Parametrizations for Families of ECM-Friendly Curves

Alexandre Gélin

joint work with Thorsten Kleinjung and Arjen K. Lenstra

Laboratoire de Mathématiques de Versailles
UVSQ – CNRS – Université Paris-Saclay

CAEN

2018/06/21

Factoring using elliptic curves

- Problem: To factor a composite number N

Factoring using elliptic curves

- Problem: To factor a composite number N
- Best solution: The Number Field Sieve (NFS)

Factoring using elliptic curves

- Problem: To factor a composite number N
- Best solution: The Number Field Sieve (NFS)
- Our purposes: The Elliptic Curve Method (ECM)

Factoring using elliptic curves

- Problem: To factor a composite number N
- Best solution: The Number Field Sieve (NFS)
- Our purposes: The Elliptic Curve Method (ECM)
  - Introduced by H.W. Lenstra in 1985

Factoring using elliptic curves

- Problem: To factor a composite number N
- Best solution: The Number Field Sieve (NFS)
- Our purposes: The Elliptic Curve Method (ECM)
  - Introduced by H.W. Lenstra in 1985
  - Best strategy for small factors p

Factoring using elliptic curves

- Problem: To factor a composite number N
- Best solution: The Number Field Sieve (NFS)
- Our purposes: The Elliptic Curve Method (ECM)
  - Introduced by H.W. Lenstra in 1985
  - Best strategy for small factors p
  - Part of the NFS

Factoring using elliptic curves

- Problem: To factor a composite number N
- Best solution: The Number Field Sieve (NFS)
- Our purposes: The Elliptic Curve Method (ECM)
  - Introduced by H.W. Lenstra in 1985
  - Best strategy for small factors p
  - Part of the NFS
- How does it work? We perform arithmetic operations $\bmod N$

How does it work?

- Inputs: An e.c. E over $\mathbf{Z}/N\mathbf{Z}$, a point P on E and a param. k

How does it work?

- Inputs: An e.c. E over $\mathbf{Z}/N\mathbf{Z}$, a point P on E and a param. k
- Algorithm: ECM computes the multiple $k \cdot P$ on E, modulo N

How does it work?

- Inputs: An e.c. E over $\mathbf{Z}/N\mathbf{Z}$, a point P on E and a param. k
- Algorithm: ECM computes the multiple $k \cdot P$ on E, modulo N
- Solution: ECM finds a factor p of N when

$$k \cdot P = \mathcal{O} \text{ on } E_p = E \bmod p$$

How does it work?

- Inputs: An e.c. E over $\mathbf{Z}/N\mathbf{Z}$, a point P on E and a param. k
- Algorithm: ECM computes the multiple $k \cdot P$ on E, modulo N
- Solution: ECM finds a factor p of N when

$$k \cdot P = \mathcal{O} \text{ on } E_p = E \bmod p$$

$$\Longleftrightarrow$$

k is a multiple of the order of P over E_p

How does it work?

- Inputs: An e.c. E over $\mathbf{Z}/N\mathbf{Z}$, a point P on E and a param. k
- Algorithm: ECM computes the multiple $k \cdot P$ on E, modulo N
- Solution: ECM finds a factor p of N when

$$k \cdot P = \mathcal{O} \text{ on } E_p = E \bmod p$$

$$\Longleftrightarrow$$

$$k \text{ is a multiple of the order of } P \text{ over } E_p$$

- Goal: Find curves E such that $\#E_p \mid k$ for a lot of primes p

Find the best curves

- Solution: We want $\#E_p$ to be smooth and we choose $k = \prod p_i^{e_i}$

Find the best curves

- Solution: We want $\#E_p$ to be smooth and we choose $k = \prod p_i^{e_i}$
- New goal: To look for curves with smooth cardinalities

Find the best curves

- Solution: We want $\#E_p$ to be smooth and we choose $k = \prod p_i^{e_i}$
- New goal: To look for curves with smooth cardinalities
- Fact: The torsion group of E over $\mathbf{Q}$ injects in every E_p

