Finding ECM friendly curves: A Galois approach

Sudarshan SHINDE

Sorbonne Universités, Paris (UPMC, IMJ-PRG)

25/01/2018

Motivation : Cryptology

Integer factorization is an important problem in cryptology. There are two types of algorithms to do so.

1. Algorithms which find all the factors $< m$ with cost depending on m and polynomially on the integer to factor. Ex. Trial division, ECM - Elliptic Curve Method .
2. Algorithms whose cost depends on the size of integer to factor. Ex. QS (Quadratic Sieve), NFS (Number Field Sieve).

Motivation : Cryptology

Integer factorization is an important problem in cryptology. There are two types of algorithms to do so.

1. Algorithms which find all the factors $< m$ with cost depending on m and polynomially on the integer to factor. Ex. Trial division, ECM - Elliptic Curve Method .
2. Algorithms whose cost depends on the size of integer to factor. Ex. QS (Quadratic Sieve), NFS (Number Field Sieve). The building block which takes a non-negligible proportion of time in NFS is ECM.

Preliminaries - 1

1. K a field, E is a curve defined by $y^2 = x^3 + ax + b$ where $a, b \in \mathrm{K}$ such that $4a^3 + 27b^2 \neq 0$. We call E an elliptic curve over K.
2. We note the set of points on E with coordinates in K by $\mathrm{E}(\mathrm{K})$. With a distinguished point $\mathcal{O}_{\mathrm{E}}$, $\mathrm{E}(\mathrm{K})$ has a group law under which it forms an Abelian group.
3. An important quantity associated with an elliptic curve is its j-invariant which is $1728\frac{4a^3}{4a^3+27b^2}$.

ECM algorithm

Algorithm 1 Practical version of ECM (Lenstra + Montgomery)

INPUT : Integers n and B
OUTPUT : a non-trivial factor of n.

while No factor is found **do**
  $\mathrm{E}/\mathbb{Q} \leftarrow$ an elliptic curve and $\mathrm{P} = (x : y : z) \in \mathrm{E}(\mathbb{Q})$.
  $\mathrm{P}_\mathrm{B} \leftarrow [\mathrm{B}!]\mathrm{P} = (x_\mathrm{B} : y_\mathrm{B} : z_\mathrm{B})$ mod n
  $g \leftarrow \gcd(z_\mathrm{B}, n)$
  if $g \notin \{1, n\}$ **then return** g
  end if
end while

Correctness

Idea

Let p be an unknown prime factor of n. If $\mathrm{ord}(\mathrm{P})$ in $\mathrm{E}(\mathbb{F}_p)$ divides $\mathrm{B}!$, then

$$[\mathrm{B}!](x_\mathrm{P} : y_\mathrm{P} : z_\mathrm{P}) \equiv (0 : 1 : 0) \bmod p.$$

In this case p divides $\gcd(z_\mathrm{P}, n)$.

Sufficient condition

$\#\mathrm{E}(\mathbb{F}_p)$ is $\mathrm{B}-$smooth i.e. all its prime factors are $< \mathrm{B}$.

Idea of Montgomery

Question : What if $\#\mathrm{E}(\mathbb{F}_p)$ is even for all primes p?
Theorem : If m divides torsion order of $\mathrm{E}(\mathbb{Q})$ then m divides $\#\mathrm{E}(\mathbb{F}_p)$ for almost all p.

Montgomery heuristic

Definition

Let E be an elliptic curve, ℓ be a prime and n be a sufficiently large integer. We define empirical average valuation,

$$\bar{v}_\ell(\mathrm{E}) = \frac{\sum_{p<n}(\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))}{\#\{p < n\}}.$$

Heuristic

Curves with larger average valuation are ECM-friendly.

How to improve average valuation ?

Some ways

1. Montgomery (1985), Suyama (1985), Atkin et Morain (1993), Bernstein et al (2010) : Torsion points over $\mathbb{Q}$

How to improve average valuation ?

Some ways

1. Montgomery (1985), Suyama (1985), Atkin et Morain (1993), Bernstein et al (2010) : Torsion points over $\mathbb{Q}$
2. Brier and Clavier (2010) : Torsion points over $\mathbb{Q}(i)$
   $\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)) = \frac{1}{2}\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)|p \equiv 1 \bmod 4) + \frac{1}{2}\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p) \mid p \equiv 3 \bmod 4)$

How to improve average valuation ?

