Finding ECM friendly curves: A Galois approach

Sudarshan SHINDE

Université Pierre et Marie Curie, France

Algorithm 1 ECM algorithm

INPUT : n
OUTPUT : a non-trivial factor of n.

1: $B \leftarrow B_n$.
2: **while** No factor is found **do**
3: $E \leftarrow$ an elliptic curve on $\mathbb{Q}$ and $P \in E(\mathbb{Q})$, ord(P)=∞.
4: $P_B \leftarrow [B!]P = (x_B : y_B : z_B)$ mod n
5: $g \leftarrow \gcd(z_B, n)$
6: **if** $g \notin \{1, n\}$ **then return** g
7: **end if**
8: **end while**

Idea of ECM

Idea

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

$$(x_B : y_B : z_B) \equiv (0 : 1 : 0) \bmod p.$$

In this case p divides $\gcd(z_B, n)$.

Sufficient condition

$\#E(\mathbb{F}_p)$ is $B-$smooth.

Idea of Montgomery

Lenstra : Prob($\#E(\mathbb{F}_p)$ is $B-$smooth)
$\simeq$ Prob((random integer $\simeq p$ is $B-$ smooth).
Montgomery : What if $\#E(\mathbb{F}_p)$ is even for all primes p ?

Motivation - ECM algorithm

Algorithm 2 ECM algorithm + Montgomery

INPUT : n
OUTPUT : a non-trivial factor of n.

$B \leftarrow B_n$, $m \leftarrow B!$
while No factor is found **do**
  $E \leftarrow$ an elliptic curve from a family and $P = (x : y : z) \in E(\mathbb{Q})$. ▷ Ex. higher probability that $2 | \#E(\mathbb{F}_p)$.
  $P_m \leftarrow [m]P = (x_m : y_m : z_m) \bmod n$
  $g \leftarrow \gcd(z_m, n)$
  if $g \notin \{1, n\}$ **then return** g
  end if
end while

Motivation

Montgomery heuristic

Larger $\frac{\sum_{p<B}(\mathrm{val}_2(\#E(\mathbb{F}_p))}{\sum_{p<B}1}$ means bigger chance of success with ECM.

Average valuation

We define average valuation of $\#E(\mathbb{F}_p)$ at l using Chebotarev density as $\overline{\mathrm{val}}_l = \sum_{k\geq 0} k\mathrm{Prob}(\mathrm{val}_l(\#E(\mathbb{F}_p)) = k)$.

How to change average valuation ?

1. Montgomery : Torsion points over $\mathbb{Q}$

Motivation

Montgomery heuristic

Larger $\frac{\sum_{p<B}(\mathrm{val}_2(\#E(\mathbb{F}_p))}{\sum_{p<B} 1}$ means bigger chance of success with ECM.

Average valuation

We define average valuation of $\#E(\mathbb{F}_p)$ at l using Chebotarev density as $\overline{\mathrm{val}_l} = \sum_{k\geq 0} k\mathrm{Prob}(\mathrm{val}_l(\#E(\mathbb{F}_p)) = k)$.

How to change average valuation ?

1. Montgomery : Torsion points over $\mathbb{Q}$
2. Brier and Clavier : Torsion points over $\mathbb{Q}(i)$
   $\overline{\mathrm{val}_2}(\#E(\mathbb{F}_p)) = \frac{1}{2}\overline{\mathrm{val}_2}(\#E(\mathbb{F}_p)|p \equiv 1(4)) + \frac{1}{2}\overline{\mathrm{val}_2}(\#E(\mathbb{F}_p)\,|\,p \equiv 3\,(4))$

Motivation

Montgomery heuristic

Larger $\frac{\sum_{p<B}(\mathrm{val}_2(\#E(\mathbb{F}_p))}{\sum_{p<B} 1}$ means bigger chance of success with ECM.

Average valuation

We define average valuation of $\#E(\mathbb{F}_p)$ at l using Chebotarev density as $\overline{\mathrm{val}}_l = \sum_{k\geq 0} k\mathrm{Prob}(\mathrm{val}_l(\#E(\mathbb{F}_p)) = k)$.

How to change average valuation ?

