Magma

Example 4

		$\sigma = 10$	$\sigma = 11$
n		2	2
$\mathbb{P}(2^3 \mid \#E(\mathbb{F}_p))$		$\frac{5}{8}$	$\frac{3}{4}$
$\mathbb{P}(2^3 \mid \#E(\mathbb{F}_p))$ for $p \equiv 1 \bmod 4$		$\frac{1}{2}$	$\frac{3}{4}$
$\mathbb{P}(2^3 \mid \#E(\mathbb{F}_p))$ for $p \equiv 3 \bmod 4$		$\frac{3}{4}$	$\frac{3}{4}$
Average valuation of 2	Th.	$\frac{10}{3} \approx 3.333$	$\frac{11}{3} \approx 3.667$
	Exp.	3.332	3.669
Average valuation of 2 for $p \equiv 1 \bmod 4$	Th.	$\frac{19}{6} \approx 3.167$	$\frac{23}{6} \approx 3.833$
	Exp.	3.164	3.835
Average valuation of 2 for $p \equiv 3 \bmod 4$	Th.	$\frac{7}{2} = 3.5$	$\frac{7}{2} = 3.5$
	Exp.	3.500	3.503
n		1	1
Average valuation of 3	Th.	$\frac{27}{16} \approx 1.688$	$\frac{27}{16} \approx 1.688$
	Exp.	1.687	1.687

Comparison between the two Suyama curves with $\sigma = 10$ and $\sigma = 11$.

Plan

1. Torsion properties of elliptic curves
   - Probability and torsion subgroup
   - Probability, cardinality and average valuation
2. Application
   - Twisted Edwards curves with rational torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
   - Montgomery curves with Suyama parametrization

Division Polynomial and Galois Group

Definition

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.

- The division polynomial P_m is used to compute $\mathbb{Q}(E[m])$ and so is linked with the computation of the divisibility probabilities.
- Adding some equations in order to split a division polynomial, thus modifying the Galois group, may improve the divisibility probabilities. The next example will illustrate this method.

Twisted Edwards Curves with Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$$\begin{aligned} P_8^{\text{new}} &= (x^{16} + \cdots)(x^4 + \cdots)(x^4 + \cdots) && \text{twisted Edwards curves} \\ &= P_{8,0} P_{8,1} P_{8,2} (x^4 + \cdots)(x^4 + \cdots) && d = -e^4 \end{aligned}$$

$e =$	"generic"	g^2	$\frac{2g^2+2g+1}{2g+1}$	$\frac{g^2}{2}$	$\frac{g-\frac{1}{g}}{2}$
degree of factors of $P_{8,0}$	4	4	4	2, 2	2, 2
degree of factors of $P_{8,1}$	4	4	4	4	2, 2
degree of factors of $P_{8,2}$	8	4, 4	4, 4	8	8
average valuation of 2	$\frac{14}{3}$	$\frac{29}{6}$	$\frac{29}{6}$	$\frac{29}{6}$	$\frac{16}{3}$
for $p = 3 \bmod 4$	4	4	4	4	5
for $p = 1 \bmod 4$	$\frac{16}{3}$	$\frac{17}{3}$	$\frac{17}{3}$	$\frac{17}{3}$	$\frac{17}{3}$

These four families cover all the good curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$-torsion found in "Starfish on strike" †, except two curves. The "interesting curve" with $e = \frac{77}{36}$ belongs to the best subfamily (rightmost column).

† D. Bernstein, P. Birkner, T. Lange, *Starfish on Strike*. Table 3.1.

Twisted Edward Curves: new parametrization

- Only an elliptic parametrization was known for twisted Edwards curves with rational $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$-torsion and a rational non-torsion point. Using ideas from Brier and Clavier [‡], we found a parametrization which does not involve a generating curve.
- This rational parametrization allowed us to impose additional conditions on the parameter e.
- For $e = g^2$, the parameter e is given by an elliptic curve of rank 1 over $\mathbb{Q}$. For the three others families, the parameter e is given by an elliptic curve of rank 0 over $\mathbb{Q}$.

[‡] E. Brier, C. Clavier, *New families of ECM curves for Cunningham numbers.*

Suyama-11 Subfamily

- Suyama-11 is the set of Suyama curves which verify: $\exists c \in \mathbb{Q}$ such that $A + 2 = -Bc^2$. The Suyama curve with $\sigma = 11$ belongs to this subfamily. This new equation does not affect division polynomials but modifies directly the 4-torsion Galois group.
- The Suyama curve with $\sigma = \frac{9}{4}$ is also special among Suyama curves and can be extended to a family, called Suyama-$\frac{9}{4}$. Suyama-$\frac{9}{4}$ curves have the same division polynomials as Suyama curves but have a different 8-torsion Galois group.
- Both families can be parametrized by an elliptic curve of rank 1 over $\mathbb{Q}$.

Suyama-11 and Twisted Edwards Curves with torsion $\mathbb{Z}/6\mathbb{Z}$

- In "Starfish on strike", the authors point out the good torsion properties of the "$a = -1$" twisted Edwards curve family with rational $\mathbb{Z}/6\mathbb{Z}$-torsion.
- The equality $a = -1$ for twisted Edwards curves is the same as the equality $A + 2 = -B$ for Montgomery curves. So every twisted Edwards curve with torsion $\mathbb{Z}/6\mathbb{Z}$ is birationnaly equivalent to a curve of the Suyama-11 family.
- So previous examples for $\sigma = 11$ also explain the good behaviour of the twisted Edwards curves with torsion $\mathbb{Z}/6\mathbb{Z}$.

Conclusion

- The use of Galois theory allows us to have a theoretical point of view on torsion properties of elliptic curves.
- The new techniques suggested by the theoretical study helped us to find infinite families of curves having good torsion properties.

Some questions which were not addressed in our work:

- What can we say about 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 that we were able to compute?

Thank you for your attention.
Any questions?