



# Lecture 1

## Elliptic curves over finite fields

### First steps

**Research School: Algebraic curves over finite fields**

*CIMPA-ICTP-UNESCO-MESR-MINECO-PHILIPPINES*

University of the Philippines Diliman, July 22, 2013

#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

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:

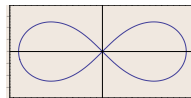
- $\pi = 2i \log \frac{1-i}{1+i}$
- Length of *Lemniscate*



Carlo Fagnano



Collegio Clementino



Lemniscate

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



### Introduction

#### History

length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates.

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Length of Ellipses



## Introduction

History

length of ellipses

why Elliptic curves?

Fields

## Weierstraß Equations

Singular points

The Discriminant

Elliptic curves /  $\mathbb{F}_2$

Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane

Homogeneous Polynomials

Points at infinity

Homogeneous Coordinates

## The sum of points

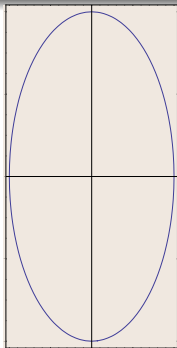
## Examples

Structure of  $E(\mathbb{F}_2)$

Structure of  $E(\mathbb{F}_3)$

Further Examples

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



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

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

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

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

Apply the invertible change of variables:

$$\begin{cases} x \rightarrow 1 - 2/x \\ y \rightarrow \frac{y}{x-1} \end{cases}$$

Arrive to

$$y^2 = x^3 - 4x^2 + 6x - 3$$

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

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

## Reasons to study them

- 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!!

### Further Examples

## Fields of characteristics 0

- 1  $\mathbb{Q}$  is the field of rational numbers
- 2  $\mathbb{R}$  and  $\mathbb{C}$  are the fields of real and complex numbers
- 3  $K \subset \mathbb{C}$ ,  $\dim_{\mathbb{Q}} K < \infty$  is a *number field*
  - $\mathbb{Q}[\sqrt{d}]$ ,  $d \in \mathbb{Q}$
  - $\mathbb{Q}[\alpha]$ ,  $f(\alpha) = 0$ ,  $f \in \mathbb{Q}[X]$  irreducible

## Finite fields

- 1  $\mathbb{F}_p = \{0, 1, \dots, p-1\}$  is the prime field;
- 2  $\mathbb{F}_q$  is a finite field with  $q = p^n$  elements
- 3  $\mathbb{F}_q = \mathbb{F}_p[\xi]$ ,  $f(\xi) = 0$ ,  $f \in \mathbb{F}_p[X]$  irreducible,  $\partial f = n$
- 4  $\mathbb{F}_4 = \mathbb{F}_2[\xi]$ ,  $\xi^2 = 1 + \xi$
- 5  $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ ,  $\alpha^3 = \alpha + 1$  but also  $\mathbb{F}_8 = \mathbb{F}_2[\beta]$ ,  $\beta^3 = \beta^2 + 1$ ,  
( $\beta = \alpha^2 + 1$ )
- 6  $\mathbb{F}_{101^{101}} = \mathbb{F}_{101}[\omega]$ ,  $\omega^{101} = \omega + 1$



### Introduction

History  
length of ellipses  
why Elliptic curves?

### Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples



## Algebraic Closure of $\mathbb{F}_q$

- $\mathbb{C} \supset \mathbb{Q}$  satisfies that *Fundamental Theorem of Algebra!* (i.e.  $\forall f \in \mathbb{Q}[x], \partial f > 1, \exists \alpha \in \mathbb{C}, f(\alpha) = 0$ )
- We need a field that plays the role, for  $\mathbb{F}_q$ , that  $\mathbb{C}$  plays for  $\mathbb{Q}$ . It will be  $\overline{\mathbb{F}}_q$ , called *algebraic closure of  $\mathbb{F}_q$*

- 1  $\forall n \in \mathbb{N}$ , we fix an  $\mathbb{F}_{q^n}$
- 2 We also require that  $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$  if  $n \mid m$
- 3 We let  $\overline{\mathbb{F}}_q = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{q^n}$

- **Fact:**  $\overline{\mathbb{F}}_q$  is *algebraically closed* (i.e.  $\forall f \in \mathbb{F}_q[x], \partial f > 1, \exists \alpha \in \overline{\mathbb{F}}_q, f(\alpha) = 0$ )

If  $F(x, y) \in \mathbb{Q}[x, y]$  a point of the curve  $F = 0$ , means  $(x_0, y_0) \in \mathbb{C}^2$  s.t.  $F(x_0, y_0) = 0$ .

