



Lecture 2

Elliptic curves over finite fields

The Group structure

Research School: Algebraic curves over finite fields

CIMPA-ICTP-UNESCO-MESR-MINECO-PHILIPPINES

University of the Philippines Diliman, July 24, 2013

[Reminder from Monday](#)

[the \$j\$ -invariant](#)

[Points of finite order](#)

Points of order 2

Points of order 3

Points of finite order

The group structure

[sketch of proof](#)

[Important Results](#)

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

[Further reading](#)

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre



Definition (Elliptic curve)

An elliptic curve over a field K is the data of a non singular Weierstraß equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K$$

If $p = \text{char } K > 3$,

$$\begin{aligned} \Delta_E := & \frac{1}{2^4} (-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16a_1 a_2^2 a_3 a_4 + 36a_1^2 a_3^2 a_4 \\ & - a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16a_2^2 a_4^2 + 96a_1 a_3 a_4^2 + 64a_4^3 + \\ & a_1^6 a_6 + 12a_1^4 a_2 a_6 + 48a_1^2 a_2^2 a_6 + 64a_2^3 a_6 - 36a_1^3 a_3 a_6 \\ & - 144a_1 a_2 a_3 a_6 - 72a_1^2 a_4 a_6 - 288a_2 a_4 a_6 + 432a_6^2) \end{aligned}$$

Reminder from Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading



After applying a suitable affine transformation we can always assume that E/K has a Weierstraß equation of the following form

Example (Classification ($p = \text{char } K$))

E	p	Δ_E
$y^2 = x^3 + Ax + B$	≥ 5	$4A^3 + 27B^2$
$y^2 + xy = x^3 + a_2x^2 + a_6$	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	$4A^3C - A^2B^2 - 18ABC + 4B^3 + 27C^2$

Let E/\mathbb{F}_q elliptic curve, $\infty := [0, 1, 0]$. Set

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

Reminder from Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

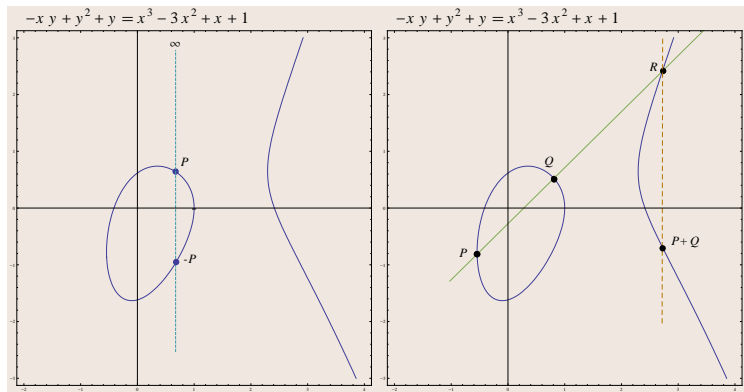
Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

If $P, Q \in E(\mathbb{F}_q)$, $r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q, \end{cases}$
 $r_{P,\infty} : \text{vertical line through } P$



$$r_{P,\infty} \cap E(\mathbb{F}_q) = \{P, \infty, P'\}$$

$$\leadsto -P := P'$$

$$r_{P,Q} \cap E(\mathbb{F}_q) = \{P, Q, R\}$$

$$\leadsto P +_E Q := -R$$





Theorem

The addition law on E/K (K field) has the following properties:

$$(a) \quad P +_E Q \in E \qquad \forall P, Q \in E$$

$$(b) \quad P +_E \infty = \infty +_E P = P \qquad \forall P \in E$$

$$(c) \quad P +_E (-P) = \infty \qquad \forall P \in E$$

$$(d) \quad P +_E (Q +_E R) = (P +_E Q) +_E R \qquad \forall P, Q, R \in E$$

$$(e) \quad P +_E Q = Q +_E P \qquad \forall P, Q \in E$$

So $(E(\bar{K}), +_E)$ is an abelian group.