Find the best curves

- Solution: We want $\#E_p$ to be smooth and we choose $k = \prod p_i^{e_i}$
- New goal: To look for curves with smooth cardinalities
- Fact: The torsion group of E over $\mathbf{Q}$ injects in every E_p
- Mazur's theorem: A torsion group over $\mathbf{Q}$ is isomorphic to

  $\mathbf{Z}/n\mathbf{Z}$ with $1 \le n \le 10$ or $n = 12$, or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z}$ with $1 \le n \le 4$

Quick history of curves in ECM

- Lenstra presented ECM with short Weierstrass equations
  $y^2 = x^3 + ax + b$

Quick history of curves in ECM

- Lenstra presented ECM with short Weierstrass equations $y^2 = x^3 + ax + b$
- `GMP-ECM` uses Montgomery curves $By^2 = x^3 + Ax^2 + x$

Quick history of curves in ECM

- Lenstra presented ECM with short Weierstrass equations $y^2 = x^3 + ax + b$
- `GMP-ECM` uses Montgomery curves $By^2 = x^3 + Ax^2 + x$
- 2008 : *Twisted* Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$

  Torsion groups: 12, 2×8, or smaller than 8

Quick history of curves in ECM

- Lenstra presented ECM with short Weierstrass equations $y^2 = x^3 + ax + b$
- `GMP-ECM` uses Montgomery curves $By^2 = x^3 + Ax^2 + x$
- $2008:$ *Twisted* Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$

  Torsion groups: 12, 2×8, or smaller than 8
- $a = -1$ Twisted Edwards curves: gain a field multiplication

  Torsion groups: 2×4, 6, 8 or smaller than 4

Characterization of $\mathbf{Z}/12\mathbf{Z}$ curves

If $u \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where

$$x_3 = \frac{u^2 - 1}{u^2 + 1}, \quad y_3 = -\frac{(u-1)^2}{u^2+1}, \quad d = \frac{(u^2+1)^3(u^2-4u+1)}{(u-1)^6(u+1)^2}$$

has (x_3, y_3) as a point of order 3 and has $\mathbf{Q}$-torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with a point of order 3 arises in this way.

Characterization of $\mathbf{Z}/12\mathbf{Z}$ curves

If $u \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where

$$x_3 = \frac{u^2 - 1}{u^2 + 1}, \quad y_3 = -\frac{(u-1)^2}{u^2+1}, \quad d = \frac{(u^2+1)^3(u^2-4u+1)}{(u-1)^6(u+1)^2}$$

has (x_3, y_3) as a point of order 3 and has $\mathbf{Q}$-torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with a point of order 3 arises in this way.

Montgomery [Mon87]

Let $(s, t) \notin \{(0,0), (-2, \pm 4), (6, \pm 12)\}$ be a rational point on the curve $T^2 = S^3 - 12S$. Define

$$d = -\frac{(s-2)^3(s+6)^3(s^2-12s-12)}{1024s^2t^2}.$$

Then the Edwards curve $E : x^2 + y^2 = 1 + dx^2y^2$ has $\mathbf{Q}$-torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$ and has a non-torsion point (x_1, y_1) where

$$x_1 = \frac{8t(s^2+12)}{(s-2)(s+6)(s^2+12s-12)} \quad \text{and} \quad y_1 = -\frac{4s(s^2-12s-12)}{(s-2)(s+6)(s^2-12)}.$$

$a = -1$ Twisted Edwards curve with torsion $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$

Characterization

If $e \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the $a = -1$ Twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where $d = -e^4$ has $\mathbf{Q}$-torsion group isomorphic tp $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with such a torsion group arises in this way.

$a = -1$ Twisted Edwards curve with torsion $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$

Characterization

If $e \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the $a = -1$ Twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where $d = -e^4$ has $\mathbf{Q}$-torsion group isomorphic tp $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with such a torsion group arises in this way.

- Galois properties studied in [BBBKM12]

$a = -1$ Twisted Edwards curve with torsion $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$

Characterization

If $e \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the $a = -1$ Twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where $d = -e^4$ has $\mathbf{Q}$-torsion group isomorphic tp $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with such a torsion group arises in this way.