1. Montgomery : Torsion points over $\mathbb{Q}$
2. Brier and Clavier : Torsion points over $\mathbb{Q}(i)$
   $\overline{\mathrm{val}_2}(\#E(\mathbb{F}_p)) = \frac{1}{2}\overline{\mathrm{val}_2}(\#E(\mathbb{F}_p)|p \equiv 1(4)) + \frac{1}{2}\overline{\mathrm{val}_2}(\#E(\mathbb{F}_p)\,|\,p \equiv 3\,(4))$
3. Barbulescu et al : Better valuation without additional torsion points (Suyama-11)

Motivation

Definition (m-torsion field)

Let E be an elliptic curve on $\mathbb{Q}$, m a positive integer. The m-torsion field $\mathbb{Q}(E[m])$ is defined as the smallest extension of $\mathbb{Q}$ containing all the m-torsion points.

Let us note that $G = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is always a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Theorem (Serre)

- *For all primes l and $k \geq 1$, the index $[\mathrm{GL}_2(\mathbb{Z}/l^k\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[l^k])/\mathbb{Q})]$ is non-decreasing and bounded by a constant depending on E and l.*
- *For all primes l outside a finite set depending on E and for all $k \geq 1$, $\mathrm{GL}_2(\mathbb{Z}/l^k\mathbb{Z}) = \mathrm{Gal}(\mathbb{Q}(E[l^k])/\mathbb{Q})$.*

How to change the average valuation ?

Theorem (Barbulescu et al. 2012)

Let l be a prime and E_1 and E_2 be two elliptic curves. If $\forall n \in \mathbb{N}, \mathrm{Gal}(\mathbb{Q}(E_1[l^n])) \simeq \mathrm{Gal}(\mathbb{Q}(E_2[l^n]))$ *then* $\mathrm{v}_l(E_1) = \mathrm{v}_l(E_2)$.

Thus in order to change the average valuation,
we must change $\mathrm{Gal}(\mathbb{Q}(E_2[l^n]))$ for at least one n.

Constructing the m-torsion field

Definition - Theorem

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

$$\Psi_{(E,m)}(X) = \prod_{(x_P, \pm y_P) \in E[m] - O} (X - x_P) \qquad \in \mathbb{Q}[X].$$

We have $\deg(\Psi_{(E,m)}) = \frac{m^2+2-3\eta}{2}$ where $\eta = m\%2$.
From now on, we will restrict ourselves to prime torsion.
Given $E : y^2 = x^3 + ax + b$ and a prime l, we construct :

$$\mathbb{Q} \quad \to \mathbb{Q}(x_1) \quad \to \quad \mathbb{Q}(x_1, x_2) \quad \to \quad \mathbb{Q}(x_1, x_2, y_1) \quad \to \quad \mathbb{Q}(x_1, x_2, y_1, y_2)$$

where the polynomials defining the extensions are ;

1. (An irreducible factor of) $\Psi_{(E,l)}$
2. An irreducible factor of $\Psi_{(E,l)}$ on $\mathbb{Q}(x_1)$.
3. $f_1(y) = y^2 - (x_1^3 + ax_1 + b)$.
4. $f_2(y) = y^2 - (x_2^3 + ax_2 + b)$.

$\mathbb{Q}(x_1, x_2, y_1, y_2) = \mathbb{Q}(E[l])$.

Let P be an irreducible polynomial of degree n in $K[X]$ and let $\theta_1, \ldots, \theta_n$ be its roots in $\bar{K}$.

Definition (Resolvent polynomial)

Let $F(X_1, \ldots, X_n)$ be a polynomial in $K[X_1, \ldots, X_n]$ and G be a subgroup of S_n such that $G = \{\sigma \in S_n | F(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = F(X_1, \ldots, X_n)\}$. We define the resolvent polynomial

$$R_G(F, P)(X) = \prod_{\sigma \in S_n/G} (X - F(\theta_{\sigma(1)}, \ldots, \theta_{\sigma(n)})).$$

Theorem

Let P be a polynomial of degree n, G a transitive subgroup of S_n and F as above. Then, $R_G(F, P)(X) \in K[X]$ and if it has a simple root in K then $Gal(P) \subset G$ upto conjugacy.

Example : Let us consider the field $K = \mathbb{Q}(a, b, c, d)$ and the polynomial $P = X^4 + aX^3 + bX^2 + cX + d$. Let $G = D_8 =< (3,4), (1,3)(2,4), (1,4)(2,3) >$ and $F = X_1X_2 + X_3X_4$.