Remark:

If $E/K \Rightarrow \forall L, K \subseteq L \subseteq \bar{K}, E(L)$ is an abelian group.

$$-P = -(x_1, y_1) = (x_1, -a_1 x_1 - a_3 - y_1)$$

Reminder from
Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

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 $P_1 \neq P_2$

- $x_1 = x_2$
- $x_1 \neq x_2$

$$\Rightarrow P_1 +_E P_2 = \infty$$

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

- If $P_1 = P_2$

- $2y_1 + a_1x + a_3 = 0$
- $2y_1 + a_1x + a_3 \neq 0$

$$\Rightarrow P_1 +_E P_2 = 2P_1 = \infty$$

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

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)



Reminder from
Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

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

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

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$

- $x_1 = x_2$
- $x_1 \neq x_2$

$$\Rightarrow P_1 +_E P_2 = \infty$$

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

- If $P_1 = P_2$

- $y_1 = 0$
- $y_1 \neq 0$

$$\Rightarrow P_1 +_E P_2 = 2P_1 = \infty$$

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

Then

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

Finite fields

- 1 $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ is the prime field;
- 2 \mathbb{F}_q is a finite field with $q = p^n$ elements;
- 3 $\mathbb{F}_q = \mathbb{F}_p[\xi]$, $f(\xi) = 0$, $f \in \mathbb{F}_p[X]$ irreducible, $\partial f = n$;
- 4 $\mathbb{F}_4 = \mathbb{F}_2[\xi]$, $\xi^2 = 1 + \xi$;
- 5 $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, $\alpha^3 = \alpha + 1$ but also $\mathbb{F}_8 = \mathbb{F}_2[\beta]$, $\beta^3 = \beta^2 + 1$,
($\beta = \alpha^2 + 1$);
- 6 $\mathbb{F}_{101^{101}} = \mathbb{F}_{101}[\omega]$, $\omega^{101} = \omega + 1$

Algebraic Closure of \mathbb{F}_q

- 1 $\forall n \in \mathbb{N}$, we fix an \mathbb{F}_{q^n}
- 2 We also require that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if $n \mid m$
- 3 We let $\overline{\mathbb{F}}_q = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{q^n}$
- 4 $\overline{\mathbb{F}}_q$ is *algebraically closed*

If $F(x, y) \in \mathbb{F}_q[x, y]$ a point of the curve $F = 0$, means $(x_0, y_0) \in \overline{\mathbb{F}}_q^2$ s.t. $F(x_0, y_0) = 0$.



The j -invariant

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

$$\begin{cases} x \longleftarrow u^{-2}x \\ y \longleftarrow u^{-3}y \end{cases} \quad u \in K^* \Rightarrow E \longrightarrow E_u : y^2 = x^3 + u^4Ax + u^6B$$

Definition

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

Properties of j -invariants

- 1 $j(E) = j(E_u), \forall u \in K^*$
- 2 $j(E'/K) = j(E''/K) \Rightarrow \exists u \in \bar{K}^*$ s.t. $E'' = E'_u$
if $K = \mathbb{F}_q$ can take $u \in \mathbb{F}_{q^{12}}$
- 3 $j \neq 0, 1728 \Rightarrow E : y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}, j(E) = j$
- 4 $j = 0 \Rightarrow E : y^2 = x^3 + B, j = 1728 \Rightarrow E : y^2 = x^3 + Ax$
- 5 $j : K \longleftrightarrow \{\bar{K}\text{-affinely equivalent classes of } E/K\}.$
- 6 $p = 2, 3$ different definition



Examples of j invariants

From monday $E_1 : y^2 = x^3 + 1$ and $E_2 : y^2 = x^3 + 2$

$$\#E_1(\mathbb{F}_5) = \#E_2(\mathbb{F}_5) = 6 \quad \text{and} \quad j(E_1) = j(E_2) = 0$$

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

E_1 and E_2 affinely equivalent
over $\mathbb{F}_5[\sqrt{3}] = \mathbb{F}_{25}$ (*twists*)

Definition (twisted curve)

Let $E/\mathbb{F}_q : y^2 = x^3 + Ax + B, \mu \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$.

$$E_\mu : y^2 = x^3 + \mu^2 Ax + \mu^3 B$$

is called **twisted curve**.