- Galois properties studied in [BBBKM12]
- for a generic d, P_8 splits into 3 irred. factors deg. 4, 4, 16

$a = -1$ Twisted Edwards curve with torsion $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$

Characterization

If $e \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the $a = -1$ Twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where $d = -e^4$ has $\mathbf{Q}$-torsion group isomorphic tp $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with such a torsion group arises in this way.

- Galois properties studied in [BBBKM12]
- for a generic d, P_8 splits into 3 irred. factors deg. 4, 4, 16
- for $d = -e^4$, the deg-16 pol. splits into 3 factors of deg. 4, 4, 8

$a=-1$ Twisted Edwards curve with torsion $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$

Characterization

If $e\in\mathbf{Q}\setminus\{0,\pm1\}$ then the $a=-1$ Twisted Edwards curve $-x^2+y^2=1+dx^2y^2$ over $\mathbf{Q}$, where $d=-e^4$ has $\mathbf{Q}$-torsion group isomorphic tp $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$. Conversely, every Edwards curve over $\mathbf{Q}$ with such a torsion group arises in this way.

- Galois properties studied in [BBBKM12]
- for a generic d, P_8 splits into 3 irred. factors deg. 4, 4, 16
- for $d=-e^4$, the deg-16 pol. splits into 3 factors of deg. 4, 4, 8

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

Consequences for smoothness probabilities

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 $GL_2(\mathbb{Z}/\pi\mathbb{Z})$.

First rational parametrization [BBBKM12]

Theorem

For nonzero $t \in \mathbf{Q} \setminus \{\pm 1, \pm 3^{\pm 1}\}$ let $e_1 = \frac{3(t^2-1)}{8t}$,

$$x_1 = \frac{128t^3}{27t^6 + 63t^4 - 63t^2 - 27} \quad \text{and} \quad y_1 = \frac{9t^4 - 2t^2 + 9}{9t^4 - 9}.$$

Then (x_1, y_1) is a non-torsion point on the curve $-x^2 + y^2 = 1 - e_1^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

First rational parametrization [BBBKM12]

Theorem

For nonzero $t \in \mathbf{Q} \setminus \{\pm 1, \pm 3^{\pm 1}\}$ let $e_1 = \frac{3(t^2-1)}{8t}$,

$$x_1 = \frac{128t^3}{27t^6 + 63t^4 - 63t^2 - 27} \quad \text{and} \quad y_1 = \frac{9t^4 - 2t^2 + 9}{9t^4 - 9}.$$

Then (x_1, y_1) is a non-torsion point on the curve $-x^2 + y^2 = 1 - e_1^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

- Eases the curves generation

First rational parametrization [BBBKM12]

Theorem

For nonzero $t \in \mathbf{Q} \setminus \{\pm 1, \pm 3^{\pm 1}\}$ let $e_1 = \frac{3(t^2-1)}{8t}$,

$$x_1 = \frac{128t^3}{27t^6 + 63t^4 - 63t^2 - 27} \quad \text{and} \quad y_1 = \frac{9t^4 - 2t^2 + 9}{9t^4 - 9}.$$

Then (x_1, y_1) is a non-torsion point on the curve $-x^2 + y^2 = 1 - e_1^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

- Eases the curves generation
- Allows to look for additional constraints

First rational parametrization [BBBKM12]

Theorem

For nonzero $t \in \mathbf{Q} \setminus \{\pm 1, \pm 3^{\pm 1}\}$ let $e_1 = \frac{3(t^2-1)}{8t}$,

$$x_1 = \frac{128t^3}{27t^6 + 63t^4 - 63t^2 - 27} \quad \text{and} \quad y_1 = \frac{9t^4 - 2t^2 + 9}{9t^4 - 9}.$$

Then (x_1, y_1) is a non-torsion point on the curve $-x^2 + y^2 = 1 - e_1^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

- Eases the curves generation
- Allows to look for additional constraints

$$e = \frac{2g^2 + 2g + 1}{2g + 1} \Longleftrightarrow e^2 - 1 \text{ is a square}$$

First rational parametrization [BBBKM12]

