Lecture 3

Elliptic curves over finite fields

The group order

Research School: Algebraic curves over finite fields

CIMPA-ICTP-UNESCO-MESR-MINECO-PHILIPPINES

University of the Phillipines Diliman, July 25, 2013

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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*

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, $P = (x, y) \in E$)

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Points of order m

Definition (m–torsion point)

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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* $m \in \mathbb{N}$. *If* $p = \mathrm{char}(K) \nmid m$,

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

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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

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

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

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

Idea of the proof:

Let $[m] : E \to E, P \mapsto mP$. Then

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

equality holds iff $p \nmid m$.

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Remark.

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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

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

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

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

Group Structure of $E(\mathbb{F}_q)$

Exercise

Use division polynomials in Sage to write a list of all curves E over $\mathbb{F}_{103}$ such that $E(\mathbb{F}_{103}) \supset E[6]$. Do the same for curves over $\mathbb{F}_{5^4}$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Group Structure of $E(\mathbb{F}_q)$

Exercise

Use division polynomials in Sage to write a list of all curves E over $\mathbb{F}_{103}$ such that $E(\mathbb{F}_{103}) \supset E[6]$. Do the same for curves over $\mathbb{F}_{5^4}$.

Corollary (Corollary of the Theorem of Structure for torsion)

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

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

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Group Structure of $E(\mathbb{F}_q)$

Exercise

Use division polynomials in Sage to write a list of all curves E over $\mathbb{F}_{103}$ such that $E(\mathbb{F}_{103}) \supset E[6]$. Do the same for curves over $\mathbb{F}_{5^4}$.

Corollary (Corollary of the Theorem of Structure for torsion)

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

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

Theorem

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \;\Rightarrow\; P = \infty$ *(non degeneracy)*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \;\Rightarrow\; P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \Rightarrow P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$
4. $e_m(P, Q) = e_m(Q, P)^{-1}$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ *called Weil Pairing, s.t.* $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \ \Rightarrow \ P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$
4. $e_m(P, Q) = e_m(Q, P)^{-1}$
5. $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) \ \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R) e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \;\Rightarrow\; P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$
4. $e_m(P, Q) = e_m(Q, P)^{-1}$
5. $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) \; \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$
6. $e_m(\alpha(P), \alpha(Q)) = e_m(P, Q)^{\deg \alpha} \; \forall \alpha$ *separable endomorphism*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \Rightarrow P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$
4. $e_m(P, Q) = e_m(Q, P)^{-1}$
5. $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) \; \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$
6. $e_m(\alpha(P), \alpha(Q)) = e_m(P, Q)^{\deg \alpha} \; \forall \alpha$ *separable endomorphism*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Weil Pairing

Let E/K and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

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

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

μ_m is a cyclic group with m elements(since $p \nmid m$)

Theorem (Existence of Weil Pairing)

There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ *called Weil Pairing, s.t.* $\forall P, Q \in E[m]$

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \ \Rightarrow \ P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$
4. $e_m(P, Q) = e_m(Q, P)^{-1}$
5. $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) \ \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$
6. $e_m(\alpha(P), \alpha(Q)) = e_m(P, Q)^{\deg \alpha} \ \forall \alpha$ *separable endomorphism*

The last one needs to be discussed further!!!

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Properties of Weil pairing

1. $E[m] \cong C_m \oplus C_m \;\Rightarrow\; E[m]$ has a $\mathbb{Z}/m\mathbb{Z}$–*basis*

i.e. $\exists P, Q \in E[m] : \forall R \in E[m], \exists! \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, R = \alpha P + \beta Q$

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Properties of Weil pairing

1. $E[m] \cong C_m \oplus C_m \Rightarrow E[m]$ has a $\mathbb{Z}/m\mathbb{Z}$*–basis*

i.e. $\exists P, Q \in E[m] : \forall R \in E[m], \exists! \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, R = \alpha P + \beta Q$

2. If (P, Q) is a $\mathbb{Z}/m\mathbb{Z}$–basis, then $\zeta = e_m(P, Q) \in \mu_m$ is *primitive* (i.e. $\operatorname{ord}\zeta = m$)

Proof. Let $d = \operatorname{ord}\zeta$. Then $1 = e_m(P, Q)^d = e_m(P, dQ)$.
$\forall R \in E[m]$, $e_m(R, dQ) = e_m(P, dQ)^\alpha e_m(Q, Q)^{d\beta} = 1$.
So $dQ = \infty \Rightarrow m \mid d$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Properties of Weil pairing

❶ $E[m] \cong C_m \oplus C_m \;\Rightarrow\; E[m]$ has a $\mathbb{Z}/m\mathbb{Z}$–*basis*

i.e. $\exists P, Q \in E[m] : \forall R \in E[m], \exists! \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, R = \alpha P + \beta Q$

❷ If (P, Q) is a $\mathbb{Z}/m\mathbb{Z}$–basis, then $\zeta = e_m(P, Q) \in \mu_m$ is *primitive* (i.e. $\operatorname{ord} \zeta = m$)

Proof. Let $d = \operatorname{ord} \zeta$. Then $1 = e_m(P, Q)^d = e_m(P, dQ)$.
$\forall R \in E[m]$, $e_m(R, dQ) = e_m(P, dQ)^{\alpha} e_m(Q, Q)^{d\beta} = 1$.
So $dQ = \infty \;\Rightarrow\; m \mid d$.

