Introduction to Elliptic Cryptosystems

An invitation to Elliptic curves

Journée d'Aritmétique

Universitè de Cocody – UFR Matématique et Informatique

Abidjan *Juillet 24, 2014*,

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre

Proto–History (from WIKIPEDIA)

Giulio Carlo, Count Fagnano, and Marquis de Toschi (December 6, 1682 – September 26, 1766) was an Italian mathematician. He was probably the first to direct attention to the theory of *elliptic integrals*. Fagnano was born in Senigallia.

He made his higher studies at the *Collegio Clementino* in Rome and there won great distinction, except in mathematics, to which his aversion was extreme. Only after his college course he took up the study of mathematics.

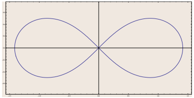
Later, without help from any teacher, he mastered mathematics from its foundations.

Some of His Achievements:

- $\pi = 2i \log \frac{1-i}{1+1}$
- Length of *Lemniscate*

Carlo Fagnano

Collegio Clementino



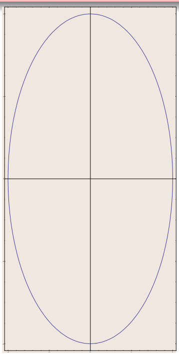
Lemniscate

$(x^2 + y^2)^2 = 2a^2(x^2 - y^2)$

$\ell = 4 \int_0^a \frac{a^2 dr}{\sqrt{a^4 - r^4}} = \frac{a\sqrt{\pi}\Gamma(\frac{5}{4})}{\Gamma(\frac{3}{4})}$

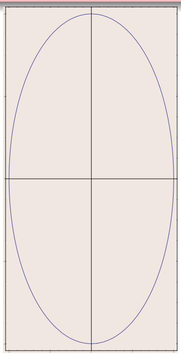
Length of Ellipses

$$\mathcal{E} : \frac{x^2}{4} + \frac{y^2}{16} = 1$$



Length of Ellipses

$$\mathcal{E} : \frac{x^2}{4} + \frac{y^2}{16} = 1$$

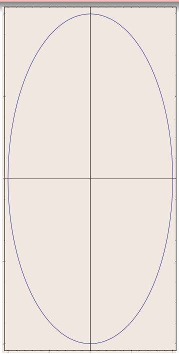


The length of the arc of a plane curve $y = f(x)$, $f : [a, b] \to \mathbb{R}$ is:

$$\ell = \int_a^b \sqrt{1 + (f'(t))^2}\, dt$$

Length of Ellipses

$$\mathcal{E} : \frac{x^2}{4} + \frac{y^2}{16} = 1$$



The length of the arc of a plane curve $y = f(x)$, $f : [a, b] \to \mathbb{R}$ is:

$$\ell = \int_a^b \sqrt{1 + (f'(t))^2}\, dt$$

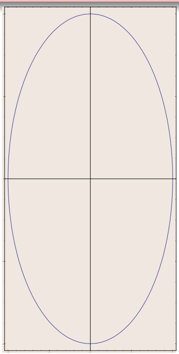
Applying this formula to $\mathcal{E}$:

$$\ell(\mathcal{E}) = 4 \int_0^4 \sqrt{1 + \left(\frac{d\sqrt{16(1 - t^2/4)}}{dt} \right)^2}\, dt$$

$$= 4 \int_0^1 \sqrt{\frac{1 + 3x^2}{1 - x^2}}\, dx \qquad x = t/2$$

Length of Ellipses

$$\mathcal{E} : \frac{x^2}{4} + \frac{y^2}{16} = 1$$



The length of the arc of a plane curve $y = f(x)$, $f : [a, b] \to \mathbb{R}$ is:

$$\ell = \int_a^b \sqrt{1 + (f'(t))^2}\, dt$$

Applying this formula to $\mathcal{E}$:

$$\ell(\mathcal{E}) = 4\int_0^4 \sqrt{1 + \left(\frac{d\sqrt{16(1 - t^2/4)}}{dt}\right)^2}\, dt$$

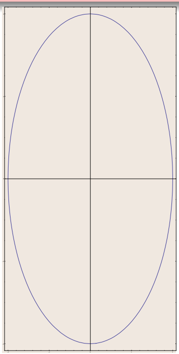
$$= 4\int_0^1 \sqrt{\frac{1 + 3x^2}{1 - x^2}}\, dx \qquad x = t/2$$

If y is the integrand, then we have the identity:

$$y^2(1 - x^2) = 1 + 3x^2$$

Length of Ellipses

$$\mathcal{E} : \frac{x^2}{4} + \frac{y^2}{16} = 1$$



The length of the arc of a plane curve $y = f(x)$, $f : [a, b] \to \mathbb{R}$ is:

$$\ell = \int_a^b \sqrt{1 + (f'(t))^2}\, dt$$

Applying this formula to $\mathcal{E}$:

$$\ell(\mathcal{E}) = 4 \int_0^4 \sqrt{1 + \left(\frac{d\sqrt{16(1 - t^2/4)}}{dt} \right)^2}\, dt$$
$$= 4 \int_0^1 \sqrt{\frac{1 + 3x^2}{1 - x^2}}\, dx \qquad x = t/2$$

If y is the integrand, then we have the identity:

$$y^2(1 - x^2) = 1 + 3x^2$$

Apply the invertible change of variables:

$$\begin{cases} x = 1 - 2/t \\ y = \frac{u}{t-1} \end{cases}$$

Arrive to

$$u^2 = t^3 - 4t^2 + 6t - 3$$

What are Elliptic Curves?

Reasons to study them

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time
2. are non singular projective curves of *genus* 1

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time
2. are non singular projective curves of *genus* 1
3. have important applications in Algorithmic Number Theory and Cryptography

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time
2. are non singular projective curves of *genus* 1
3. have important applications in Algorithmic Number Theory and Cryptography
4. are the topic of the Birch and Swinnerton-Dyer conjecture (one of the seven Millennium Prize Problems)

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time
2. are non singular projective curves of *genus* 1
3. have important applications in Algorithmic Number Theory and Cryptography
4. are the topic of the Birch and Swinnerton-Dyer conjecture (one of the seven Millennium Prize Problems)
5. have a group law that is a consequence of the fact that they intersect every line in exactly three points (in the projective plane over $\mathbb{C}$ and counted with multiplicity)

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time
2. are non singular projective curves of *genus* 1
3. have important applications in Algorithmic Number Theory and Cryptography
4. are the topic of the Birch and Swinnerton-Dyer conjecture (one of the seven Millennium Prize Problems)
5. have a group law that is a consequence of the fact that they intersect every line in exactly three points (in the projective plane over $\mathbb{C}$ and counted with multiplicity)
6. represent a mathematical world in itself ... Each of them does!!

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

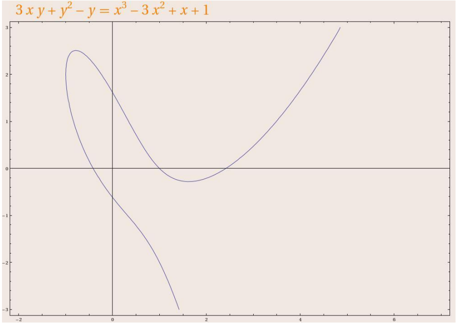
where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

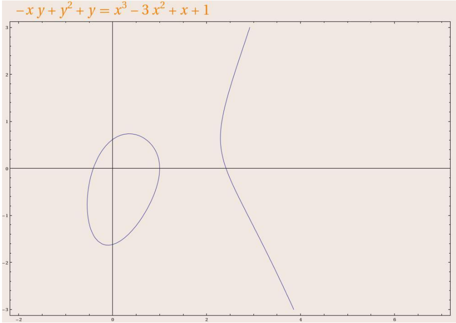


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

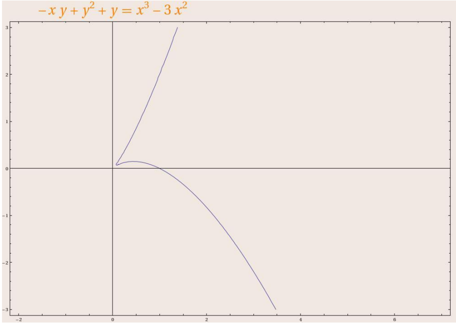


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$



Dipartim. Mat. & Fis.