Example : Let us consider the field $K = \mathbb{Q}(a, b, c, d)$ and the polynomial $P = X^4 + aX^3 + bX^2 + cX + d$. Let $G = D_8 =< (3,4), (1,3)(2,4), (1,4)(2,3) >$ and $F = X_1X_2 + X_3X_4$.

In this case,

$R_G(F, P) = X^3 - (\theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4)X^2 + (\theta_1^2\theta_2\theta_3 + \theta_1^2\theta_2\theta_4 + \theta_1^2\theta_3\theta_4 + \theta_1\theta_2^2\theta_3 + \theta_1\theta_2^2\theta_4 + \theta_1\theta_2\theta_3^2 + \theta_1\theta_2\theta_4^2 + \theta_1\theta_3^2\theta_4 + \theta_1\theta_3\theta_4^2 + \theta_2^2\theta_3\theta_4 + \theta_2\theta_3^2\theta_4 + \theta_2\theta_3\theta_4^2)X - \theta_1^2\theta_2^2\theta_3^2 - \theta_1^2\theta_2^2\theta_4^2 - \theta_1^2\theta_3^2\theta_4^2 - \theta_2^2\theta_3^2\theta_4^2 - \theta_1^3\theta_2\theta_3\theta_4 - \theta_1\theta_2^3\theta_3\theta_4 - \theta_1\theta_2\theta_3^3\theta_4 - \theta_1\theta_2\theta_3\theta_4^3.$

Example : Let us consider the field $K = \mathbb{Q}(a, b, c, d)$ and the polynomial $P = X^4 + aX^3 + bX^2 + cX + d$. Let $G = D_8 =< (3,4), (1,3)(2,4), (1,4)(2,3) >$ and $F = X_1X_2 + X_3X_4$.
In this case,
$R_G(F, P) = X^3 - (\theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4)X^2 + (\theta_1^2\theta_2\theta_3 + \theta_1^2\theta_2\theta_4 + \theta_1^2\theta_3\theta_4 + \theta_1\theta_2^2\theta_3 + \theta_1\theta_2^2\theta_4 + \theta_1\theta_2\theta_3^2 + \theta_1\theta_2\theta_4^2 + \theta_1\theta_3^2\theta_4 + \theta_1\theta_3\theta_4^2 + \theta_2^2\theta_3\theta_4 + \theta_2\theta_3^2\theta_4 + \theta_2\theta_3\theta_4^2)X - \theta_1^2\theta_2^2\theta_3^2 - \theta_1^2\theta_2^2\theta_4^2 - \theta_1^2\theta_3^2\theta_4^2 - \theta_2^2\theta_3^2\theta_4^2 - \theta_1^3\theta_2\theta_3\theta_4 - \theta_1\theta_2^3\theta_3\theta_4 - \theta_1\theta_2\theta_3^3\theta_4 - \theta_1\theta_2\theta_3\theta_4^3$.

We now apply the fundamental theorem of symmetric polynomials to get $R_G(F, P) = X^3 - bX^2 + (ac - 4d)X - a^2d - c^2 + 4bd$.

Theorem

Let $P = X^4 + bX^2 + cX + d$ be an irreducible rational polynomial. Then we have,

1. $Gal(P) \subset D_8$ *if, and only if,* $X^3 - bX^2 - 4dX - c^2 + 4bd$ *has a rational root.*
2. $Gal(P) \subset V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if, and only if,* $X^6 - 6bX^5 + (13b^2 - 24d)X^4 + (-12b^3 + 96bd)X^3 + (4b^4 - 120b^2d + 144d^2)X^2 + (48b^3d - 288bd^2)X + 4b^3c^2 - 16b^4d + 27c^4 - 144bc^2d + 272b^2d^2 - 256d^3$ *has a rational root.*

Remark

When $P = \Psi_{(E,m)}$ of degree $n \geq \frac{m^2-m}{2}$, we have

$$\deg(R_G) = [S_n : G] > [S_n : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})] > \frac{\#S_{\frac{m^2-m}{2}}}{\#\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})} > \frac{(\frac{m^2-m}{2})!}{\#\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})} > \frac{2^{\frac{m^2-m}{2}}}{m^4}.$$

(Hyper-exponential, in practice only $m = 2, 3, 4$ work.)

