Elliptic curves Cryptography

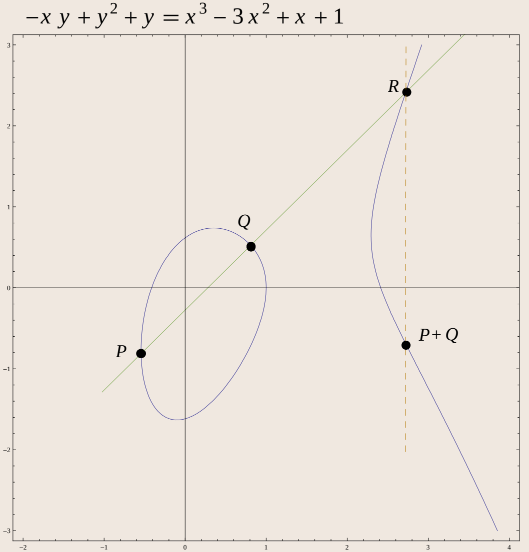
Francesco Pappalardi

#2 - Second Lecture.

June 17th 2019

WAMS School:
o Introductory topics in Number Theory
and Differential Geometry
King Khalid University
Abha, Saudi Arabia

$E/\mathbb{F}_q$ elliptic curve ($D_E = D_E(a_1, a_2, a_3, a_4, a6) \neq 0$)
$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : \; y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\infty\}$



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

- $\left(E(\mathbb{F}_q), +_E\right)$ 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 $(E(K), +_E)$
- $-P = -(x_1, y_1) = (x_1, -a_1x_1 - a_3 - y_1)$

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

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

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)

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

From our previous list:

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 $\mathbb{F}_3$

From our previous list:

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 $/\mathbb{F}_3$

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:

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

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

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