# Introduction to Galois Representations

## Definitions and basic properties

**NATO ASI, Ohrid 2014**

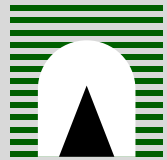
*Arithmetic of Hyperelliptic Curves*

August 25 - September 5, 2014

*Ohrid, the former Yugoslav Republic of Macedonia*,

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre





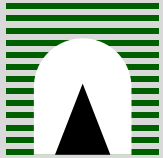
# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$



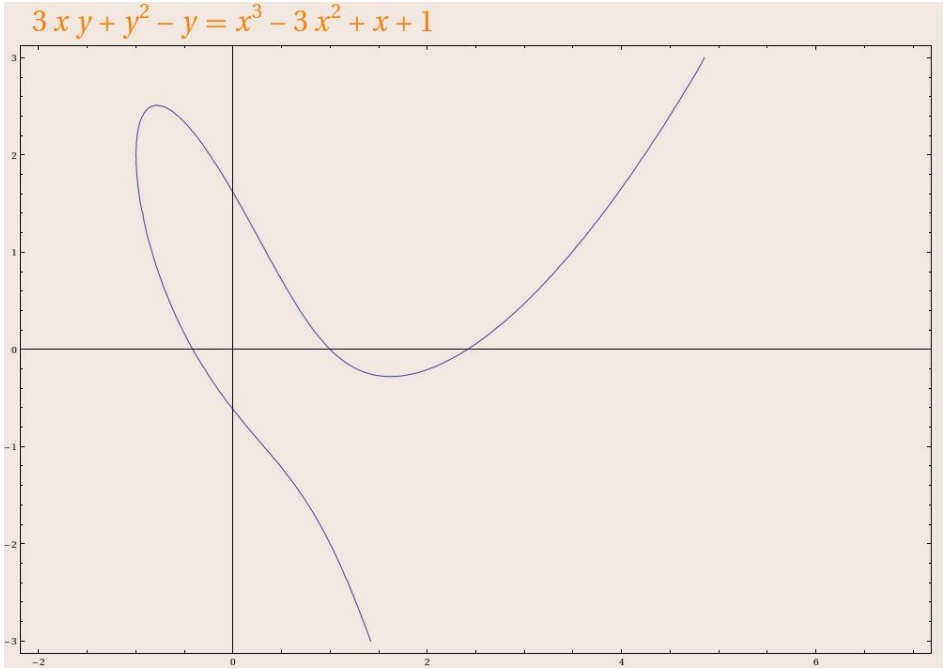


# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




Dipartim. Mat. & Fis.

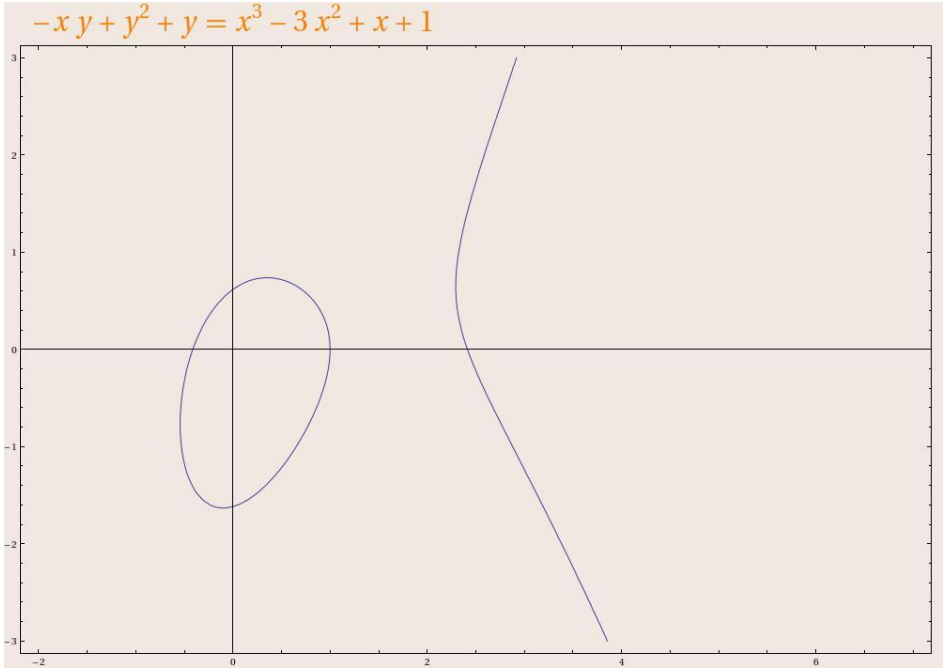
Università Roma Tre

# The (general) Weierstraß Equation

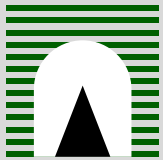
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





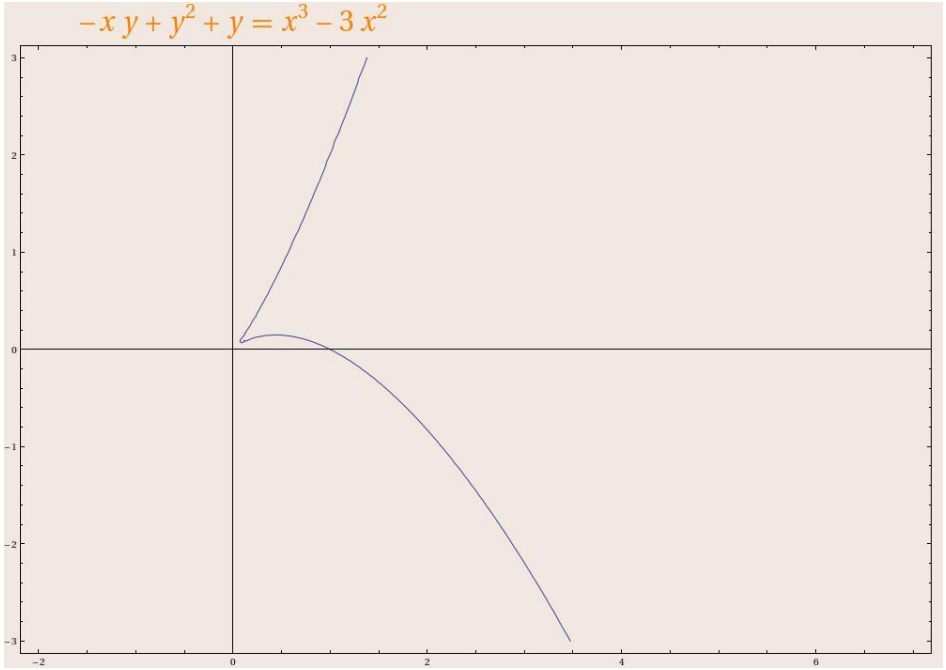



# The (general) Weierstraß Equation

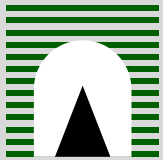
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





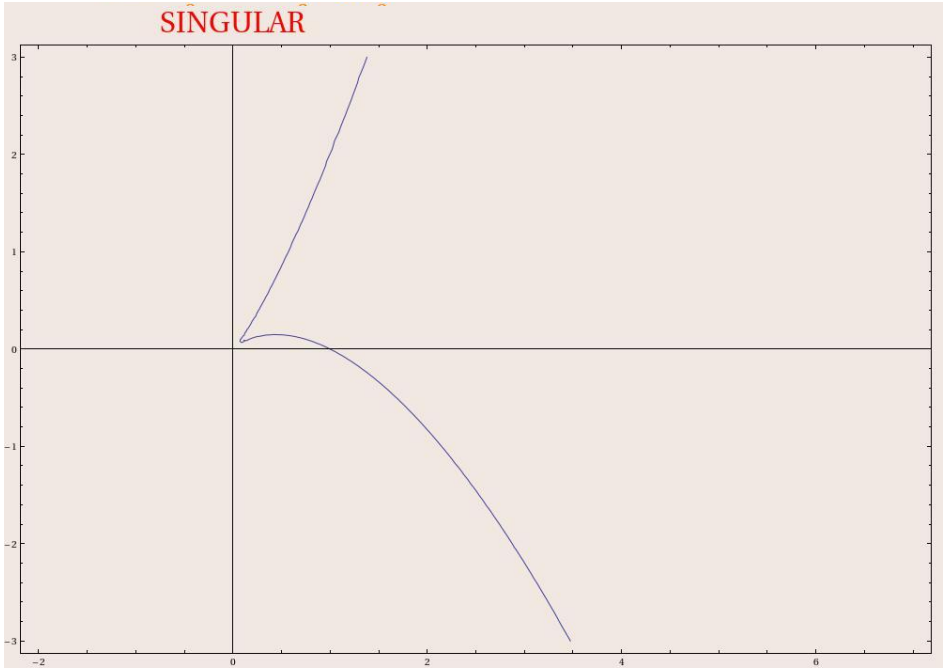



# The (general) Weierstraß Equation

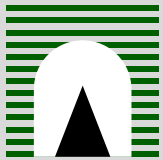
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





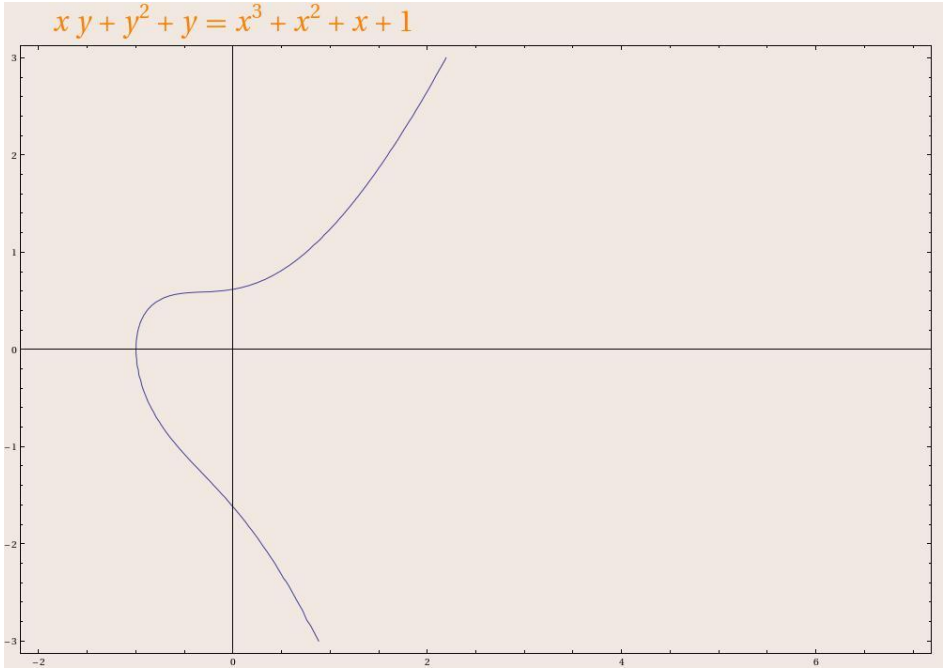



# The (general) Weierstraß Equation

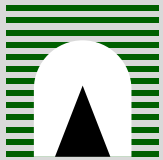
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





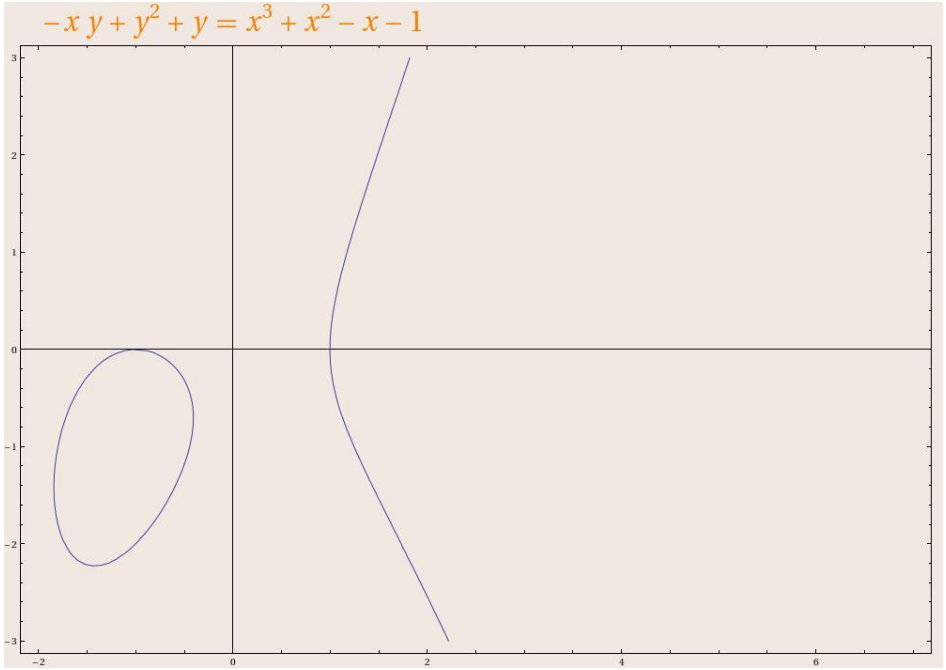



# The (general) Weierstraß Equation

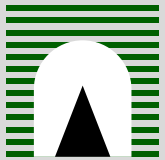
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





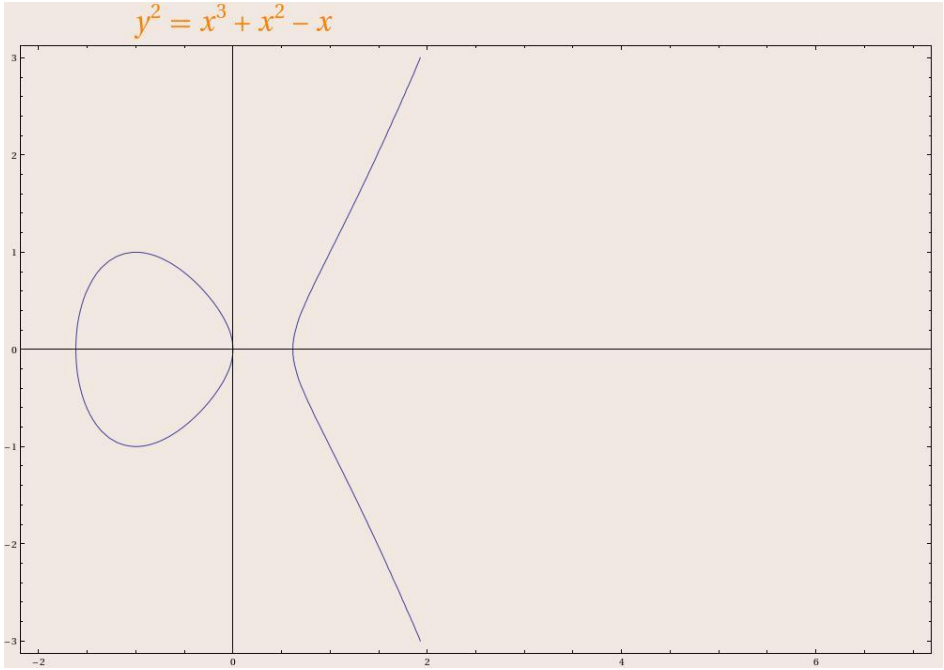



# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




Dipartim. Mat. & Fis.