❸ $E[m] \subset E(K) \;\Rightarrow\; \mu_m \subset K$

Proof. Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$ since the basis $(P, Q) \subset E(K)$,
$\sigma(P) = P$, $\sigma(Q) = Q$. Hence
$\zeta = e_m(P, Q) = e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) = \sigma \zeta$
So $\zeta \in \bar{K}^{\mathrm{Gal}(\bar{K}/K)} = K \;\Rightarrow\; \mu_n = \langle \zeta \rangle \subset K^*$

Properties of Weil pairing

1. $E[m] \cong C_m \oplus C_m \;\Rightarrow\; E[m]$ has a $\mathbb{Z}/m\mathbb{Z}$–*basis*

i.e. $\exists P, Q \in E[m] : \forall R \in E[m], \exists! \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, R = \alpha P + \beta Q$

2. If (P, Q) is a $\mathbb{Z}/m\mathbb{Z}$–basis, then $\zeta = e_m(P, Q) \in \mu_m$ is *primitive* (i.e. $\operatorname{ord} \zeta = m$)

Proof. Let $d = \operatorname{ord} \zeta$. Then $1 = e_m(P, Q)^d = e_m(P, dQ)$.
$\forall R \in E[m]$, $e_m(R, dQ) = e_m(P, dQ)^\alpha e_m(Q, Q)^{d\beta} = 1$.
So $dQ = \infty \;\Rightarrow\; m \mid d$.

3. $E[m] \subset E(K) \;\Rightarrow\; \mu_m \subset K$

Proof. Let $\sigma \in \operatorname{Gal}(\bar{K}/K)$ since the basis $(P, Q) \subset E(K)$,
$\sigma(P) = P$, $\sigma(Q) = Q$. Hence
$\zeta = e_m(P, Q) = e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) = \sigma\zeta$
So $\zeta \in \bar{K}^{\operatorname{Gal}(\bar{K}/K)} = K \;\Rightarrow\; \mu_n = \langle \zeta \rangle \subset K^*$

4. if $E(\mathbb{F}_q) \cong C_n \oplus C_{kn} \;\Rightarrow q \equiv 1 \bmod n$

Proof. $E[n] \subset E(\mathbb{F}_q) \Rightarrow \mu_n \subset \mathbb{F}_q^* \Rightarrow n \mid q - 1$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Properties of Weil pairing

1 $E[m] \cong C_m \oplus C_m \;\Rightarrow\; E[m]$ has a $\mathbb{Z}/m\mathbb{Z}$–*basis*

i.e. $\exists P, Q \in E[m] : \forall R \in E[m], \exists ! \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, R = \alpha P + \beta Q$

2 If (P, Q) is a $\mathbb{Z}/m\mathbb{Z}$–basis, then $\zeta = e_m(P, Q) \in \mu_m$ is *primitive* (i.e. $\operatorname{ord} \zeta = m$)

Proof. Let $d = \operatorname{ord} \zeta$. Then $1 = e_m(P, Q)^d = e_m(P, dQ)$.
$\forall R \in E[m]$, $e_m(R, dQ) = e_m(P, dQ)^{\alpha} e_m(Q, Q)^{d\beta} = 1$.
So $dQ = \infty \;\Rightarrow\; m \mid d$.

3 $E[m] \subset E(K) \;\Rightarrow\; \mu_m \subset K$

Proof. Let $\sigma \in \operatorname{Gal}(\bar{K}/K)$ since the basis $(P, Q) \subset E(K)$,
$\sigma(P) = P$, $\sigma(Q) = Q$. Hence
$\zeta = e_m(P, Q) = e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) = \sigma \zeta$
So $\zeta \in \bar{K}^{\operatorname{Gal}(\bar{K}/K)} = K \;\Rightarrow\; \mu_n = \langle \zeta \rangle \subset K^*$

4 if $E(\mathbb{F}_q) \cong C_n \oplus C_{kn} \;\Rightarrow q \equiv 1 \bmod n$

Proof. $E[n] \subset E(\mathbb{F}_q) \Rightarrow \mu_n \subset \mathbb{F}_q^* \Rightarrow n \mid q - 1$

5 If $E/\mathbb{Q} \;\Rightarrow\; E[m] \not\subseteq E(\mathbb{Q})$ for $m \geq 3$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

($\bar{K}(x, y)$ is the field of *rational functions*,

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

($\bar{K}(x, y)$ is the field of *rational functions*, $\alpha(\infty) = \infty$)

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

($\bar{K}(x, y)$ is the field of *rational functions*, $\alpha(\infty) = \infty$)

Exercise (Show that we can always assume)

$$\alpha(x, y) = (r_1(x), y r_2(x)), \qquad \exists r_1, r_2 \in \bar{K}(x)$$

Hint: use $y^2 = x^3 + Ax + B$ and $\alpha(-(x, y)) = -\alpha(x, y)$,

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

($\bar{K}(x, y)$ is the field of *rational functions*, $\alpha(\infty) = \infty$)

Exercise (Show that we can always assume)

$$\alpha(x, y) = (r_1(x), y r_2(x)), \qquad \exists r_1, r_2 \in \bar{K}(x)$$

Hint: use $y^2 = x^3 + Ax + B$ and $\alpha(-(x, y)) = -\alpha(x, y)$,

Remarks/Examples:

- if $r_1(x) = p(x)/q(x)$ with $\gcd(p, q) = 1$ and $(x_0, y_0) \in E(\bar{K})$ with $q(x_0) = 0 \Rightarrow \alpha(x_0, y_0) = \infty$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \text{Ker}(\alpha)$

($\bar{K}(x, y)$ is the field of *rational functions*, $\alpha(\infty) = \infty$)

Exercise (Show that we can always assume)

$$\alpha(x, y) = (r_1(x), y r_2(x)), \qquad \exists r_1, r_2 \in \bar{K}(x)$$

Hint: use $y^2 = x^3 + Ax + B$ and $\alpha(-(x, y)) = -\alpha(x, y)$,

Remarks/Examples:

- if $r_1(x) = p(x)/q(x)$ with $\gcd(p, q) = 1$ and $(x_0, y_0) \in E(\bar{K})$ with $q(x_0) = 0 \Rightarrow \alpha(x_0, y_0) = \infty$
- $[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ is an endomorphism $\forall m \in \mathbb{Z}$

Endomorphisms

Definition

A map $\alpha : E(\bar{K}) \to E(\bar{K})$ is called an endomorphism if

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ (α is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \operatorname{Ker}(\alpha)$

($\bar{K}(x, y)$ is the field of *rational functions*, $\alpha(\infty) = \infty$)

Exercise (Show that we can always assume)

$$\alpha(x, y) = (r_1(x), y r_2(x)), \qquad \exists r_1, r_2 \in \bar{K}(x)$$

Hint: use $y^2 = x^3 + Ax + B$ and $\alpha(-(x, y)) = -\alpha(x, y)$,

Remarks/Examples:

- if $r_1(x) = p(x)/q(x)$ with $\gcd(p, q) = 1$ and $(x_0, y_0) \in E(\bar{K})$ with $q(x_0) = 0 \Rightarrow \alpha(x_0, y_0) = \infty$
- $[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ is an endomorphism $\forall m \in \mathbb{Z}$
- $\Phi_q : E(\bar{\mathbb{F}}_q)) \to E(\bar{\mathbb{F}}_q)), (x, y) \mapsto (x^q, y^q)$ is called *Frobenius Endomorphism*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

If $\alpha \neq [0]$ is an endomorphism, then it is surjective.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

If $\alpha \neq [0]$ is an endomorphism, then it is surjective.

Sketch of the proof.

Assume $p > 3$, $\alpha(x, y) = (p(x)/q(x), yr_2(x))$ and $(a, b) \in E(\bar{K})$.

- If $p(x) - aq(x)$ is not constant, let x_0 be one of its roots. Choose y_0 a square root of $x_0^2 + AX_0 + B$.

  Then either $\alpha(x_0, y_0) = (a, b)$ or $\alpha(x_0, -y_0) = (a, b)$.

- If $p(x) - aq(x)$ is constant,

  this happens only for one value of a!

  Let $(a_1, b_1) \in E(\bar{K})$:
  $(a_1, b_1) \neq (a, \pm b)$ and $(a_1, b_1) +_E (a, b) \neq (a, \pm b)$.

  Then $(a_1, b_1) = \alpha(P_1)$ and $(a_1, b_1) +_E (a, b) = \alpha(P_2)$

  Finally $(a, b) = \alpha(P_2 - P_1)$

□

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism. Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism.
Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism.
Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism.
Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- *$\Phi_q(x, y) = (x^q, y^q)$ is a non separable endomorphism of degree q*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism.
Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- $\Phi_q(x, y) = (x^q, y^q)$ *is a non separable endomorphism of degree q*
- $[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ *has degree* m^2

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism. Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg\alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- $\Phi_q(x, y) = (x^q, y^q)$ *is a non separable endomorphism of degree q*
- $[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ *has degree* m^2
- $[m]$ *separable iff* $p \nmid m$.

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism.
Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- *$\Phi_q(x, y) = (x^q, y^q)$ is a non separable endomorphism of degree q*
- *$[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ has degree m^2*
- *$[m]$ separable iff $p \nmid m$.*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism. Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- *$\Phi_q(x, y) = (x^q, y^q)$ is a non separable endomorphism of degree q*
- *$[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ has degree m^2*
- *$[m]$ separable iff $p \nmid m$.*

Proof.

First: Use the fact that $x \mapsto x^q$ is the identity on $\mathbb{F}_q$ hence it fixes the coefficients of the Weierstraß equation.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism. Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- $\Phi_q(x, y) = (x^q, y^q)$ *is a non separable endomorphism of degree q*
- $[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ *has degree* m^2
- $[m]$ *separable iff* $p \nmid m$.

Proof.

First: Use the fact that $x \mapsto x^q$ is the identity on $\mathbb{F}_q$ hence it fixes the coefficients of the Weierstraß equation. *Second:* already done.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Definition

Suppose $\alpha : E \to E, (x, y) = (r_1(x), yr_2(x))$ endomorphism.
Write $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.

- The **degree** of α is $\deg \alpha := \max\{\deg p, \deg q\}$
- α is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)

Lemma

- $\Phi_q(x, y) = (x^q, y^q)$ *is a non separable endomorphism of degree q*
- $[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ *has degree* m^2
- $[m]$ *separable iff* $p \nmid m$.

Proof.