Exercise: prove that

- $j(E) = j(E_\mu)$
- E and E_μ are $\mathbb{F}_q[\sqrt{\mu}]$ -affinely equivalent
- $\#E(\mathbb{F}_{q^2}) = \#E_\mu(\mathbb{F}_{q^2})$
- 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 $\Delta_E \neq 0$
- $E(\mathbb{F}_{q^6})$ has always 3 points of order 2 if E/\mathbb{F}_q
- $E[2] := \{P \in E(\bar{\mathbb{F}}_q) : 2P = \infty\} \cong C_2 \oplus C_2$



Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3y = x^3 + a_2x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

Absurd ($a_3 = 0$) and there are no points of order 2.

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4x + a_6$

$$-P = (x_1, x_1 + y_1) = (x_1, y_1) = P \implies x_1 = 0, y_1^2 = a_6$$

So there is exactly one point of order 2 namely $(0, \sqrt{a_6})$

Definition

2-torsion points

$$E[2] = \{P \in E : 2P = \infty\}.$$

In conclusion

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





Each curve $/\mathbb{F}_2$ has cyclic $E(\mathbb{F}_2)$.

E	$E(\mathbb{F}_2)$	$ E(\mathbb{F}_2) $
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0, 1)\}$	2
$y^2 + xy = x^3 + 1$	$\{\infty, (0, 1), (1, 0), (1, 1)\}$	4
$y^2 + y = x^3 + x$	$\{\infty, (0, 0), (0, 1), (1, 0), (1, 1)\}$	5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0, 0), (0, 1)\}$	3

- $E_1 : y^2 = x^3 + x$
 $E_2 : y^2 = x^3 - x$

$$E_1(\mathbb{F}_3) \cong C_4 \quad \text{and} \quad E_2(\mathbb{F}_3) \cong C_2 \oplus C_2$$

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

$$E_3(\mathbb{F}_5) \cong C_2 \oplus C_2 \quad \text{and} \quad E_4(\mathbb{F}_5) \cong C_4$$

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

$$E_5(\mathbb{F}_5) \cong C_2 \oplus C_4 \quad \text{and} \quad E_6(\mathbb{F}_5) \cong C_8$$

[Reminder from Monday](#)

[the \$j\$ -invariant](#)

[Points of finite order](#)

Points of order 2

Points of order 3

Points of finite order

The group structure

[sketch of proof](#)

[Important Results](#)

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

[Further reading](#)

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

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

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

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

Note

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ the 3rd division polynomial
- $(x_1, y_1) \in E(\mathbb{F}_q)$ has order 3 $\Rightarrow \psi_3(x_1) = 0$
- $E(\mathbb{F}_q)$ has at most 8 points of order 3
- If $p \neq 3$, $E[3] := \{P \in E : 3P = \infty\} \cong C_3 \oplus C_3$



Determining points of order 3 (continues)



Exercise

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. Prove that if $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ 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

Example (from Monday)

If $E : y^2 = x^3 + x + 1$, then $\#E(\mathbb{F}_5) = 9$.

$$\psi_3(x) = (x + 3)(x + 4)(x^2 + 3x + 4)$$

Hence

$$E[3] = \left\{ \infty, (2, \pm 1), (1, \pm \sqrt{3}), (1 \pm 2\sqrt{3}, \pm(1 \pm \sqrt{3})) \right\}$$

- ① $E(\mathbb{F}_5) = \{\infty, (2, \pm 1), (0, \pm 1), (3, \pm 1), (4, \pm 2)\} \cong C_9$
- ② Since $\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{3}] \Rightarrow E[3] \subset E(\mathbb{F}_{25})$
- ③ $\#E(\mathbb{F}_{25}) = 27 \Rightarrow E(\mathbb{F}_{25}) \cong C_3 \oplus C_9$

[Reminder from Monday](#)

[the \$j\$ -invariant](#)

[Points of finite order](#)

[Points of order 2](#)

[Points of order 3](#)

[Points of finite order](#)

[The group structure](#)

[sketch of proof](#)

[Important Results](#)

[Hasse's Theorem](#)

[Waterhouse's Theorem](#)

[Rück's Theorem](#)

[Further reading](#)

Determining points of order 3 (continues)

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

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

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

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

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

Exercise (Suppose $(x_0, y_0) \in E/\mathbb{F}_{2^n}$ has order 3. Show that)

① $E : y^2 + a_3y = x^3 + a_4x + a_6 \Rightarrow x_0^4 + a_3^2x_0 + (a_4a_3)^2 = 0$

② $E : y^2 + xy = x^3 + a_2x^2 + a_6 \Rightarrow x_0^4 + x_0^3 + a_6 = 0$



Determining points of order (dividing) m

Definition (m -torsion point)

Let E/K and let \bar{K} an algebraic closure of K .