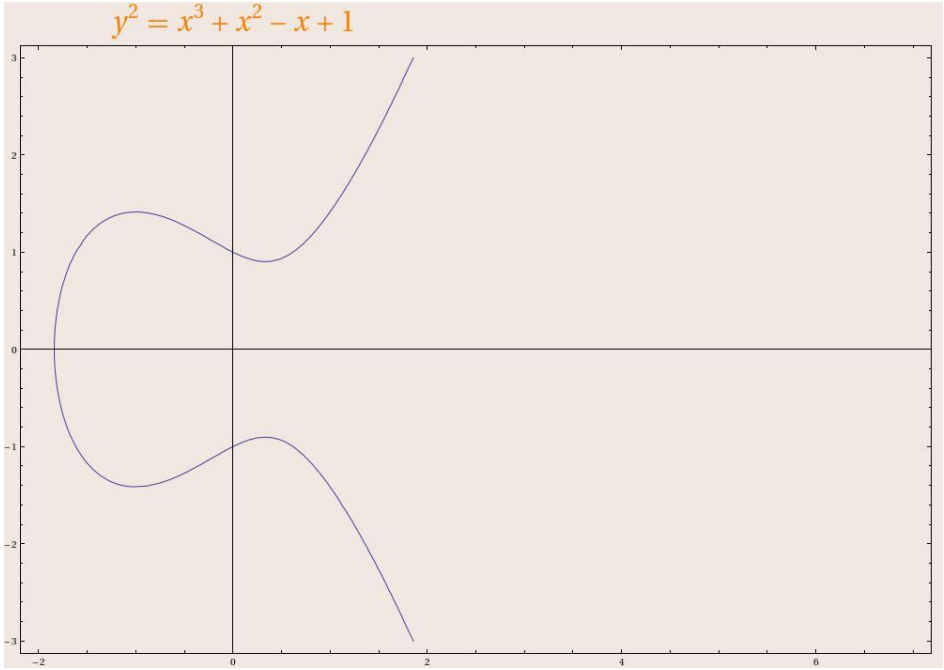
Università Roma Tre

# The (general) Weierstraß Equation

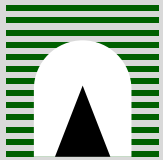
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





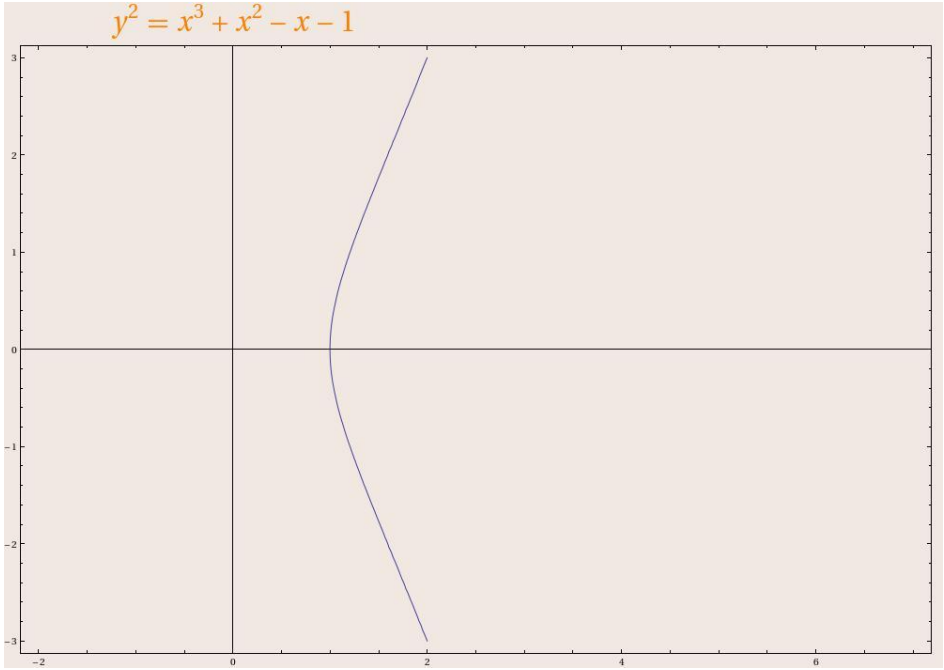



# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




Dipartim. Mat. & Fis.

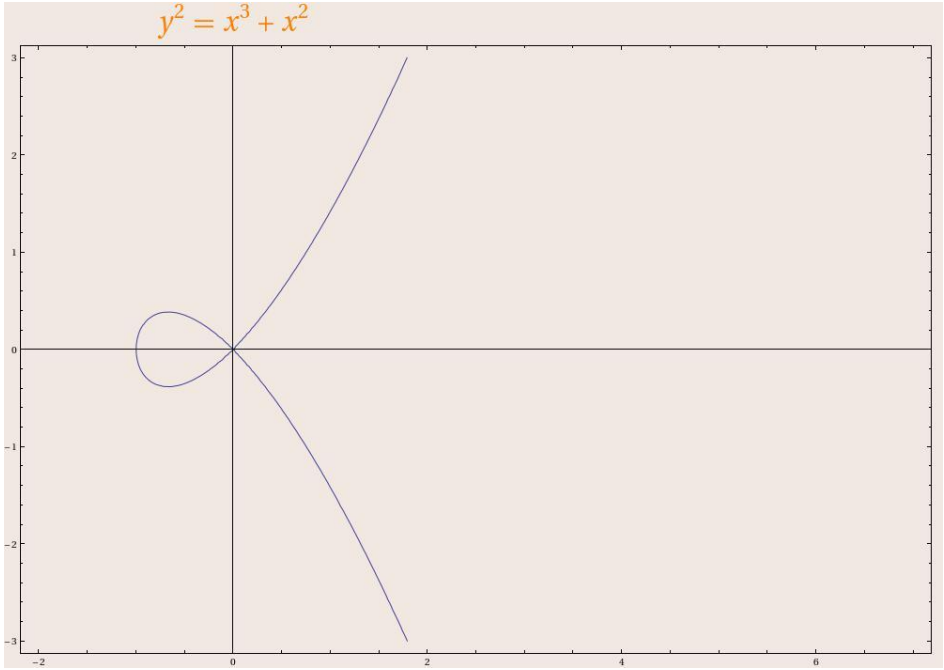
Università Roma Tre

# The (general) Weierstraß Equation

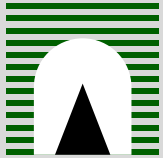
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





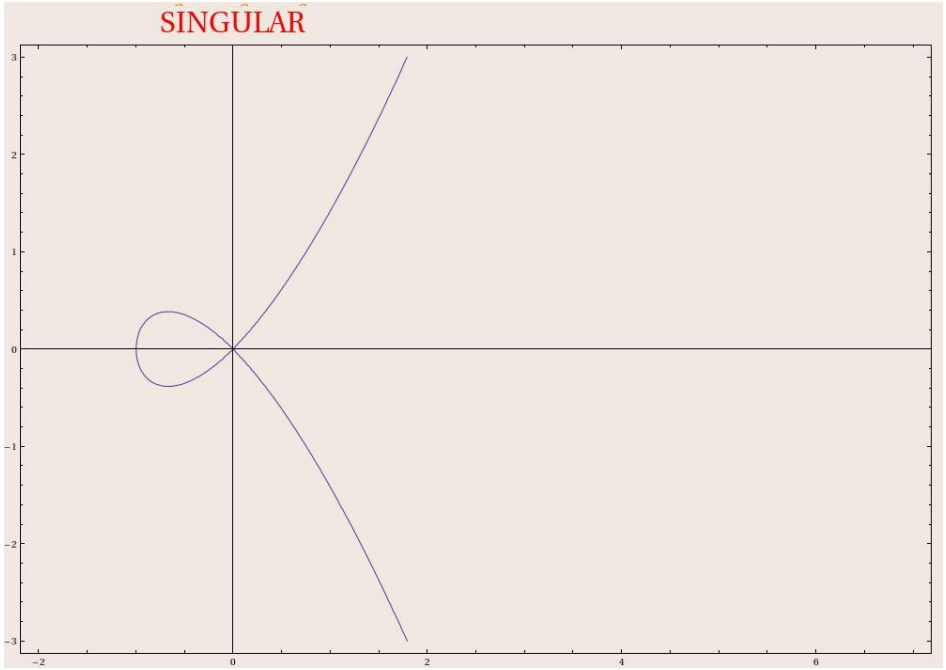



# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




Dipartim. Mat. & Fis.

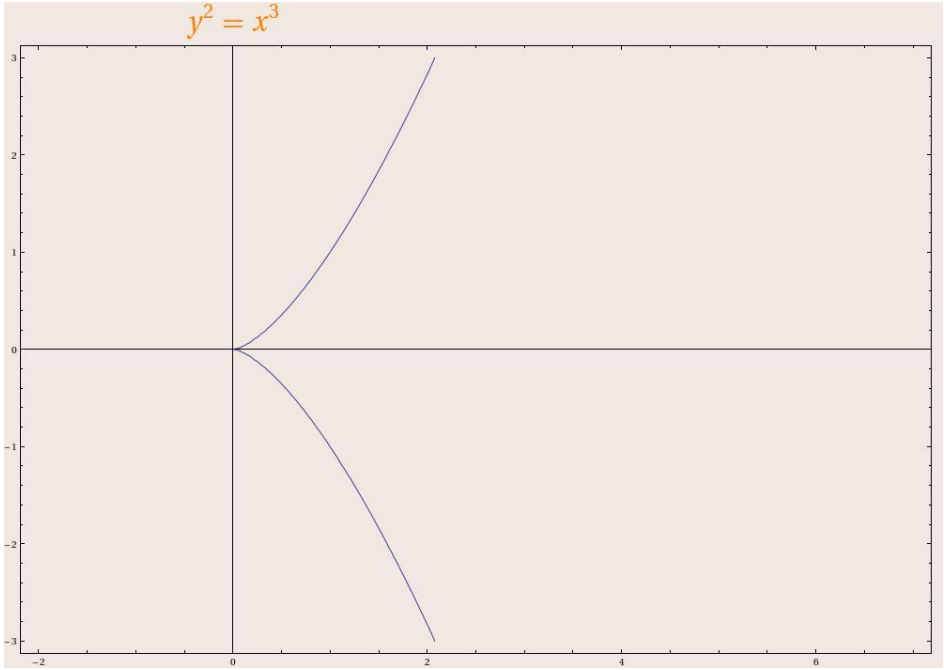
Università Roma Tre

# The (general) Weierstraß Equation

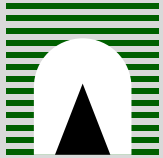
An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$





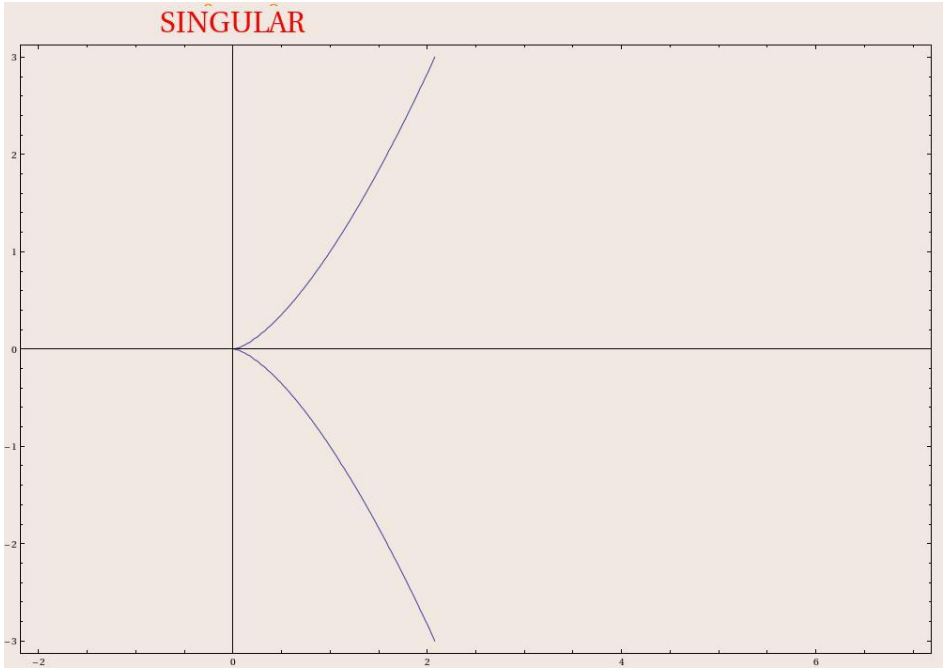



# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




Dipartim. Mat. & Fis.

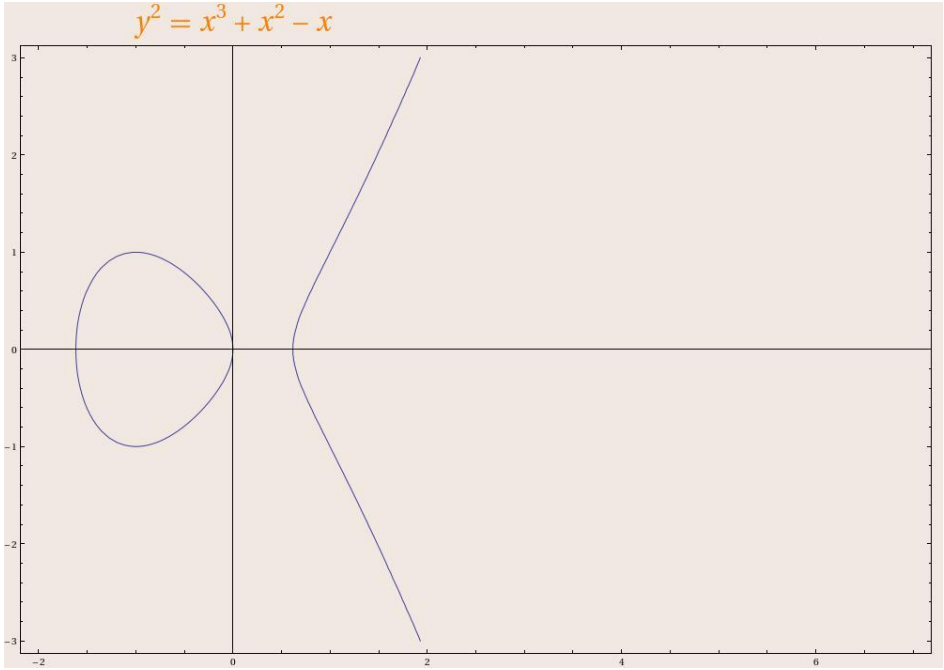
Università Roma Tre

# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




Dipartim. Mat. & Fis.

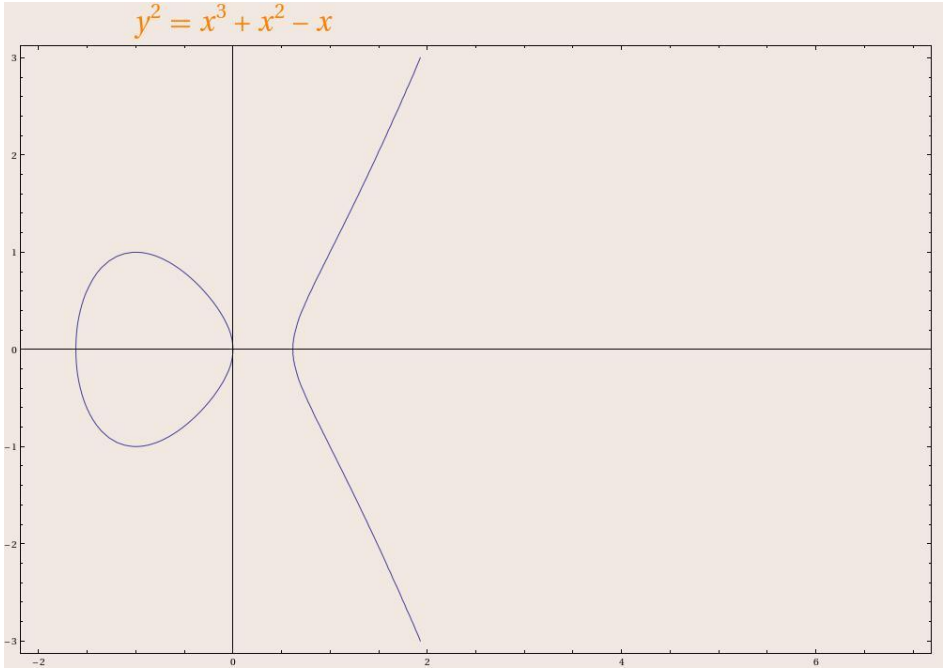
Università Roma Tre

# The (general) Weierstraß Equation

An elliptic curve $E$ over a field $K$ is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in K$




The equation should not be *singular*

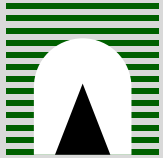
Dipartim. Mat. & Fis.