First: Use the fact that $x \mapsto x^q$ is the identity on $\mathbb{F}_q$ hence it fixes the coefficients of the Weierstraß equation. *Second:* already done. *Third* See [8, Proposition 2.28] □

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

Let $\alpha \neq 0$ be an endomorphism. Then

$$\#\,\mathrm{Ker}(\alpha) \begin{cases} = \deg\alpha & \textit{if } \alpha \textit{ is separable} \\ < \deg\alpha & \textit{otherwise} \end{cases}$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

Let $\alpha \neq 0$ be an endomorphism. Then

$$\#\mathrm{Ker}(\alpha) \begin{cases} = \deg \alpha & \text{if } \alpha \text{ is separable} \\ < \deg \alpha & \text{otherwise} \end{cases}$$

Proof.

It is same proof as $\#E[m] = \#\mathrm{Ker}[m] \leq \partial\phi_m = m^2$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

Let $\alpha \neq 0$ be an endomorphism. Then

$$\#\operatorname{Ker}(\alpha) \begin{cases} = \deg \alpha & \textit{if } \alpha \textit{ is separable} \\ < \deg \alpha & \textit{otherwise} \end{cases}$$

Proof.

It is same proof as $\#E[m] = \#\operatorname{Ker}[m] \leq \partial\phi_m = m^2$ (equality for $p \nmid m$) □

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Endomorphisms (continues)

Theorem

Let $\alpha \neq 0$ be an endomorphism. Then

$$\# \operatorname{Ker}(\alpha) \begin{cases} = \deg \alpha & \text{if } \alpha \text{ is separable} \\ < \deg \alpha & \text{otherwise} \end{cases}$$

Proof.

It is same proof as $\#E[m] = \#\operatorname{Ker}[m] \leq \partial\phi_m = m^2$ (equality for $p \nmid m$) □

Definition

Let E/K. The *ring of endomorphisms*

$$\operatorname{End}(E) := \{\alpha : E \to E, \alpha \text{ is an endomorphism}\}.$$

where for all $\alpha_1, \alpha_2 \in \operatorname{End}(E)$,

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

Let $\alpha \neq 0$ be an endomorphism. Then

$$\#\operatorname{Ker}(\alpha) \begin{cases} = \deg \alpha & \textit{if } \alpha \textit{ is separable} \\ < \deg \alpha & \textit{otherwise} \end{cases}$$

Proof.

It is same proof as $\#E[m] = \#\operatorname{Ker}[m] \leq \partial\phi_m = m^2$ (equality for $p \nmid m$) □

Definition

Let E/K. The *ring of endomorphisms*

$$\operatorname{End}(E) := \{\alpha : E \to E, \alpha \text{ is an endomorphism}\}.$$

where for all $\alpha_1, \alpha_2 \in \operatorname{End}(E)$,

- $(\alpha_1 + \alpha_2)P := \alpha_1(P) +_E \alpha_2(P)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Theorem

Let $\alpha \neq 0$ be an endomorphism. Then

$$\#\mathrm{Ker}(\alpha) \begin{cases} = \deg\alpha & \text{if } \alpha \text{ is separable} \\ < \deg\alpha & \text{otherwise} \end{cases}$$

Proof.

It is same proof as $\#E[m] = \#\mathrm{Ker}[m] \leq \partial\phi_m = m^2$ (equality for $p \nmid m$) □

Definition

Let E/K. The *ring of endomorphisms*

$$\mathrm{End}(E) := \{\alpha : E \to E, \alpha \text{ is an endomorphism}\}.$$

where for all $\alpha_1, \alpha_2 \in \mathrm{End}(E)$,

- $(\alpha_1 + \alpha_2)P := \alpha_1(P) +_E \alpha_2(P)$
- $(\alpha_1\alpha_2)P = \alpha_1(\alpha_2(P))$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of $\text{End}(E)$:

- $[0] : P \mapsto \infty$ is the zero element

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$
- End(E) is not necessarily commutative

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of $\mathrm{End}(E)$**:**

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$
- $\mathrm{End}(E)$ is not necessarily commutative
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$
- $\mathrm{End}(E)$ is not necessarily commutative
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$
- $\mathrm{End}(E)$ is not necessarily commutative
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$

Recall that $\alpha \in \mathrm{End}(E)$ is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ where $\alpha(x, y) = (p(x)/q(x), yr(x))$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$
- $\mathrm{End}(E)$ is not necessarily commutative
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$

Recall that $\alpha \in \mathrm{End}(E)$ is said **separable** if $(p'(x), q'(x)) \neq (0,0)$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

Let $\Phi_q : (x,y) \mapsto (x^q, y^q)$ be the Frobenius endomorphism and let $r, s \in \mathbb{Z}$. Then

$$r\Phi_q + s \in \mathrm{End}(E) \text{ is separable } \Leftrightarrow \; p \nmid s$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Endomorphisms (continues)

Properties of End(E):

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $m \mapsto [m]$
- $\mathrm{End}(E)$ is not necessarily commutative
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$

Recall that $\alpha \in \mathrm{End}(E)$ is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ where $\alpha(x, y) = (p(x)/q(x), yr(x))$.

Lemma

Let $\Phi_q : (x, y) \mapsto (x^q, y^q)$ be the Frobenius endomorphism and let $r, s \in \mathbb{Z}$. Then

$$r\Phi_q + s \in \mathrm{End}(E) \text{ is separable } \Leftrightarrow \ p \nmid s$$

Proof.