Theorem

For nonzero $t \in \mathbf{Q} \setminus \{\pm 1, \pm 3^{\pm 1}\}$ let $e_1 = \frac{3(t^2-1)}{8t}$,

$$x_1 = \frac{128t^3}{27t^6 + 63t^4 - 63t^2 - 27} \quad \text{and} \quad y_1 = \frac{9t^4 - 2t^2 + 9}{9t^4 - 9}.$$

Then (x_1, y_1) is a non-torsion point on the curve $-x^2 + y^2 = 1 - e_1^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

- Eases the curves generation
- Allows to look for additional constraints

$$e = \frac{2g^2 + 2g + 1}{2g + 1} \Longleftrightarrow e^2 - 1 \text{ is a square}$$

$$e = \frac{g - \frac{1}{g}}{2} \Longleftrightarrow e^2 + 1 \text{ is a square}$$

First parametrization for a subfamily [BBBKM12]

Corollary

Consider the elliptic curve $y^2 = x^3 - 36x$ of rank one, with the point $(-3, 9)$ generating a non-torsion subgroup. For any point (x, y) on this curve and

$$t = \frac{x+6}{x-6}$$

the $a = -1$ twisted Edwards curve with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ defined as in the prior Theorem belongs to family $e = g^2$ and has positive rank over $\mathbf{Q}$.

Proof

$$e_1 = \frac{3(t^2-1)}{8t} = \frac{9x}{x^2-36} = \left(\frac{3x}{y}\right)^2$$

Our work [GKL17]

- Goal: Find more rational parametrizations

Our work [GKL17]

- Goal: Find more rational parametrizations
- Hope to find one that matches with the best subfamily $e = \frac{g - \frac{1}{g}}{2}$

Our work [GKL17]

- Goal: Find more rational parametrizations
- Hope to find one that matches with the best subfamily $e = \frac{g - \frac{1}{g}}{2}$
- Idea: Search, search, and search again...

Our work [GKL17]

- Goal: Find more rational parametrizations
- Hope to find one that matches with the best subfamily $e = \frac{g - \frac{1}{g}}{2}$
- Idea: Search, search, and search again...

Our work [GKL17]

- Goal: Find more rational parametrizations
- Hope to find one that matches with the best subfamily $e = \frac{g - \frac{1}{g}}{2}$
- Idea: Search, search, and search again...

$$-x^2 + y^2 = 1 - e^4 x^2 y^2 \iff y^2 = \frac{1 + x^2}{1 + e^4 x^2} \iff e^4 x^4 + (1 + e^4) x^2 + 1 = \square$$

Our work [GKL17]

- Goal: Find more rational parametrizations
- Hope to find one that matches with the best subfamily $e = \frac{g - \frac{1}{g}}{2}$
- Idea: Search, search, and search again...

$$-x^2+y^2 = 1-e^4x^2y^2 \iff y^2 = \frac{1+x^2}{1+e^4x^2} \iff e^4x^4+(1+e^4)x^2+1 = \square$$

$$x = \frac{u(e)}{v(e)} \implies e^4u^4+(1+e^4)u^2v^2+v^4 \quad \text{must be a square}$$

Our work [GKL17]

- Goal: Find more rational parametrizations
- Hope to find one that matches with the best subfamily $e = \frac{g - \frac{1}{g}}{2}$
- Idea: Search, search, and search again...

$$-x^2 + y^2 = 1 - e^4 x^2 y^2 \iff y^2 = \frac{1 + x^2}{1 + e^4 x^2} \iff e^4 x^4 + (1 + e^4) x^2 + 1 = \square$$

$$x = \frac{u(e)}{v(e)} \implies e^4 u^4 + (1 + e^4) u^2 v^2 + v^4 \quad \text{must be a square}$$

- Large number of tries for small polynomials

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves
- Idea: To recognize parametrized families of curves

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves
- Idea: To recognize parametrized families of curves
- Example:

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves
- Idea: To recognize parametrized families of curves
- Example:
  - For $x = \frac{e+k}{ke-1}$, we have $y^2 = \frac{k^2+1}{e^4+2ke^3+(k^2-1)e^2-2ke+1}$