Università Roma Tre

# The Discriminant of an Equation

## The condition of absence of singular points in terms of $a_1, a_2, a_3, a_4, a_6$





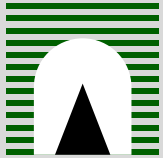
# The Discriminant of an Equation

## The condition of absence of singular points in terms of $a_1, a_2, a_3, a_4, a_6$

**Definition (The discriminant of a Weierstraß equation)**

$$\begin{aligned}\Delta_E := &-a_1^5a_3a_4 - 8a_1^3a_2a_3a_4 - 16a_1a_2^2a_3a_4 + 36a_1^2a_3^2a_4 \\ &- a_1^4a_4^2 - 8a_1^2a_2a_4^2 - 16a_2^2a_4^2 + 96a_1a_3a_4^2 + 64a_4^3 + \\ &a_1^6a_6 + 12a_1^4a_2a_6 + 48a_1^2a_2^2a_6 + 64a_2^3a_6 - 36a_1^3a_3a_6 \\ &- 144a_1a_2a_3a_6 - 72a_1^2a_4a_6 - 288a_2a_4a_6 + 432a_6^2\end{aligned}$$





# The Discriminant of an Equation

## The condition of absence of singular points in terms of $a_1, a_2, a_3, a_4, a_6$

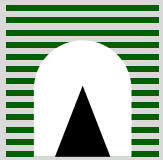
**Definition (The discriminant of a Weierstraß equation)**

$$\begin{aligned}\Delta_E := &-a_1^5a_3a_4 - 8a_1^3a_2a_3a_4 - 16a_1a_2^2a_3a_4 + 36a_1^2a_3^2a_4 \\ &- a_1^4a_4^2 - 8a_1^2a_2a_4^2 - 16a_2^2a_4^2 + 96a_1a_3a_4^2 + 64a_4^3 + \\ &a_1^6a_6 + 12a_1^4a_2a_6 + 48a_1^2a_2^2a_6 + 64a_2^3a_6 - 36a_1^3a_3a_6 \\ &- 144a_1a_2a_3a_6 - 72a_1^2a_4a_6 - 288a_2a_4a_6 + 432a_6^2\end{aligned}$$

$E$ is non singular if and only if $\Delta_E \neq 0$

Dipartim. Mat. & Fis.

Università Roma Tre



# The Discriminant of an Equation

## The condition of absence of singular points in terms of $a_1, a_2, a_3, a_4, a_6$

### Definition (The discriminant of a Weierstraß equation)

$$\begin{aligned}\Delta_E := &-a_1^5a_3a_4 - 8a_1^3a_2a_3a_4 - 16a_1a_2^2a_3a_4 + 36a_1^2a_3^2a_4 \\ &- a_1^4a_4^2 - 8a_1^2a_2a_4^2 - 16a_2^2a_4^2 + 96a_1a_3a_4^2 + 64a_4^3 + \\ &a_1^6a_6 + 12a_1^4a_2a_6 + 48a_1^2a_2^2a_6 + 64a_2^3a_6 - 36a_1^3a_3a_6 \\ &- 144a_1a_2a_3a_6 - 72a_1^2a_4a_6 - 288a_2a_4a_6 + 432a_6^2\end{aligned}$$

$E$ is non singular if and only if $\Delta_E \neq 0$

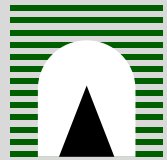
### Definition

Two Weierstraß equations over $K$ are said *(affinely) equivalent* if there exists a (affine) transformation of the following form

$$\begin{cases} x \longleftarrow u^2x + r \\ y \longleftarrow u^3y + u^2sx + t \end{cases} \qquad r, s, t, u \in K$$

that "takes" one equation into the other



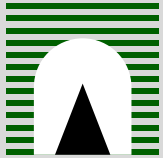


# The Weierstraß equation

## Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/K(p = \mathrm{char}(K))$ has a Weierstraß equation of the following form





# The Weierstraß equation

## Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/K(p = \mathrm{char}(K))$ has a Weierstraß equation of the following form

**Example (Classification)**

| $E$ | $p$ | $\Delta_E$ |
|---|---|---|
| $y^2 = x^3 + Ax + B$ | $\geq 5$ | $4A^3 + 27B^2$ |
| $y^2 + xy = x^3 + a_2x^2 + a_6$ | 2 | $a_6^2$ |
| $y^2 + a_3y = x^3 + a_4x + a_6$ | 2 | $a_3^4$ |
| $y^2 = x^3 + Ax^2 + Bx + C$ | 3 | $4A^3C - A^2B^2 - 18ABC$ $+4B^3 + 27C^2$ |

# The Weierstraß equation

## Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/K(p = \mathrm{char}(K))$ has a Weierstraß equation of the following form

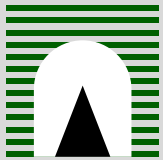
### Example (Classification)

| $E$ | $p$ | $\Delta_E$ |
|---|---|---|
| $y^2 = x^3 + Ax + B$ | $\geq 5$ | $4A^3 + 27B^2$ |
| $y^2 + xy = x^3 + a_2x^2 + a_6$ | 2 | $a_6^2$ |
| $y^2 + a_3y = x^3 + a_4x + a_6$ | 2 | $a_3^4$ |
| $y^2 = x^3 + Ax^2 + Bx + C$ | 3 | $4A^3C - A^2B^2 - 18ABC$ $+4B^3 + 27C^2$ |

### Definition (Elliptic curve)

An elliptic curve is a non singular Weierstraß equation (i.e. $\Delta_E \neq 0$)





# The Weierstraß equation

## Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/K(p = \mathrm{char}(K))$ has a Weierstraß equation of the following form

**Example (Classification)**

| $E$ | $p$ | $\Delta_E$ |
|---|---|---|
| $y^2 = x^3 + Ax + B$ | $\geq 5$ | $4A^3 + 27B^2$ |
| $y^2 + xy = x^3 + a_2x^2 + a_6$ | 2 | $a_6^2$ |
| $y^2 + a_3y = x^3 + a_4x + a_6$ | 2 | $a_3^4$ |
| $y^2 = x^3 + Ax^2 + Bx + C$ | 3 | $4A^3C - A^2B^2 - 18ABC + 4B^3 + 27C^2$ |

**Definition (Elliptic curve)**

An elliptic curve is a non singular Weierstraß equation (i.e. $\Delta_E \neq 0$)

**Note:** If $p = 0$ or $p \geq 3$, $\Delta_E = 0 \Leftrightarrow x^3 + Ax^2 + Bx + C$ has double roots

# The definition of $E(K)$

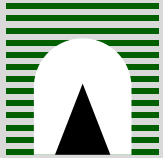
Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

or equivalently

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





# The definition of $E(K)$

Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

or equivalently

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

We can think either

# The definition of $E(K)$

Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

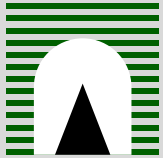
or equivalently

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

We can think either

- $E(K) \subset \mathbb{P}_2(K)$





# The definition of $E(K)$

Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

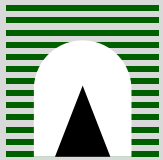
or equivalently

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

We can think either

- $E(K) \subset \mathbb{P}_2(K)$ $\dashrightarrow$ geometric advantages
- $E(K) \subset K^2 \cup \{\infty\}$





# The definition of $E(K)$

Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

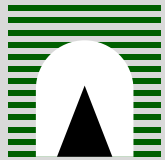
or equivalently

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

We can think either

- $E(K) \subset \mathbb{P}_2(K)$ $\dashrightarrow$ geometric advantages
- $E(K) \subset K^2 \cup \{\infty\}$ $\dashrightarrow$ algebraic advantages





# The definition of $E(K)$

Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

or equivalently

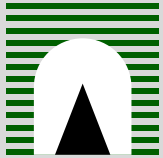
$$E(K) = \\ \{(x,y) \in K^2 : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

We can think either

- $E(K) \subset \mathbb{P}_2(K)$ $\dashrightarrow$ geometric advantages
- $E(K) \subset K^2 \cup \{\infty\}$ $\dashrightarrow$ algebraic advantages

$\infty$ might be though as the "vertical direction"





# The definition of $E(K)$

Let $E/K$ elliptic curve, $\infty := [0,1,0]$. Set

$$E(K) = \{[X,Y,Z] \in \mathbb{P}_2(K) : \\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

or equivalently

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

We can think either

- $E(K) \subset \mathbb{P}_2(K)$ ⇢ geometric advantages
- $E(K) \subset K^2 \cup \{\infty\}$ ⇢ algebraic advantages

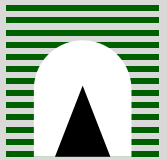
$\infty$ might be though as the "vertical direction"

**Definition (line through points $P, Q \in E(K)$)**

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

projective or affine

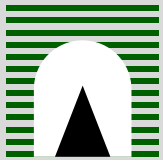




$$\text{If } P, Q \in E(K), r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q, \end{cases}$$

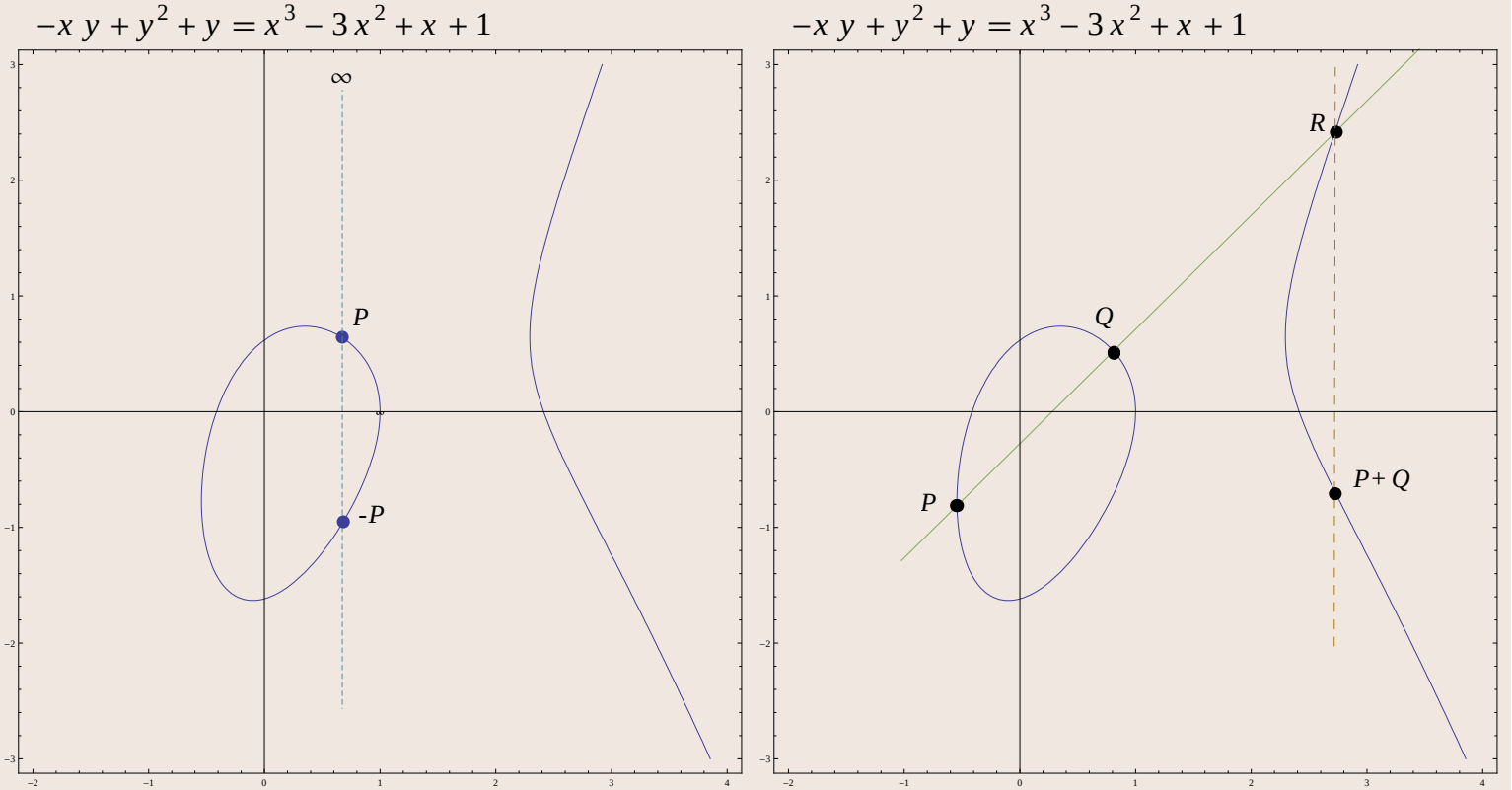
$$r_{P,\infty} : \text{vertical line through } P$$



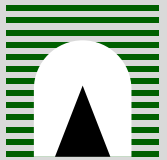


If $P, Q \in E(K), r_{P,Q}$ : $\begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q, \end{cases}$

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

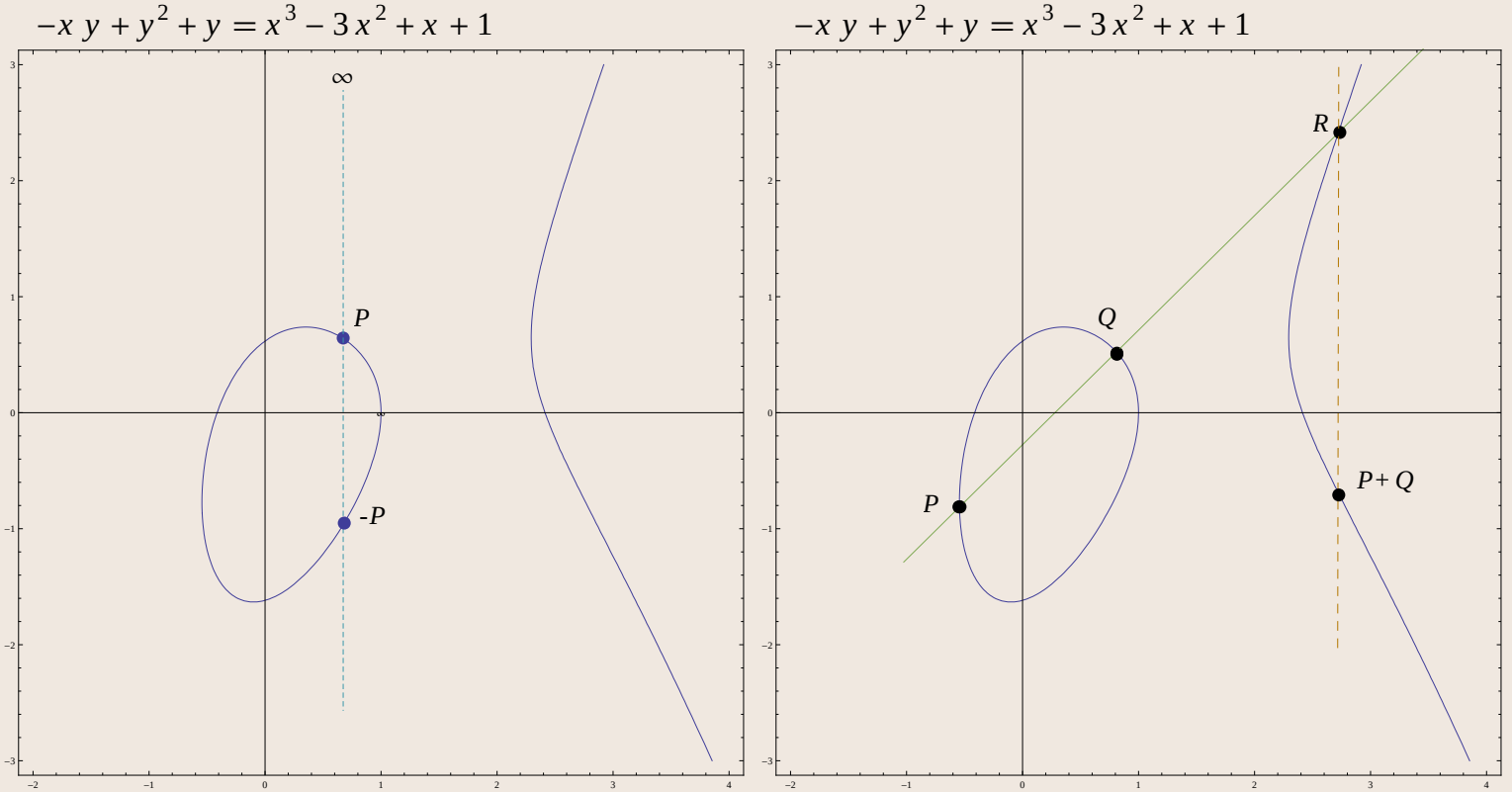




If $P, Q \in E(K), r_{P,Q}$ : $\begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q, \end{cases}$

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




$r_{P,\infty} \cap E(K) = \{P, \infty, P'\}$ $\rightsquigarrow$ $-P := P'$

$r_{P,Q} \cap E(K) = \{P, Q, R\}$ $\rightsquigarrow$ $P +_E Q := -R$

## Theorem

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

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

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

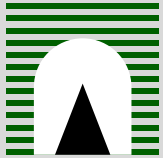
(c) $P +_E (-P) = \infty$ $\quad \forall P \in E$

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

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

*So $(E(\bar{K}), +_E)$ is an abelian group.*





**Theorem**

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

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

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

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

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

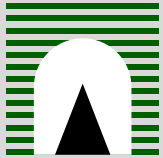
(e) $P +_E Q = Q +_E P$ $\quad \forall P, Q \in E$

*So $(E(\bar{K}), +_E)$ is an abelian group.*

**Remark:**

If $E/K \Rightarrow \forall L, K \subseteq L \subseteq \bar{K}, E(L)$ is an abelian group.