Another method

Question : When does the Galois group of the field of l-torsion differs from its generic value ?
Answer : When one of the 4 extensions given below has smaller degree than its generic value.

$$K_4 = \mathbb{Q}(x_1, x_2, y_1, y_2) = \mathbb{Q}(E[l])$$
$$\Big|\ P_3 = y^2 - (x_2^3 + ax_2 + b)$$
$$K_3 = \mathbb{Q}(x_1, x_2, y_1)$$
$$\Big|\ P_2 = y^2 - (x_1^3 + ax_1 + b)$$
$$K_2 = \mathbb{Q}(x_1, x_2)$$
$$\Big|\ P_1 = \text{a factor of } \Psi \text{ of degree } \tfrac{l^2-l}{2}$$
$$K_1 = \mathbb{Q}(x_1)$$
$$\Big|\ P_0 = \Psi \text{ of degree } \tfrac{l^2-1}{2}$$
$$\mathbb{Q}$$

This is equivalent to testing whether $\Psi_{(E,l)}$ factorizes on $\mathbb{Q}$ or a factor of $\Psi_{(E,l)}$ factorizes on $\mathbb{Q}(x_1)$ or two polynomials of degree 2 factorize on appropriate fields.

Example :

Let $E : y^2 = x^3 + ax + b$ be a rational elliptic curve. Then $\Psi_3 = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$. We consider a partition of 4 of length 2.

- For $[2, 2]$, we write,

$$x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2 = (x^2 + e_2x + e_1)(x^2 + f_2x + f_1)$$

and equate the coefficients on both sides. We get a system of polynomial equations,

$$\begin{cases} e_2 + f_2 = 0 \\ e_2 f_2 + e_1 + f_1 = 2a \\ e_1 f_2 + e_2\, f_1 = 4b \\ e_1 f_1 = -1/3\, a^2 \end{cases} \Leftrightarrow \begin{cases} f_2 = -e_2 \\ f_1 = 2a + e_2 f_2 - e_1 \\ e_1\, \left(e_2{}^2 + 2\,a - e_1\right) + \frac{1}{3}\, a^2 = 0. \\ e_2{}^6 + 4\,a e_2{}^4 + \frac{16}{3}\, e_2{}^2 a^2 - 16\, b^2 = 0 \end{cases}$$

Thus if $3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$ does not have a rational root, then the factorization pattern of Ψ_3 is not $[2, 2]$.

Algorithm 1 (CONDITIONS)
INPUT : $F \in \mathbb{Q}[X]$ and $P \in \mathbb{Q}[X]/F$ of degree n.
OUTPUT : Necessary conditions under which P has a certain factorization pattern on $\mathbb{Q}[X]/F$.

1. **For** every partition of n, **create a system of equations as shown in the example.**
2. **Solve it to get polynomial conditions.**

Algorithm 2
INPUT : E a rational elliptic curve and l a prime.
OUTPUT : Necessary conditions under which $\mathrm{Gal}(\mathbb{Q}(E[l]))$ is non-generic.

1. **For** $i \in \{1, 2, 3, 4\}$
2. $F_i = \mu(K_{i-1})$ (absolute polynomial of K_{i-1}.)
3. **CONDITIONS**(F_i, P_i)

Case $l = 3$

Theorem

Let $E : y^2 = x^3 + ax + b$ be a rational elliptic curve with $ab \neq 0$. Let Ψ_3 be its 3-division polynomial and Δ its discriminant. Then we have,

Fact. Pattern of Ψ_3	Condition(s)	$\#G_E(3)$
$(1,1,2)$	C_1 and a 3-torsion point	2
$(1,1,2)$	C_1	4
$(1,3)$	$C_{2'}$ or [C_2 and a 3-torsion point]	6
$(1,3)$	C_2	12
$(2,2)$	C_3	8
(4)	C_4	16

$C_1 = 27\,x^{12} + 594\,ax^{10} + 972\,bx^9 + 4761\,a^2x^8 + 14256\,abx^7 + \left(17100\,a^3 + 15120\,b^2\right)x^6 + 61992\,a^2bx^5 + 3\,a\left(11519\,a^3 + 52704\,b^2\right)x^4 + 432\,b\left(293\,a^3 + 972\,b^2\right)x^3 + 486\,a^2\left(59\,a^3 + 312\,b^2\right)x^2 + 324\,ab\left(587\,a^3 + 3456\,b^2\right)x - 5329\,a^6 + 162432\,b^2a^3 + 1492992\,b^4$