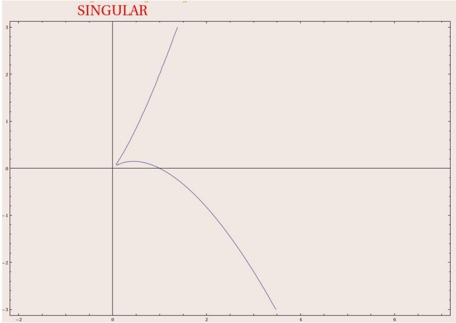
Università Roma Tre

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

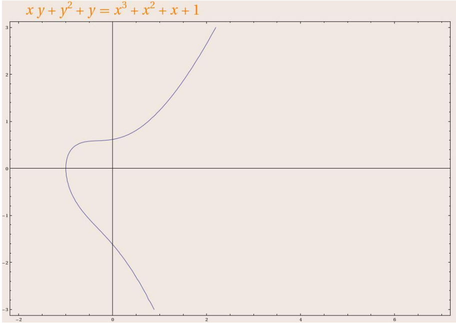


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

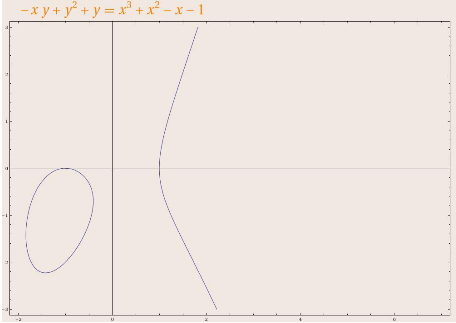


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

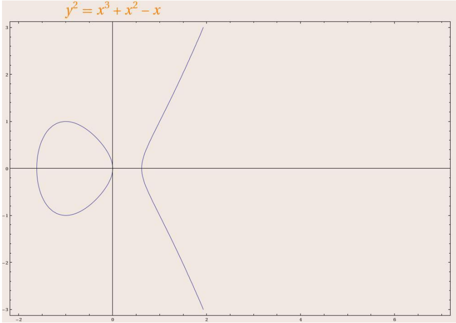


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

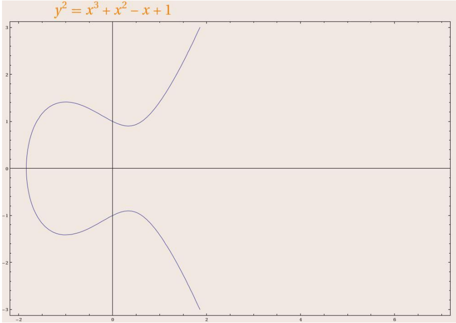


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

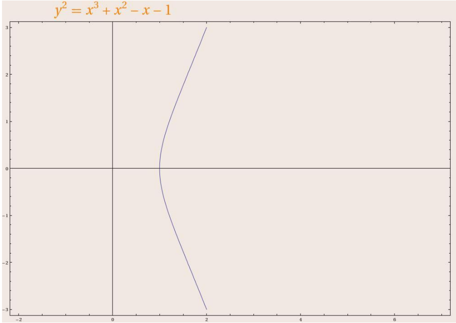


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

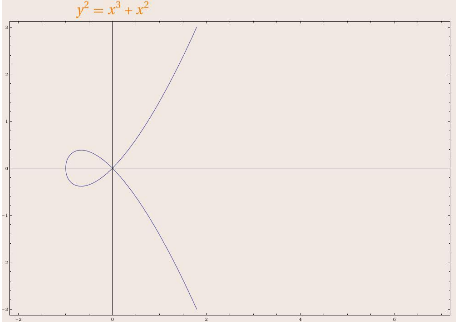


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

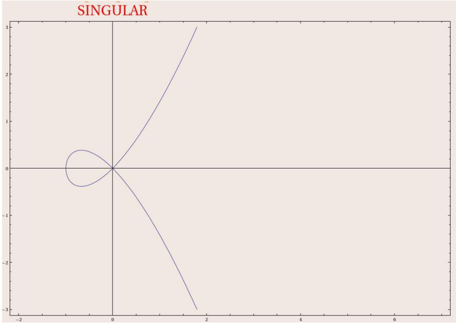


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

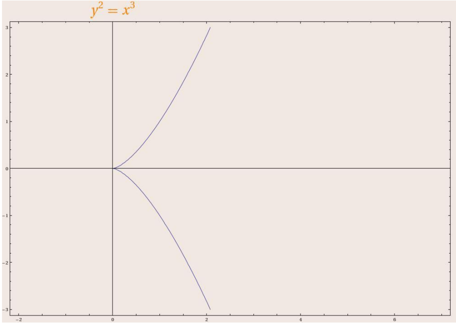


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$



Dipartim. Mat. & Fis.

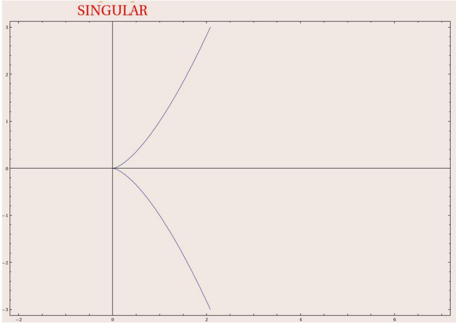
Università Roma Tre

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

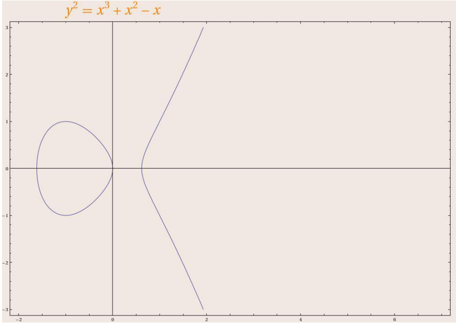


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$

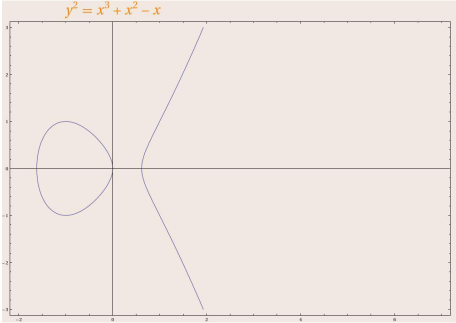


The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$



The equation should not be *singular*

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 Weierstraßequation is the following quantity)

$$\Delta'_E := \frac{1}{2^4 3^3} \left(-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16 a_1 a_2^2 a_3 a_4 + 36 a_1^2 a_3^2 a_4 \right.$$
$$- a_1^4 a_4^2 - 8 a_1^2 a_2 a_4^2 - 16 a_2^2 a_4^2 + 96 a_1 a_3 a_4^2 + 64 a_4^3 +$$
$$a_1^6 a_6 + 12 a_1^4 a_2 a_6 + 48 a_1^2 a_2^2 a_6 + 64 a_2^3 a_6 - 36 a_1^3 a_3 a_6$$
$$\left. -144 a_1 a_2 a_3 a_6 - 72 a_1^2 a_4 a_6 - 288 a_2 a_4 a_6 + 432 a_6^2 \right)$$