**Theorem**

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

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

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

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

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

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

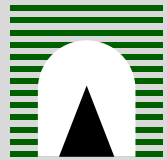
*So $(E(\bar{K}), +_E)$ is an abelian group.*

**Remark:**

If $E/K \Rightarrow \forall L, K \subseteq L \subseteq \bar{K}, E(L)$ is an abelian group.

$$-P = -(x_1, y_1) = (x_1, -a_1 x_1 - a_3 - y_1)$$

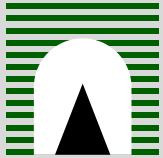




# Proof of the associativity

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



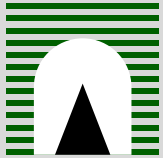


# Proof of the associativity

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

We should verify the above in many different cases according if $Q = R$, $P = Q$, $P = Q +_E R, \ldots$





# Proof of the associativity

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

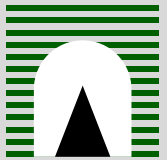
We should verify the above in many different cases according if $Q = R$, $P = Q$, $P = Q +_E R, \ldots$

Here we deal with the *generic case*. i.e. All the points $\pm P, \pm R, \pm Q, \pm(Q +_E R), \pm(P +_E Q), \infty$ all different

Mathematica code

```
L[x_,y_,r_,s_]:=(s-y)/(r-x);
M[x_,y_,r_,s_]:=(yr-sx)/(r-x);
A[{x_,y_},{r_,s_}]:={(L[x,y,r,s])^2-(x+r),
              -(L[x,y,r,s])^3+L[x,y,r,s](x+r)-M[x,y,r,s]}
Together[A[A[{x,y},{u,v}],{h,k}]-A[{x,y},A[{u,v},{h,k}]]]
det = Det[({{1,x1,x1^3-y1^2},{1,x2,x2^3-y2^2},{1,x3,x3^3-y3^2}})]
PolynomialQ[Together[Numerator[Factor[res[[1]]]]/det],
                          {x1,x2,x3,y1,y2,y3}]
PolynomialQ[Together[Numerator[Factor[res[[2]]]]/det],
                          {x1,x2,x3,y1,y2,y3}]
```





# Proof of the associativity

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

We should verify the above in many different cases according if $Q = R$, $P = Q$, $P = Q +_E R, \ldots$

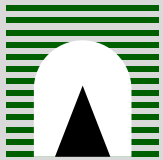
Here we deal with the *generic case*. i.e. All the points $\pm P, \pm R, \pm Q, \pm(Q +_E R), \pm(P +_E Q), \infty$ all different

Mathematica code

```
L[x_,y_,r_,s_]:=(s-y)/(r-x);
M[x_,y_,r_,s_]:=(yr-sx)/(r-x);
A[{x_,y_},{r_,s_}]:={(L[x,y,r,s])^2-(x+r),
              -(L[x,y,r,s])^3+L[x,y,r,s](x+r)-M[x,y,r,s]}
Together[A[A[{x,y},{u,v}],{h,k}]-A[{x,y},A[{u,v},{h,k}]]]
det = Det[({{1,x1,x1^3-y1^2},{1,x2,x2^3-y2^2},{1,x3,x3^3-y3^2}})]
PolynomialQ[Together[Numerator[Factor[res[[1]]]]/det],
                          {x1,x2,x3,y1,y2,y3}]
PolynomialQ[Together[Numerator[Factor[res[[2]]]]/det],
                          {x1,x2,x3,y1,y2,y3}]
```

- runs in 2 seconds on a PC





# Proof of the associativity

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

We should verify the above in many different cases according if $Q = R$, $P = Q$, $P = Q +_E R, \ldots$

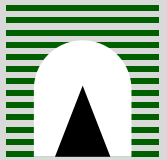
Here we deal with the *generic case*. i.e. All the points $\pm P, \pm R, \pm Q, \pm(Q +_E R), \pm(P +_E Q), \infty$ all different

Mathematica code

```
L[x_,y_,r_,s_]:=(s-y)/(r-x);
M[x_,y_,r_,s_]:=(yr-sx)/(r-x);
A[{x_,y_},{r_,s_}]:={(L[x,y,r,s])^2-(x+r),
              -(L[x,y,r,s])^3+L[x,y,r,s](x+r)-M[x,y,r,s]}
Together[A[A[{x,y},{u,v}],{h,k}]-A[{x,y},A[{u,v},{h,k}]]]
det = Det[({{1,x1,x1^3-y1^2},{1,x2,x2^3-y2^2},{1,x3,x3^3-y3^2}})]
PolynomialQ[Together[Numerator[Factor[res[[1]]]]/det],
                          {x1,x2,x3,y1,y2,y3}]
PolynomialQ[Together[Numerator[Factor[res[[2]]]]/det],
                          {x1,x2,x3,y1,y2,y3}]
```

- runs in 2 seconds on a PC
- More cases to check. e.g $P +_E 2Q = (P +_E Q) +_E Q$





# Formulas for Addition on $E$ (Summary)

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

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

## Addition Laws for the sum of affine points

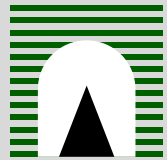
- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

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

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





# Formulas for Addition on $E$ (Summary)

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

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

## Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

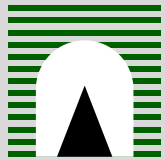
- If $P_1 = P_2$
  - $2y_1 + a_1x + a_3 = 0$ $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$
  - $2y_1 + a_1x + a_3 \neq 0$

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

Then

$$P_1 +_E P_2 = (\lambda^2 - a_1\lambda - a_2 - x_1 - x_2, -\lambda^3 - a_1^2\lambda + (\lambda + a_1)(a_2 + x_1 + x_2) - a_3 - \nu)$$





# Formulas for Addition on $E$ (Summary for special equation)

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

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

## Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

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

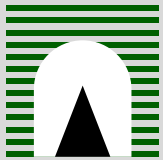
- If $P_1 = P_2$
  - $y_1 = 0$ $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$
  - $y_1 \neq 0$

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}$$

Then

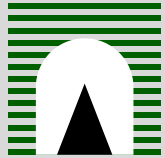
$$P_1 +_E P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu)$$





# Points of order (dividing) $m$





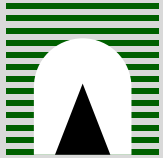
# Points of order (dividing) $m$

## Definition ($m$–torsion point)

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

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





# Points of order (dividing) $m$

**Definition ($m$–torsion point)**

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

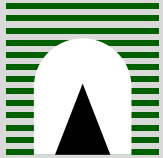
$$E[m] = \{P \in E(\bar{K}) : \ mP = \infty\}$$

**Theorem (Structure of Torsion Points)**

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

Dipartim. Mat. & Fis.

Università Roma Tre



# Points of order (dividing) $m$

**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)**

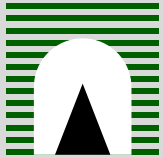
*Let* $E/K$ *and* $m \in \mathbb{N}$. *If* $p = \mathrm{char}(K) \nmid m$,

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

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

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





# Points of order (dividing) $m$

**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* $p = \mathrm{char}(K) \nmid m$,

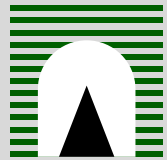
$$E[m] \cong C_m \oplus C_m$$

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

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

$$E/\mathbb{F}_p \text{ is called } \begin{cases} \textit{ordinary} & \text{if } E[p] \cong C_p \\ \textit{supersingular} & \text{if } E[p] = \{\infty\} \end{cases}$$





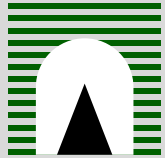
# Group Structure of $E(\mathbb{F}_q)$

## Corollary

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

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





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

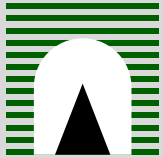
## Corollary

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

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

## Proof.





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

## Corollary

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

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

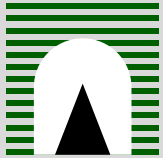
## Proof.

From classification Theorem of finite abelian group

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

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





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

## Corollary

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

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

## Proof.

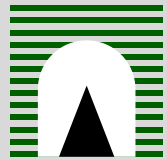
From classification Theorem of finite abelian group

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

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

Hence $E(\mathbb{F}_q)$ contains $n_1^r$ points of order dividing $n_1$.





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

## Corollary

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

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

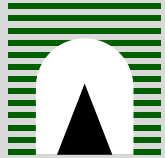
## Proof.

From classification Theorem of finite abelian group

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

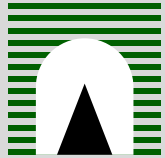
with $n_i | n_{i+1}$ for $i \geq 1$.
Hence $E(\mathbb{F}_q)$ contains $n_1^r$ points of order dividing $n_1$.
From *Structure of Torsion Theorem*, $\#E[n_1] \leq n_1^2$. So $r \leq 2$ □





# The division polynomials

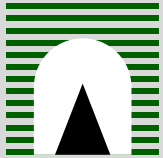




# The division polynomials

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





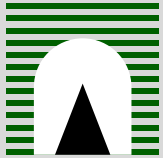
# The division polynomials

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

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

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





# The division polynomials

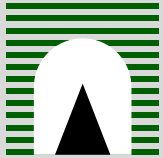
**Definition (Division Polynomials of $E : y^2 = x^3 + Ax + B$)**

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

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

There are more more complicated formulas for general Weierstraß equations.



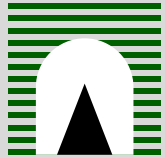


# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$



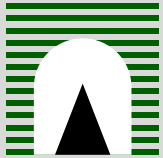


# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$



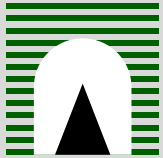


# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left( x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)} \right) = \left( \frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right)$





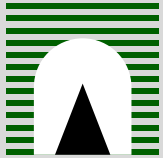
# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$

  where





# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$

  where

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

# The division polynomials (continues)

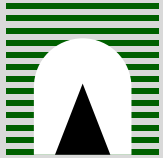
## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$

  where

  $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$
- $\#E[m] = \#\{P \in E(\bar{K}) : mP = \infty\} \begin{cases} = m^2 & \text{if } p \nmid m \\ < m^2 & \text{if } p \mid m \end{cases}$



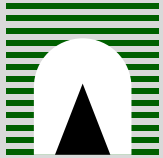


# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$
  where
  $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$
- $\#E[m] = \#\{P \in E(\bar{K}) : mP = \infty\} \begin{cases} = m^2 & \text{if } p \nmid m \\ < m^2 & \text{if } p \mid m \end{cases}$
- $E[2m+1] = \{\infty\} \cup \{(x,y) \in E(\bar{K}) : \psi_{2m+1}(x) = 0\}$





# The division polynomials (continues)

## Properties of division polynomials

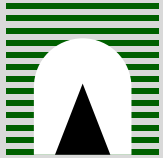
- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$

  where

  $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$
- $\#E[m] = \#\{P \in E(\bar{K}) : mP = \infty\} \begin{cases} = m^2 & \text{if } p \nmid m \\ < m^2 & \text{if } p \mid m \end{cases}$
- $E[2m+1] = \{\infty\} \cup \{(x,y) \in E(\bar{K}) : \psi_{2m+1}(x) = 0\}$
- $E[2m] = E[2] \cup \{(x,y) \in E(\bar{K}) : \psi'_{2m}(x) = 0\}$

  $\psi'_{2m} := \psi_{2m}/2y$





# The division polynomials (continues)

## Properties of division polynomials

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$

  where

  $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$
- $\#E[m] = \#\{P \in E(\bar{K}) : mP = \infty\} \begin{cases} = m^2 & \text{if } p \nmid m \\ < m^2 & \text{if } p \mid m \end{cases}$
- $E[2m+1] = \{\infty\} \cup \{(x,y) \in E(\bar{K}) : \psi_{2m+1}(x) = 0\}$
- $E[2m] = E[2] \cup \{(x,y) \in E(\bar{K}) : \psi'_{2m}(x) = 0\}$

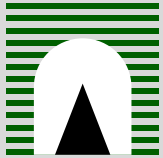
  $\psi'_{2m} := \psi_{2m}/2y$
- The structure theorem of $E[m]$ follows form these properties

# Endomorphisms

## Definition

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





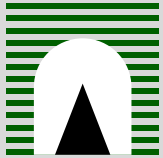
# Endomorphisms

## Definition

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

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





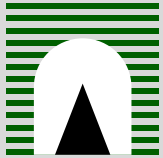
# Endomorphisms

## Definition

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

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





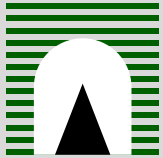
# Endomorphisms

## Definition

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

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





# Endomorphisms

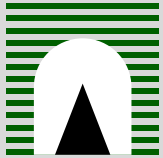
## Definition

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

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ 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*,





# Endomorphisms

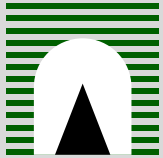
## Definition

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

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ 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*, $\alpha(\infty) = \infty$ )





# Endomorphisms

## Definition

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

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ 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*, $\alpha(\infty) = \infty$ )

## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$

# Endomorphisms

## Definition

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

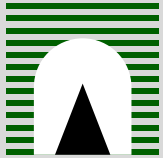
- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

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

## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$
- if $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.