See [8, Proposition 2.29] □

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg \alpha := \max\{\deg p, \deg q\}$ where $\alpha(x, y) = (p(x)/q(x), yr(x))$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,

$$\deg(r\alpha + s\beta) = r^2 \deg\alpha + s^2 \deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,
$$\deg(r\alpha + s\beta) = r^2 \deg\alpha + s^2 \deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \text{End}(E)$,
$\deg(r\alpha + s\beta) = r^2 \deg\alpha + s^2 \deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,
$\deg(r\alpha + s\beta) = r^2 \deg\alpha + s^2 \deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

We claim that $\deg(\alpha) \equiv \det \alpha_m \bmod m$. In fact if $\zeta = e_m(P, Q)$ is the Weil pairing (primitive root).

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg \alpha := \max\{\deg p, \deg q\}$ where $\alpha(x, y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,
$$\deg(r\alpha + s\beta) = r^2 \deg \alpha + s^2 \deg \beta + rs(\deg(\alpha + \beta) - \deg \alpha - \deg \beta)$$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

We claim that $\deg(\alpha) \equiv \det \alpha_m \bmod m$. In fact if $\zeta = e_m(P, Q)$ is the Weil pairing (primitive root).
$$\zeta^{\deg(\alpha)} = e_m(\alpha(P), \alpha(Q)) = e_m(aP + bQ, cP + dQ) = \zeta^{ad-bc}$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg \alpha := \max\{\deg p, \deg q\}$ where $\alpha(x, y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,
$\deg(r\alpha + s\beta) = r^2 \deg \alpha + s^2 \deg \beta + rs(\deg(\alpha + \beta) - \deg \alpha - \deg \beta)$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

We claim that $\deg(\alpha) \equiv \det \alpha_m \bmod m$. In fact if $\zeta = e_m(P, Q)$ is the Weil pairing (primitive root).

$$\zeta^{\deg(\alpha)} = e_m(\alpha(P), \alpha(Q)) = e_m(aP + bQ, cP + dQ) = \zeta^{ad-bc}$$

So $\deg(\alpha) \equiv ad - bc = \det \alpha_m (\bmod m)$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,
$\deg(r\alpha + s\beta) = r^2 \deg\alpha + s^2 \deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

We claim that $\deg(\alpha) \equiv \det\alpha_m \bmod m$. In fact if $\zeta = e_m(P,Q)$ is the Weil pairing (primitive root).

$$\zeta^{\deg(\alpha)} = e_m(\alpha(P), \alpha(Q)) = e_m(aP + bQ, cP + dQ) = \zeta^{ad-bc}$$

So $\deg(\alpha) \equiv ad - bc = \det\alpha_m (\bmod m)$. A calculation shows

$$\det(r\alpha_m + s\beta_m) = r^2 \det\alpha_m + s^2 \det\beta_m + rs \det(\alpha_m + \beta_m) - \det\alpha_m - \det\beta_m)$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,

$$\deg(r\alpha + s\beta) = r^2 \deg\alpha + s^2 \deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

We claim that $\deg(\alpha) \equiv \det\alpha_m \bmod m$. In fact if $\zeta = e_m(P,Q)$ is the Weil pairing (primitive root).

$$\zeta^{\deg(\alpha)} = e_m(\alpha(P), \alpha(Q)) = e_m(aP + bQ, cP + dQ) = \zeta^{ad-bc}$$

So $\deg(\alpha) \equiv ad - bc = \det\alpha_m (\bmod m)$. A calculation shows

$$\det(r\alpha_m + s\beta_m) = r^2 \det\alpha_m + s^2 \det\beta_m + rs\det(\alpha_m + \beta_m) - \det\alpha_m - \det\beta_m)$$

So $\deg(r\alpha + s\beta) \equiv r^2 \deg\alpha + s^2 \deg\beta + rs\deg(\alpha+\beta) - \deg\alpha - \deg\beta \bmod m$

Recall that the **degree** if α is $\deg\alpha := \max\{\deg p, \deg q\}$ where $\alpha(x,y) = (p(x)/q(x), yr(x))$.

Lemma

$\forall r, s \in \mathbb{Z}$ *and* $\forall \alpha, \beta \in \mathrm{End}(E)$,

$$\deg(r\alpha + s\beta) = r^2\deg\alpha + s^2\deg\beta + rs(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$$

Proof.

Let $m \in \mathbb{N}$ with $p \nmid m$ and fix a basis P, Q of $E[m] \cong C_m \oplus C_m$. Then $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$ with

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with entries in } \mathbb{Z}/m\mathbb{Z}.$$

We claim that $\deg(\alpha) \equiv \det\alpha_m \bmod m$. In fact if $\zeta = e_m(P,Q)$ is the Weil pairing (primitive root).

$$\zeta^{\deg(\alpha)} = e_m(\alpha(P), \alpha(Q)) = e_m(aP + bQ, cP + dQ) = \zeta^{ad-bc}$$

$$\deg(\alpha) \equiv ad - bc = \det\alpha_m (\bmod m).$$

So A calculation shows

$$\det(r\alpha_m + s\beta_m) = r^2\det\alpha_m + s^2\det\beta_m + rs\det(\alpha_m + \beta_m) - \det\alpha_m - \det\beta_m)$$

So $\quad \deg(r\alpha + s\beta) \equiv r^2\deg\alpha + s^2\deg\beta + rs\deg(\alpha+\beta) - \deg\alpha - \deg\beta \bmod m$

Since it holds for ∞–many m's the above is an equality. □

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Theorem (Hasse)

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q$ is a field automorphism

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q$ is a field automorphism

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \iff \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q$ is a field automorphism

