Elliptic curves Cryptography

Francesco Pappalardi

#3 - Third Lecture.

June 18th 2019

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

A Finite Field Example

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

Example

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

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

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

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

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

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

Exercise

- Compute the order and the Group Structure of $E(\mathbb{F}_{37})$

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 the exceptions:

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

- $E_1 : y^2 = x^3 + 1$ and $E_2 : y^2 = x^3 + 2$ both order 6 and $E_1(\mathbb{F}_5) \cong E_2(\mathbb{F}_5) \cong C_6$
- $E_3 : y^2 = x^3 + x$ and $E_4 : y^2 = x^3 + x + 2$ 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

Definition

2–torsion points $\quad E[2] = \{P \in E(\overline{\mathbb{F}_p}) : 2P = \infty\}.$

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

FACTS (from yesterday):

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

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

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

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 $E(\mathbb{F}_p)$

Corollary

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

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

Proof.

From classification Theorem of finite abelian group

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

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

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

Theorem

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

The division polynomials

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

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

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

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

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

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

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

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 (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	$\{10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$
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	$\{22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44\}$