# Endomorphisms

## Definition

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

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ 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*, $\alpha(\infty) = \infty$ )

## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$
- if $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.
  - The **degree** of $\alpha$ is $\deg \alpha := \max\{\deg p, \deg q\}$

# Endomorphisms

## Definition

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

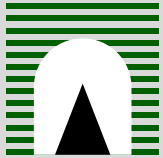
- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

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

## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$
- if $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.
  - The **degree** of $\alpha$ is $\deg \alpha := \max\{\deg p, \deg q\}$
  - $\alpha$ is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)





# Endomorphisms

## Definition

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

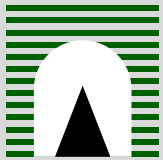
- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

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

## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$
- if $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.
  - The **degree** of $\alpha$ is $\deg \alpha := \max\{\deg p, \deg q\}$
  - $\alpha$ is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)
- $[m](x, y) = \left( \frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3} \right)$ 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

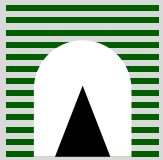
- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ is a group homomorphism)
- $\exists R_1, R_2 \in \bar{K}(x, y)$ s.t.
  $\alpha(x, y) = (R_1(x, y), R_2(x, y)) \qquad \forall (x, y) \notin \mathrm{Ker}(\alpha)$

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

## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$
- if $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.
  - The **degree** of $\alpha$ is $\deg \alpha := \max\{\deg p, \deg q\}$
  - $\alpha$ is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)
- $[m](x, y) = \left( \frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3} \right)$ is an endomorphism $\forall m \in \mathbb{Z}$
- if $E/\mathbb{F}_q$, $\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q)$ is called *Frobenius Endomorphism*





# Endomorphisms

## Definition

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

- $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$ ($\alpha$ 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*, $\alpha(\infty) = \infty$ )

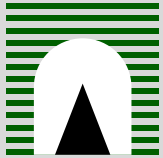
## Facts about Endomorphisms

- can assume that $\alpha(x, y) = (r_1(x), y r_2(x)), \qquad r_1, r_2 \in \bar{K}(x)$
- if $r_1(x) = p(x)/q(x)$ with $\gcd(p(x), q(x)) = 1$.
  - The **degree** of $\alpha$ is $\deg \alpha := \max\{\deg p, \deg q\}$
  - $\alpha$ is said **separable** if $(p'(x), q'(x)) \neq (0, 0)$ (identically)
- $[m](x, y) = \left( \frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3} \right)$ is an endomorphism $\forall m \in \mathbb{Z}$
- if $E/\mathbb{F}_q$, $\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q)$ is called *Frobenius Endomorphism*
- If $\alpha \neq [0]$ is an endomorphism, then it is surjective

## Facts about Endomorphisms (continues)

- $\Phi_q(x, y) = (x^q, y^q)$ is endomorphism

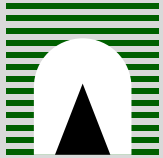




## Facts about Endomorphisms (continues)

- $\Phi_q(x, y) = (x^q, y^q)$ is endomorphism
- $\Phi_q$ is non separable and $\deg \Phi_q = q$

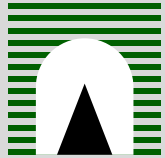




## Facts about Endomorphisms (continues)

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

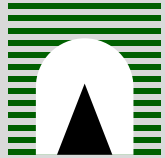




## Facts about Endomorphisms (continues)

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



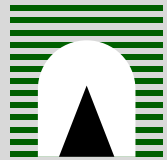


## Facts about Endomorphisms (continues)

- $\Phi_q(x,y) = (x^q, y^q)$ is endomorphism
- $\Phi_q$ is non separable and $\deg \Phi_q = q$
- $[m](x,y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right)$ has degree $m^2$
- $[m]$ separable iff $p \nmid m$.
- Let $\alpha \neq 0$ be an endomorphism. Then

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

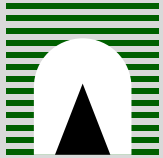




# The ring Endomorphisms

## Definition





# The ring Endomorphisms

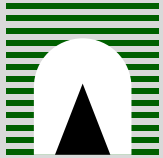
## Definition

Let $E/K$. The *ring of endomorphisms*

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

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





# The ring Endomorphisms

## Definition

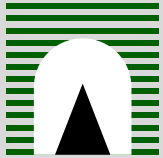
Let $E/K$. The *ring of endomorphisms*

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

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

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





# The ring Endomorphisms

## Definition

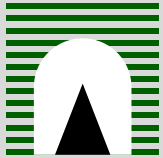
Let $E/K$. The *ring of endomorphisms*

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

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

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





# The ring Endomorphisms

## Definition

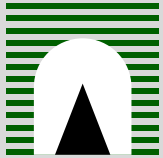
Let $E/K$. The *ring of endomorphisms*

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

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

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





# The ring Endomorphisms

## Definition

Let $E/K$. The *ring of endomorphisms*

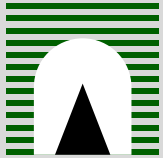
$$\mathrm{End}(E) := \{\alpha : E \to E, \alpha \text{ is an endomorphism}\}.$$

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

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

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





# The ring Endomorphisms

## Definition

Let $E/K$. The *ring of endomorphisms*

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

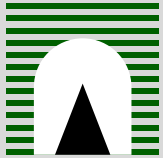
where for all $\alpha_1, \alpha_2 \in \mathrm{End}(E)$,

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

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

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





# The ring Endomorphisms

## Definition

Let $E/K$. The *ring of endomorphisms*

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

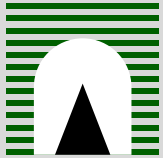
where for all $\alpha_1, \alpha_2 \in \mathrm{End}(E)$,

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

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

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





# The ring Endomorphisms

## Definition

Let $E/K$. The *ring of endomorphisms*

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

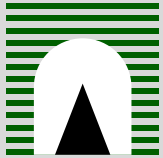
where for all $\alpha_1, \alpha_2 \in \mathrm{End}(E)$,

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

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

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





# The ring Endomorphisms

## Definition

Let $E/K$. The *ring of endomorphisms*

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

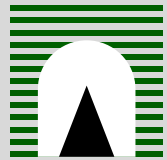
where for all $\alpha_1, \alpha_2 \in \mathrm{End}(E)$,

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

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

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \subseteq \mathrm{End}(E)$
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$





# The ring Endomorphisms

## Definition

Let $E/K$. The *ring of endomorphisms*

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

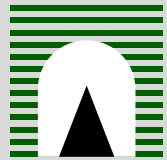
where for all $\alpha_1, \alpha_2 \in \mathrm{End}(E)$,

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

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

- $[0] : P \mapsto \infty$ is the zero element
- $[1] : P \mapsto P$ is the identity element
- $\mathbb{Z} \subseteq \mathrm{End}(E)$
- if $K = \mathbb{F}_q$, $\Phi_q \in \mathrm{End}(E)$. So $\mathbb{Z}[\Phi_q] \subset \mathrm{End}(E)$
- $\Phi_q$ satisfied in $\mathrm{End}(E)$ the polynomial $X^2 - a_q X + q$ where $E(\mathbb{F}_q) = q + 1 - a_q$

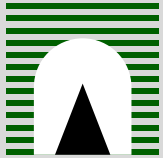




# Complex Multiplication curves

If $E/\mathbb{Q}$, then



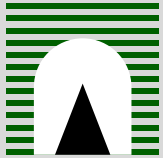


# Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)



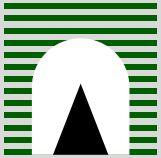


## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.



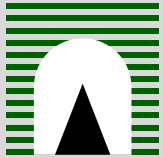


## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.





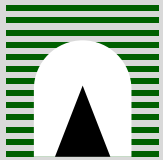
## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples





## Complex Multiplication curves

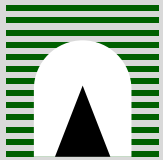
If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples

If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,





## Complex Multiplication curves

If $E/\mathbb{Q}$, then

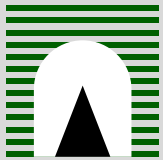
- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples

If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,

$$\iota : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (-x, iy) \quad (\infty \mapsto \infty)$$





## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

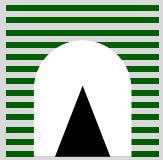
### Examples

If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,

$$\iota : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (-x, iy) \quad (\infty \mapsto \infty)$$

$\iota \in \mathrm{End}(E)$, $\iota$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\iota^2 = [-1]$).





## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples

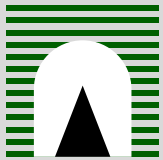
If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,

$$\iota : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (-x, iy) \quad (\infty \mapsto \infty)$$

$\iota \in \mathrm{End}(E)$, $\iota$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\iota^2 = [-1]$). Hence

$$\mathrm{End}(E) \supset \mathbb{Z}[i].$$





## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples

If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,

$$\iota : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (-x, iy) \quad (\infty \mapsto \infty)$$

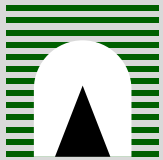
$\iota \in \mathrm{End}(E)$, $\iota$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\iota^2 = [-1]$). Hence

$$\mathrm{End}(E) \supset \mathbb{Z}[i].$$

If $E : y^2 = x^3 + d, d \in \mathbb{Z} \setminus \{0\}$, then

$$\omega : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (e^{2\pi i/3}x, y) \quad (\infty \mapsto \infty)$$





## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples

If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,

$$\iota : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (-x, iy) \quad (\infty \mapsto \infty)$$

$\iota \in \mathrm{End}(E)$, $\iota$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\iota^2 = [-1]$). Hence

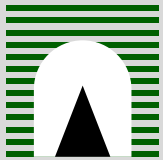
$$\mathrm{End}(E) \supset \mathbb{Z}[i].$$

If $E : y^2 = x^3 + d, d \in \mathbb{Z} \setminus \{0\}$, then

$$\omega : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (e^{2\pi i/3}x, y) \quad (\infty \mapsto \infty)$$

$\omega \in \mathrm{End}(E)$, $\omega$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\omega^3 = [1]$)





## Complex Multiplication curves

If $E/\mathbb{Q}$, then

- either $\mathrm{End}(E) \cong \mathbb{Z}$ (it happens most of the times)
- or $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

### Examples

If $E : y^2 = x^3 + dx, d \in \mathbb{Z} \setminus \{0\}$,

$$\iota : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (-x, iy) \quad (\infty \mapsto \infty)$$

$\iota \in \mathrm{End}(E)$, $\iota$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\iota^2 = [-1]$). Hence

$$\mathrm{End}(E) \supset \mathbb{Z}[i].$$

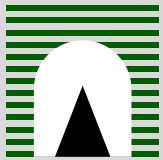
If $E : y^2 = x^3 + d, d \in \mathbb{Z} \setminus \{0\}$, then

$$\omega : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), (x, y) \mapsto (e^{2\pi i/3}x, y) \quad (\infty \mapsto \infty)$$

$\omega \in \mathrm{End}(E)$, $\omega$ is NOT of the form $[m], m \in \mathbb{Z}$ ($\omega^3 = [1]$)

$$\mathrm{End}(E) \cong \mathbb{Z}[\omega]$$





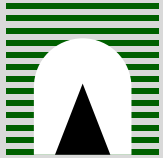
# Complex Multiplication curves (continues)

## Definition

Complex Multiplication Curves $E/\mathbb{Q}$ is called a *complex multiplication* (CM) curve if

$$\mathrm{End}(E) \supsetneq \mathbb{Z}$$





# Complex Multiplication curves (continues)

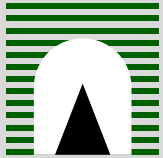
**Definition**

Complex Multiplication Curves $E/\mathbb{Q}$ is called a *complex multiplication* (CM) curve if

$$\mathrm{End}(E) \supsetneq \mathbb{Z}$$

- For $E/\mathbb{Q}$ CM, $\mathrm{End}(E)$ is always an order in a ring of integer of a quadratic field with class number $1$





# Complex Multiplication curves (continues)

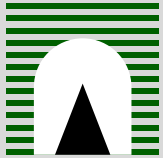
**Definition**

Complex Multiplication Curves $E/\mathbb{Q}$ is called a *complex multiplication* (CM) curve if

$$\mathrm{End}(E) \supsetneq \mathbb{Z}$$

- For $E/\mathbb{Q}$ CM, $\mathrm{End}(E)$ is always an order in a ring of integer of a quadratic field with class number $1$
- There are exactly 13 CM curves $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$





# Complex Multiplication curves (continues)

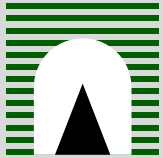
**Definition**

Complex Multiplication Curves $E/\mathbb{Q}$ is called a *complex multiplication* (CM) curve if

$$\mathrm{End}(E) \supsetneq \mathbb{Z}$$

- For $E/\mathbb{Q}$ CM, $\mathrm{End}(E)$ is always an order in a ring of integer of a quadratic field with class number $1$
- There are exactly 13 CM curves $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$
- They are completely classified





# Complex Multiplication curves (continues)

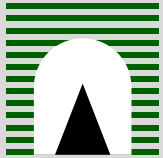
**Definition**

Complex Multiplication Curves $E/\mathbb{Q}$ is called a *complex multiplication* (CM) curve if

$$\mathrm{End}(E) \supsetneq \mathbb{Z}$$

- For $E/\mathbb{Q}$ CM, $\mathrm{End}(E)$ is always an order in a ring of integer of a quadratic field with class number $1$
- There are exactly 13 CM curves $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$
- They are completely classified





# Complex Multiplication curves (continues)

**Definition**

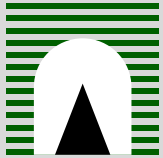
Complex Multiplication Curves $E/\mathbb{Q}$ is called a *complex multiplication* (CM) curve if

$$\mathrm{End}(E) \supsetneq \mathbb{Z}$$

- For $E/\mathbb{Q}$ CM, $\mathrm{End}(E)$ is always an order in a ring of integer of a quadratic field with class number $1$
- There are exactly 13 CM curves $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$
- They are completely classified

We shall focus on elliptic curves without CM.

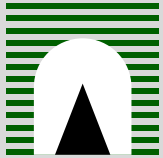




# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.

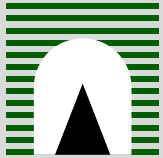




# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points



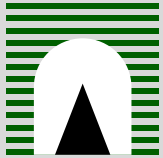


# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.





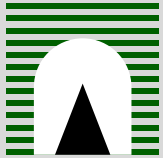
# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$





# Definition of Galois Representation

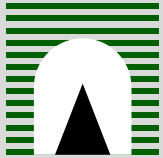
- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$





# Definition of Galois Representation

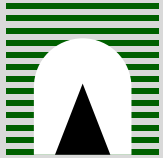
- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:





# Definition of Galois Representation

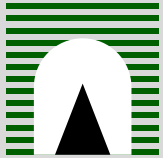
- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$





# Definition of Galois Representation

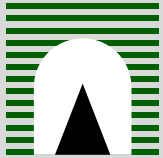
- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$
  - $\sigma P = (\sigma x_P, \sigma y_P) \in E[m]$





# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

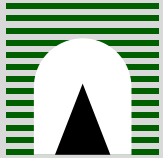
  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$
  - $\sigma P = (\sigma x_P, \sigma y_P) \in E[m]$

    $\sigma P \in E[m]$ is a consequence of the rationality $\psi_m$





# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points

  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

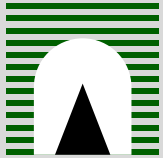
$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$
  - $\sigma P = (\sigma x_P, \sigma y_P) \in E[m]$

    $\sigma P \in E[m]$ is a consequence of the rationality $\psi_m$

    $\psi_m(\sigma x_P, \sigma y_P) = \sigma\psi_m(x_P, y_P) = 0$





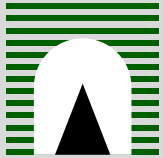
# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points
  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$
  - $\sigma P = (\sigma x_P, \sigma y_P) \in E[m]$
    $\sigma P \in E[m]$ is a consequence of the rationality $\psi_m$
    $\psi_m(\sigma x_P, \sigma y_P) = \sigma\psi_m(x_P, y_P) = 0$
  - $\sigma(\tau(P)) = (\sigma\tau)P$ and $1_{G_m}$ acts trivially





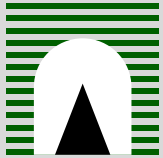
# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points
  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$
  - $\sigma P = (\sigma x_P, \sigma y_P) \in E[m]$
    $\sigma P \in E[m]$ is a consequence of the rationality $\psi_m$
    $\psi_m(\sigma x_P, \sigma y_P) = \sigma\psi_m(x_P, y_P) = 0$
  - $\sigma(\tau(P)) = (\sigma\tau)P$ and $1_{G_m}$ acts trivially
  - $\sigma(P+Q) = \sigma P + \sigma Q$





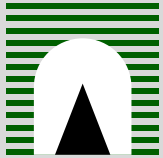
# Definition of Galois Representation

- $E/\mathbb{Q}$ be an elliptic curve.
- $\mathbb{Q}(E[m])$ is the Galois extension of $\mathbb{Q}$ of the $m$–torsion points
  it is obtained by adjoining to $\mathbb{Q}$ the cohordinates of the points in $E[m]$ i.e.

$$\mathbb{Q}(E[m]) = \prod_{(x,y)\in E[m]} \mathbb{Q}(x,y)$$

- $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$
- $G_m$ acts linearly on $E[m]$ in the following way:
  - if $\sigma \in G_m$, $P = (x_P, y_P) \in E[m]$
  - $\sigma P = (\sigma x_P, \sigma y_P) \in E[m]$
    $\sigma P \in E[m]$ is a consequence of the rationality $\psi_m$
    $\psi_m(\sigma x_P, \sigma y_P) = \sigma\psi_m(x_P, y_P) = 0$
  - $\sigma(\tau(P)) = (\sigma\tau)P$ and $1_{G_m}$ acts trivially
  - $\sigma(P+Q) = \sigma P + \sigma Q$
    apply $\sigma$ to the equations defining the group law



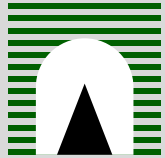


# Galois images

- The action of $G_m = \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q})$ on $E[m]$ induces a representation

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m])$$





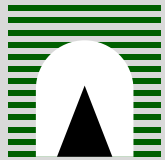
# Galois images

- The action of $G_m = \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q})$ on $E[m]$ induces a representation

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m])$$

we will refer to $\rho_{E,m}$ as the *mod-$m$ Galois representation attached to $E$*





# Galois images

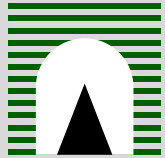
- The action of $G_m = \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q})$ on $E[m]$ induces a representation

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m])$$

  we will refer to $\rho_{E,m}$ as the *mod-$m$ Galois representation attached to $E$*
- By identifying $\mathrm{Aut}(E[m])$ with $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z})$,

Dipartim. Mat. & Fis.