Some ways

1. Montgomery (1985), Suyama (1985), Atkin et Morain (1993), Bernstein et al (2010) : Torsion points over $\mathbb{Q}$
2. Brier and Clavier (2010) : Torsion points over $\mathbb{Q}(i)$
$\overline{\mathrm{v}}_2(\#\mathrm{E}(\mathbb{F}_p)) = \frac{1}{2}\overline{\mathrm{v}}_2(\#\mathrm{E}(\mathbb{F}_p)|p \equiv 1 \bmod 4) + \frac{1}{2}\overline{\mathrm{v}}_2(\#\mathrm{E}(\mathbb{F}_p)\,|\,p \equiv 3 \bmod 4)$
3. Barbulescu et al (2012) : Better average valuation without additional torsion points by reducing the size of a "specific" Galois group.

Preliminaries - 2

Definition - Theorem

For an elliptic curve E and a an integer m, we define the m-division polynomial as

$$\Psi_{(\mathrm{E},m)}(X) = \prod_{(x:\pm y:1)\in \mathrm{E}(\bar{\mathbb{Q}})[m]} (X - x) \qquad \in \mathbb{Q}[X].$$

Example

Let $\mathrm{E} : y^2 = x^3 + ax + b$ then $\Psi_{(\mathrm{E},3)} = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$

Preliminaries - 2

Definition - Theorem

For an elliptic curve E and a an integer m, we define the m-division polynomial as

$$\Psi_{(\mathrm{E},m)}(X) = \prod_{(x:\pm y:1)\in \mathrm{E}(\bar{\mathbb{Q}})[m]} (X - x) \qquad \in \mathbb{Q}[X].$$

Example

Let $\mathrm{E} : y^2 = x^3 + ax + b$ then $\Psi_{(\mathrm{E},3)} = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$

Division polynomials can be computed recursively thus it is not necessary to know $\mathrm{E}(\bar{\mathbb{Q}})[m]$ and they are used to construct the torsion fields.

Preliminaries - 3

Definition (m-torsion field)

Let E be an elliptic curve on $\mathbb{Q}$, m a positive integer. The m-torsion field $\mathbb{Q}(\mathrm{E}[m])$ is the extension of $\mathbb{Q}$ by the coordinates of m-torsion points in $\bar{\mathbb{Q}}$.

As $\mathrm{E}(\bar{\mathbb{Q}})[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $\mathrm{G} = \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q})$ is always a subgroup of $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Preliminaries - 3

Definition (m-torsion field)

Let E be an elliptic curve on $\mathbb{Q}$, m a positive integer. The m-torsion field $\mathbb{Q}(\mathrm{E}[m])$ is the extension of $\mathbb{Q}$ by the coordinates of m-torsion points in $\bar{\mathbb{Q}}$.

As $\mathrm{E}(\bar{\mathbb{Q}})[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $\mathrm{G} = \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q})$ is always a subgroup of $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Mod m Galois Image (Definition)

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

Weil pairing

$\mathbb{Q}(\zeta_m)$ is contained in $\mathbb{Q}(\mathrm{E}[m])$ and we have

$$\det(\rho_{\mathrm{E},m}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q}))) = (\mathbb{Z}/m\mathbb{Z})^*.$$

Galois images

Theorem (Serre, 1972)

Let E be an elliptic curve without complex multiplication.

- (Generic case) For all primes ℓ outside a finite set depending on E and for all $k \geq 1$, $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$.
- For all primes ℓ and $k \geq 1$, the sequence

$$\iota_k = [\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) : \rho_{\mathrm{E},\ell^k}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}))]$$

is non-decreasing and eventually stationary.

A conjecture of Serre

"La condition $\ell \geq 41$ *suffit-elle* à assurer que ρ_{E} est surjectif ?"

How to improve average valuation ?

Theorem (Barbulescu et al. 2012)

Let ℓ be a prime and E_1 and E_2 be two elliptic curves. If $\forall n \in \mathbb{N}, \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_1[\ell^n])/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_2[\ell^n])/\mathbb{Q})$ then $\bar{v}_\ell(\mathrm{E}_1) = \bar{v}_\ell(\mathrm{E}_2)$.

Thus in order to change the average valuation, we must change $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q})$ for at least one n.

How to improve average valuation ?

Theorem (Barbulescu et al. 2012)

Let ℓ be a prime and E_1 and E_2 be two elliptic curves. If $\forall n \in \mathbb{N}, \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_1[\ell^n])/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_2[\ell^n])/\mathbb{Q})$ then $\bar{v}_\ell(\mathrm{E}_1) = \bar{v}_\ell(\mathrm{E}_2)$.