$C_{2'} = x^{16} - 24bx^{12} + 6\Delta x^8 - 3\Delta^2$

$C_2 = 3x^4 + 6ax^2 + 12bx - a^2$

$C_3 = 3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$

$C_4 = x^3 - 2\Delta$ *i.e. the j of E is a cube.*

From conditions to families of curves

1. Let us assume that a family is given by the condition that $\exists x \in \mathbb{Q}$ such that $C(x, a, b) = 0$.
2. Replace a and b in C by random polynomials in t. We then compute the genus of $C(x, t)$.
3. Compute genus g of C.
   - If $g \geq 2$, only finitely many solutions.
   - If $g = 0$, try to find a rational point and parametrize.
   - If $g = 1$, try to find a rational point and put C in Weierstrass form and compute the rank r.
     - If $r = 0$, only finitely many points.
     - If $r > 0$, compute generators.

From conditions to families of curves : Example

Let $E : y^2 = x^3 + ax + b$ be a rational elliptic curve. We saw that if Ψ_3 factorizes into two quadratic factors then $C = 3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$ has a rational root.
If we put $b = 2a$, we get $C = 3x^6 + 12ax^4 + 16a^2x^2 - 192a^2$.
This curve is of genus 0 thus we get a parametrization

$$a(t) = \frac{27t^3(19t+2)^3}{(242t^2+54t+3)(271t^2+57t+3)^2} \text{ and } b(t) = 2a(t).$$

Case $l = 3$

Theorem

Let $E : y^2 = x^3 + ax + b$ be a rational elliptic curve with $ab \neq 0$. Let Ψ_3 be its 3-division polynomial and Δ its discriminant. Then we have,

Fact. Pattern of Ψ_3	Condition(s)	$\#G_E(3)$
$(1,1,2)$	C_1 and a 3-torsion point	2
$(1,1,2)$	C_1	4
$(1,3)$	$C_{2'}$ or [C_2 and a 3-torsion point]	6
$(1,3)$	C_2	12
$(2,2)$	C_3	8
(4)	C_4	16

$$C_1 = 27\,x^{12} + 594\,ax^{10} + 972\,bx^9 + 4761\,a^2x^8 + 14256\,abx^7 + \left(17100\,a^3 + 15120\,b^2\right)x^6 + 61992\,a^2bx^5 + 3\,a\left(11519\,a^3 + 52704\,b^2\right)x^4 + 432\,b\left(293\,a^3 + 972\,b^2\right)x^3 + 486\,a^2\left(59\,a^3 + 312\,b^2\right)x^2 + 324\,ab\left(587\,a^3 + 3456\,b^2\right)x - 5329\,a^6 + 162432\,b^2a^3 + 1492992\,b^4$$

$$C_{2'} = x^{16} - 24bx^{12} + 6\Delta x^8 - 3\Delta^2$$

$$C_2 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$C_3 = 3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$$

$$C_4 = x^3 - 2\Delta$$

In all the above cases, we obtained $g = 0$.

Computing the generic valuation of a family

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(t)(E_t[l])/\mathbb{Q}(t)) & \xrightarrow{\text{eval}} & \mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) \\ \downarrow \rho & & \downarrow \rho \\ \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}) & \xrightarrow{=} & \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}) \end{array}$$

As the families are constructed to have $\mathrm{Gal}(\mathbb{Q}(t)(E_t[l])/\mathbb{Q}(t)) \subset H$ where H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$, it suffices to find one value of $t \in \mathbb{Q}$ for which $\#\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) = \#H$ to determine $\mathrm{Gal}(\mathbb{Q}(t)(E_t[l])/\mathbb{Q}(t))$.

Valuations $l = 3$

Theorem

Let $E : y^2 = x^3 + ax + b$, $ab \neq 0$ be a rational elliptic curve. Then the generic average valuation $\overline{val}_3(E(\mathbb{F}_p))$ is 0.68, except when one the following cases occurs.