Università Roma Tre



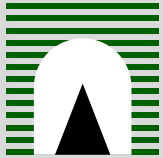
# Galois images

- The action of $G_m = \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q})$ on $E[m]$ induces a representation

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m])$$

  we will refer to $\rho_{E,m}$ as the *mod-$m$ Galois representation attached to $E$*
- By identifying $\mathrm{Aut}(E[m])$ with $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z})$, we can think at the image of $\rho_{E,m}$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$

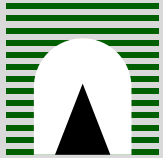




# Surjectivity of $\rho_{E,\ell}, \ell$ prime

Assume that $E$ is without complex multiplication ($\mathrm{End}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$, is usually surjective.

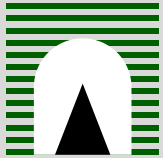




# Surjectivity of $\rho_{E,\ell}, \ell$ prime

Assume that $E$ is without complex multiplication ($\mathrm{End}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$, is usually surjective.
But if $E$ has CM, then $\rho_{E,\ell}$, is never surjective for $\ell > 2$.

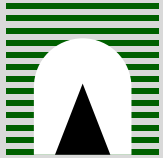




# Surjectivity of $\rho_{E,\ell}, \ell$ prime

Assume that $E$ is without complex multiplication ($\mathrm{End}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$, is usually surjective.
But if $E$ has CM, then $\rho_{E,\ell}$, is never surjective for $\ell > 2$.
Let $K$ be a number field and let $E/K$ be an elliptic curve.





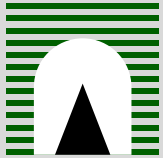
# Surjectivity of $\rho_{E,\ell}, \ell$ prime

Assume that $E$ is without complex multiplication ($\mathrm{End}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$, is usually surjective.
But if $E$ has CM, then $\rho_{E,\ell}$, is never surjective for $\ell > 2$.
Let $K$ be a number field and let $E/K$ be an elliptic curve.

**Theorem (Serre)**

*If $E/K$ does not have CM then $\mathrm{im}\,\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all sufficiently large primes $\ell$.*





# Surjectivity of $\rho_{E,\ell}, \ell$ prime

Assume that $E$ is without complex multiplication ($\mathrm{End}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$, is usually surjective.
But if $E$ has CM, then $\rho_{E,\ell}$, is never surjective for $\ell > 2$.
Let $K$ be a number field and let $E/K$ be an elliptic curve.

**Theorem (Serre)**

*If $E/K$ does not have CM then $\mathrm{im}\,\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all sufficiently large primes $\ell$.*

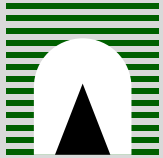
**Conjecture**

For each number field $K$ there is a uniform bound $\ell_{\max}$ such that

$$\mathrm{im}\,\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

for every $E/K$ and every $\ell > \ell_{\max}$.





# Surjectivity of $\rho_{E,\ell}, \ell$ prime

Assume that $E$ is without complex multiplication ($\mathrm{End}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$, is usually surjective.
But if $E$ has CM, then $\rho_{E,\ell}$, is never surjective for $\ell > 2$.
Let $K$ be a number field and let $E/K$ be an elliptic curve.

**Theorem (Serre)**

*If $E/K$ does not have CM then $\mathrm{im}\,\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all sufficiently large primes $\ell$.*

**Conjecture**

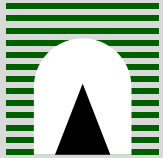
For each number field $K$ there is a uniform bound $\ell_{\max}$ such that

$$\mathrm{im}\,\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

for every $E/K$ and every $\ell > \ell_{\max}$.

For $K = \mathbb{Q}$, it is generally believed that $\ell_{\max} = 37$.

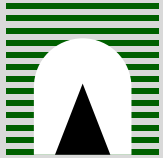




# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.



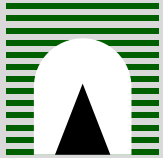


# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$





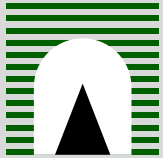
# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ this occurs for $\ell \leq 7$ (Mazur).





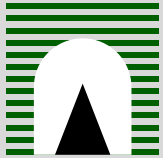
# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ this occurs for $\ell \leq 7$ (Mazur).
If $E$ admits a rational $\ell$-isogeny, then $\rho_{E,\ell}$, is not surjective.





# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

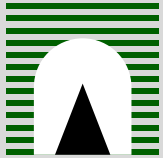
If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ this occurs for $\ell \leq 7$ (Mazur).
If $E$ admits a rational $\ell$-isogeny, then $\rho_{E,\ell}$, is not surjective.
In fact in such a case, a base of $E[\ell]$ can be chosen is such a way that

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z}, a, c \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$





# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

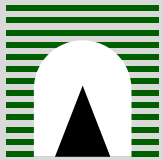
$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ this occurs for $\ell \leq 7$ (Mazur).
If $E$ admits a rational $\ell$-isogeny, then $\rho_{E,\ell}$, is not surjective.
In fact in such a case, a base of $E[\ell]$ can be chosen is such a way that

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z}, a, c \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ without CM, this occurs for $\ell \leq 17$ and $\ell = 37$ (Mazur).





# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

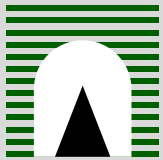
$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ this occurs for $\ell \leq 7$ (Mazur).
If $E$ admits a rational $\ell$-isogeny, then $\rho_{E,\ell}$, is not surjective.
In fact in such a case, a base of $E[\ell]$ can be chosen is such a way that

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z}, a, c \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ without CM, this occurs for $\ell \leq 17$ and $\ell = 37$ (Mazur).
But $\rho_{E,\ell}$, may be non-surjective even when $E$ does not admit a rational $\ell$-isogeny.





# Non–surjectivity of $\rho_{E,\ell}$, $\ell$ prime

If $E$ has a rational point of order $\ell$, then $\rho_{E,\ell}$, is NOT surjective.
In fact if $P$ is such a point, and $E[\ell] = \langle P, Q \rangle$, then

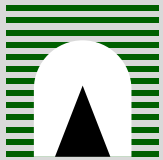
$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}, b \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ this occurs for $\ell \leq 7$ (Mazur).
If $E$ admits a rational $\ell$-isogeny, then $\rho_{E,\ell}$, is not surjective.
In fact in such a case, a base of $E[\ell]$ can be chosen is such a way that

$$\operatorname{im} \rho_{E,\ell} \subset \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z}, a, c \in \mathbb{Z}/\ell\mathbb{Z}^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

For $E/\mathbb{Q}$ without CM, this occurs for $\ell \leq 17$ and $\ell = 37$ (Mazur).
But $\rho_{E,\ell}$, may be non-surjective even when $E$ does not admit a rational $\ell$-isogeny.
Even when $E$ has a rational $\ell$-torsion point, this does not determine the image of $\rho_{E,\ell}$.

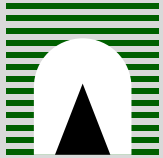




# Absolute Galois Group

- The absolute Galois group
  $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}},\ \text{field automorphism}\}$
  is a profinite group



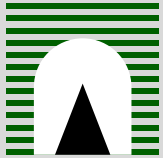


# Absolute Galois Group

- The absolute Galois group
  $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}},\ \text{field automorphism}\}$
  is a profinite group
- If $K$ is any Galois extension of $\mathbb{Q}$, then

$$\mathrm{Gal}(K/\mathbb{Q}) \cong G_{\mathbb{Q}}/\{\sigma \in G_{\mathbb{Q}} : \sigma_{|K} = \mathrm{id}_K\}$$





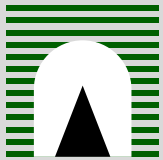
# Absolute Galois Group

- The absolute Galois group
  $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}},\ \text{field automorphism}\}$
  is a profinite group
- If $K$ is any Galois extension of $\mathbb{Q}$, then

$$\mathrm{Gal}(K/\mathbb{Q}) \cong G_{\mathbb{Q}}/\{\sigma \in G_{\mathbb{Q}} : \sigma_{|K} = \mathrm{id}_K\}$$

- So $G_{\mathbb{Q}}$ admits as quotient any possible Galois Group of Galois extensions of $\mathbb{Q}$ and it is the projective limit of its finite quotients





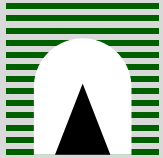
# Absolute Galois Group

- The absolute Galois group
  $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}},\ \text{field automorphism}\}$
  is a profinite group
- If $K$ is any Galois extension of $\mathbb{Q}$, then

$$\mathrm{Gal}(K/\mathbb{Q}) \cong G_{\mathbb{Q}}/\{\sigma \in G_{\mathbb{Q}} : \sigma_{|K} = \mathrm{id}_K\}$$

- So $G_{\mathbb{Q}}$ admits as quotient any possible Galois Group of Galois extensions of $\mathbb{Q}$ and it is the projective limit of its finite quotients
- Recall *$n$–torsion field* $\mathbb{Q}(E[n])$ and $G_m = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.





# Absolute Galois Group

- The absolute Galois group
  $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}},\ \text{field automorphism}\}$
  is a profinite group
- If $K$ is any Galois extension of $\mathbb{Q}$, then

$$\mathrm{Gal}(K/\mathbb{Q}) \cong G_{\mathbb{Q}}/\{\sigma \in G_{\mathbb{Q}} : \sigma_{|_K} = \mathrm{id}_K\}$$

- So $G_{\mathbb{Q}}$ admits as quotient any possible Galois Group of Galois extensions of $\mathbb{Q}$ and it is the projective limit of its finite quotients
- Recall *$n$–torsion field* $\mathbb{Q}(E[n])$ and $G_m = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.
- The mod $m$–representation

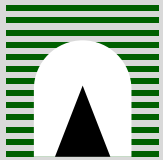
$$\rho_{E,n} : G_n \hookrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

can be extended to

$$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\infty])$$

where $E[\infty] = \cup_{m\in\mathbb{N}} E[m]$ is the *torsion subgroup* of $E(\overline{\mathbb{Q}})$.





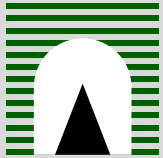
# $\ell$–adic representations

Consider the decomposition:

$$\mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where





# $\ell$–adic representations

Consider the decomposition:

$$\mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where $E[\ell^\infty] = \cup_{m \in \mathbb{N}} E[\ell^m]$ and $\mathbb{Z}_\ell$ denoted the ring of $\ell$–*adic integers*.

# $\ell$–adic representations

Consider the decomposition:

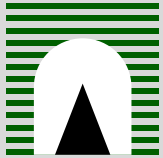
$$\mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where $E[\ell^\infty] = \cup_{m\in\mathbb{N}} E[\ell^m]$ and $\mathbb{Z}_\ell$ denoted the ring of $\ell$–*adic integers*.
For every fixed prime $\ell$, the projection

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is called $\ell$–adic representation attached to $E$.





# $\ell$–adic representations

Consider the decomposition:

$$\mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where $E[\ell^\infty] = \cup_{m\in\mathbb{N}} E[\ell^m]$ and $\mathbb{Z}_\ell$ denoted the ring of $\ell$–*adic integers*.
For every fixed prime $\ell$, the projection

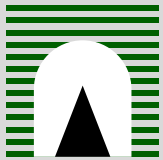
$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is called $\ell$–adic representation attached to $E$.

- $\rho_{E,\ell^\infty}$ is *unramified* at all $p \nmid \ell\Delta_E$ (i.e. $\rho_\ell|_{I_\mathfrak{p}} = \mathrm{Id}_{\mathbb{Z}_\ell}$ where, if $\mathfrak{p}$ is a prime of $\bar{\mathbb{Q}}$ over $p$, the *inertia subgroup*

$$I_\mathfrak{p} \subset G_{\mathbb{Q}} = \{\sigma \in G_{\mathbb{Q}} : \sigma(x) \equiv x \bmod \mathfrak{p}, \quad \forall x \in \bar{\mathbb{Z}}\}$$





# $\ell$–adic representations

Consider the decomposition:

$$\mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where $E[\ell^\infty] = \cup_{m\in\mathbb{N}} E[\ell^m]$ and $\mathbb{Z}_\ell$ denoted the ring of $\ell$–*adic integers*.
For every fixed prime $\ell$, the projection

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

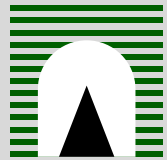
is called $\ell$–adic representation attached to $E$.

- $\rho_{E,\ell^\infty}$ is *unramified* at all $p \nmid \ell\Delta_E$ (i.e. $\rho_\ell|_{I_\mathfrak{p}} = \mathrm{Id}_{\mathbb{Z}_\ell}$ where, if $\mathfrak{p}$ is a prime of $\bar{\mathbb{Q}}$ over $p$, the *inertia subgroup*

$$I_\mathfrak{p} \subset G_{\mathbb{Q}} = \{\sigma \in G_{\mathbb{Q}} : \sigma(x) \equiv x \bmod \mathfrak{p}, \quad \forall x \in \bar{\mathbb{Z}}\}$$

- For all primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open in the $\ell$–adic topology





# $\ell$–adic representations

Consider the decomposition:

$$\mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where $E[\ell^\infty] = \cup_{m\in\mathbb{N}} E[\ell^m]$ and $\mathbb{Z}_\ell$ denoted the ring of $\ell$–*adic integers*.
For every fixed prime $\ell$, the projection

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

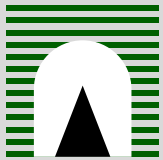
is called $\ell$–adic representation attached to $E$.

- $\rho_{E,\ell^\infty}$ is *unramified* at all $p \nmid \ell\Delta_E$ (i.e. $\rho_\ell|_{I_\mathfrak{p}} = \mathrm{Id}_{\mathbb{Z}_\ell}$ where, if $\mathfrak{p}$ is a prime of $\bar{\mathbb{Q}}$ over $p$, the *inertia subgroup*

$$I_\mathfrak{p} \subset G_{\mathbb{Q}} = \{\sigma \in G_{\mathbb{Q}} : \sigma(x) \equiv x \bmod \mathfrak{p}, \quad \forall x \in \bar{\mathbb{Z}}\}$$

- For all primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open in the $\ell$–adic topology
- For all but finitely many primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}}) = \mathrm{Aut}(E[\ell^\infty])$.





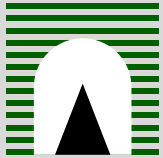
# Serre Uniformity Theorem

The statements:

1. For all primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open subgroup with respect to the $\ell$–adic topology,
2. For all but finitely many primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}}) = \mathrm{Aut}(E[\ell^\infty])$.

are equivalent to





# Serre Uniformity Theorem

The statements:

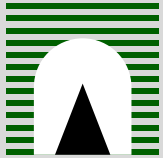
1. For all primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open subgroup with respect to the $\ell$–adic topology,
2. For all but finitely many primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}}) = \mathrm{Aut}(E[\ell^\infty])$.

are equivalent to

**Theorem (Serre's Uniformity Theorem)**

*If $E$ is not CM, then the index of $\rho_n(G(n))$ inside $\mathrm{Aut}(E[n])$ is bounded by a constant that depends only on $E$.*





# Serre Uniformity Theorem

The statements:

1. For all primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open subgroup with respect to the $\ell$–adic topology,
2. For all but finitely many primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}}) = \mathrm{Aut}(E[\ell^\infty])$.

are equivalent to

**Theorem (Serre's Uniformity Theorem)**

*If $E$ is not CM, then the index of $\rho_n(G(n))$ inside $\mathrm{Aut}(E[n])$ is bounded by a constant that depends only on $E$.*

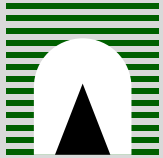
which in particular implies

**Corollary**

*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$





# Serre Uniformity Theorem

The statements:

1. For all primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open subgroup with respect to the $\ell$–adic topology,
2. For all but finitely many primes $\ell$, $\rho_{\ell^\infty}(G_{\mathbb{Q}}) = \mathrm{Aut}(E[\ell^\infty])$.

are equivalent to

**Theorem (Serre's Uniformity Theorem)**

*If $E$ is not CM, then the index of $\rho_n(G(n))$ inside $\mathrm{Aut}(E[n])$ is bounded by a constant that depends only on $E$.*

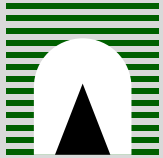
which in particular implies

**Corollary**

*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$





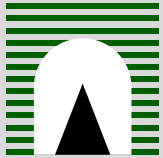
# The Definition of Serre Curve

## Corollary

*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$





# The Definition of Serre Curve

## Corollary

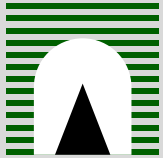
*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$

## Question:

Is it possible that for some curve $E/\mathbb{Q}$,
$G_m = \mathrm{Aut}(E[m])$ for all $m \in \mathbb{N}$?