Thus in order to change the average valuation,
we must change $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q})$ for at least one n.

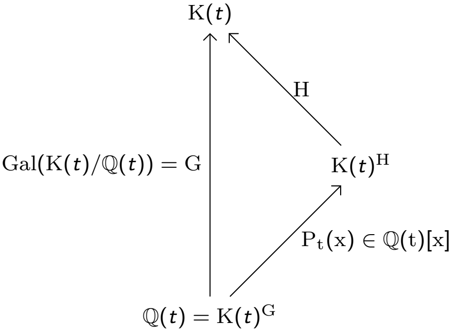
Example

Family	Torsion	$\bar{v}_2$	Primes found between $2^{15}, 2^{22}$
Suyama	$\mathbb{Z}/6\mathbb{Z}$	$^{10}/_3$	7529
Suyama - 11	$\mathbb{Z}/6\mathbb{Z}$	$^{11}/_3$	9041 (20% more)

Computer algebra Approach

Computer algebra approach : Subfields

Question : Under which conditions on $t_0 \in \mathbb{Q}$,
$\mathrm{Gal}(\mathrm{K}(t_0)/\mathbb{Q}) \subseteq \mathrm{H}$?



Answer : When $\mathrm{P}_{t_0}(x)$ has a root in $\mathbb{Q}$.

For particular subgroups H

Let $\mathrm{G} = \mathrm{Gal}(\mathrm{K}(t)/\mathbb{Q}(t))$ and $\mathrm{H} \subseteq \mathrm{G}$.

1. $\mathrm{G} = \mathrm{H}$: It suffices to check that for any tower of extensions between $\mathbb{Q}(t)$ and $\mathrm{K}(t)$, every defining polynomial remains irreducible. The complexity is the complexity of multivariate polynomial factorization of degrees $< [\mathrm{K}(t) : \mathbb{Q}(t)]$. This case becomes easy when $[\mathrm{K}(t) : \mathbb{Q}(t)]$ is small.

2. $[\mathrm{G} : \mathrm{H}] = 2$:
   1. Factorize $\mathrm{Disc}(\mathrm{K}(t)) \in \mathbb{Z}[t]$.
   2. For each squarefree factor $f \in \mathbb{Z}[t]$ of $\mathrm{Disc}(\mathrm{K}(t))$, check using specializations if $\mathrm{K}(t)^{\mathrm{H}}$ is defined by $X^2 - f$.

   This case becomes easy if the factors of $\mathrm{Disc}(\mathrm{K}(t))$ are known.

Particular case : $\mathrm{K} = \mathbb{Q}(a,b)(\mathrm{E}[\ell])$ et $G = H$

Idea : Formal construction of torsion field and sufficient condition that its Galois group is generic.
Sufficient condition : When all the following extensions have generic degrees.

$$\begin{array}{l}
\mathrm{K}_4 = \mathbb{Q}(a,b)(x_1,x_2,y_1,y_2) = \mathbb{Q}(a,b)(\mathrm{E}[\ell]) \\
\quad \Big| \; \mathrm{P}_4 = y^2 - (x_2^3 + a x_2 + b) \\
\mathrm{K}_3 = \mathbb{Q}(a,b)(x_1,x_2,y_1) \\
\quad \Big| \; \mathrm{P}_3 = y^2 - (x_1^3 + a x_1 + b) \\
\mathrm{K}_2 = \mathbb{Q}(a,b)(x_1,x_2) \\
\quad \Big| \; \mathrm{P}_2 = \text{a factor of } \Psi \text{ of degree } \frac{\ell^2-\ell}{2} \\
\mathrm{K}_1 = \mathbb{Q}(a,b)(x_1) \\
\quad \Big| \; \mathrm{P}_1 = \Psi \text{ of degree } \frac{\ell^2-1}{2} \\
\mathrm{K}_0 = \mathbb{Q}(a,b)
\end{array}$$

As $\mathrm{E}[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, $\mathbb{Q}(a,b)(\mathrm{E}[\ell])$ is constructed by only 4 extensions.

