ELLIPTIC CURVES AN ELEMENTARY APPROACH

FRANCESCO PAPPALARDI

APRIL 13TH 2017

Université Félix Houphouët Boigny
Théorie Algébrique des nombres et applications
notamment à la cryptographie
Ecole CIMPA-ICTP, Abidjan 2017

The Discriminant of an Equation

The condition of absence of singular points in terms of a_1, a_2, a_3, a_4, a_6

The *discriminant* of a Weierstraß equation over any field K is

$$D_E := -\Big(-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16 a_1 a_2^2 a_3 a_4 + 36 a_1^2 a_3^2 a_4 - a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16 a_2^2 a_4^2 + 96 a_1 a_3 a_4^2 + 64 a_4^3 + a_1^6 a_6 + 12 a_1^4 a_2 a_6 + 48 a_1^2 a_2^2 a_6 + 64 a_2^3 a_6 - 36 a_1^3 a_3 a_6 - 144 a_1 a_2 a_3 a_6 - 72 a_1^2 a_4 a_6 - 288 a_2 a_4 a_6 + 432 a_6^2\Big)$$

Note

E is *non singular* if and only if $D_E \neq 0$

The Weierstraß equation

After a suitable affine transformation we can assume that E/K has a *Special Weierstraß* equation:

Example (Classification)

E	$p = \text{char } K$	D_E
$y^2 = x^3 + Ax + B$	≥ 5 or $= 0$	$-16(4A^3 + 27B^2)$
$y^2 + xy = x^3 + a_2x^2 + a_6$	2	a_6^2
$y^2 + a_3y = x^3 + a_4x + a_6$	2	a_3^4
$y^2 = x^3 + Ax^2 + Bx + C$	3	$-16(4A^3C - A^2B^2 - 18ABC + 4B^3 + 27C^2)$

Definition (An elliptic curve is a non singular Weierstraß equation (i.e. $D_E \neq 0$))

Note: If $p \geq 3$, $D_E \neq 0 \Leftrightarrow x^3 + Ax^2 + Bx + C$ has no double root

Formulas for Addition on E (Summary)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K) \setminus \{\infty\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $2y_1 + a_1x_1 + a_3 = 0$ $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$
  - $2y_1 + a_1x_1 + a_3 \neq 0$

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x + a_3}, \nu = -\frac{a_3y_1 + x_1^3 - a_4x_1 - 2a_6}{2y_1 + a_1x_1 + a_3}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - a_1\lambda - a_2 - x_1 - x_2, -\lambda^3 - a_1^2\lambda + (\lambda + a_1)(a_2 + x_1 + x_2) - a_3 - \nu)$$

Formulas for Addition on E (Summary for special equation)

$$E : y^2 = x^3 + Ax + B$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K) \setminus \{\infty\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2 \Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $y_1 = 0 \Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$
  - $y_1 \neq 0$

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu)$$

Fact 1: the number of $\overline{\mathbb{F}}_q$–isomorphism classes of elliptic curves over $\mathbb{F}_q$ is

$$q$$

Fact 2: the number of $\mathbb{F}_q$–isomorphism classes of elliptic curves over $\mathbb{F}_q$ is

$$2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$$

q	$2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$
2	5
3	8
5	12
7	18

Theorem (Hasse)

Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

So $\#E(\mathbb{F}_q) \in [(\sqrt{q} - 1)^2, (\sqrt{q} + 1)^2]$ the *Hasse interval* $\mathcal{I}_q$

Example (Hasse Intervals)

q	$\mathcal{I}_q$
2	$\{1, 2, 3, 4, 5\}$
3	$\{1, 2, 3, 4, 5, 6, 7\}$
4	$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
5	$\{2, 3, 4, 5, 6, 7, 8, 9, 10\}$
7	$\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
8	$\{4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
9	$\{4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
11	$\{6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$
13	$\{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}$
16	$\{9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25\}$
17	$\{10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$