# The Definition of Serre Curve

## Corollary

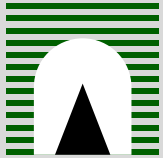
*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$

## Question:

Is it possible that for some curve $E/\mathbb{Q}$,
$G_m = \mathrm{Aut}(E[m])$ for all $m \in \mathbb{N}$? Answer is NO!!





# The Definition of Serre Curve

## Corollary

*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$

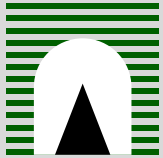
## Question:

Is it possible that for some curve $E/\mathbb{Q}$,
$G_m = \mathrm{Aut}(E[m])$ for all $m \in \mathbb{N}$? Answer is NO!!

The above statement is equivalent to

$$\rho_E : G_{\mathbb{Q}} \cong \mathrm{Aut}(E[\infty])$$





# The Definition of Serre Curve

## Corollary

*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$

## Question:

Is it possible that for some curve $E/\mathbb{Q}$,
$G_m = \mathrm{Aut}(E[m])$ for all $m \in \mathbb{N}$? Answer is NO!!

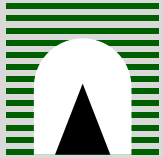
The above statement is equivalent to

$$\rho_E : G_{\mathbb{Q}} \cong \mathrm{Aut}(E[\infty])$$

Serre showed

$$\rho(G_{\mathbb{Q}}) \subseteq \mathcal{H}_E \subset \mathrm{Aut}(E[\infty])$$





# The Definition of Serre Curve

## Corollary

*If $E$ in not CM, then $\forall \ell$ large enough*

$$G_\ell = \mathrm{Aut}(E[\ell])$$

## Question:

Is it possible that for some curve $E/\mathbb{Q}$,
$G_m = \mathrm{Aut}(E[m])$ for all $m \in \mathbb{N}$? Answer is NO!!

The above statement is equivalent to

$$\rho_E : G_{\mathbb{Q}} \cong \mathrm{Aut}(E[\infty])$$

Serre showed

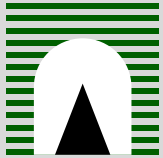
$$\rho(G_{\mathbb{Q}}) \subseteq \mathcal{H}_E \subset \mathrm{Aut}(E[\infty])$$

where

$$[\mathrm{Aut}(E[\infty]) : \mathcal{H}_E] = 2$$

$\mathcal{H}_E$ is the *Serre's Subgroup*





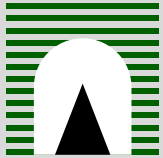
# The Definition of Serre Curve

The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where





# The Definition of Serre Curve

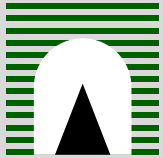
The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where

- $\pi_m : \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,





# The Definition of Serre Curve

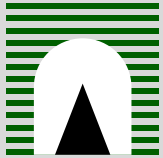
The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where

- $\pi_m : \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,
- $m_E$ is the *Serre number of* $E$: $m_E = [2, \mathrm{disc}(\mathbb{Q}(\sqrt{|\Delta_E|}))]$





# The Definition of Serre Curve

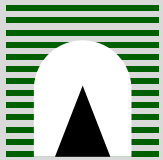
The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where

- $\pi_m : \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,
- $m_E$ is the *Serre number of* $E$: $\quad m_E = [2, \mathrm{disc}(\mathbb{Q}(\sqrt{|\Delta_E|}))]$
- $\varepsilon$ is the *signature map* (i.e. $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \to \{\pm 1\}$)





# The Definition of Serre Curve

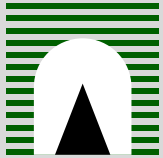
The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where

- $\pi_m : \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,
- $m_E$ is the *Serre number of* $E$: $\quad m_E = [2, \mathrm{disc}(\mathbb{Q}(\sqrt{|\Delta_E|}))]$
- $\varepsilon$ is the *signature map* (i.e. $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \to \{\pm 1\}$)





# The Definition of Serre Curve

The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where

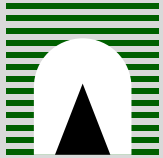
- $\pi_m : \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,
- $m_E$ is the *Serre number of* $E$: $\quad m_E = [2, \mathrm{disc}(\mathbb{Q}(\sqrt{|\Delta_E|}))]$
- $\varepsilon$ is the *signature map* (i.e. $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \to \{\pm 1\}$)

An elliptic curve $E/\mathbb{Q}$ is called *a Serre curve* if $\rho(G_{\mathbb{Q}}) = \mathcal{H}_E$.

**Theorem (N. Jones (2010))**

*Almost all elliptic curves are Serre's curves*





# The Definition of Serre Curve

The Serre's Subgroup:

$$\mathcal{H}_E = \pi_{m_E}^{-1}\left(\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}\right)$$

where

- $\pi_m : \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,
- $m_E$ is the *Serre number of* $E$: $\quad m_E = [2, \mathrm{disc}(\mathbb{Q}(\sqrt{|\Delta_E|}))]$
- $\varepsilon$ is the *signature map* (i.e. $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \to \{\pm 1\}$)

An elliptic curve $E/\mathbb{Q}$ is called *a Serre curve* if $\rho(G_{\mathbb{Q}}) = \mathcal{H}_E$.

**Theorem (N. Jones (2010))**

*Almost all elliptic curves are Serre's curves*

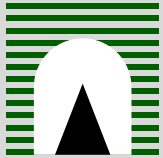
If $E$ admits a rational $\ell$–isogeny (a $\mathbb{Q}$–rational morphism of degree $\ell$, $E' \to E$), then $E$ it is NOT a Serre's curve

# The Frobenius Elements

## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.





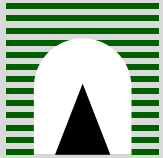
# The Frobenius Elements

## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$





# The Frobenius Elements

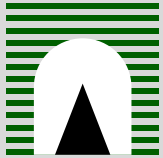
## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$

The *Artin symbol* $\left[\frac{K/\mathbb{Q}}{p}\right]$ is the conjugation class of all such $\sigma_{\mathcal{P}}$





# The Frobenius Elements

## Definition

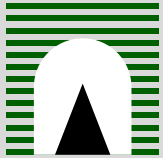
Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$

The *Artin symbol* $\left[\frac{K/\mathbb{Q}}{p}\right]$ is the conjugation class of all such $\sigma_{\mathcal{P}}$

If $\left[\frac{K/\mathbb{Q}}{p}\right] = \{id\}$ then $p$ splits completely in $K/\mathbb{Q}$





# The Frobenius Elements

## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

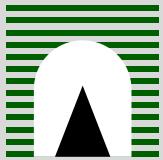
$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$

The *Artin symbol* $\left[\frac{K/\mathbb{Q}}{p}\right]$ is the conjugation class of all such $\sigma_{\mathcal{P}}$

If $\left[\frac{K/\mathbb{Q}}{p}\right] = \{id\}$ then $p$ splits completely in $K/\mathbb{Q}$

- If $K = \mathbb{Q}(E[n])$ is the division fields, the Artin symbol is thought as a conjugation class of matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.





# The Frobenius Elements

## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

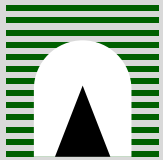
$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$

The *Artin symbol* $\left[\frac{K/\mathbb{Q}}{p}\right]$ is the conjugation class of all such $\sigma_{\mathcal{P}}$

If $\left[\frac{K/\mathbb{Q}}{p}\right] = \{id\}$ then $p$ splits completely in $K/\mathbb{Q}$

- If $K = \mathbb{Q}(E[n])$ is the division fields, the Artin symbol is thought as a conjugation class of matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.
- The characteristic polynomial $\det(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] - T)$ does not depend on $n$:





# The Frobenius Elements

## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

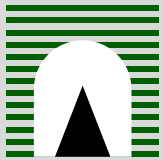
$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$

The *Artin symbol* $\left[\frac{K/\mathbb{Q}}{p}\right]$ is the conjugation class of all such $\sigma_{\mathcal{P}}$

If $\left[\frac{K/\mathbb{Q}}{p}\right] = \{id\}$ then $p$ splits completely in $K/\mathbb{Q}$

- If $K = \mathbb{Q}(E[n])$ is the division fields, the Artin symbol is thought as a conjugation class of matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.
- The characteristic polynomial $\det(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] - T)$ does not depend on $n$:
- $\det\left(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right]\right) \equiv p \bmod n$





# The Frobenius Elements

## Definition

Let $K/\mathbb{Q}$ be Galois and let $p$ be prime, unramified in $K$, and let $\mathcal{P}$ be a prime of $K$ above $p$. The *Frobenius element* $\sigma_{\mathcal{P}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$.(i.e.

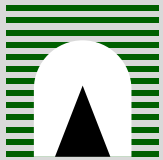
$$\sigma_{\mathcal{P}}\alpha \equiv \alpha^{N\mathcal{P}} \bmod \mathcal{P} \quad \forall \alpha \in \mathcal{O}).$$

The *Artin symbol* $\left[\frac{K/\mathbb{Q}}{p}\right]$ is the conjugation class of all such $\sigma_{\mathcal{P}}$

If $\left[\frac{K/\mathbb{Q}}{p}\right] = \{id\}$ then $p$ splits completely in $K/\mathbb{Q}$

- If $K = \mathbb{Q}(E[n])$ is the division fields, the Artin symbol is thought as a conjugation class of matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.
- The characteristic polynomial $\det(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] - T)$ does not depend on $n$:
- $\det\left(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right]\right) \equiv p \bmod n$
- $\mathrm{tr}\left(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right]\right) \equiv a_E \bmod n$ where $a_E = p - 1 - \#E(\mathbb{F}_p)$.

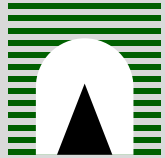




# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois

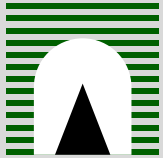




# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$

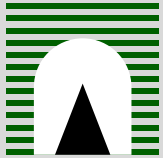




# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$
- let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes of $\mathcal{G}$

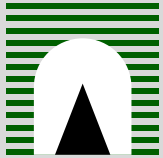




# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$
- let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes of $\mathcal{G}$





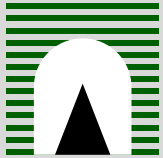
# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$
- let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes of $\mathcal{G}$

**Theorem (Chebotarev Density Theorem)**

*The density of the primes $p$ such that $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\mathcal{G}}$*





# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$
- let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes of $\mathcal{G}$

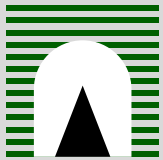
**Theorem (Chebotarev Density Theorem)**

*The density of the primes $p$ such that $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\mathcal{G}}$*

- Quantitative versions consider

$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \#\left\{p \leq x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$





# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$
- let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes of $\mathcal{G}$

**Theorem (Chebotarev Density Theorem)**

*The density of the primes $p$ such that $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\mathcal{G}}$*

- Quantitative versions consider

$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \#\left\{p \leq x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$

- we shall consider these versions in next version

# Chebotarev Density Theorem

- Let $K/\mathbb{Q}$ Galois
- let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$
- let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes of $\mathcal{G}$

**Theorem (Chebotarev Density Theorem)**

*The density of the primes $p$ such that $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\mathcal{G}}$*

- Quantitative versions consider

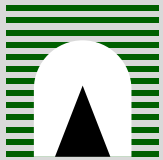
$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \#\left\{p \leq x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$

- we shall consider these versions in next version
- The Generalized Riemann Hypothesis implies

$$\pi_{\mathcal{C}/\mathcal{G}}(x) = \frac{\#\mathcal{C}}{\#\mathcal{G}} \int_2^x \frac{dt}{\log x} + O\left(\sqrt{\#\mathcal{C}}\sqrt{x}\log(xM\#\mathcal{G})\right)$$

where $M$ is the product of primes numbers that ramify in $K/\mathbb{Q}$.

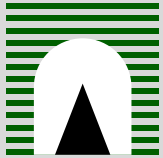




# Chebotarev Density Theorem

We will apply it in the special case when $K = \mathbb{Q}(E[n])$ where we think at the element of $\mathcal{G}$ as 2 by 2 non singular matrices. For example





# Chebotarev Density Theorem

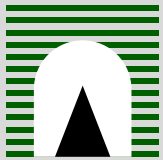
We will apply it in the special case when $K = \mathbb{Q}(E[n])$ where we think at the element of $\mathcal{G}$ as 2 by 2 non singular matrices. For example

- In the case when $\mathcal{C} = \{\mathrm{id}\}$, the condition $\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}$ is equivalent to the property that

$$E[n] \subset \bar{E}(\mathbb{F}_p)$$

where $\overline{E}(\mathbb{F}_p)$ is the group of $\mathbb{F}_p$-rational points on the reduced curve $\overline{E}$.





# Chebotarev Density Theorem

We will apply it in the special case when $K = \mathbb{Q}(E[n])$ where we think at the element of $\mathcal{G}$ as 2 by 2 non singular matrices. For example

- In the case when $\mathcal{C} = \{\mathrm{id}\}$, the condition $\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}$ is equivalent to the property that

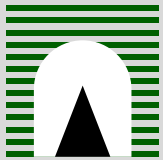
$$E[n] \subset \bar{E}(\mathbb{F}_p)$$

  where $\overline{E}(\mathbb{F}_p)$ is the group of $\mathbb{F}_p$-rational points on the reduced curve $\overline{E}$.