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

Theorem (Structure of Torsion Points)

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

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

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

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

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



[Reminder from Monday](#)

[the \$j\$ -invariant](#)

[Points of finite order](#)

[Points of order 2](#)

[Points of order 3](#)

[Points of finite order](#)

[The group structure](#)

[sketch of proof](#)

[Important Results](#)

[Hasse's Theorem](#)

[Waterhouse's Theorem](#)

[Rück's Theorem](#)

[Further reading](#)

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' points of order dividing n_1 . From *Structure of Torsion Theorem*, $\#E[n_1] \leq n_1^2$. So $r \leq 2$ □

Theorem (Corollary of Weil Pairing)

Let E/\mathbb{F}_q and $n, k \in \mathbb{N}$ s.t. $E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$. Then $n \mid q - 1$.

We shall discuss the proof of the latter tomorrow





Reminder from
Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

Sketch of the proof of Structure Theorem of Torsion Points

The division polynomials

The proof generalizes previous ideas and determine the points $P \in E(\mathbb{F}_q)$ such that $mP = \infty$ or equivalently $(m-1)P = -P$.

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

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

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

$$\vdots$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2$$

$$\psi_{2m} = \left(\frac{\psi_m}{2y} \right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3$$

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

The division polynomials

Lemma

Let $E : y^2 = x^3 + Ax + B$, ($p > 3$) and let $\psi_m \in \mathbb{Z}[x, y]$ the m^{th} division polynomial. Then

$$\psi_{2m+1} \in \mathbb{Z}[x] \quad \text{and} \quad \psi_{2m} \in 2y\mathbb{Z}[x]$$

Proof is an exercise.

True $\psi_0, \psi_1, \psi_2, \psi_3, \psi_4$ and for the rest apply induction, the identity $y^2 = x^3 + Ax + B \dots$ and consider the cases m odd and m even. □

Lemma

$$\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \dots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \dots & \text{if } m \text{ is odd.} \end{cases}$$

Hence $\psi_m^2 = m^2 x^{m^2-1} + \dots$

Proof is another exercise on induction:

□

Reminder from Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

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

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

We will omit the proof of the above (see [8, Section 9.5])

Exercise (Prove that after substituting $y^2 = x^3 + Ax + B$)

- ① $\phi_m(x) \in \mathbb{Z}[x]$
- ② $\phi_m(x) = x^{m^2} + \dots \quad \psi_m(x)^2 = m^2 x^{m^2-1} + \dots$
- ③ $\omega_{2m+1} \in y\mathbb{Z}[x], \omega_{2m} \in \mathbb{Z}[x]$
- ④ $\frac{\omega_m(x, y)}{\psi_m^3(x, y)} \in y\mathbb{Z}(x)$
- ⑤ $\gcd(\psi_m^2(x), \phi_m(x)) = 1$

this is not really an exercise!! - see [8, Corollary 3.7]



Lemma

$$\#E[m] = \#\{P \in E(\bar{K}) : mP = \infty\} \begin{cases} = m^2 & \text{if } p \nmid m \\ < m^2 & \text{if } p \mid m \end{cases}$$

Proof.

Consider the homomorphism:

$$[m] : E(\bar{K}) \rightarrow E(\bar{K}), P \mapsto mP$$

If $p \nmid m$, need to show that

$$\# \text{Ker}[m] = \#E[m] = m^2$$

We shall prove that $\exists P_0 = (a, b) \in [m](E(\bar{K})) \setminus \{\infty\}$ s.t.

$$\#\{P \in E(\bar{K}) : mP = P_0\} = m^2$$

Since $E(\bar{K})$ infinite, we can choose $(a, b) \in [m](E(\bar{K}))$ s.t.