Valuation $m = 4$, Montgomery curve

Theorem

Let $\mathrm{E} : By^2 = x^3 + Ax^2 + x$ be a rational elliptic curve with $B(A^2 - 4) \neq 0$. Then the generic average valuation $\bar{v}_2(\mathrm{E})$ is $^{10}/_3 \approx 3.33$, except,

- If $A^2 - 4 \neq \square$ i.e. $\mathrm{E}(\mathbb{Q})[2] \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we note Ψ be the quartic factor of its 4-division polynomial. Then we have,

Fact. Pat. of Ψ	Condition(s)	Index	Valuation
$(2,2)$	$A = -2\frac{t^4-4}{t^4+4}$	24	$^{10}/_3 \approx 3.33$
(4)	$\frac{A\pm 2}{B} = \pm\square$	12	$^{11}/_3 \approx 3.67$

- If $A^2 - 4 = \square$ i.e. if $A = \frac{t^2+4}{2t}$. Then we have,

Fact. Pat. of Ψ	Condition(s)	Index	Valuation
$(1,1,2)$	$A = \frac{t^4+24\,t^2+16}{4\left(t^2+4\right)t}$ and $B = -t(t^2+4)\square$	48	$^{14}/_3 \approx 4.67$
$(1,1,2)$	$A = \frac{t^4+24\,t^2+16}{4\left(t^2+4\right)t}$	24	$^{23}/_6 \approx 3.83$
$(2,2)$	$A = \frac{t^2+4}{2t}$ and $\frac{A\pm 2}{B} = \square$	24	$^{13}/_3 \approx 4.33$
$(2,2)$	$A = \frac{t^2+4}{2t}$	12	$^{11}/_3 \approx 3.67$

Modular curves approach

Modular curves approach

Theorem (Attributed to Shimura,1973)

If $\mathrm{H} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is such that $-1 \in \mathrm{H}$ and $\det(\mathrm{H}) = (\mathbb{Z}/\ell^n\mathbb{Z})^*$. Then $\exists\ X_{\mathrm{H}}(j, t) \in \mathbb{Q}(j, t)$ such that the following conditions are equivalent.

1. $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q}) \subseteq \mathrm{H}$
2. $\exists t_0 \in \mathbb{Q}$ such that $X_{\mathrm{H}}(j(\mathrm{E}), t_0) = 0$.

Modular curves approach

Theorem (Attributed to Shimura,1973)

If $\mathrm{H} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is such that $-1 \in \mathrm{H}$ and $\det(\mathrm{H}) = (\mathbb{Z}/\ell^n\mathbb{Z})^*$. Then $\exists\ X_{\mathrm{H}}(j,t) \in \mathbb{Q}(j,t)$ such that the following conditions are equivalent.

1. $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q}) \subseteq \mathrm{H}$
2. $\exists t_0 \in \mathbb{Q}$ such that $X_{\mathrm{H}}(j(\mathrm{E}), t_0) = 0$.

Fast computations of X_{H}

[RZB] Jeremy Rouse and David Zureick-Brown, "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois" (2015)

- Complete description of possible 2-adic Galois images.

[SZ] Andrew Sutherland and David Zywina, "Modular curves of prime-power level with infinitely many rational points" (2017)

- Complete description of possible ℓ-adic Galois images contained in subgroups containing -1.

Example

Curve	$j(E)$	$\#\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$	$\bar{v}_3$
$y^2 = x^3 - 336x + 448$	1792	12	$^{39}/_{32}$
$y^2 = x^3 - 7^2 \cdot 336x + 7^3 \cdot 448$	1792	6	$^{54}/_{32}$

The modular curves approach does not work for arbitrary H.

Example

Curve	$j(E)$	$\#\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$	$\bar{v}_3$
$y^2 = x^3 - 336x + 448$	1792	12	$^{39}/_{32}$
$y^2 = x^3 - 7^2 \cdot 336x + 7^3 \cdot 448$	1792	6	$^{54}/_{32}$

The modular curves approach does not work for arbitrary H.

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

	$-1 \notin \mathrm{H}$	$-1 \in \mathrm{H}$
$\ell = 2$	[RZB]	[RZB], [SZ]
$\ell \neq 2$		[SZ]

Our contribution

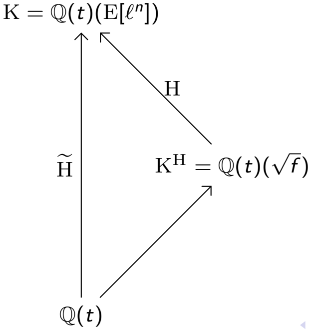
List of parametrized elliptic curves having non-generic Galois image not containing -1 when $\ell^n \in \{3, 3^2, 3^3, 5, 5^2, 7, 13\}$.

