Lecture 4

Elliptic curves over finite fields

First steps

College of Sciences
Department of Mathematics
University of Salahaddin,
Erbil, Kurdistan December 7^{th}, 2014

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre

Elliptic curves over $\mathbb{F}_q$

Definition (Elliptic curve)

An elliptic curve over a field K is the data of a non singular Weierstraß equation
$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, a_i \in K$

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

$$\Delta_E := \frac{1}{2^4}\left(-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16 a_1 a_2^2 a_3 a_4 + 36 a_1^2 a_3^2 a_4 \right.$$
$$- a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16 a_2^2 a_4^2 + 96 a_1 a_3 a_4^2 + 64 a_4^3 +$$
$$a_1^6 a_6 + 12 a_1^4 a_2 a_6 + 48 a_1^2 a_2^2 a_6 + 64 a_2^3 a_6 - 36 a_1^3 a_3 a_6$$
$$\left. -144 a_1 a_2 a_3 a_6 - 72 a_1^2 a_4 a_6 - 288 a_2 a_4 a_6 + 432 a_6^2\right) \neq 0$$

Elliptic curves over K

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, set $\infty := [0, 1, 0]$. Set

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

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve. Set

$$E(\mathbb{F}_q)=\{(x,y)\in\mathbb{F}_q^2 : y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{\infty\}$$

Hence

$$E(\mathbb{F}_q)\subset\mathbb{F}_q^2\cup\{\infty\}$$

∞ might be though as the "vertical direction"

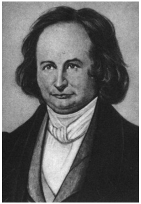
Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

$$r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P\neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P=Q \end{cases}$$

- if $\#(r_{P,Q}\cap E(\mathbb{F}_q))\geq 2 \ \Rightarrow\ \#(r_{P,Q}\cap E(\mathbb{F}_q))=3$
  if tangent line, contact point is counted with multiplicity
- $r_{\infty,\infty}\cap E(\mathbb{F}_q)=\{\infty,\infty,\infty\}$
- $r_{P,Q} : aX+b=0$ (vertical) $\Rightarrow \infty =\in r_{P,Q}$

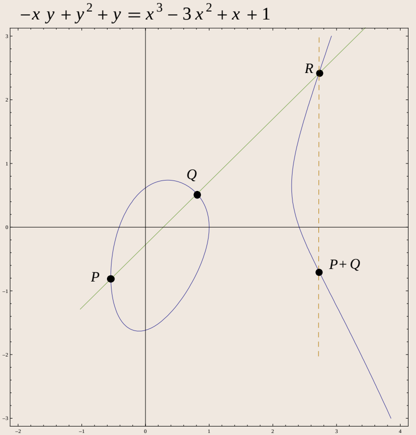
History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$



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

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

$$P +_E Q := R'$$

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

$$-P := P'$$

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

(a) $P +_E Q \in E(\mathbb{F}_q)$ $\quad \forall P, Q \in E(\mathbb{F}_q)$

(b) $P +_E \infty = \infty +_E P = P$ $\quad \forall P \in E(\mathbb{F}_q)$

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

(d) $P +_E (Q +_E R) = (P +_E Q) +_E R$ $\quad \forall P, Q, R \in E(\mathbb{F}_q)$

(e) $P +_E Q = Q +_E P$ $\quad \forall P, Q \in E(\mathbb{F}_q)$

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*
- can substitute $\mathbb{F}_q$ with any field K; Theorem holds for $(E(K), +_E)$
- In particular, if $E/\mathbb{F}_q$, can consider the groups $E(\overline{\mathbb{F}}_q)$ or $E(\mathbb{F}_{q^n})$

Computing the inverse $-P$

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

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

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

Write $P' = (x_1', y_1')$. Since $r_{P,\infty} : x = x_1 \ \Rightarrow x_1' = x_1$ and y_1 satisfies

$$y^2+a_1x_1y+a_3y-(x_1^3+a_2x_1^2+a_4x_1+a_6) = (y-y_1)(y-y_1')$$

So $y_1 + y_1' = -a_1x_1 - a_3$ (both coefficients of y) and

$$-P = -(x_1, y_1) = (x_1, -a_1x_1 - a_3 - y_1)$$

So, if $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{F}_q)$,

Definition: $P_1 +_E P_2 = -P_3$ where $r_{P_1,P_2} \cap E(\mathbb{F}_q) = \{P_1, P_2, P_3\}$

Finally, if $P_3 = (x_3, y_3)$, then

$$P_1 +_E P_2 = -P_3 = (x_3, -a_1x_3 - a_3 - y_3)$$

Lines through points of E

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$,

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{F}_q)$

1. $P_1 \neq P_2$ and $x_1 \neq x_2 \quad \Longrightarrow \quad r_{P_1,P_2} : y = \lambda x + \nu$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1x_2 - x_1y_2}{x_2 - x_1}$$

2. $P_1 \neq P_2$ and $x_1 = x_2 \quad \Longrightarrow \quad r_{P_1,P_2} : x = x_1$
3. $P_1 = P_2$ and $2y_1 + a_1x_1 + a_3 \neq 0 \Longrightarrow r_{P_1,P_2} : y = \lambda x + \nu$