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 Weierstraßequation is the following quantity)

$$\Delta'_E := \frac{1}{2^4 3^3}\left(-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16 a_1 a_2^2 a_3 a_4 + 36 a_1^2 a_3^2 a_4 - a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16 a_2^2 a_4^2 + 96 a_1 a_3 a_4^2 + 64 a_4^3 + a_1^6 a_6 + 12 a_1^4 a_2 a_6 + 48 a_1^2 a_2^2 a_6 + 64 a_2^3 a_6 - 36 a_1^3 a_3 a_6 -144 a_1 a_2 a_3 a_6 - 72 a_1^2 a_4 a_6 - 288 a_2 a_4 a_6 + 432 a_6^2\right)$$

Definition

Two Weierstraß equations over $\mathbb{F}_q$ are said (affinely) equivalent if there exists a (affine) of the following form

$$\begin{cases} x \longleftarrow u^2 x + r \\ y \longleftarrow u^3 y + u^2 s x + t \end{cases} \quad r, s, t, u \in \mathbb{F}_q$$

The Weierstraß equation

Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/\mathbb{F}_q (q = p^n)$ 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 $E/\mathbb{F}_q(q = p^n)$ has a Weierstraß equation of the following form

Example (Classification)

E	p	Δ_E
$y^2 = x^3 + Ax + B$	≥ 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 $E/\mathbb{F}_q (q = p^n)$ has a Weierstraß equation of the following form

Example (Classification)

E	p	Δ_E
$y^2 = x^3 + Ax + B$	≥ 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 the data of 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 $E/\mathbb{F}_q(q = p^n)$ has a Weierstraß equation of the following form

Example (Classification)

E	p	Δ_E
$y^2 = x^3 + Ax + B$	≥ 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 the data of a non singular Weierstraß equation (i.e. $\Delta_E \neq 0$)

Note: If $p \geq 3, \Delta_E \neq 0 \Leftrightarrow x^3 + Ax^2 + Bx + C$ has no double root

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Weierstraß equations over $\mathbb{F}_2$

1. $y^2 + xy = x^3 + x^2 + 1$
2. $y^2 + xy = x^3 + 1$
3. $y^2 + y = x^3 + x$
4. $y^2 + y = x^3 + x + 1$
5. $y^2 + y = x^3$
6. $y^2 + y = x^3 + 1$

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Weierstraß equations over $\mathbb{F}_2$

1. $y^2 + xy = x^3 + x^2 + 1$
2. $y^2 + xy = x^3 + 1$
3. $y^2 + y = x^3 + x$
4. $y^2 + y = x^3 + x + 1$
5. $y^2 + y = x^3$
6. $y^2 + y = x^3 + 1$

However the change of variables $\begin{cases} x \leftarrow x + 1 \\ y \leftarrow y + x \end{cases}$ takes the sixth curve into the fifth. Hence we can remove the sixth from the list.

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Weierstraß equations over $\mathbb{F}_2$

1. $y^2 + xy = x^3 + x^2 + 1$
2. $y^2 + xy = x^3 + 1$
3. $y^2 + y = x^3 + x$
4. $y^2 + y = x^3 + x + 1$
5. $y^2 + y = x^3$
6. $y^2 + y = x^3 + 1$

However the change of variables $\begin{cases} x \leftarrow x + 1 \\ y \leftarrow y + x \end{cases}$ takes the sixth curve into the fifth. Hence we can remove the sixth from the list.

Fact:

There are 5 affinely inequivalent elliptic curves over $\mathbb{F}_2$

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Weierstraß equations over $\mathbb{F}_3$

1. $y^2 = x^3 + x$
2. $y^2 = x^3 - x$
3. $y^2 = x^3 - x + 1$
4. $y^2 = x^3 - x - 1$
5. $y^2 = x^3 + x^2 + 1$
6. $y^2 = x^3 + x^2 - 1$
7. $y^2 = x^3 - x^2 + 1$
8. $y^2 = x^3 - x^2 - 1$

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Weierstraß equations over $\mathbb{F}_3$

1. $y^2 = x^3 + x$
2. $y^2 = x^3 - x$
3. $y^2 = x^3 - x + 1$
4. $y^2 = x^3 - x - 1$
5. $y^2 = x^3 + x^2 + 1$
6. $y^2 = x^3 + x^2 - 1$
7. $y^2 = x^3 - x^2 + 1$
8. $y^2 = x^3 - x^2 - 1$

Observations

1. Over $\mathbb{F}_5$ there are 12 elliptic curves

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Weierstraß equations over $\mathbb{F}_3$

1. $y^2 = x^3 + x$
2. $y^2 = x^3 - x$
3. $y^2 = x^3 - x + 1$
4. $y^2 = x^3 - x - 1$
5. $y^2 = x^3 + x^2 + 1$
6. $y^2 = x^3 + x^2 - 1$
7. $y^2 = x^3 - x^2 + 1$
8. $y^2 = x^3 - x^2 - 1$

Observations

1. Over $\mathbb{F}_5$ there are 12 elliptic curves
2. Over $\mathbb{F}_p$ there are approximately $2p$

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0, 1, 0]$. Set

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

or equivalently

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

We can think either

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

We can think either

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

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

We can think either

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

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

We can think either

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

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0, 1, 0]$. Set

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

or equivalently

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

We can think either

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

∞ might be though as the "vertical direction"

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

We can think either

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

∞ might be though as the "vertical direction"

Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

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

projective or affine

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

We can think either

- $E(\mathbb{F}_q) \subset \mathbb{P}_2(\mathbb{F}_q)$ - - → geometric advantages
- $E(\mathbb{F}_q) \subset \mathbb{F}_q^2 \cup \{\infty\}$ - - → algebraic advantages

∞ might be though as the "vertical direction"

Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

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

projective or affine

- if $\#(r_{P,Q} \cap E(\mathbb{F}_q)) \geq 2 \Rightarrow \#(r_{P,Q} \cap E(\mathbb{F}_q)) = 3$

if tangent line, contact point is counted with multiplicity

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0, 1, 0]$. Set

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

or equivalently

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

We can think either

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

∞ might be though as the "vertical direction"

Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

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

projective or affine

- if $\#(r_{P,Q} \cap E(\mathbb{F}_q)) \geq 2 \Rightarrow \#(r_{P,Q} \cap E(\mathbb{F}_q)) = 3$
  if tangent line, contact point is counted with multiplicity
- $r_{\infty,\infty} \cap E(\mathbb{F}_q) = \{\infty, \infty, \infty\}$

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve, $\infty := [0,1,0]$. Set

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

or equivalently

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

We can think either

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

∞ might be though as the "vertical direction"

Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

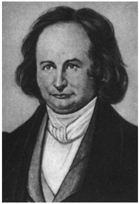
$$r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q \end{cases}$$ projective or affine

- if $\#(r_{P,Q} \cap E(\mathbb{F}_q)) \geq 2 \Rightarrow \#(r_{P,Q} \cap E(\mathbb{F}_q)) = 3$
  if tangent line, contact point is counted with multiplicity
- $r_{\infty,\infty} \cap E(\mathbb{F}_q) = \{\infty, \infty, \infty\}$
- $r_{P,Q} : aX + bZ = 0$ (vertical) $\Rightarrow \infty = [0,1,0] \in r_{P,Q}$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.