Example (Hasse Intervals)

q	$\mathcal{I}_q$
2	$\{1, 2, 3, 4, 5\}$
3	$\{1, 2, 3, 4, 5, 6, 7\}$
4	$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
5	$\{2, 3, 4, 5, 6, 7, 8, 9, 10\}$
7	$\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
8	$\{4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
9	$\{4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
11	$\{6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$
13	$\{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}$
16	$\{9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25\}$
17	$\{10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$
19	$\{12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28\}$
23	$\{15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33\}$
25	$\{16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36\}$
27	$\{18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38\}$
29	$\{20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40\}$
31	$\{21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43\}$
32	$\{22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44\}$

EXAMPLE: Elliptic curves over $\mathbb{F}_2$

Groups of points of curves over $\mathbb{F}_2$

E	$E(\mathbb{F}_2)$	$E(\mathbb{F}_2)$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	C_2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	C_4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	C_5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	C_3

Note: each $C_i, i = 1, \ldots, 5$ is represented by a curve $/\mathbb{F}_2$

EXAMPLE: Elliptic curves over $\mathbb{F}_3$

Groups of points of curves over $\mathbb{F}_3$

i	E_i	$E_i(\mathbb{F}_3)$	$E_i(\mathbb{F}_3)$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	C_4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	$C_2 \oplus C_2$
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	C_7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	$\{1\}$
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	C_3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	C_6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	C_5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	C_2

Note: each $C_i, i = 1, \ldots, 7$ is represented by a curve $/\mathbb{F}_3$

EXAMPLE: Elliptic curves over $\mathbb{F}_5$

$(12\ E/\mathbb{F}_5)$ $(2 \le \#E(\mathbb{F}_5) \le 10$, 8 values$)$ $\forall n \in \{2,3,5,7,10\} \exists! E/\mathbb{F}_5 : \#E(\mathbb{F}_5) \cong C_n$

Example (Curves with $\#E(\mathbb{F}_5) \in \{4,6,8,9\}$)

- $E_1 : y^2 = x^3 + 1$ and $E_2 : y^2 = x^3 + 2$ order 6

  $\begin{cases} x \longleftarrow 2x \\ y \longleftarrow \sqrt{3}y \end{cases}$

  $$E_1 \cong_{\mathbb{F}_{25}} E_2 \quad (j(E_1) = j(E_2) = 0)$$

- $E_3 : y^2 = x^3 + x$ and $E_4 : y^2 = x^3 + x + 2$ order 4

  $$E_3(\mathbb{F}_5) \cong C_2 \oplus C_2\ (j(E_3) = 1728 = 3) \qquad E_4(\mathbb{F}_5) \cong C_4\ (j(E_4) = 1)$$

- $E_5 : y^2 = x^3 + 4x$ and $E_6 : y^2 = x^3 + 4x + 1$ order 8

  $$E_5(\mathbb{F}_5) \cong C_2 \oplus C_4\ (j(E_5) = 3) \qquad E_6(\mathbb{F}_5) \cong C_8\ (j(E_6) = 1)$$

- $E_7 : y^2 = x^3 + x + 1$ order 9 and $E_7(\mathbb{F}_5) \cong C_9\ (j(E_7) = 2)$

Group Structure

Theorem (Classification of finite abelian groups)

If G is abelian and finite, $\exists n_1, \ldots, n_k \in \mathbb{N}^{>1}$ *such that*

1. $n_1 \mid n_2 \mid \cdots \mid n_k$
2. $G \cong C_{n_1} \oplus \cdots \oplus C_{n_k}$

Furthermore $n_1, \ldots, n_k$ *(Group Structure) are unique*

Theorem (Structure Theorem for Elliptic curves over a finite field)

Let $E/\mathbb{F}_q$ be an elliptic curve, then

$$E(\mathbb{F}_q) \cong C_n \oplus C_{nk} \qquad \exists n, k \in \mathbb{N}^{>0}.$$

(i.e. $E(\mathbb{F}_q)$ is either cyclic ($n = 1$) or the product of 2 cyclic groups)

The j-invariant

Let $E/K : y^2 = x^3 + Ax + B$, $p \geq 5$ and $D_E := 4A^3 + 27B^2$.

