Elliptic curves Cryptography

Francesco Pappalardi

#4 - Fourth Lecture.

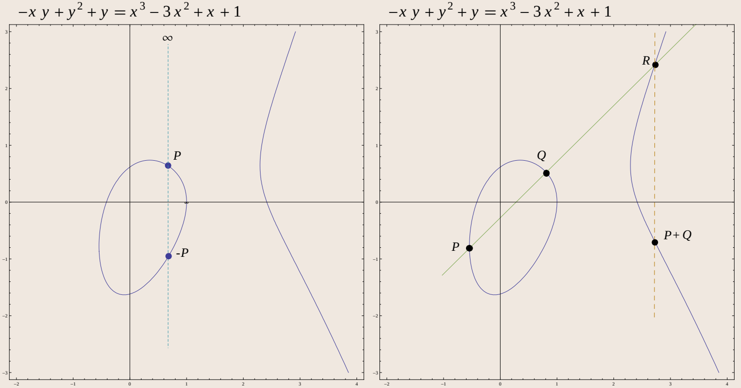
June 18$^{\text{th}}$ 2019

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

Reminder

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

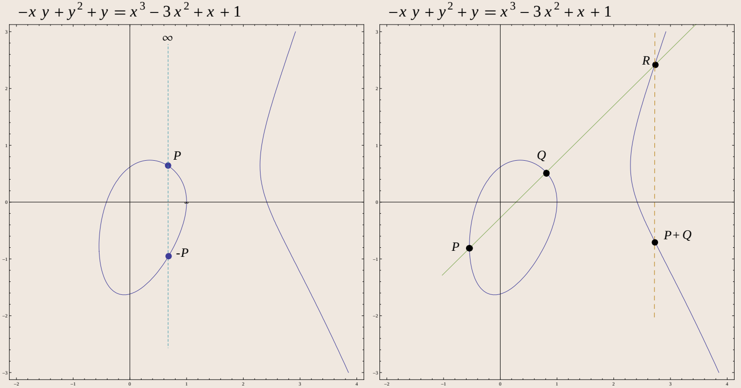
$r_{P,\infty}$: vertical line through P



Reminder

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

$r_{P,\infty}$: vertical line through P



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

$r_{P,Q} \cap E(\mathbb{F}_q) = \{P, Q, R\}$ $\rightsquigarrow$ $\boxed{P +_E Q := -R}$

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

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

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 the m^{th} *division polynomial*

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 the m^{th} *division polynomial*

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

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

Points of order m

Definition (m–torsion point)

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

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

Points of order 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 $m \in \mathbb{N}$.

$$E[m] \cong \begin{cases} C_m \oplus C_m & \text{if } p = \mathrm{char}(K) \nmid m \\ C_m \oplus C_{m'} \quad \text{or} \quad E[m] \cong C_{m'} \oplus C_{m'} & \text{if } m = p^r m', p \nmid m' \end{cases}$$

Points of order 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 $m \in \mathbb{N}$.

$$E[m] \cong \begin{cases} C_m \oplus C_m & \text{if } p = \mathrm{char}(K) \nmid m \\ C_m \oplus C_{m'} \quad \text{or} \quad E[m] \cong C_{m'} \oplus C_{m'} & \text{if } m = p^r m', p \nmid m' \end{cases}$$

FACTS:

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

Points of order 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 $m \in \mathbb{N}$.

$$E[m] \cong \begin{cases} C_m \oplus C_m & \text{if } p = \operatorname{char}(K) \nmid m \\ C_m \oplus C_{m'} \quad \text{or} \quad E[m] \cong C_{m'} \oplus C_{m'} & \text{if } m = p^r m', p \nmid m' \end{cases}$$

FACTS:

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

Points of order 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 $m \in \mathbb{N}$.

$$E[m] \cong \begin{cases} C_m \oplus C_m & \text{if } p = \mathrm{char}(K) \nmid m \\ C_m \oplus C_{m'} \quad \text{or} \quad E[m] \cong C_{m'} \oplus C_{m'} & \text{if } m = p^r m', p \nmid m' \end{cases}$$

FACTS:

- $E[2m+1] \setminus \{\infty\} = \{(x, y) \in E(\bar{K}) : \; \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x, y) \in E(\bar{K}) : \; y^{-1}\psi_{2m}(x) = 0\}$
- Corollary (Theorem of Torsion) $\exists n, k \in \mathbb{N}$ such that $E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$

Points of order m

Definition (m–torsion point)

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

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

Theorem (Structure of Torsion Points)

Let E/K and $m \in \mathbb{N}$.

$$E[m] \cong \begin{cases} C_m \oplus C_m & \text{if } p = \mathrm{char}(K) \nmid m \\ C_m \oplus C_{m'} \quad \text{or} \quad E[m] \cong C_{m'} \oplus C_{m'} & \text{if } m = p^r m', p \nmid m' \end{cases}$$

FACTS:

- $E[2m+1] \setminus \{\infty\} = \{(x, y) \in E(\bar{K}) : \ \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x, y) \in E(\bar{K}) : \ y^{-1}\psi_{2m}(x) = 0\}$
- Corollary (Theorem of Torsion) $\exists n, k \in \mathbb{N}$ such that $E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$
- Further Property $n \mid q - 1$.

Theorem (Hasse)

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

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

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	$\{22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44\}$

Theorem (Waterhouse)

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:

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

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:*

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. $a = \pm 2\sqrt{q}$;

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 $a = \pm\sqrt{q}$;

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* $a = 0$;

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:*

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* $a = \pm p^{(n+1)/2}$;

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. $a = 0$.

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. $a = 0$.

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;*

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.*

Theorem (Rück)

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

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

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.*

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
$$E(\mathbb{F}_q) \cong C_{p^n \pm 1} \oplus C_{p^n \pm 1}.$$

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.
$$E_1(\mathbb{F}_{101}) \cong C_{10} \oplus C_{10} \qquad E_2(\mathbb{F}_{101}) \cong C_2 \oplus C_{50}$$
$$E_3(\mathbb{F}_{101}) \cong C_5 \oplus C_{20} \qquad E_4(\mathbb{F}_{101}) \cong C_{100}$$

Subfield curves

Definition

Let $E/\mathbb{F}_q$ and write $E(\mathbb{F}_q) = q + 1 - a$, ($|a| \leq 2\sqrt{q}$). The *characteristic* polynomial of E is

$$P_E(T) = T^2 - aT + q \in \mathbb{Z}[T].$$

and its roots:

$$\alpha = \frac{1}{2}\left(a + \sqrt{a^2 - 4q}\right) \qquad \beta = \frac{1}{2}\left(a - \sqrt{a^2 - 4q}\right)$$

are called *characteristic roots of Frobenius*

Subfield curves

Definition

Let $E/\mathbb{F}_q$ and write $E(\mathbb{F}_q) = q+1-a$, ($|a| \leq 2\sqrt{q}$). The *characteristic* polynomial of E is

$$P_E(T) = T^2 - aT + q \in \mathbb{Z}[T].$$

and its roots:

$$\alpha = \frac{1}{2}\left(a + \sqrt{a^2 - 4q}\right) \qquad \beta = \frac{1}{2}\left(a - \sqrt{a^2 - 4q}\right)$$

are called *characteristic roots of Frobenius*

Theorem

$\forall n \in \mathbb{N}$

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Subfield curves (continues)

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Subfield curves (continues)

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Curves $/\mathbb{F}_2$	E	a	$P_E(T)$	(α, β)
	$y^2 + xy = x^3 + x^2 + 1$	1	$T^2 - T + 2$	$\frac{1}{2}(1 \pm \sqrt{-7})$
	$y^2 + xy = x^3 + 1$	-1	$T^2 + T + 2$	$\frac{1}{2}(-1 \pm \sqrt{-7})$
	$y^2 + y = x^3 + x$	-2	$T^2 + 2T + 2$	$-1 \pm i$
	$y^2 + y = x^3 + x + 1$	2	$T^2 - 2T + 2$	$1 \pm i$
	$y^2 + y = x^3$	0	$T^2 + 2$	$\pm\sqrt{-2}$

Subfield curves (continues)