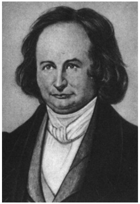


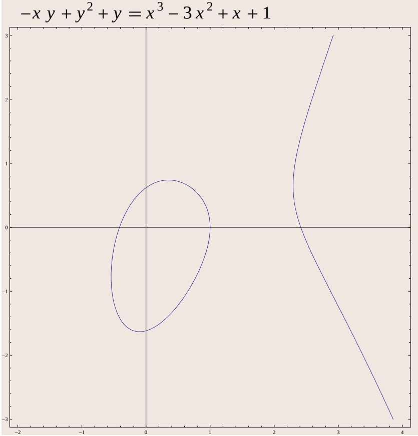
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





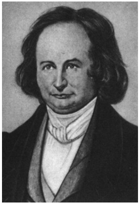
Some of His Achievements:

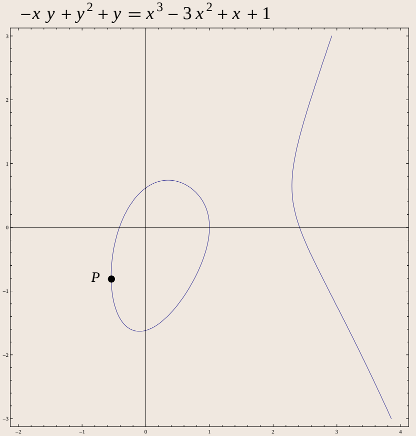
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





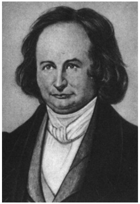
Some of His Achievements:

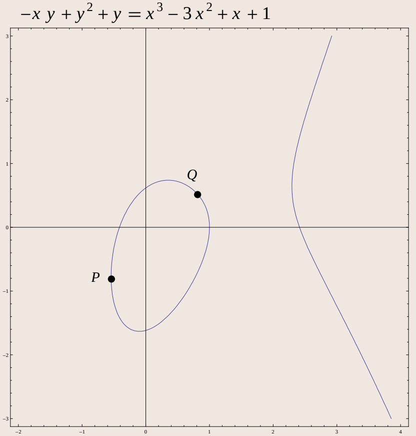
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



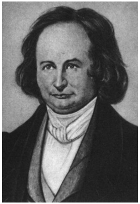


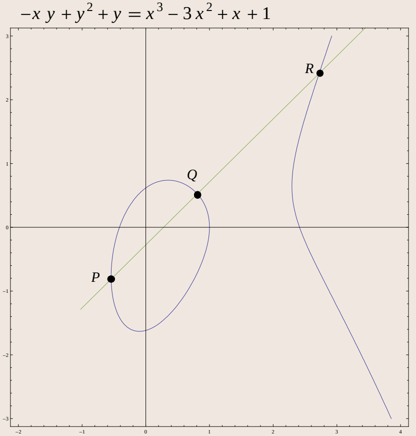
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





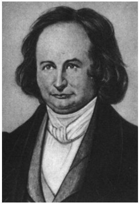
Some of His Achievements:

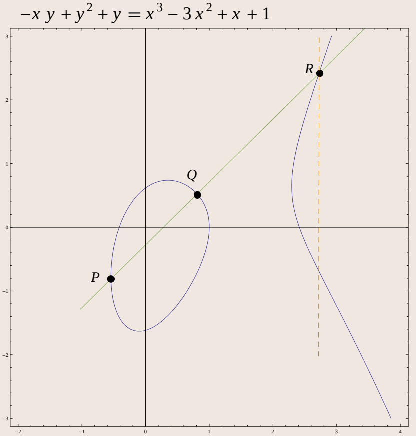
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





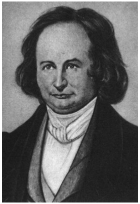
Some of His Achievements:

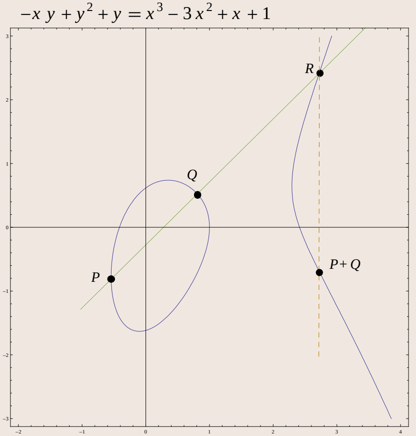
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





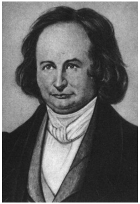
Some of His Achievements:

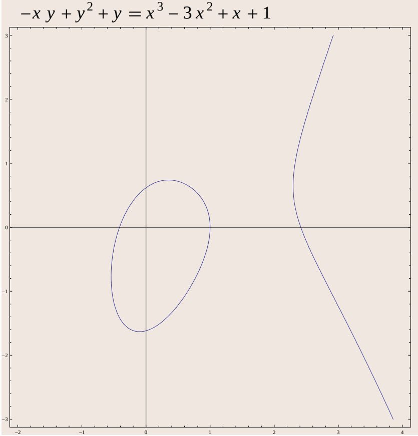
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



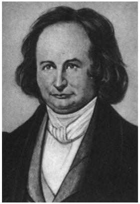


Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$

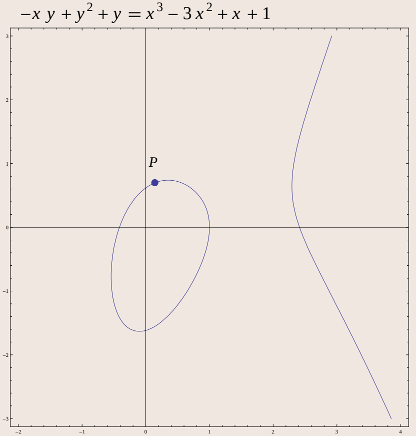
History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

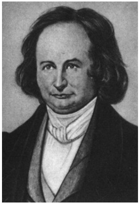
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

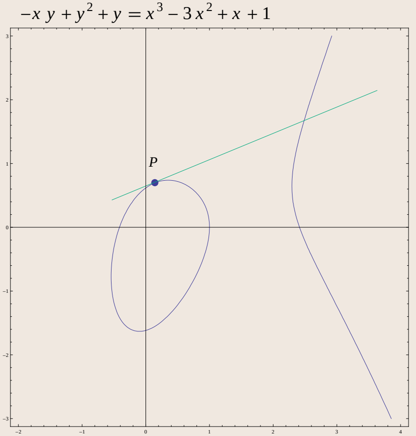


History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





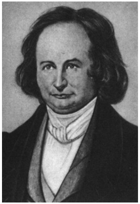
Some of His Achievements:

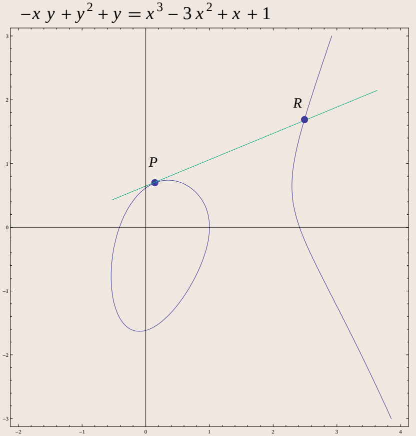
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



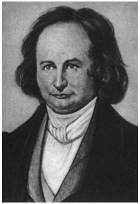


Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

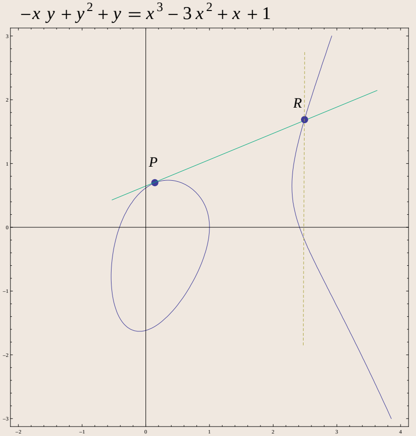
History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

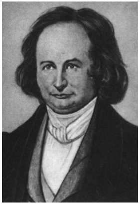
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$