Definition

The j–invariant of E is $j = j(E) = 1728\frac{4A^3}{4A^3+27B^2}$

Definition

Let $u \in K^*$. The elliptic curve $E_u : y^2 = x^3 + u^2Ax + u^3B$ is called the twist of E by u

The j-invariant (2)

Properties of j–invariants

1. $j(E) = j(E_u), \forall u \in K^*$
2. $j(E'/K) = j(E''/K) \;\Rightarrow\; \exists u \in \overline{K}^*$ s.t. $E'' = E'_u$
3. $j \neq 0, 1728 \Rightarrow E : y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}, j(E) = j$
4. $j = 0 \;\Rightarrow\; E : y^2 = x^3 + B, \quad j = 1728 \;\Rightarrow\; E : y^2 = x^3 + Ax$
5. $j : K \longleftrightarrow \{\bar{K}$–affinely equivalent classes of $E/K\}$.
6. $p = 2, 3$ different definition
7. E and E_μ are $\mathbb{F}_q[\sqrt{\mu}]$–affinely equivalent
8. $\#E(\mathbb{F}_{q^2}) = \#E_\mu(\mathbb{F}_{q^2})$
9. usually $\#E(\mathbb{F}_q) \neq \#E_\mu(\mathbb{F}_q)$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Note

- the number of points of order 2 in $E(\mathbb{F}_q)$ equals the number of roots of $X^3 + Ax^2 + Bx + C$ in $\mathbb{F}_q$
- roots are distinct since discriminant $D_E \neq 0$

Determining points of order 2 (continues)

Definition

2–torsion points

$$E[2] = \{P \in E(\overline{\mathbb{F}_q}) : 2P = \infty\}.$$

FACTS:

$$E[2] \cong \begin{cases} C_2 \oplus C_2 & \text{if } p > 2 \\ C_2 & \text{if } p = 2, E : y^2 + xy = x^3 + a_4x + a_6 \\ \{\infty\} & \text{if } p = 2, E : y^2 + a_3y = x^3 + a_2x^2 + a_6 \end{cases}$$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu) \text{where } \lambda = \frac{3x_1^2+A}{2y_1}, \nu = -\frac{x_1^3-Ax_1-2B}{2y_1}.$$

$$P \text{ has order } 3 \iff x_{2P} = \lambda^2 - 2x_1 = x_1$$

Substituting λ,

$$x_{2P} - x_1 = \frac{-3x_1^4-6Ax_1^2-12Bx_1+A^2}{4(x_1^3+Ax_1+4B)} = 0$$

Determining points of order 3

Note (Conclusions)

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ called the 3rd *division* polynomial
- $(x_1, y_1) \in E(\mathbb{F}_q)$ has order 3 $\quad \Rightarrow \psi_3(x_1) = 0$
- $E(\mathbb{F}_q)$ has at most 8 points of order 3
- If $p \neq 3$, $E[3] := \{P \in E(\overline{\mathbb{F}_q}) : 3P = \infty\} \cong C_3 \oplus C_3$
- If $p = 3$, $E : y^2 = x^3 + Ax^2 + Bx + C$ and $P = (x_1, y_1)$ has order 3, then
  1. $Ax_1^3 + AC - B^2 = 0$
  2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Determining points of order 3 (continues)

FACTS:

$$E[3] \cong \begin{cases} C_3 \oplus C_3 & \text{if } p \neq 3 \\ C_3 & \text{if } p = 3, E : y^2 = x^3 + Ax^2 + Bx + C, A \neq 0 \\ \{\infty\} & \text{if } p = 3, E : y^2 = x^3 + Bx + C \end{cases}$$

Example: inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$	j
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\{\infty, (0, \pm 3), (-1, \pm 1), (5, \pm 1), (3, \pm 1)\}$	$C_3 \oplus C_3$	0
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9	3
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9	3
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9	3