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Curves $/\mathbb{F}_2$

E	a	$P_E(T)$	(α, β)
$y^2 + xy = x^3 + x^2 + 1$	1	$T^2 - T + 2$	$\frac{1}{2}(1 \pm \sqrt{-7})$
$y^2 + xy = x^3 + 1$	-1	$T^2 + T + 2$	$\frac{1}{2}(-1 \pm \sqrt{-7})$
$y^2 + y = x^3 + x$	-2	$T^2 + 2T + 2$	$-1 \pm i$
$y^2 + y = x^3 + x + 1$	2	$T^2 - 2T + 2$	$1 \pm i$
$y^2 + y = x^3$	0	$T^2 + 2$	$\pm\sqrt{-2}$

$$E : y^2 + xy = x^3 + x^2 + 1 \;\Rightarrow\; E(\mathbb{F}_{2^{100}}) = 2^{100} + 1 - \left(\frac{1+\sqrt{-7}}{2}\right)^{100} - \left(\frac{1-\sqrt{-7}}{2}\right)^{100}$$

Subfield curves (continues)

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Curves $/\mathbb{F}_2$

E	a	$P_E(T)$	(α, β)
$y^2 + xy = x^3 + x^2 + 1$	1	$T^2 - T + 2$	$\frac{1}{2}(1 \pm \sqrt{-7})$
$y^2 + xy = x^3 + 1$	-1	$T^2 + T + 2$	$\frac{1}{2}(-1 \pm \sqrt{-7})$
$y^2 + y = x^3 + x$	-2	$T^2 + 2T + 2$	$-1 \pm i$
$y^2 + y = x^3 + x + 1$	2	$T^2 - 2T + 2$	$1 \pm i$
$y^2 + y = x^3$	0	$T^2 + 2$	$\pm\sqrt{-2}$

$$E : y^2 + xy = x^3 + x^2 + 1 \;\Rightarrow\; E(\mathbb{F}_{2^{100}}) = 2^{100} + 1 - \left(\frac{1+\sqrt{-7}}{2}\right)^{100} - \left(\frac{1-\sqrt{-7}}{2}\right)^{100}$$

$$=1267650600228229382588845215376$$

Subfield curves

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Subfield curves

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T-\alpha)(T-\beta) \in \mathbb{Z}[T]$

Curves $/\mathbb{F}_3$

i	E_i	a	$P_{E_i}(T)$	(α, β)
1	$y^2 = x^3 + x$	0	$T^2 + 3$	$\pm\sqrt{-3}$
2	$y^2 = x^3 - x$	0	$T^2 + 3$	$\pm\sqrt{-3}$
3	$y^2 = x^3 - x + 1$	-3	$T^2 + 3T + 3$	$\frac{1}{2}(-3 \pm \sqrt{-3})$
4	$y^2 = x^3 - x - 1$	3	$T^2 - 3T + 3$	$\frac{1}{2}(3 \pm \sqrt{-3})$
5	$y^2 = x^3 + x^2 - 1$	1	$T^2 - T + 3$	$\frac{1}{2}(1 \pm \sqrt{-11})$
6	$y^2 = x^3 - x^2 + 1$	-1	$T^2 + T + 3$	$\frac{1}{2}(-1 \pm \sqrt{-11})$
7	$y^2 = x^3 + x^2 + 1$	-2	$T^2 + 2T + 3$	$-1 \pm \sqrt{-2}$
8	$y^2 = x^3 - x^2 - 1$	2	$T^2 - 2T + 3$	$1 \pm \sqrt{-2}$

Subfield curves

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Curves $/\mathbb{F}_3$

i	E_i	a	$P_{E_i}(T)$	(α, β)
1	$y^2 = x^3 + x$	0	$T^2 + 3$	$\pm\sqrt{-3}$
2	$y^2 = x^3 - x$	0	$T^2 + 3$	$\pm\sqrt{-3}$
3	$y^2 = x^3 - x + 1$	-3	$T^2 + 3T + 3$	$\frac{1}{2}(-3 \pm \sqrt{-3})$
4	$y^2 = x^3 - x - 1$	3	$T^2 - 3T + 3$	$\frac{1}{2}(3 \pm \sqrt{-3})$
5	$y^2 = x^3 + x^2 - 1$	1	$T^2 - T + 3$	$\frac{1}{2}(1 \pm \sqrt{-11})$
6	$y^2 = x^3 - x^2 + 1$	-1	$T^2 + T + 3$	$\frac{1}{2}(-1 \pm \sqrt{-11})$
7	$y^2 = x^3 + x^2 + 1$	-2	$T^2 + 2T + 3$	$-1 \pm \sqrt{-2}$
8	$y^2 = x^3 - x^2 - 1$	2	$T^2 - 2T + 3$	$1 \pm \sqrt{-2}$