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves
- Idea: To recognize parametrized families of curves
- Example:
  - For $x = \frac{e+k}{ke-1}$, we have $y^2 = \frac{k^2+1}{e^4+2ke^3+(k^2-1)e^2-2ke+1}$
  - Choosing $e = \frac{3}{4k}$, the denominator becomes $\left(\frac{4k^2+9}{16k^2}\right)^2$

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves
- Idea: To recognize parametrized families of curves
- Example:
  - For $x = \frac{e+k}{ke-1}$, we have $y^2 = \frac{k^2+1}{e^4+2ke^3+(k^2-1)e^2-2ke+1}$
  - Choosing $e = \frac{3}{4k}$, the denominator becomes $\left(\frac{4k^2+9}{16k^2}\right)^2$
  - If k^2+1 is a square, then (x,y) is on $E: -x^2+y^2 = 1-\left(\frac{3}{4k}\right)^4 x^2y^2$

Our work [GKL17]

- Square-free part of degree ≥ 6: hyperelliptic curves ☹
- Square-free part of degree 2: lead to the rational parametrization
- Square-free part of degree 4: elliptic curves
- Idea: To recognize parametrized families of curves
- Example:
  - For $x = \frac{e+k}{ke-1}$, we have $y^2 = \frac{k^2+1}{e^4+2ke^3+(k^2-1)e^2-2ke+1}$
  - Choosing $e = \frac{3}{4k}$, the denominator becomes $\left(\frac{4k^2+9}{16k^2}\right)^2$
  - If k^2+1 is a square, then (x, y) is on $E: -x^2+y^2 = 1-\left(\frac{3}{4k}\right)^4 x^2y^2$
  - Results in infinitely many curves

Our results [GKL17]

Theorem

For $1 \leq j \leq 7$, the point (x_j, y_j) is a non-torsion point on the curve defined by $-x^2 + y^2 = 1 - e_j^4 x^2 y^2$:

j	e_j	x_j	y_j
1	$\frac{3(t^2-1)}{8t}$	$\frac{128t^3}{27t^6+63t^4-63t^2-27}$	$\frac{9t^4-2t^2+9}{9t^4-9}$
2	$\frac{t^2+2t+4}{2t+2}$	$\frac{2t^3+2t^2-8t-8}{t^4+6t^3+12t^2+16t}$	$\frac{2t^5+14t^4+40t^3+44t^2+32t+16}{t^6+4t^5+10t^4+20t^3+40t^2+64t+64}$
3	$\frac{t^2+4}{3t}$	$\frac{12t^2-24}{t^4-4t^2-32}$	$\frac{3t^6-12t^4+120t^2}{5t^6+12t^4+128}$
4	$\frac{t^2+4t}{t^2-4}$	$\frac{2t^3+2t^2-8t-8}{t^4+6t^3+12t^2+16t}$	$\frac{t^6+6t^5+10t^4-16t^3-48t^2-32t-32}{t^6+6t^5+10t^4+16t^3+48t^2+64t}$
5	$\frac{4t^4-1024}{t^5+512t}$	$\frac{96t^6+49152t^2}{t^8-1280t^4+262144}$	$\frac{t^{12}+3840t^8+1966080t^4+134217728}{t^{12}-768t^8+786432t^4-167772160}$
6	$\frac{t^3+8t}{4t^2+8}$	$\frac{12t^2+24}{t^4+4t^2-32}$	$\frac{4t^6+24t^4+192t^2+320}{5t^6+48t^4+96t^2+256}$
7	$\frac{t^3-8t}{4t^2-8}$	$\frac{12t^2-24}{t^4-4t^2-32}$	$\frac{4t^6-24t^4+192t^2-320}{5t^6-48t^4+96t^2-256}$

Our results [GKL17]