Note

Let $E : y^2 = x^3 + 3x + 2$ and $E' : y^2 = x^3 + 5x + 2$. Then $E' \cong_{\mathbb{F}_{7^2}} E$. They are twists but not $\mathbb{F}_7$–isomorphic

Determining points of order 3 (continues)

One count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$

Example (A curve over $\mathbb{F}_4 = \mathbb{F}_2(\xi), \xi^2 = \xi + 1$; $E : y^2 + y = x^3$)

We know $E(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\} \subset E(\mathbb{F}_4)$.

$E(\mathbb{F}_4) = \{\infty, (0,0), (0,1), (1,\xi), (1,\xi+1), (\xi,\xi), (\xi,\xi+1), (\xi+1,\xi), (\xi+1,\xi+1)\}$

$$\psi_3(x) = x^4 + x = x(x+1)(x+\xi)(x+\xi+1) \Rightarrow E(\mathbb{F}_4) \cong C_3 \oplus C_3$$

Determining points of order (dividing) m

Definition (m–torsion point)

Let E/K and let $\overline{K}$ an *algebraic closure of* K.

$$E[m] = \{P \in E(\overline{K}) : \; mP = \infty\}$$

Theorem (Structure of Torsion Points)

Let E/K *and* $m \in \mathbb{N}$. *If* $p = \mathrm{char}(K) \nmid m$,

$$E[m] \cong C_m \oplus C_m$$

If $m = p^r m'$, $p \nmid m'$,

$$E[m] \cong C_m \oplus C_{m'} \qquad \text{or} \qquad E[m] \cong C_{m'} \oplus C_{m'}$$

$$E/\mathbb{F}_p \text{ is called } \begin{cases} \textit{ordinary} & \text{if } E[p] \cong C_p \\ \textit{supersingular} & \text{if } E[p] = \{\infty\} \end{cases}$$

Group Structure of $E(\mathbb{F}_q)$

Corollary

Let $E/\mathbb{F}_q$. $\exists n, k \in \mathbb{N}$ *are such that*

$$E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$$

Proof.

From classification Theorem of finite abelian group

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$$

with $n_i | n_{i+1}$ for $i \geq 1$.

Hence $E(\mathbb{F}_q)$ contains n_1^r points of order dividing n_1. From *Structure of Torsion Theorem*, $\#E[n_1] \leq n_1^2$. So $r \leq 2$ $\square$

The division polynomials

Definition (Division Polynomials of $E : y^2 = x^3 + Ax + B$ ($p > 3$))

$$\begin{aligned}
\psi_0 &= 0\\
\psi_1 &= 1\\
\psi_2 &= 2y\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)\\
&\vdots\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{for } m \geq 2\\
\psi_{2m} &= \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3
\end{aligned}$$

The polynomial $\psi_m \in \mathbb{Z}[x, y]$ is called the m^{th} *division polynomial*

The division polynomials 2

FACTS:

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $\psi_m^2 = m^2 x^{m^2-1} + \cdots$

Remark.

- $E[2m+1] \setminus \{\infty\} = \{(x,y) \in E(\bar{K}) : \ \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x,y) \in E(\bar{K}) : \ y^{-1}\psi_{2m}(x) = 0\}$

Example

$\psi_4(x) = 2y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4BAx - A^3 - 8B^2)$

$\psi_5(x) = 5x^{12} + 62Ax^{10} + 380Bx^9 - 105A^2x^8 + 240BAx^7 + \left(-300A^3 - 240B^2\right)x^6 - 696BA^2x^5 + \left(-125A^4 - 1920B^2A\right)x^4$
$+ \left(-80BA^3 - 1600B^3\right)x^3 + \left(-50A^5 - 240B^2A^2\right)x^2 + \left(-100BA^4 - 640B^3A\right)x + \left(A^6 - 32B^2A^3 - 256B^4\right)$