Lemma

Let $s_n = \alpha^n + \beta^n$ *where* $\alpha\beta = q$ *and* $\alpha + \beta = a$*. Then* $s_0 = 2$, $s_1 = a$ *and* $s_{n+1} = as_n - qs_{n-1}$

Legendre Symbols

Recall the *Finite field Legendre symbols*: let $x \in \mathbb{F}_q$,

Legendre Symbols

Recall the *Finite field Legendre symbols*: let $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^* \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q \\ 0 & \text{if } x = 0 \end{cases}$$

Legendre Symbols

Recall the *Finite field Legendre symbols*: let $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^* \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q \\ 0 & \text{if } x = 0 \end{cases}$$

Theorem

Let $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Then

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

Legendre Symbols

Recall the *Finite field Legendre symbols*: let $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^* \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q \\ 0 & \text{if } x = 0 \end{cases}$$

Theorem

Let $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Then

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

Proof.

Note that

$$1 + \left(\frac{x_0^3+Ax_0+B}{\mathbb{F}_q}\right) = \begin{cases} 2 & \text{if } \exists y_0 \in \mathbb{F}_q^* \text{ s.t. } (x_0, \pm y_0) \in E(\mathbb{F}_q) \\ 1 & \text{if } (x_0, 0) \in E(\mathbb{F}_q) \\ 0 & \text{otherwise} \end{cases}$$

Legendre Symbols

Recall the *Finite field Legendre symbols*: let $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^* \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q \\ 0 & \text{if } x = 0 \end{cases}$$

Theorem

Let $E : y^2 = x^3 + Ax + B$ *over* $\mathbb{F}_q$. *Then*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

Proof.

Note that

$$1 + \left(\frac{x_0^3+Ax_0+B}{\mathbb{F}_q}\right) = \begin{cases} 2 & \text{if } \exists y_0 \in \mathbb{F}_q^* \text{ s.t. } (x_0, \pm y_0) \in E(\mathbb{F}_q) \\ 1 & \text{if } (x_0, 0) \in E(\mathbb{F}_q) \\ 0 & \text{otherwise} \end{cases}$$

Hence $\quad \#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)\right)$ □

Last Slide

Corollary

Let $E : y^2 = x^3 + Ax + B$ *over* $\mathbb{F}_q$ *and* $E_\mu : y^2 = x^3 + \mu^2 Ax + \mu^3 B$, $\mu \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$ *its twist. Then*

$$\#E(\mathbb{F}_q) = q + 1 - a \iff \#E_\mu(\mathbb{F}_q) = q + 1 + a$$

and

$$\#E(\mathbb{F}_{q^2}) = \#E_\mu(\mathbb{F}_{q^2}).$$

Last Slide

Corollary

Let $E : y^2 = x^3 + Ax + B$ *over* $\mathbb{F}_q$ *and* $E_\mu : y^2 = x^3 + \mu^2 Ax + \mu^3 B$, $\mu \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$ *its twist. Then*

$$\#E(\mathbb{F}_q) = q + 1 - a \Leftrightarrow \#E_\mu(\mathbb{F}_q) = q + 1 + a$$

and

$$\#E(\mathbb{F}_{q^2}) = \#E_\mu(\mathbb{F}_{q^2}).$$

Proof.

$$\begin{aligned}\#E_\mu(\mathbb{F}_q) &= q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + \mu^2 Ax + \mu^3 B}{\mathbb{F}_q} \right) \\ &= q + 1 + \left(\frac{\mu}{\mathbb{F}_q} \right) \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right)\end{aligned}$$

and $\left(\frac{\mu}{\mathbb{F}_q} \right) = -1$ $\square$

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.