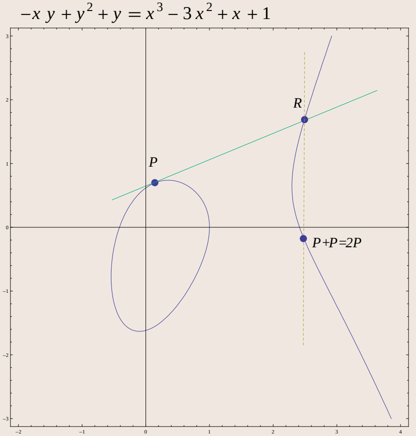


History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



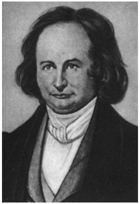


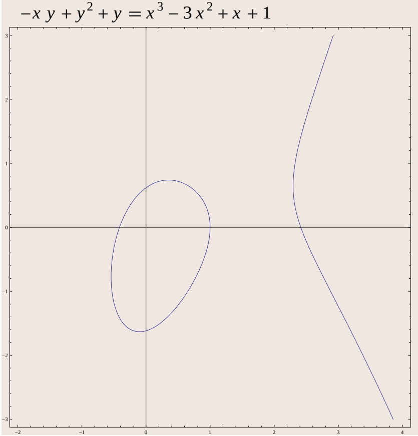
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A, [B, C]] + [B, [C, A]] +$
  $[C, [A, B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





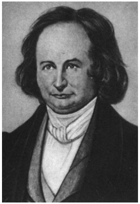
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi

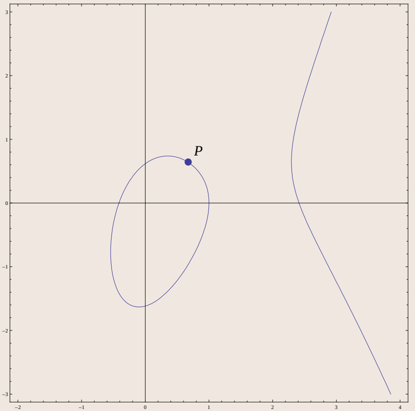
(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

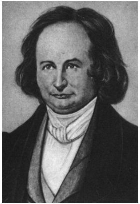
- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$

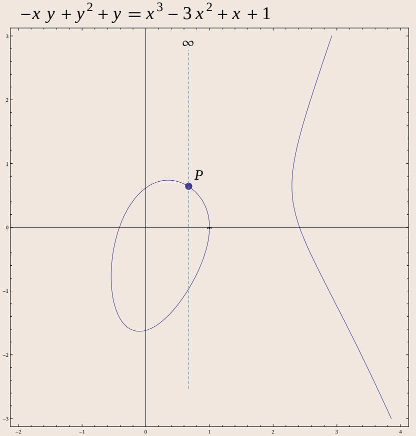
$$-x\,y + y^2 + y = x^3 - 3\,x^2 + x + 1$$



History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



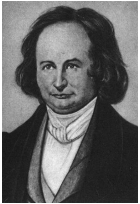


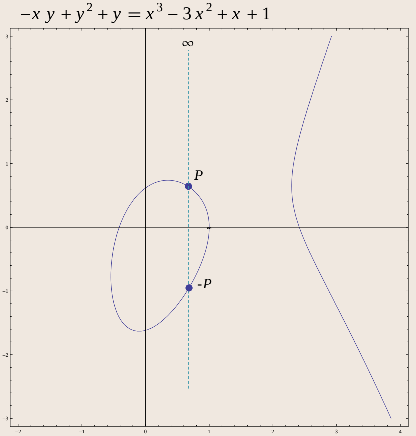
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



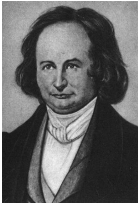


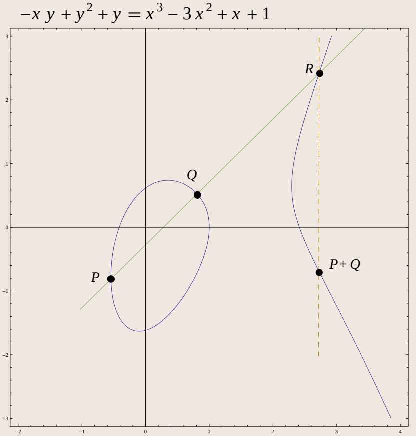
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$

History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.





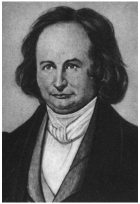
Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

History (from WIKIPEDIA)

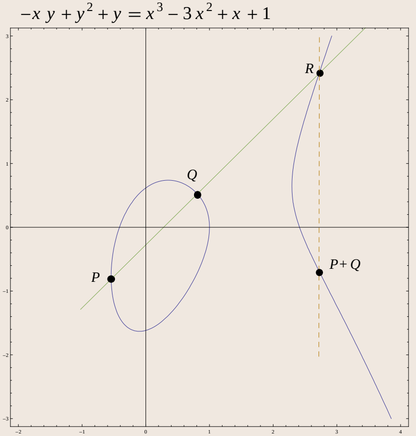
Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$



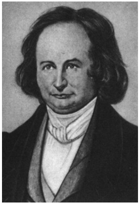
$$r_{P,Q}\cap E(\mathbb{F}_q)=\{P,Q,R\}$$
$$r_{R,\infty}\cap E(\mathbb{F}_q)=\{\infty,R,R'\}$$

$$P+_E Q := R'$$

History (from WIKIPEDIA)

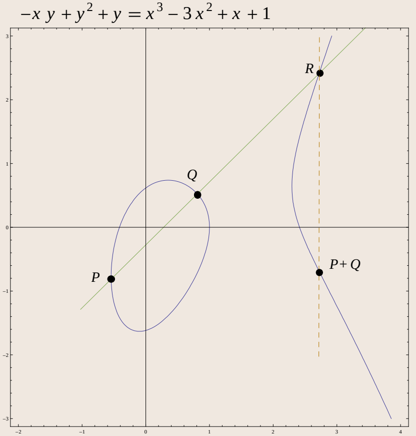
Carl Gustav Jacob Jacobi

(10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$



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

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

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

(b) $P +_E \infty = \infty +_E P = P$ $\forall P \in E(\mathbb{F}_q)$

Properties of the operation “$+_E$”

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

(b) $P +_E \infty = \infty +_E P = P$ $\qquad \forall P \in E(\mathbb{F}_q)$

(c) $P +_E (-P) = \infty$ $\qquad \forall P \in E(\mathbb{F}_q)$

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

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

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

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

Properties of the operation “$+_E$”

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

(b) $P +_E \infty = \infty +_E P = P \qquad \forall P \in E(\mathbb{F}_q)$

(c) $P +_E (-P) = \infty \qquad \forall P \in E(\mathbb{F}_q)$

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

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

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

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

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

- $(E(\mathbb{F}_q), +_E)$ commutative group

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

(b) $P +_E \infty = \infty +_E P = P$ $\forall P \in E(\mathbb{F}_q)$

(c) $P +_E (-P) = \infty$ $\forall P \in E(\mathbb{F}_q)$

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

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

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

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

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

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

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

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

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*
- We shall comment on how to do it by explicit computation

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

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

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

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*
- We shall comment on how to do it by explicit computation
- can substitute $\mathbb{F}_q$ with any field K; Theorem holds for $(E(K), +_E)$

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

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

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

(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$

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

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

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*
- We shall comment on how to do it by explicit computation
- can substitute $\mathbb{F}_q$ with any field K; Theorem holds for $(E(K), +_E)$
- In particular, if $E/\mathbb{F}_q$, can consider the groups $E(\overline{\mathbb{F}}_q)$ or $E(\mathbb{F}_{q^n})$