- In the case when $\mathcal{C} = \mathcal{G}_{\mathrm{tr}=r} = \{\sigma \in \mathcal{G} : \mathrm{tr}\,\sigma = t\}$, and $\ell$ is a sufficiently large prime so that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_\ell)$, then

$$\#\,\mathrm{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r} = \begin{cases} \ell^2(\ell-1) & \text{if } r = 0 \\ \ell(\ell^2-\ell-1) & \text{otherwise.} \end{cases}$$

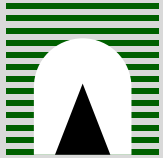




# Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set



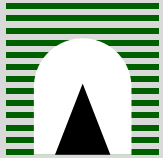


# Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set

$$\pi_E^{\text{cyclic}}(x) = \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$





# Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set

$$\pi_E^{\text{cyclic}}(x) = \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

## Conjecture (Serre)

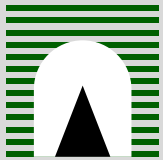
The following asymptotic formula holds

$$\pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x} \qquad x \to \infty$$

where

$$\delta_E^{\text{cyclic}} = \sum_{n=1}^{\infty} \frac{\mu(n)}{\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})}.$$





# Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set

$$\pi_E^{\text{cyclic}}(x) = \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

**Conjecture (Serre)**

The following asymptotic formula holds

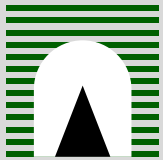
$$\pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x} \qquad x \to \infty$$

where

$$\delta_E^{\text{cyclic}} = \sum_{n=1}^{\infty} \frac{\mu(n)}{\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})}.$$

- Heuristics based on Chebotarev Density Theorem





# Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set

$$\pi_E^{\text{cyclic}}(x) = \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

**Conjecture (Serre)**

The following asymptotic formula holds

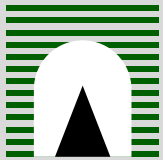
$$\pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x} \qquad x \to \infty$$

where

$$\delta_E^{\text{cyclic}} = \sum_{n=1}^{\infty} \frac{\mu(n)}{\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})}.$$

- Heuristics based on Chebotarev Density Theorem
- Serre proved that GRH implies the conjecture





# Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set

$$\pi_E^{\text{cyclic}}(x) = \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

**Conjecture (Serre)**

The following asymptotic formula holds

$$\pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x} \qquad x \to \infty$$

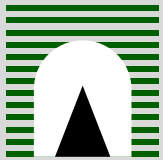
where

$$\delta_E^{\text{cyclic}} = \sum_{n=1}^{\infty} \frac{\mu(n)}{\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})}.$$

- Heuristics based on Chebotarev Density Theorem
- Serre proved that GRH implies the conjecture
- If $E$ has no CM, $\delta_E^{\text{cyclic}}$ is a rational multiple of the quantity

$$\prod_{\ell} \left(1 - \frac{1}{(\ell^2 - \ell)(\ell^2 - 1)}\right).$$

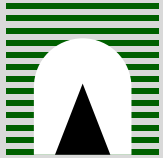




# Lang Trotter Conjecture for trace of Frobenius

Let $E/\mathbb{Q}$, $r \in \mathbb{Z}$ and set



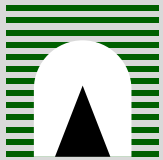


# Lang Trotter Conjecture for trace of Frobenius

Let $E/\mathbb{Q}$, $r \in \mathbb{Z}$ and set

$$\pi_E^r(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } \#\overline{E}(\mathbb{F}_p) = p + 1 - r\}$$





# Lang Trotter Conjecture for trace of Frobenius

Let $E/\mathbb{Q}$, $r \in \mathbb{Z}$ and set

$$\pi_E^r(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } \#\overline{E}(\mathbb{F}_p) = p + 1 - r\}$$

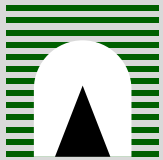
**Conjecture (Lang – Trotter (1970))**

If either $r \neq 0$ or if $E$ has no CM, then the following asymptotic formula holds

$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x} \qquad x \to \infty$$

where $C_{E,r}$ is the *Lang–Trotter constant*





# Lang Trotter Conjecture for trace of Frobenius

Let $E/\mathbb{Q}$, $r \in \mathbb{Z}$ and set

$$\pi_E^r(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } \#\overline{E}(\mathbb{F}_p) = p + 1 - r\}$$

## Conjecture (Lang – Trotter (1970))

If either $r \neq 0$ or if $E$ has no CM, then the following asymptotic formula holds

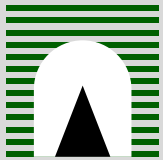
$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x} \qquad x \to \infty$$

where $C_{E,r}$ is the *Lang–Trotter constant*

## Definition

Let $(k_m)_{m\in\mathbb{N}} \subset \mathbb{N}$ be s.t. $\forall k \in \mathbb{N}$, $k \mid k_m$ $\forall m$ is large enough. (Example: $k_m = m!$ has this property). The the Lang–Trotter constants is





# Lang Trotter Conjecture for trace of Frobenius

Let $E/\mathbb{Q}$, $r \in \mathbb{Z}$ and set

$$\pi_E^r(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } \#\overline{E}(\mathbb{F}_p) = p + 1 - r\}$$

## Conjecture (Lang – Trotter (1970))

If either $r \neq 0$ or if $E$ has no CM, then the following asymptotic formula holds

$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x} \qquad x \to \infty$$

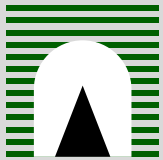
where $C_{E,r}$ is the *Lang–Trotter constant*

## Definition

Let $(k_m)_{m\in\mathbb{N}} \subset \mathbb{N}$ be s.t. $\forall k \in \mathbb{N}$, $k \mid k_m$ $\forall m$ is large enough. (Example: $k_m = m!$ has this property). The the Lang–Trotter constants is

$$C_{E,r} = \frac{2}{\pi} \lim_{m\to\infty} \frac{k_m \# \operatorname{Gal}(\mathbb{Q}(E[k_m])/\mathbb{Q})_{\text{trace}=r}}{\# \operatorname{Gal}(\mathbb{Q}(E[K_m])/\mathbb{Q})}$$





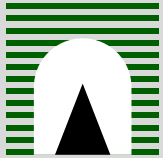
# Lang Trotter Conjecture for trace of Frobenius

## Definition of the Lang Trotter Constant

### Definition

Let $E/\mathbb{Q}$ be an elliptic curve with out CM and consider the representation of the torsion points:





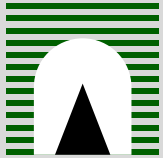
# Lang Trotter Conjecture for trace of Frobenius

## Definition of the Lang Trotter Constant

### Definition

Let $E/\mathbb{Q}$ be an elliptic curve with out CM and consider the representation of the torsion points:$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\infty])$.





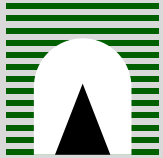
# Lang Trotter Conjecture for trace of Frobenius

## Definition of the Lang Trotter Constant

### Definition

Let $E/\mathbb{Q}$ be an elliptic curve with out CM and consider the representation of the torsion points:$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\infty])$.Let $m \in \mathbb{N}$ and denote by $\hat{G}_m$ the projection of $\rho_E(G_Q)$ in $\prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell)$





# Lang Trotter Conjecture for trace of Frobenius

## Definition of the Lang Trotter Constant

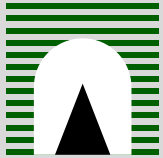
### Definition

Let $E/\mathbb{Q}$ be an elliptic curve with out CM and consider the representation of the torsion points:$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\infty])$.Let $m \in \mathbb{N}$ and denote by $\hat{G}_m$ the projection of $\rho_E(G_Q)$ in $\prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell)$

- We say that $m$ **splits** $\rho_E$ if

$$\rho_E(G_{\mathbb{Q}}) \cong \hat{G}_m \times \prod_{\ell \nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell)$$





# Lang Trotter Conjecture for trace of Frobenius

## Definition of the Lang Trotter Constant

### Definition

Let $E/\mathbb{Q}$ be an elliptic curve with out CM and consider the representation of the torsion points:$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\infty])$.Let $m \in \mathbb{N}$ and denote by $\hat{G}_m$ the projection of $\rho_E(G_Q)$ in $\prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell)$

- We say that $m$ **splits** $\rho_E$ if

$$\rho_E(G_{\mathbb{Q}}) \cong \hat{G}_m \times \prod_{\ell \nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

- We say that $m$ **stabilizes** $\rho_E$ if

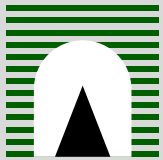
$$\hat{G}_m = r_m^{-1}(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}))$$

where

$$r_m : \prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$$

is the reduction map



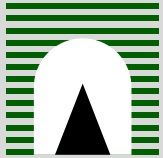


# Lang Trotter Conjecture for trace of Frobenius

**Theorem (Serre)**

*Let $E/\mathbb{Q}$ be an elliptic curve with out CM. Then there exists $m \in \mathbb{N}$ that splits and stabilizes $\rho_E$*





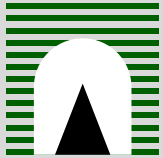
# Lang Trotter Conjecture for trace of Frobenius

**Theorem (Serre)**

*Let $E/\mathbb{Q}$ be an elliptic curve with out CM. Then there exists $m \in \mathbb{N}$ that splits and stabilizes $\rho_E$*

The smallest such an $m$ is called the *Serre's conductor* of $E$ and denoted by $m_E$.





# Lang Trotter Conjecture for trace of Frobenius

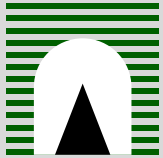
**Theorem (Serre)**

*Let $E/\mathbb{Q}$ be an elliptic curve with out CM. Then there exists $m \in \mathbb{N}$ that splits and stabilizes $\rho_E$*

The smallest such an $m$ is called the *Serre's conductor* of $E$ and denoted by $m_E$.
Lang and Trotter showed that

$$\begin{aligned} C_{E,r} &= \frac{2}{\pi} \lim_{m\to\infty} \frac{m! \# \operatorname{Gal}\mathbb{Q}(E[m!])/\mathbb{Q})_{\mathrm{tr}=r}}{\# \operatorname{Gal}\mathbb{Q}(E[m!])/\mathbb{Q})} \\ &= \frac{2}{\pi} \frac{m_E \# \operatorname{Gal}\mathbb{Q}(E[m_E])/\mathbb{Q})_{\mathrm{tr}=r}}{\# \operatorname{Gal}\mathbb{Q}(E[m_E])/\mathbb{Q})} \times \prod_{\ell \nmid m_E} \frac{\ell \# \operatorname{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r}}{\# \operatorname{GL}_2(\mathbb{F}_\ell)} \end{aligned}$$





# Lang Trotter Conjecture for trace of Frobenius

**Theorem (Serre)**

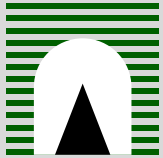
*Let $E/\mathbb{Q}$ be an elliptic curve with out CM. Then there exists $m \in \mathbb{N}$ that splits and stabilizes $\rho_E$*

The smallest such an $m$ is called the *Serre's conductor* of $E$ and denoted by $m_E$.
Lang and Trotter showed that

$$\begin{aligned} C_{E,r} &= \frac{2}{\pi} \lim_{m\to\infty} \frac{m! \# \operatorname{Gal}\mathbb{Q}(E[m!])/\mathbb{Q})_{\mathrm{tr}=r}}{\# \operatorname{Gal}\mathbb{Q}(E[m!])/\mathbb{Q})} \\ &= \frac{2}{\pi} \frac{m_E \# \operatorname{Gal}\mathbb{Q}(E[m_E])/\mathbb{Q})_{\mathrm{tr}=r}}{\# \operatorname{Gal}\mathbb{Q}(E[m_E])/\mathbb{Q})} \times \prod_{\ell \nmid m_E} \frac{\ell \# \operatorname{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r}}{\# \operatorname{GL}_2(\mathbb{F}_\ell)} \end{aligned}$$

Although it is hard to compute in General, there is a simple formula to compute the Serre's conductor of Serre's curves. (more next lecture)

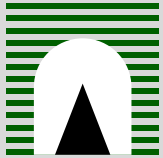




# Lang Trotter Conjecture for trace of Frobenius

## An application of $\ell$–adic representations and of the Chebotarev density Theorem





# Lang Trotter Conjecture for trace of Frobenius

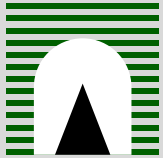
## An application of $\ell$–adic representations and of the Chebotarev density Theorem

**Theorem (Serre)**

*Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then*

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$





# Lang Trotter Conjecture for trace of Frobenius

## An application of $\ell$–adic representations and of the Chebotarev density Theorem

**Theorem (Serre)**

*Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then*

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

- If $E/\mathbb{Q}$ is CM and $r = 0$. It is classical

$$\pi_E^0(x) \sim \frac{1}{2}\frac{x}{\log x} \qquad x \to \infty$$

# Lang Trotter Conjecture for trace of Frobenius

## An application of $\ell$–adic representations and of the Chebotarev density Theorem

**Theorem (Serre)**

*Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then*

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

- If $E/\mathbb{Q}$ is CM and $r = 0$. It is classical

$$\pi_E^0(x) \sim \frac{1}{2}\frac{x}{\log x} \qquad x \to \infty$$

- Murty, Murty and Sharadha: If $r \neq 0$, on GRH, $\pi_E^r(x) \ll x^{4/5}/(\log x)$.

# Lang Trotter Conjecture for trace of Frobenius

## An application of $\ell$–adic representations and of the Chebotarev density Theorem

**Theorem (Serre)**

*Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then*

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

- If $E/\mathbb{Q}$ is CM and $r = 0$. It is classical

$$\pi_E^0(x) \sim \frac{1}{2}\frac{x}{\log x} \qquad x \to \infty$$

- Murty, Murty and Sharadha: If $r \neq 0$, on GRH, $\pi_E^r(x) \ll x^{4/5}/(\log x)$.
- Elkies $\pi_E^0(x) \to \infty \quad x \to \infty$

# Lang Trotter Conjecture for trace of Frobenius

## An application of $\ell$–adic representations and of the Chebotarev density Theorem

**Theorem (Serre)**

*Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then*

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

- If $E/\mathbb{Q}$ is CM and $r = 0$. It is classical

$$\pi_E^0(x) \sim \frac{1}{2}\frac{x}{\log x} \qquad x \to \infty$$

- Murty, Murty and Sharadha: If $r \neq 0$, on GRH, $\pi_E^r(x) \ll x^{4/5}/(\log x)$.
- Elkies $\pi_E^0(x) \to \infty \quad x \to \infty$
- Elkies & Murty $\pi_E^0(x) \gg \log\log x$

# Lang Trotter Conjecture for trace of Frobenius

## An application of $\ell$–adic representations and of the Chebotarev density Theorem

**Theorem (Serre)**

*Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then*

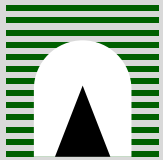
$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

- If $E/\mathbb{Q}$ is CM and $r = 0$. It is classical

$$\pi_E^0(x) \sim \frac{1}{2}\frac{x}{\log x} \qquad x \to \infty$$

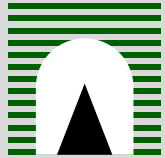
- Murty, Murty and Sharadha: If $r \neq 0$, on GRH, $\pi_E^r(x) \ll x^{4/5}/(\log x)$.
- Elkies $\pi_E^0(x) \to \infty \quad x \to \infty$
- Elkies & Murty $\pi_E^0(x) \gg \log\log x$
- Average Versions tomorrow





# Lang Trotter Conjecture for Primitive points



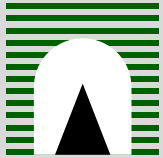


# Lang Trotter Conjecture for Primitive points

## Definition

Let $E/\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be of infinite order. $P$ is called *primitive* for a prime $p$ if the reduction $\overline{P}$ of $P \bmod p$ $\langle \overline{P} \rangle = \overline{E}(\mathbb{F}_p)$





# Lang Trotter Conjecture for Primitive points

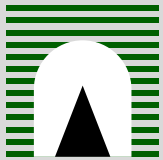
## Definition

Let $E/\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be of infinite order. $P$ is called *primitive* for a prime $p$ if the reduction $\overline{P}$ of $P \bmod p$ $\langle \overline{P} \rangle = \overline{E}(\mathbb{F}_p)$

Set

$$\pi_{E,P}(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } P \text{ is primitive for } p\}.$$





# Lang Trotter Conjecture for Primitive points

## Definition

Let $E/\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be of infinite order. $P$ is called *primitive* for a prime $p$ if the reduction $\overline{P}$ of $P \bmod p$ $\langle \overline{P} \rangle = \overline{E}(\mathbb{F}_p)$

Set

$$\pi_{E,P}(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } P \text{ is primitive for } p\}.$$

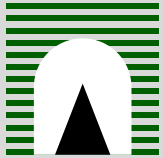
## Conjecture (Lang–Trotter for primitive points (1976))

The following asymptotic formula holds

$$\pi_{E,P}(x) \sim \delta_{E,P} \frac{x}{\log x} \qquad x \to \infty.$$

with





# Lang Trotter Conjecture for Primitive points

## Definition

Let $E/\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be of infinite order. $P$ is called *primitive* for a prime $p$ if the reduction $\overline{P}$ of $P \bmod p$ $\langle \overline{P} \rangle = \overline{E}(\mathbb{F}_p)$

Set

$$\pi_{E,P}(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } P \text{ is primitive for } p\}.$$

## Conjecture (Lang–Trotter for primitive points (1976))

The following asymptotic formula holds

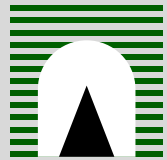
$$\pi_{E,P}(x) \sim \delta_{E,P} \frac{x}{\log x} \qquad x \to \infty.$$

with

$$\delta_{E,P} = \sum_{n=1}^{\infty} \mu(n) \frac{\#\mathcal{C}_{P,n}}{\#\operatorname{Gal}(\mathbb{Q}(E[n], n^{-1}P)/\mathbb{Q})}$$

where $\mathbb{Q}(E[n], n^{-1}P)$ is the extension of $\mathbb{Q}(E[n])$ of the coordinates of the points $Q \in E(\bar{\mathbb{Q}})$ such that $nQ = P$ and $\mathcal{C}_{P,n}$ is a union of conjugacy classes in $\operatorname{Gal}(\mathbb{Q}(E[n], n^{-1}P)/\mathbb{Q})$. (more next lecture)





# Some 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.