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \Leftrightarrow \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \ \Leftrightarrow\ \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \;\Leftrightarrow\; \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \;\Leftrightarrow\; \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \;\Leftrightarrow\; \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q
- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \Leftrightarrow \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q
- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$
- $\mathrm{Ker}(\Phi_q - 1) = E(\mathbb{F}_q)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \Leftrightarrow \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q
- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$
- $\mathrm{Ker}(\Phi_q - 1) = E(\mathbb{F}_q)$
- $\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$ (since $\Phi_q - 1$ is separable)

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \;\Leftrightarrow\; \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q
- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$
- $\mathrm{Ker}(\Phi_q - 1) = E(\mathbb{F}_q)$
- $\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$ (since $\Phi_q - 1$ is separable)
- if we can compute $\deg(\Phi_q - 1)$, we can compute $\#E(\mathbb{F}_q)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q$ is a field automorphism

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \;\Leftrightarrow\; \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q
- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$
- $\mathrm{Ker}(\Phi_q - 1) = E(\mathbb{F}_q)$
- $\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$ (since $\Phi_q - 1$ is separable)
- if we can compute $\deg(\Phi_q - 1)$, we can compute $\#E(\mathbb{F}_q)$
- $\Phi_q^n(x, y) = (x^{q^n}, y^{q^n})$ so $\Phi_q^n(x, y) = (x, y) \Leftrightarrow (x, y) \in \mathbb{F}_{q^n}$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

The Frobenius endomorphism Φ_q

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \;\Leftrightarrow\; \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of Φ_q are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

Properties of Φ_q

- $\Phi_q \in \mathrm{End}(E)$, it is not separable and has degree q
- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$
- $\mathrm{Ker}(\Phi_q - 1) = E(\mathbb{F}_q)$
- $\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$ (since $\Phi_q - 1$ is separable)
- if we can compute $\deg(\Phi_q - 1)$, we can compute $\#E(\mathbb{F}_q)$
- $\Phi_q^n(x, y) = (x^{q^n}, y^{q^n})$ so $\Phi_q^n(x, y) = (x, y) \Leftrightarrow (x, y) \in \mathbb{F}_{q^n}$
- $\mathrm{Ker}(\Phi_q^n - 1) = E(\mathbb{F}_{q^n})$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ *and write* $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\Phi_q - 1)$.
Then $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ *and write* $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\Phi_q - 1)$. *Then* $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

$$\deg(r\phi + s) = r^2 q + s^2 - rsa$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ *and write* $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\Phi_q - 1)$. *Then* $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

$$\deg(r\phi + s) = r^2 q + s^2 - rsa$$

Proof.

Proof of the Lemma From a previous proposition, we know that

$$\deg(r\Phi_q + s) = r^2 \deg(\Phi_q) + s^2 \deg([-1]) - rs(\deg(\Phi_q - 1) - \deg(\Phi_q) - \deg([-1]))$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ *and write* $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\Phi_q - 1)$.
Then $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

$$\deg(r\phi + s) = r^2 q + s^2 - rsa$$

Proof.

Proof of the Lemma From a previous proposition, we know that
$\deg(r\Phi_q + s) = r^2 \deg(\Phi_q) + s^2 \deg([-1]) - rs(\deg(\Phi_q - 1) - \deg(\Phi_q) - \deg([-1]))$
But

$$\deg(\Phi_q) = q, \deg([-1]) = 1 \text{ and } \deg(\Phi_q - 1) - q - 1 = -a$$

□

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ and write $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\Phi_q - 1)$. Then $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

$$\deg(r\phi + s) = r^2 q + s^2 - rsa$$

Proof.

Proof of the Lemma From a previous proposition, we know that

$\deg(r\Phi_q + s) = r^2 \deg(\Phi_q) + s^2 \deg([-1]) - rs(\deg(\Phi_q - 1) - \deg(\Phi_q) - \deg([-1]))$

But

$$\deg(\Phi_q) = q, \deg([-1]) = 1 \text{ and } \deg(\Phi_q - 1) - q - 1 = -a$$

□

Proof of Hasse's Theorem.

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 = \frac{\deg(r\Phi_q + s)}{s^2} \geq 0$$

on a dense set of rational numbers.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ and write $a = q+1-\#E(\mathbb{F}_q) = q+1-\deg(\Phi_q - 1)$. Then $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

$$\deg(r\phi + s) = r^2 q + s^2 - rsa$$

Proof.

Proof of the Lemma From a previous proposition, we know that

$$\deg(r\Phi_q + s) = r^2 \deg(\Phi_q) + s^2 \deg([-1]) - rs(\deg(\Phi_q - 1) - \deg(\Phi_q) - \deg([-1]))$$

But

$$\deg(\Phi_q) = q, \deg([-1]) = 1 \text{ and } \deg(\Phi_q - 1) - q - 1 = -a$$

□

Proof of Hasse's Theorem.

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 = \frac{\deg(r\Phi_q + s)}{s^2} \geq 0$$

on a dense set of rational numbers.

This implies $\forall X \in \mathbb{R}$, $X^2 - aX + q \geq 0$.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem

Lemma

Let $E/\mathbb{F}_q$ and write $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\Phi_q - 1)$. Then $\forall r, s \in \mathbb{Z}$, $\gcd(q, s) = 1$,

$$\deg(r\phi + s) = r^2 q + s^2 - rsa$$

Proof.