Formulas for Addition on E (Summary)

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

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

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

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

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

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

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

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

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

- If $P_1 = P_2$

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

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

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

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

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

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

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

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

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

Addition Laws for the sum of affine points

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

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

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

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

Formulas for Addition on E (Summary)

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

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

Addition Laws for the sum of affine points

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

    $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$
- If $P_1 = P_2$
  - $2y_1 + a_1x + a_3 = 0 \quad \Rightarrow \quad P_1 +_E P_2 = 2P_1 = \infty$
  - $2y_1 + a_1x + a_3 \neq 0$

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

Then

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

Formulas for Addition on E (Summary for special equation)

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

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

Addition Laws for the sum of affine points

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

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

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

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

Then

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

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

From our previous list:

Groups of points

E	$E(\mathbb{F}_2)$	$\lvert E(\mathbb{F}_2)\rvert$
$y^2+xy=x^3+x^2+1$	$\{\infty,(0,1)\}$	2
$y^2+xy=x^3+1$	$\{\infty,(0,1),(1,0),(1,1)\}$	4
$y^2+y=x^3+x$	$\{\infty,(0,0),(0,1),(1,0),(1,1)\}$	5
$y^2+y=x^3+x+1$	$\{\infty\}$	1
$y^2+y=x^3$	$\{\infty,(0,0),(0,1)\}$	3

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

From our previous list:

Groups of points

E	$E(\mathbb{F}_2)$	$\|E(\mathbb{F}_2)\|$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	3

So for each curve $E(\mathbb{F}_2)$ is cyclic except possibly for the second for which we need to distinguish between C_4 and $C_2 \oplus C_2$.

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

From our previous list:

Groups of points

E	$E(\mathbb{F}_2)$	$\lvert E(\mathbb{F}_2)\rvert$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	3

So for each curve $E(\mathbb{F}_2)$ is cyclic except possibly for the second for which we need to distinguish between C_4 and $C_2 \oplus C_2$.

Note: each $C_i, i = 1, \ldots, 5$ is represented by a curve $/\mathbb{F}_2$

EXAMPLE: Elliptic curves over $\mathbb{F}_3$

From our previous list:

Groups of points

i	E_i	$E_i(\mathbb{F}_3)$	$\lvert E_i(\mathbb{F}_3)\rvert$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	4
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	1
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	2

EXAMPLE: Elliptic curves over $\mathbb{F}_3$

From our previous list:

Groups of points

i	E_i	$E_i(\mathbb{F}_3)$	$\lvert E_i(\mathbb{F}_3)\rvert$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	4
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	1
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	2

Each $E_i(\mathbb{F}_3)$ is cyclic except possibly for $E_1(\mathbb{F}_3)$ and $E_2(\mathbb{F}_3)$ that could be either C_4 or $C_2 \oplus C_2$. We shall see that:

EXAMPLE: Elliptic curves over $\mathbb{F}_3$

From our previous list:

Groups of points

i	E_i	$E_i(\mathbb{F}_3)$	$\|E_i(\mathbb{F}_3)\|$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	4
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	1
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	2

Each $E_i(\mathbb{F}_3)$ is cyclic except possibly for $E_1(\mathbb{F}_3)$ and $E_2(\mathbb{F}_3)$ that could be either C_4 or $C_2 \oplus C_2$. We shall see that:

$$E_1(\mathbb{F}_3) \cong C_4 \qquad \text{and} \qquad E_2(\mathbb{F}_3) \cong C_2 \oplus C_2$$

EXAMPLE: Elliptic curves over $\mathbb{F}_3$

From our previous list:

Groups of points

i	E_i	$E_i(\mathbb{F}_3)$	$\lvert E_i(\mathbb{F}_3)\rvert$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	4
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	1
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	2

Each $E_i(\mathbb{F}_3)$ is cyclic except possibly for $E_1(\mathbb{F}_3)$ and $E_2(\mathbb{F}_3)$ that could be either C_4 or $C_2 \oplus C_2$. We shall see that:

$$E_1(\mathbb{F}_3) \cong C_4 \qquad \text{and} \qquad E_2(\mathbb{F}_3) \cong C_2 \oplus C_2$$

Note: each $C_i, i = 1, \ldots, 7$ is represented by a curve $/\mathbb{F}_3$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P$$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

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

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Note

- the number of points of order 2 in $E(\mathbb{F}_q)$ equals the number of roots of $X^3 + Ax^2 + Bx + C$ in $\mathbb{F}_q$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Note

- the number of points of order 2 in $E(\mathbb{F}_q)$ equals the number of roots of $X^3 + Ax^2 + Bx + C$ in $\mathbb{F}_q$
- roots are distinct since discriminant $\Delta_E \neq 0$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Note

- the number of points of order 2 in $E(\mathbb{F}_q)$ equals the number of roots of $X^3 + Ax^2 + Bx + C$ in $\mathbb{F}_q$
- roots are distinct since discriminant $\Delta_E \neq 0$
- $E(\mathbb{F}_{q^6})$ has always 3 points of order 2 if $E/\mathbb{F}_q$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Note

- the number of points of order 2 in $E(\mathbb{F}_q)$ equals the number of roots of $X^3 + Ax^2 + Bx + C$ in $\mathbb{F}_q$
- roots are distinct since discriminant $\Delta_E \neq 0$
- $E(\mathbb{F}_{q^6})$ has always 3 points of order 2 if $E/\mathbb{F}_q$
- $E[2] := \{P \in E(\bar{\mathbb{F}}_q) : 2P = \infty\} \cong C_2 \oplus C_2$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

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

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

  Absurd ($a_3 = 0$) and there are no points of order 2.

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4 x + a_6$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

  Absurd ($a_3 = 0$) and there are no points of order 2.
- If $p = 2$ and $E : y^2 + xy = x^3 + a_4 x + a_6$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

  Absurd ($a_3 = 0$) and there are no points of order 2.

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4 x + a_6$

$$-P = (x_1, x_1 + y_1) = (x_1, y_1) = P$$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3y = x^3 + a_2x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

Absurd ($a_3 = 0$) and there are no points of order 2.

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4x + a_6$

$$-P = (x_1, x_1 + y_1) = (x_1, y_1) = P \implies x_1 = 0, y_1^2 = a_6$$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3y = x^3 + a_2x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

Absurd ($a_3 = 0$) and there are no points of order 2.

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4x + a_6$

$$-P = (x_1, x_1 + y_1) = (x_1, y_1) = P \implies x_1 = 0, y_1^2 = a_6$$

So there is exactly one point of order 2 namely $(0, \sqrt{a_6})$

Determining points of order 2 (continues)

- If $p = 2$ and $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_6$

$$-P = (x_1, a_3 + y_1) = (x_1, y_1) = P \implies a_3 = 0$$

Absurd ($a_3 = 0$) and there are no points of order 2.

- If $p = 2$ and $E : y^2 + xy = x^3 + a_4 x + a_6$

$$-P = (x_1, x_1 + y_1) = (x_1, y_1) = P \implies x_1 = 0, y_1^2 = a_6$$

So there is exactly one point of order 2 namely $(0, \sqrt{a_6})$

Definition

2–torsion points

$$E[2] = \{P \in E : 2P = \infty\}.$$

In conclusion

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

Elliptic curves over $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_5$

Each curve $/\mathbb{F}_2$ has cyclic $E(\mathbb{F}_2)$.

E	$E(\mathbb{F}_2)$	$\|E(\mathbb{F}_2)\|$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	3

Elliptic curves over $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_5$

Each curve $/\mathbb{F}_2$ has cyclic $E(\mathbb{F}_2)$.