Corollary

For $1 \leq j \leq 4$ let (e_j, x_j, y_j) be functions of t as in the previous theorem. For each case below the elliptic curve E has rank one, and for each point (x, y) on E the pair (x_j, y_j) is a non-torsion point on the curve defined by $-x^2 + y^2 = 1 - e_j^4 x^2 y^2$:

family	j	E	t	Proof
(i)	1	$y^2 = x^3 - 36x$	$\frac{x+6}{x-6}$	$e_1 = \left(\frac{3x}{y}\right)^2$
(ii)	2	$y^2 = x^3 + 3x$	$x - 1$	$e_2 = \frac{1}{2}\left(\frac{y}{x}\right)^2$
(ii)	3	$y^2 = x^3 + 9x$	$\frac{2x}{3}$	$e_3 = \frac{1}{2}\left(\frac{2y}{3x}\right)^2$
(iii)	3	$y^2 = x^3 - x^2 - 64x + 64$	$\frac{8x-8}{y}$	$e_3^2 - 1 = \left(\frac{x^2-2x+64}{6y}\right)^2$
(iii)	4	$y^2 = x^3 - 12x$	$\frac{x-2}{2}$	$e_4^2 - 1 = \left(\frac{4y^2}{x^2-4x-12}\right)^2$
(iv)	4	$y^2 = x^3 - x^2 - 9x + 9$	$\frac{4x+4}{y-4}$	$e_4^2 + 1 = \left(\frac{x^4+4x^3+14x^2-108x+153}{x^4-4x^3-18x^2-16xy+12x+48y+9}\right)^2$

Our results [GKL17]

Corollary

For $1 \le j \le 4$ let (e_j, x_j, y_j) be functions of t as in the previous theorem. For each case below the elliptic curve E has rank one, and for each point (x,y) on E the pair (x_j, y_j) is a non-torsion point on the curve defined by $-x^2 + y^2 = 1 - e_j^4 x^2 y^2$:

family	j	E	t	Proof
(i)	1	$y^2 = x^3 - 36x$	$\frac{x+6}{x-6}$	$e_1 = \left(\frac{3x}{y}\right)^2$
(ii)	2	$y^2 = x^3 + 3x$	$x-1$	$e_2 = \frac{1}{2}\left(\frac{y}{x}\right)^2$
(ii)	3	$y^2 = x^3 + 9x$	$\frac{2x}{3}$	$e_3 = \frac{1}{2}\left(\frac{2y}{3x}\right)^2$
(iii)	3	$y^2 = x^3 - x^2 - 64x + 64$	$\frac{8x-8}{y}$	$e_3^2 - 1 = \left(\frac{x^2-2x+64}{6y}\right)^2$
(iii)	4	$y^2 = x^3 - 12x$	$\frac{x-2}{2}$	$e_4^2 - 1 = \left(\frac{4y^2}{x^2-4x-12}\right)^2$
(iv)	4	$y^2 = x^3 - x^2 - 9x + 9$	$\frac{4x+4}{y-4}$	$e_4^2 + 1 = \left(\frac{x^4+4x^3+14x^2-108x+153}{x^4-4x^3-18x^2-16xy+12x+48y+9}\right)^2$

So we have a parametrization for the best subfamily $e = \frac{g - \frac{1}{g}}{2}$. ☺

Effectiveness of our curves

b	$\#p$	$\mathscr{C}_6$	$\mathscr{C}_{2\times 4}$	#1	average	#100	$^{\#1}/_{\mathscr{C}_6}$	$^{\#1}/_{\#100}$
				(among $\mathscr{C}_{[1]}, \mathscr{C}_{[2]}, \ldots, \mathscr{C}_{[100]}$)				
15	1612	1127	1049	1202	1155.4	1103	1.0665	1.0897
16	3030	1693	1564	1806	1737.3	1664	1.0667	1.0853
17	5709	3299	2985	3324	3197.9	3077	1.0075	1.0802
18	10749	6150	5529	6168	6020.0	5921	1.0029	1.0417
19	20390	10802	10200	10881	10723.8	10500	1.0073	1.0362
20	38635	16148	15486	16396	16197.7	15955	1.0153	1.0276
21	73586	24160	22681	24312	24003.3	23655	1.0062	1.0277
22	140336	48378	46150	48894	48515.6	48114	1.0106	1.0162
23	268216	83339	82743	85525	84840.0	84254	1.0262	1.0150
24	513708	193069	187596	193558	192825.7	191961	1.0025	1.0083
25	985818	318865	311864	320498	319154.8	317304	1.0051	1.0100
26	1894120	493470	480006	495082	493556.4	492364	1.0032	1.0055

Thanks

Merci