Proof of the Lemma From a previous proposition, we know that

$\deg(r\Phi_q + s) = r^2 \deg(\Phi_q) + s^2 \deg([-1]) - rs(\deg(\Phi_q - 1) - \deg(\Phi_q) - \deg([-1]))$

But

$$\deg(\Phi_q) = q, \deg([-1]) = 1 \text{ and } \deg(\Phi_q - 1) - q - 1 = -a$$

□

Proof of Hasse's Theorem.

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 = \frac{\deg(r\Phi_q + s)}{s^2} \geq 0$$

on a dense set of rational numbers.

This implies $\forall X \in \mathbb{R}$, $X^2 - aX + q \geq 0$.So

$$a^2 - 4q \leq 0 \Leftrightarrow |a| \leq 2\sqrt{q}!!$$

□

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$
2. $\Phi_q - 1$ is separable

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$
2. $\Phi_q - 1$ is separable
3. $\#\,\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$

Reminder from Yesterday

Points of finite order

The group structure

Weil Pairing

Endomorphisms

Separability

the degree of endomorphism

Hasse's Theorem

Frobenius endomorphism

proof

Legendre Symbols

Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$
2. $\Phi_q - 1$ is separable
3. $\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$
2. $\Phi_q - 1$ is separable
3. $\#\,\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$

Corollary

Let $a = q + 1 - \#E(\mathbb{F}_q)$. Then

1. $$\Phi_q^2 - a\Phi_q + q = 0$$

is an identity of endomorphisms.

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$
2. $\Phi_q - 1$ is separable
3. $\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$

Corollary

Let $a = q + 1 - \#E(\mathbb{F}_q)$. Then

1. $$\Phi_q^2 - a\Phi_q + q = 0$$
   is an identity of endomorphisms.
2. *$a \in \mathbb{Z}$ is the unique integer k such that $\Phi_q^2 - k\Phi_q + q = 0$*

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Proof of Hasse's Theorem (continues)

Ingredients for the proof:

1. $E(\mathbb{F}_q) = \mathrm{Ker}(\Phi_q - 1)$
2. $\Phi_q - 1$ is separable
3. $\#\,\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1)$

Corollary

Let $a = q + 1 - \#E(\mathbb{F}_q)$. Then

1. $$\Phi_q^2 - a\Phi_q + q = 0$$ *is an identity of endomorphisms.*
2. *$a \in \mathbb{Z}$ is the unique integer k such that $\Phi_q^2 - k\Phi_q + q = 0$*
3. $$a \equiv \mathrm{Tr}((\Phi_q)_m) \bmod m \;\forall m \text{ s.t. } \gcd(m, q) = 1$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Sketch of the Proof of Corollary.

Let $m \in \mathbb{N}$ s.t. $\gcd(m, q) = 1$. Choose a basis for $E[m]$ and write

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Sketch of the Proof of Corollary.

Let $m \in \mathbb{N}$ s.t. $\gcd(m, q) = 1$. Choose a basis for $E[m]$ and write

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

$\Phi_q - 1$ separable implies

$$\begin{aligned} \#\operatorname{Ker}(\Phi_q - 1) &= \deg(\Phi_q - 1) \equiv \det((\Phi_q)_m - I)) \\ &= \det((\Phi_q)_m) - \operatorname{Tr}((\Phi_q)_m) + 1 (\operatorname{mod} m). \end{aligned}$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Sketch of the Proof of Corollary.

Let $m \in \mathbb{N}$ s.t. $\gcd(m, q) = 1$. Choose a basis for $E[m]$ and write

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

$\Phi_q - 1$ separable implies

$$\begin{aligned} \# \mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1) &\equiv \det((\Phi_q)_m - I)) \\ &= \det((\Phi_q)_m) - \mathrm{Tr}((\Phi_q)_m) + 1 \pmod{m}. \end{aligned}$$

Hence

$$\mathrm{Tr}((\Phi_q)_m) \equiv a \pmod{m}$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Sketch of the Proof of Corollary.

Let $m \in \mathbb{N}$ s.t. $\gcd(m, q) = 1$. Choose a basis for $E[m]$ and write

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

$\Phi_q - 1$ separable implies

$$\begin{aligned} \#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1) &\equiv \det((\Phi_q)_m - I)) \\ &= \det((\Phi_q)_m) - \mathrm{Tr}((\Phi_q)_m) + 1 (\mathrm{mod}\, m). \end{aligned}$$

Hence

$$\mathrm{Tr}((\Phi_q)_m) \equiv a (\mathrm{mod}\, m)$$

By Cayley–Hamilton

$$(\Phi_q)_m^2 - a(\Phi_q)_m + qI \equiv 0 (\mathrm{mod}\, m)$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Sketch of the Proof of Corollary.

Let $m \in \mathbb{N}$ s.t. $\gcd(m, q) = 1$. Choose a basis for $E[m]$ and write

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

$\Phi_q - 1$ separable implies

$$\begin{aligned} \#\operatorname{Ker}(\Phi_q - 1) &= \deg(\Phi_q - 1) \equiv \det((\Phi_q)_m - I)) \\ &= \det((\Phi_q)_m) - \operatorname{Tr}((\Phi_q)_m) + 1 (\operatorname{mod} m). \end{aligned}$$

Hence

$$\operatorname{Tr}((\Phi_q)_m) \equiv a (\operatorname{mod} m)$$

By Cayley–Hamilton

$$(\Phi_q)_m^2 - a(\Phi_q)_m + qI \equiv 0 (\operatorname{mod} m)$$

Since this happens for infinitely many m's,

$$\Phi_q^2 - a\Phi_q + q = 0$$

as endomorphism.