Conditions	*A parametrization*	*Example* (a, b)	*Valuation*
C_1 *and a 3-torsion point*	a, b *complicated.*	$(5805, -285714)$	*2.06*
C_1	a, b *complicated.*	$(284445, 97999902)$	*1.41*
C_2 *and a 3-torsion point*	$a = 3t^2, b = -\frac{243t^6+162t^4-9t^2}{36}$	$(3, -11)$	*1.68*
$C_{2'}$	$a = \frac{-192\,t^3-254803968}{t^4}, b = \frac{-t^6-5308416\,t^3-4696546738176}{3t^6}$	$(-254804160, -\frac{4696552046593}{3})$	*1.68*
C_2	$a = \frac{-36t(t+2)^3}{(t^2+4t+1)^2}, b = 2a$	$(\frac{-4608}{169}, \frac{-9216}{169})$	*1.22*
C_3	$a = \frac{27t^3(19t+2)^3}{(242t^2+54t+3)(271t^2+57t+3)^2}, b = 2a$	$(\frac{250047}{32758739}, \frac{500094}{32758739})$	*1.08*
C_4	$a = \frac{216}{(t^3-8)}, b = 2a$	$(\frac{-216}{7}, \frac{-432}{7})$	*0.54*

$$C_1 = 27\,x^{12} + 594\,ax^{10} + 972\,bx^9 + 4761\,a^2x^8 + 14256\,abx^7 + \left(17100\,a^3 + 15120\,b^2\right)x^6 + 61992\,a^2bx^5 + 3\,a\left(11519\,a^3 + 52704\,b^2\right)x^4 + 432\,b\left(293\,a^3 + 972\,b^2\right)x^3 + 486\,a^2\left(59\,a^3 + 312\,b^2\right)x^2 + 324\,ab\left(587\,a^3 + 3456\,b^2\right)x - 5329\,a^6 + 162432\,b^2a^3 + 1492992\,b^4$$

$$C_{2'} = x^{16} - 24bx^{12} + 6\Delta x^8 - 3\Delta^2$$

$$C_2 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$C_3 = 3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$$

$$C_4 = x^3 - 2\Delta$$

Goal

- **INPUT :** A number field K, a prime l and $a(\alpha,\beta)$ and $b(\alpha,\beta)$.
- **OUTPUT :** Complete list of equations of negligible density necessary for non-generic valuation.

Popular parametrizations

- Montgomery $By^2 = x^3 + Ax^2 + x$ or $y^2 = x^3 + \frac{3-A^2}{3B^2}x + \frac{2A^3-3A}{27B^3}$
- Edwards $ax^2 + y^2 = 1 + dx^2y^2$ or $y^2 = x^3 + \frac{3-\alpha^2}{3\beta^2}x + \frac{2\alpha^3-3\alpha}{27\beta^3}$ where $\alpha = -2\frac{a+d}{a-d}$ and $\beta = \frac{4}{a-d}$.
- Hessian $y^2 + axy + by = x^3$ or $y^2 = x^3 + (-27a^4 + 648ab)x + (54a^6 - 1944a^3b + 11664b^2)$.
- etc...

Valuation $m = 4$, Montgomery curve

Theorem

Let $E : By^2 = x^3 + Ax^2 + x$ be a rational elliptic curve with $B(A^2 - 4) \neq 0$. Then the generic average valuation $\overline{val}_2(E(\mathbb{F}_p))$ is 3.33, except,

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

Fact. Pat. of Ψ	Condition(s)	$\#G_E(4)$	Valuation
$(2,2)$	C_2 $(A = -2\frac{t^4-4}{t^4+4})$	4	3.40
(4)	$\frac{A\pm 2}{B} = \pm\square$ or $\frac{4B^2}{A^2-4} = -t^4$	8	3.68

$C_2 = x^4 - 4Ax^3 + (4A^2 + 8)x^2 - 16Ax + 4A^2$

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

Fact. Pat. of Ψ	Condition(s)	$\#G_E(4)$	Valuation
$(1,1,2)$	$A = \frac{t^4+24t^2+16}{4(t^2+4)t}$ and $B = -t(t^2+4)\square$	2	4.82
$(1,1,2)$	$A = \frac{t^4+24t^2+16}{4(t^2+4)t}$	4	3.91
$(2,2)$	$A = \frac{t^2+4}{2t}$ and $\frac{A\pm 2}{B} = \square$	4	4.42
$(2,2)$	$A = \frac{t^2+4}{2t}$	8	3.78

Thank you !