① $ab \neq 0$

② $\forall x_0 \in \bar{K} : (\phi'_m \psi_m - 2\phi_m \psi'_m)(x_0) \psi_m(x_0) = 0 \Rightarrow a \neq \frac{\phi_m(x_0)}{\psi_m^2(x_0)}$

if $p \nmid m$, conditions imply that $\phi_m(x) - a\psi_m^2(x)$

has $m^2 = \partial(\phi_m(x) - a\psi_m^2(x))$ distinct roots

in fact $\partial\phi_m(x) = m^2$ and $\partial\psi_m^2(x) = m^2 - 1$





Proof continues.

Write

$$mP = m(x, y) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x, y)}{\psi_m^3(x)} \right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, yr(x) \right)$$

The map

$$\{\alpha \in \bar{K} : \phi_m(\alpha) - a\psi_m(\alpha)^2 = 0\} \leftrightarrow \{P \in E(\bar{K}) : mP = (a, b)\}$$

$$\alpha_0 \mapsto (\alpha_0, br(\alpha_0)^{-1})$$

is a well defined bijection.

Hence there are m^2 points $P \in E(\bar{K})$ with $mP = (a, b)$

So there are m^2 elements in $\text{Ker}[m]$.

If $p \mid m$, the proof is the same except that $\phi_m(x) - a\psi_m(x)^2$ has multiple roots!!

In fact $\phi'_m(x) - a\psi'_m(x)^2 = 0$



Reminder from Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

From Lemma, Theorem follows:

If $p \nmid m$, apply classification Theorem of finite Groups:

$$E[m] \cong C_{n_1} \oplus C_{n_2} \oplus \cdots C_{n_k},$$

$n_i \mid n_{i+1}$. Let $\ell \mid n_1$, then $E[\ell] \subset E[m]$. Hence $\ell^k = \ell^2 \Rightarrow k = 2$. So

$$E[m] \cong C_{n_1} \oplus C_{n_2}$$

Finally $n_2 \mid m$ and $n_1 n_2 = m^2$ so $m = n_1 = n_2$.

If $p \mid m$, write $m = p^j m'$, $p \nmid m'$ and

$$E[m] \cong E[m'] \oplus E[p^j] \cong C_{m'} \oplus C_{m'} \oplus E[p^j]$$

The statement follows from:

$$E[p^j] \cong \begin{cases} \{\infty\} \\ C_{p^j} \end{cases} \quad \text{and} \quad C_{m'} \oplus C_{p^j} \cong C_{m' p^j}$$

which is done by induction.



From Lemma, Theorem follows (continues)

Induction base:

$$E[p] \cong \begin{cases} \{\infty\} \\ C_p \end{cases} \quad \text{if follows from } \#E[p] < p^2$$

- If $E[p] = \{\infty\} \Rightarrow E[p^j] = \{\infty\} \forall j \geq 2$:
In fact if $E[p^j] \neq \{\infty\}$ then it would contain some element of order p (contradiction).
- If $E[p] \cong C_p$, then $E[p^j] \cong C_{p^j} \forall j \geq 2$:
In fact $E[p^j]$ is cyclic (otherwise $E[p]$ would not be cyclic!)

Fact: $[p] : E(\bar{K}) \rightarrow E(\bar{K})$ is surjective (to be proven tomorrow)

If $P \in E$ and $\text{ord } P = p^{j-1} \Rightarrow \exists Q \in E$ s.t. $pQ = P$ and $Q = p^j$.

Hence $E[p^j] \cong C_{p^j}$ since it contains an element of order p^j .

Remark:

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





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 I_q

Example (Hasse Intervals)

q	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}

Reminder from Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading

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

$N = p^e n_1 n_2$, $p \nmid n_1 n_2$ and $n_1 \mid n_2$ (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 $n_1 \mid q - 1$ 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.
$$\begin{aligned} E_1(\mathbb{F}_{101}) &\cong C_{10} \oplus C_{10} & E_2(\mathbb{F}_{101}) &\cong C_2 \oplus C_{50} \\ E_3(\mathbb{F}_{101}) &\cong C_5 \oplus C_{20} & E_4(\mathbb{F}_{101}) &\cong C_{100} \end{aligned}$$



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.



Reminder from
Monday

the j -invariant

Points of finite order

Points of order 2

Points of order 3

Points of finite order

The group structure

sketch of proof

Important Results

Hasse's Theorem

Waterhouse's Theorem

Rück's Theorem

Further reading