E	$E(\mathbb{F}_2)$	$\lvert E(\mathbb{F}_2)\rvert$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	3

- $E_1 : y^2 = x^3 + x$ $\qquad E_2 : y^2 = x^3 - x$

  $E_1(\mathbb{F}_3) \cong C_4$ and $E_2(\mathbb{F}_3) \cong C_2 \oplus C_2$

- $E_3 : y^2 = x^3 + x$ $\qquad E_4 : y^2 = x^3 + x + 2$

  $E_3(\mathbb{F}_5) \cong C_2 \oplus C_2$ and $E_4(\mathbb{F}_5) \cong C_4$

- $E_5 : y^2 = x^3 + 4x$ $\qquad E_6 : y^2 = x^3 + 4x + 1$

  $E_5(\mathbb{F}_5) \cong C_2 \oplus C_4$ and $E_6(\mathbb{F}_5) \cong C_8$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

Substituting λ,

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

$$\text{Substituting } \lambda, \quad x_{2P} - x_1 = \frac{-3x_1^4-6Ax_1^2-12Bx_1+A^2}{4(x_1^3+Ax_1+4B)} = 0$$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

$$\text{Substituting } \lambda, \quad x_{2P} - x_1 = \frac{-3x_1^4-6Ax_1^2-12Bx_1+A^2}{4(x_1^3+Ax_1+4B)} = 0$$

Note

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ the 3rd *division* polynomial

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

$$\text{Substituting } \lambda, \quad x_{2P} - x_1 = \frac{-3x_1^4 - 6Ax_1^2 - 12Bx_1 + A^2}{4(x_1^3 + Ax_1 + 4B)} = 0$$

Note

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ the 3rd *division* polynomial
- $(x_1, y_1) \in E(\mathbb{F}_q)$ has order $3 \quad \Rightarrow \psi_3(x_1) = 0$

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

$$\text{Substituting } \lambda, \quad x_{2P} - x_1 = \frac{-3x_1^4 - 6Ax_1^2 - 12Bx_1 + A^2}{4(x_1^3 + Ax_1 + 4B)} = 0$$

Note

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ the 3rd *division* polynomial
- $(x_1, y_1) \in E(\mathbb{F}_q)$ has order 3 $\quad \Rightarrow \psi_3(x_1) = 0$
- $E(\mathbb{F}_q)$ has at most 8 points of order 3

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order } 3 \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu)$$

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

$$P \text{ has order } 3 \iff x_{2P} = x_1$$

$$\text{Substituting } \lambda, \quad x_{2P} - x_1 = \frac{-3x_1^4 - 6Ax_1^2 - 12Bx_1 + A^2}{4(x_1^3 + Ax_1 + 4B)} = 0$$

Note

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ the 3rd *division* polynomial
- $(x_1, y_1) \in E(\mathbb{F}_q)$ has order 3 $\Rightarrow \psi_3(x_1) = 0$
- $E(\mathbb{F}_q)$ has at most 8 points of order 3
- If $p \neq 3$, $E[3] := \{P \in E : 3P = \infty\} \cong C_3 \oplus C_3$

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Example

If $E : y^2 = x^3 + x + 1$, then $\#E(\mathbb{F}_5) = 9$.

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Example

If $E : y^2 = x^3 + x + 1$, then $\#E(\mathbb{F}_5) = 9$.

$$\psi_3(x) = (x + 3)(x + 4)(x^2 + 3x + 4)$$

Hence

$$E[3] = \left\{\infty, (2, \pm 1), (1, \pm\sqrt{3}), (1 \pm 2\sqrt{3}, \pm(1 \pm \sqrt{3}))\right\}$$

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Example

If $E : y^2 = x^3 + x + 1$, then $\#E(\mathbb{F}_5) = 9$.

$$\psi_3(x) = (x+3)(x+4)(x^2+3x+4)$$

Hence

$$E[3] = \left\{\infty, (2, \pm 1), (1, \pm\sqrt{3}), (1 \pm 2\sqrt{3}, \pm(1 \pm \sqrt{3}))\right\}$$

1. $E(\mathbb{F}_5) = \{\infty, (2, \pm 1), (0, \pm 1), (3, \pm 1), (4, \pm 2)\} \cong C_9$

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Example

If $E : y^2 = x^3 + x + 1$, then $\#E(\mathbb{F}_5) = 9$.

$$\psi_3(x) = (x+3)(x+4)(x^2+3x+4)$$

Hence

$$E[3] = \left\{\infty, (2, \pm 1), (1, \pm\sqrt{3}), (1 \pm 2\sqrt{3}, \pm(1 \pm \sqrt{3}))\right\}$$

1. $E(\mathbb{F}_5) = \{\infty, (2, \pm 1), (0, \pm 1), (3, \pm 1), (4, \pm 2)\} \cong C_9$
2. Since $\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{3}] \quad \Rightarrow \quad E[3] \subset E(\mathbb{F}_{25})$

Determining points of order 3 (continues)

Note

Let $E : y^2 = x^3 + Ax^2 + Bx + C, A, B, C \in \mathbb{F}_{3^n}$. If $P = (x_1, y_1) \in E(\mathbb{F}_{3^n})$ has order 3, then

1. $Ax_1^3 + AC - B^2 = 0$
2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Example

If $E : y^2 = x^3 + x + 1$, then $\#E(\mathbb{F}_5) = 9$.

$$\psi_3(x) = (x+3)(x+4)(x^2+3x+4)$$

Hence

$$E[3] = \left\{\infty, (2, \pm 1), (1, \pm\sqrt{3}), (1 \pm 2\sqrt{3}, \pm(1 \pm \sqrt{3}))\right\}$$

1. $E(\mathbb{F}_5) = \{\infty, (2, \pm 1), (0, \pm 1), (3, \pm 1), (4, \pm 2)\} \cong C_9$
2. Since $\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{3}] \quad \Rightarrow \quad E[3] \subset E(\mathbb{F}_{25})$
3. $\#E(\mathbb{F}_{25}) = 27 \quad \Rightarrow \quad E(\mathbb{F}_{25}) \cong C_3 \oplus C_9$

Determining points of order 3 (continues)

Inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\left\{\begin{array}{l}\infty, (0, \pm 3), (-1, \pm 1), \\ (5, \pm 1), (3, \pm 1)\end{array}\right\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

Determining points of order 3 (continues)

Inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\left\{ \begin{matrix} \infty, (0, \pm 3), (-1, \pm 1), \\ (5, \pm 1), (3, \pm 1) \end{matrix} \right\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

Can one count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$?

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

Determining points of order 3 (continues)

Inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\left\{ \begin{array}{l} \infty, (0, \pm 3), (-1, \pm 1), \\ (5, \pm 1), (3, \pm 1) \end{array} \right\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

Can one count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$?

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

We know $E(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\} \subset E(\mathbb{F}_4)$.

Determining points of order 3 (continues)

Inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\left\{\begin{array}{l}\infty, (0, \pm 3), (-1, \pm 1),\\ (5, \pm 1), (3, \pm 1)\end{array}\right\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

Can one count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$?

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

We know $E(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\} \subset E(\mathbb{F}_4)$.

$E(\mathbb{F}_4) = \{\infty, (0,0), (0,1), (1,\xi), (1,\xi+1), (\xi,\xi), (\xi,\xi+1), (\xi+1,\xi), (\xi+1,\xi+1)\}$

Determining points of order 3 (continues)

Inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\left\{ \begin{array}{c} \infty, (0, \pm 3), (-1, \pm 1), \\ (5, \pm 1), (3, \pm 1) \end{array} \right\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

Can one count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$?

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

We know $E(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\} \subset E(\mathbb{F}_4)$.