Sketch of the Proof of Corollary.

Let $m \in \mathbb{N}$ s.t. $\gcd(m, q) = 1$. Choose a basis for $E[m]$ and write

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

$\Phi_q - 1$ separable implies

$$\begin{aligned} \# \mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1) &\equiv \det((\Phi_q)_m - I)) \\ &= \det((\Phi_q)_m) - \mathrm{Tr}((\Phi_q)_m) + 1 (\mathrm{mod}\, m). \end{aligned}$$

Hence

$$\mathrm{Tr}((\Phi_q)_m) \equiv a (\mathrm{mod}\, m)$$

By Cayley–Hamilton

$$(\Phi_q)_m^2 - a(\Phi_q)_m + qI \equiv 0 (\mathrm{mod}\, m)$$

Since this happens for infinitely many m's,

$$\Phi_q^2 - a\Phi_q + q = 0$$

as endomorphism. □

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

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* $(P_E(\Phi_q) = 0)$.

Theorem

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$
6. $(\Phi_q^n)^2 - (\alpha^n + \beta^n)\Phi_q^n + q^n = Q(\Phi_q))(\Phi_q^2 - a\Phi_q + q) = 0$ where $f(X) = Q(X)(X^2 - aX + q)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$
6. $(\Phi_q^n)^2 - (\alpha^n + \beta^n)\Phi_q^n + q^n = Q(\Phi_q))(\Phi_q^2 - a\Phi_q + q) = 0$ where $f(X) = Q(X)(X^2 - aX + q)$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$
6. $(\Phi_q^n)^2 - (\alpha^n + \beta^n)\Phi_q^n + q^n = Q(\Phi_q))(\Phi_q^2 - a\Phi_q + q) = 0$ where $f(X) = Q(X)(X^2 - aX + q)$

Hence Φ_q^n satisfies

$$X^2 - ((\alpha^n + \beta^n))X + q.$$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$
6. $(\Phi_q^n)^2 - (\alpha^n + \beta^n)\Phi_q^n + q^n = Q(\Phi_q))(\Phi_q^2 - a\Phi_q + q) = 0$ where $f(X) = Q(X)(X^2 - aX + q)$

Hence Φ_q^n satisfies

$$X^2 - ((\alpha^n + \beta^n))X + q.$$

So

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$
6. $(\Phi_q^n)^2 - (\alpha^n + \beta^n)\Phi_q^n + q^n = Q(\Phi_q))(\Phi_q^2 - a\Phi_q + q) = 0$ where $f(X) = Q(X)(X^2 - aX + q)$

Hence Φ_q^n satisfies

$$X^2 - ((\alpha^n + \beta^n))X + q.$$

So

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

Characteristic polynomial of Φ_{q^n}:

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

Theorem

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

Proof.

Note that

1. Result is true for $n = 1$, $\alpha + \beta = a$
2. $\alpha^n + \beta^n \in \mathbb{Z}$, $(\alpha\beta)^n = q^n$
3. $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X]$
4. $f(X)$ is divisible by $X^2 - aX + q = (X - \alpha)(X - \beta)$
5. $(\Phi_q)^n|_{\bar{\mathbb{F}}_{q^n}} = \Phi_{q^n} : (x, y) \mapsto (x^{q^n}, y^{q^n})$
6. $(\Phi_q^n)^2 - (\alpha^n + \beta^n)\Phi_q^n + q^n = Q(\Phi_q))(\Phi_q^2 - a\Phi_q + q) = 0$
   where $f(X) = Q(X)(X^2 - aX + q)$

Hence Φ_q^n satisfies

$$X^2 - ((\alpha^n + \beta^n))X + q.$$

So

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

Characteristic polynomial of Φ_{q^n}: $X^2 - (\alpha^n + \beta^n)X + q^n$ □

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Subfield curves (continues)

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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	$T^2 + 2$	$\pm\sqrt{-2}$

$E : y^2 + xy = x^3 + x^2 + 1 \;\Rightarrow$

$$E(\mathbb{F}_{2^{100}}) = 2^{100} + 1 - \left(\frac{1+\sqrt{-7}}{2}\right)^{100} - \left(\frac{1-\sqrt{-7}}{2}\right)^{100} = 1267650600228229382588845215376$$

Subfield curves

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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 $/\mathbb{F}_2$

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	$T^2 - 2T + 3$	$1 \pm \sqrt{-2}$

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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 $/\mathbb{F}_2$

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

$$s_0 = 2, \quad , s_1 = a \quad \text{and} \quad s_{n+1} = a s_n - q s_{n-1}$$

Legendre Symbols

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

Legendre Symbols

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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*

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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

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

Reminder from Yesterday
- Points of finite order
- The group structure

Weil Pairing

Endomorphisms
- Separability
- the degree of endomorphism

Hasse's Theorem
- Frobenius endomorphism
- proof

Legendre Symbols

Further reading

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

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

□

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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

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

CIMPA

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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.

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

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

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

Reminder from Yesterday
Points of finite order
The group structure
Weil Pairing
Endomorphisms
Separability
the degree of endomorphism
Hasse's Theorem
Frobenius endomorphism
proof
Legendre Symbols
Further reading

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.