When $-1 \notin \mathrm{H}$

Let $\widetilde{\mathrm{H}}$ be subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ containing -1 with full determinant ; let $\mathrm{E}_t : y^2 = x^3 + A(t)x + B(t)$ be such that

$$\mathrm{Gal}(\mathbb{Q}(t)(\mathrm{E}_t[\ell^n])/\mathbb{Q}(t)) \subset \widetilde{H}.$$

Computer Algebra Approach : Let H be subgroup of $\widetilde{\mathrm{H}}$ such that $[\widetilde{H} : H] = 2$ and $\widetilde{\mathrm{H}} = \langle \mathrm{H}, -1 \rangle$.



New results

Some families with exceptional mod ℓ^n Galois images for $\ell^n \in \{3, 9, 27\}$.

H	(Order, index)	$\mathrm{E} : y^2 = x^3 + a(t)x + b(t)$
$\langle \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \rangle \subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	$(6, 8)$	$a = -3(t+3)(t-27)^3$, $b = -2(t^2+18t-27)(t-27)^4$
$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \rangle \subset \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$	$(162, 24)$	$a = -3(t^3+9t^2+27t+3)(t+3)$, $b = (-2t^6 - 36t^5 - 270t^4 - 1008t^3 - 1782t^2 - 972t + 54)$
$\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 10 \\ 9 & 16 \end{pmatrix}, \begin{pmatrix} 19 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 10 & 0 \\ 0 & 19 \end{pmatrix}, \begin{pmatrix} 10 & 21 \\ 0 & 19 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 8 & 16 \\ 24 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 9 \\ 0 & 1 \end{pmatrix} \rangle \subset \mathrm{GL}_2(\mathbb{Z}/27\mathbb{Z})$	$(4374, 72)$	$a = -3(t^9+9t^6+27t^3+3)(t^3+3)$, $b = -2t^{18} - 36t^{15} - 270t^{12} - 1008t^9 - 1782t^6 - 972t^3 + 54$

Comparing different families

A criteria to compare smoothness properties

Notation : $s \sim t$ if $t - \sqrt{t} < s < t + \sqrt{t}$.

Can we claim the following ? For E an elliptic curve, there exists $\alpha(\mathrm{E}) \in \mathbb{R}$ is such that

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

Definition

Let E be an elliptic curve and ℓ a prime. Let $\alpha_\ell(\mathrm{E}) = (\frac{1}{\ell-1} - \bar{v}_\ell(\mathrm{E}))\log \ell$. We define,

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

In general α is negative and it works experimentally very well.

Theorem

There are only finitely many values of $\alpha(\mathrm{E})$. And the best among them is approximately -3.43.

Open questions

- Proving theoretically that α works.

Open questions

- Proving theoretically that α works.
- There are curves where 2-Galois and 3-Galois are generic however 6-Galois is not. To what extent can these curves be used for ECM ?

Open questions

- Proving theoretically that α works.
- There are curves where 2-Galois and 3-Galois are generic however 6-Galois is not. To what extent can these curves be used for ECM ?
- Generalising the above work over number fields. In the NFS algorithm for discrete logarithms, one can have to factor many integers of the form $a^4 + b^4$. In this case, we search families over $\mathbb{Q}(\zeta_8)$.

Open questions

- Proving theoretically that α works.
- There are curves where 2-Galois and 3-Galois are generic however 6-Galois is not. To what extent can these curves be used for ECM ?
- Generalising the above work over number fields. In the NFS algorithm for discrete logarithms, one can have to factor many integers of the form $a^4 + b^4$. In this case, we search families over $\mathbb{Q}(\zeta_8)$.

Thank you !

α : An efficient tool

1. Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$: For these curves $\bar{v}_2$ changes from $\frac{14}{9}$ to $\frac{16}{3}$. Thus,

$$\alpha_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}} = \alpha_{generic} + (14/9 - 16/3)\log(2) \approx -3.4355.$$

2. Suyama-11 family : For these curves, $\bar{v}_2$ changes from $\frac{14}{9}$ to $\frac{11}{3}$ and $\bar{v}_3$ changes from $\frac{87}{128}$ to $\frac{27}{16}$. Thus,

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

Numerical experiments with α. ($n = 2^{25}$)

1. Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

	n	ne^{α}	$\#\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005753	0.005126	889 %	10.89 %
$\mathrm{B}_2 = 100$	0.008892	0.03883	0.042573	378.8 %	9.63 %

2. Suyama-11

	n	ne^{α}	$\#\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005133	0.005743	1008 %	11.89 %
$\mathrm{B}_2 = 100$	0.008892	0.04013	0.04101	361%,	2.19%