$E(\mathbb{F}_4) = \{\infty, (0,0), (0,1), (1,\xi), (1,\xi+1), (\xi,\xi), (\xi,\xi+1), (\xi+1,\xi), (\xi+1,\xi+1)\}$

$$\psi_3(x) = x^4 + x = x(x+1)(x+\xi)(x+\xi+1) \Rightarrow E(\mathbb{F}_4) \cong C_3 \oplus C_3$$

Note (Suppose $(x_0, y_0) \in E/\mathbb{F}_{2^n}$ has order 3. Then)

1. $E : y^2 + a_3 y = x^3 + a_4 x + a_6 \;\Rightarrow\; x_0^4 + a_3^2 x_0 + (a_4 a_3)^2 = 0$

Determining points of order 3 (continues)

Inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\left\{ \begin{array}{l} \infty, (0, \pm 3), (-1, \pm 1), \\ (5, \pm 1), (3, \pm 1) \end{array} \right\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

Can one count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$?

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

We know $E(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\} \subset E(\mathbb{F}_4)$.

$E(\mathbb{F}_4) = \{\infty, (0,0), (0,1), (1,\xi), (1,\xi+1), (\xi,\xi), (\xi,\xi+1), (\xi+1,\xi), (\xi+1,\xi+1)\}$

$$\psi_3(x) = x^4 + x = x(x+1)(x+\xi)(x+\xi+1) \Rightarrow E(\mathbb{F}_4) \cong C_3 \oplus C_3$$

Note (Suppose $(x_0, y_0) \in E/\mathbb{F}_{2^n}$ has order 3. Then)

1. $E : y^2 + a_3 y = x^3 + a_4 x + a_6 \;\Rightarrow\; x_0^4 + a_3^2 x_0 + (a_4 a_3)^2 = 0$
2. $E : y^2 + xy = x^3 + a_2 x^2 + a_6 \;\Rightarrow\; x_0^4 + x_0^3 + a_6 = 0$

Determining points of order (dividing) m

Determining points of order (dividing) m

Definition (m–torsion point)

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

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

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

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

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

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

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

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

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.

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. From *Structure of Torsion Theorem*, $\#E[n_1] \leq n_1^2$. So $r \leq 2$ □

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 $r \leq 2$ □

Theorem (Corollary of Weil Pairing)

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

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 $r \leq 2$ □

Theorem (Corollary of Weil Pairing)

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

Theorem (Hasse)

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

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

Theorem (Hasse)

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

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

So $\#E(\mathbb{F}_q) \in [(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$ the *Hasse interval* $\mathcal{I}_q$

Example (Hasse Intervals)

q	$\mathcal{I}_q$
2	$\{1,2,3,4,5\}$
3	$\{1,2,3,4,5,6,7\}$
4	$\{1,2,3,4,5,6,7,8,9\}$
5	$\{2,3,4,5,6,7,8,9,10\}$
7	$\{3,4,5,6,7,8,9,10,11,12,13\}$
8	$\{4,5,6,7,8,9,10,11,12,13,14\}$
9	$\{4,5,6,7,8,9,10,11,12,13,14,15,16\}$
11	$\{6,7,8,9,10,11,12,13,14,15,16,17,18\}$
13	$\{7,8,9,10,11,12,13,14,15,16,17,18,19,20,21\}$
16	$\{9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25\}$
17	$\{10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26\}$
19	$\{12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28\}$
23	$\{15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33\}$
25	$\{16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36\}$
27	$\{18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38\}$
29	$\{20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40\}$
31	$\{21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43\}$
32	$\{22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44\}$

Theorem (Waterhouse)

Theorem (Waterhouse)

Let $q = p^n$ *and let* $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \; s.t. \# E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

Theorem (Waterhouse)

Let $q = p^n$ *and let* $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \le 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) *n even and one of the following is satisfied:*

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) n *even and one of the following is satisfied:*

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

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) n *even and one of the following is satisfied:*

1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \le 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) n *even and one of the following is satisfied:*

1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;
3. $p \not\equiv 1 \pmod 4$, *and* $a = 0$;

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \le 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) n *even and one of the following is satisfied:*

1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;
3. $p \not\equiv 1 \pmod 4$, *and* $a = 0$;

(iii) n *is odd, and one of the following is satisfied:*

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ *and let* $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) n *even and one of the following is satisfied:*

1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;
3. $p \not\equiv 1 \pmod 4$, *and* $a = 0$;

(iii) n *is odd, and one of the following is satisfied:*

1. $p = 2$ *or* 3, *and* $a = \pm p^{(n+1)/2}$;

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \# E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

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

(ii) n *even and one of the following is satisfied:*

1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;
3. $p \not\equiv 1 \pmod 4$, *and* $a = 0$;

(iii) n *is odd, and one of the following is satisfied:*

1. $p = 2$ *or* 3, *and* $a = \pm p^{(n+1)/2}$;
2. $a = 0$.

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Rück)

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

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

There exists $E/\mathbb{F}_q$ s.t.

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. $n_1 = n_2$ *in the case (ii).1 of Waterhouse's Theorem;*

Theorem (Rück)

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

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

There exists $E/\mathbb{F}_q$ *s.t.*

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. $n_1 = n_2$ *in the case (ii).1 of Waterhouse's Theorem;*
2. $n_1 | q - 1$ *in all other cases of Waterhouse's Theorem.*

Theorem (Rück)

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

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

There exists $E/\mathbb{F}_q$ *s.t.*

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. $n_1 = n_2$ *in the case (ii).1 of Waterhouse's Theorem;*
2. $n_1 | q - 1$ *in all other cases of Waterhouse's Theorem.*

Theorem (Rück)

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

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

There exists $E/\mathbb{F}_q$ s.t.

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. *$n_1 = n_2$ in the case (ii).1 of Waterhouse's Theorem;*
2. *$n_1 | q - 1$ in all other cases of Waterhouse's Theorem.*

Example

- If $q = p^{2n}$ and $\#E(\mathbb{F}_q) = q + 1 \pm 2\sqrt{q} = (p^n \pm 1)^2$, then $E(\mathbb{F}_q) \cong C_{p^n \pm 1} \oplus C_{p^n \pm 1}$.

Theorem (Rück)

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

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

There exists $E/\mathbb{F}_q$ s.t.

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. *$n_1 = n_2$ in the case (ii).1 of Waterhouse's Theorem;*
2. *$n_1 | q - 1$ in all other cases of Waterhouse's Theorem.*

Example

- If $q = p^{2n}$ and $\#E(\mathbb{F}_q) = q + 1 \pm 2\sqrt{q} = (p^n \pm 1)^2$, then
  $$E(\mathbb{F}_q) \cong C_{p^n \pm 1} \oplus C_{p^n \pm 1}.$$
- Let $N = 100$ and $q = 101 \Rightarrow \exists E_1, E_2, E_3, E_4/\mathbb{F}_{101}$ s.t.
  $$E_1(\mathbb{F}_{101}) \cong C_{10} \oplus C_{10} \qquad E_2(\mathbb{F}_{101}) \cong C_2 \oplus C_{50}$$
  $$E_3(\mathbb{F}_{101}) \cong C_5 \oplus C_{20} \qquad E_4(\mathbb{F}_{101}) \cong C_{100}$$

Weil Pairing

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

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

Weil Pairing

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

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

We set

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

Weil Pairing

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

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

We set

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

Weil Pairing

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

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

We set

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

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

Theorem (Existence of Weil Pairing)

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

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

The last one needs to be discussed further!!!

Further Reading...

- Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.
- J. W. S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.
- John E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.
- Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.
- Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.
- Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
- Joseph H. Silverman and John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
- Lawrence C. Washington, Elliptic curves: Number theory and cryptography, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.
- Horst G. Zimmer, Computational aspects of the theory of elliptic curves, Number theory and applications (Banff, AB, 1988) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 279–324.