$\psi_6(x) = 2y(6x^{16} + 144Ax^{14} + 1344Bx^{13} - 728A^2x^{12} + \left(-2576A^3 - 5376B^2\right)x^{10} - 9152BA^2x^9 + \left(-1884A^4 - 39744B^2A\right)x^8$
$+ \left(1536BA^3 - 44544B^3\right)x^7 + \left(-2576A^5 - 5376B^2A^2\right)x^6 + \left(-6720BA^4 - 32256B^3A\right)x^5$
$+ \left(-728A^6 - 8064B^2A^3 - 10752B^4\right)x^4 + \left(-3584BA^5 - 25088B^3A^2\right)x^3 + \left(144A^7 - 3072B^2A^4 - 27648B^4A\right)x^2$
$+ \left(192BA^6 - 512B^3A^3 - 12288B^5\right)x + \left(6A^8 + 192B^2A^5 + 1024B^4A^2\right))$

Theorem ($E : Y^2 = X^3 + AX + B$ elliptic curve, $P = (x, y) \in E$)

$$m(x, y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x, y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x, y)}{\psi_m^3(x, y)}\right)$$

where

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$$

FACTS:

- $\phi_m(x) = x^{m^2} + \cdots \qquad \psi_m(x)^2 = m^2 x^{m^2-1} + \cdots \in \mathbb{Z}[x]$
- $\omega_{2m+1} \in y\mathbb{Z}[x]$, $\omega_{2m} \in \mathbb{Z}[x]$
- $\frac{\omega_m(x,y)}{\psi_m^3(x,y)} \in y\mathbb{Z}(x)$
- $\gcd(\psi_m^2(x), \phi_m(x)) = 1$
- $E[2m+1] \setminus \{\infty\} = \{(x,y) \in E(\overline{K}) : \ \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x,y) \in E(\overline{K}) : \ y^{-1}\psi_{2m}(x) = 0\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

(i) $\gcd(a, p) = 1$;

(ii) *n even and one of the following is satisfied:*

1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;
3. $p \not\equiv 1 \pmod 4$, *and* $a = 0$;

(iii) *n is odd, and one of the following is satisfied:*

1. $p = 2$ *or* 3, *and* $a = \pm p^{(n+1)/2}$;
2. $a = 0$.

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Rück)

Suppose N is a possible order of an elliptic curve $/\mathbb{F}_q$, $q = p^n$. *Write*

$$N = p^e n_1 n_2, \quad p \nmid n_1 n_2 \quad \text{and} \quad n_1 \mid n_2 \text{ (possibly } n_1 = 1).$$

There exists $E/\mathbb{F}_q$ *s.t.*

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. $n_1 = n_2$ *in the case (ii).1 of Waterhouse's Theorem;*
2. $n_1 | q - 1$ *in all other cases of Waterhouse's Theorem.*

Example

- If $q = p^{2n}$ and $\#E(\mathbb{F}_q) = q + 1 \pm 2\sqrt{q} = (p^n \pm 1)^2$, then
$$E(\mathbb{F}_q) \cong C_{p^n \pm 1} \oplus C_{p^n \pm 1}.$$
- Let $N = 100$ and $q = 101 \Rightarrow \exists E_1, E_2, E_3, E_4/\mathbb{F}_{101}$ s.t.
$$E_1(\mathbb{F}_{101}) \cong C_{10} \oplus C_{10} \qquad E_2(\mathbb{F}_{101}) \cong C_2 \oplus C_{50}$$
$$E_3(\mathbb{F}_{101}) \cong C_5 \oplus C_{20} \qquad E_4(\mathbb{F}_{101}) \cong C_{100}$$

Further Reading...

- Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.
- J. W. S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.
- John E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.
- Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.
- Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.
- Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
- Joseph H. Silverman and John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
- Lawrence C. Washington, Elliptic curves: Number theory and cryptography, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.
- Horst G. Zimmer, Computational aspects of the theory of elliptic curves, Number theory and applications (Banff, AB, 1988) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 279–324.