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

4. $P_1 = P_2$ and $2y_1 + a_1x_1 + a_3 = 0 \quad \Longrightarrow \quad r_{P_1,P_2} : x = x_1$
5. $r_{P_1,\infty} : x = x_1 \qquad r_{\infty,\infty} : Z = 0$

Intersection between a line and E

We want to compute $P_3 = (x_3, y_3)$ where $r_{P_1,P_2} : y = \lambda x + \nu$,

$$r_{P_1,P_2} \cap E(\mathbb{F}_q) = \{P_1, P_2, P_3\}$$

We find the intersection:

$$r_{P_1,P_2} \cap E(\mathbb{F}_q) = \begin{cases} E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ r_{P_1,P_2} : y = \lambda x + \nu \end{cases}$$

Substituting

$$(\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3(\lambda x + \nu) = x^3 + a_2x^2 + a_4x + a_6$$

Since x_1 and x_2 are solutions, we can find x_3 by comparing

$$\begin{aligned} &x^3 + a_2x^2 + a_4x + a_6 - ((\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3(\lambda x + \nu)) &= \\ &x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + \cdots &= \\ &(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \cdots \end{aligned}$$

Equating coeffcients of x^2,

$$x_3 = \lambda^2 - a_1\lambda - a_2 - x_1 - x_2, \qquad y_3 = \lambda x_3 + \nu$$

Finally

$$P_3 = (\lambda^2 - a_1\lambda - a_2 - x_1 - x_2, \lambda^3 - a_1\lambda^2 - \lambda(a_2 + x_1 + x_2) + \nu)$$

Formulas for Addition on E (Summary)

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

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

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 $P_1 = P_2$
  - $2y_1 + a_1x + a_3 = 0 \Rightarrow P_1 +_E P_2 = 2P_1 = \infty$
  - $2y_1 + a_1x + a_3 \neq 0$

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

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)

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

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

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

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

Theorem

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

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

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

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

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

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

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.

$$-P = -(x_1, y_1) = (x_1, -a_1x_1 - a_3 - y_1)$$

A Finite Field Example

Over $\mathbb{F}_p$ geometric pictures don't make sense.

Example

Let $E : y^2 = x^3 - 5x + 8/\mathbb{F}_{37}, \quad P = (6,3), Q = (9,10) \in E(\mathbb{F}_{37})$

$$r_{P,Q} : y = 27x + 26 \qquad r_{P,P} : y = 11x + 11$$

$$r_{P,Q} \cap E(\mathbb{F}_{37}) = \begin{cases} y^2 = x^3 - 5x + 8 \\ y = 27x + 26 \end{cases} = \{(6,3),(9,10),(11,27)\}$$

$$r_{P,P} \cap E(\mathbb{F}_{37}) = \begin{cases} y^2 = x^3 - 5x + 8 \\ y = 11x + 11 \end{cases} = \{(6,3),(6,3),(35,26)\}$$

$$P +_E Q = (11,10) \qquad 2P = (35,11)$$

$3P = (34,25), 4P = (8,6), 5P = (16,19), \ldots 3P + 4Q = (31,28), \ldots$

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

Example (One can verify that:)

$$C_{2400} \oplus C_{72} \oplus C_{1440} \cong C_{12} \oplus C_{60} \oplus C_{15200}$$

Shall show that

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

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

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

From our previous list:

Groups of points

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

So for each curve $E(\mathbb{F}_2)$ is cyclic except possibly for the second for which we need to distinguish between C_4 and $C_2 \oplus C_2$.

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

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

From our previous list:

Groups of points

i	E_i	$E_i(\mathbb{F}_3)$	$\lvert E_i(\mathbb{F}_3)\rvert$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	4
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	1
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	2

Each $E_i(\mathbb{F}_3)$ is cyclic except possibly for $E_1(\mathbb{F}_3)$ and $E_2(\mathbb{F}_3)$ that could be either C_4 or $C_2 \oplus C_2$. We shall see that:

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

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

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

Example (Elliptic curves over $\mathbb{F}_5$)

- $\forall E/\mathbb{F}_5$ (12 elliptic curves)
- $\#E(\mathbb{F}_5) \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
- $\forall n, 2 \leq n \leq 10, \exists! \; E/\mathbb{F}_5 : \#E(\mathbb{F}_5) = n$
  with three exceptions:
- $E_1 : y^2 = x^3 + 1$ and $E_2 : y^2 = x^3 + 2$ both order 6

$$E_1(\mathbb{F}_5) \cong E_2(\mathbb{F}_5) \cong C_6$$

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

$$E_3(\mathbb{F}_5) \cong C_2 \oplus C_2 \qquad E_4(\mathbb{F}_5) \cong C_4$$

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

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

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

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 $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

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

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

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4 x + a_6$

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

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

$$E[2] \cong \begin{cases} C_2 \oplus C_2 & \text{if } p > 2 \\ C_2 & \text{if } p = 2, E : y^2 + xy = x^3 + a_4 x + a_6 \\ \{\infty\} & \text{if } p = 2, E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6 \end{cases}$$

Elliptic curves over $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_5$

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

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

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

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

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

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

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

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