If  $F(x, y) \in \mathbb{F}_q[x, y]$  a point of the curve  $F = 0$ , means  $(x_0, y_0) \in \overline{\mathbb{F}}_q^2$  s.t.  $F(x_0, y_0) = 0$ .

### Introduction

History  
length of ellipses  
why Elliptic curves?

### Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

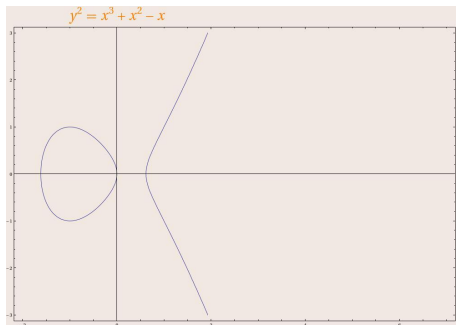
Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# 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*



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## Tangent line to a plane curve

Given  $f(x, y) \in \mathbb{F}_q[x, y]$  and a point  $(x_0, y_0)$  such that  $f(x_0, y_0) = 0$ , the *tangent line* is:

$$\frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0) = 0$$

If

$$\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0,$$

such a tangent line cannot be computed and we say that  $(x_0, y_0)$  is *singular*

### Definition

A non singular curve is a curve without any singular point

### Example

The tangent line to  $x^2 + y^2 = 1$  over  $\mathbb{F}_7$  at  $(2, 2)$  is

$$x + y = 4$$



#### Introduction

- History
- length of ellipses
- why Elliptic curves?
- Fields

#### Weierstraß Equations

##### Singular points

- The Discriminant
- Elliptic curves /  $\mathbb{F}_2$
- Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$

- Projective Plane
- Homogeneous Polynomials
- Points at infinity
- Homogeneous Coordinates

#### The sum of points

#### Examples

- Structure of  $E(\mathbb{F}_2)$
- Structure of  $E(\mathbb{F}_3)$
- Further Examples



# Singular points

## The classical definition

### Definition

A *singular* point  $(x_0, y_0)$  on a curve  $f(x, y) = 0$  is a point such that

$$\begin{cases} \frac{\partial f}{\partial x}(x_0, y_0) = 0 \\ \frac{\partial f}{\partial y}(x_0, y_0) = 0 \end{cases}$$

So, at a singular point there is no (unique) tangent line!! In the special case of Weierstraß equations:

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

we have

$$\begin{cases} \partial_x = 0 \\ \partial_y = 0 \end{cases} \longrightarrow \begin{cases} a_1y = 3x^2 + 2a_2x + a_4 \\ 2y + a_1x + a_3 = 0 \end{cases}$$

We can express this condition in terms of the coefficients  $a_1, a_2, a_3, a_4, a_5$ .



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

#### Singular points

The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# The Discriminant of an Equation

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

With a bit of Mathematica

```

Ell:=-a_6-a_4x-a_2x^2-x^3+a_3y+a_1xy+y^2;
SS:=Solve[{D[Ell,x]==0,D[Ell,y]==0},{y,x}];
Simplify[ReplaceAll[Ell,SS[[1]]]*ReplaceAll[Ell,SS[[2]]]]

```

we obtain

$$\begin{aligned}
\Delta'_E := \frac{1}{243} & \left( -a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16a_1 a_2^2 a_3 a_4 + 36a_1^2 a_3^2 a_4 \right. \\
& - a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16a_2^2 a_4^2 + 96a_1 a_3 a_4^2 + 64a_4^3 + \\
& a_1^6 a_6 + 12a_1^4 a_2 a_6 + 48a_1^2 a_2^2 a_6 + 64a_2^3 a_6 - 36a_1^3 a_3 a_6 \\
& \left. - 144a_1 a_2 a_3 a_6 - 72a_1^2 a_4 a_6 - 288a_2 a_4 a_6 + 432a_6^2 \right)
\end{aligned}$$

## Definition

The *discriminant* of a Weierstraß equation over  $\mathbb{F}_q$ ,  $q = p^n$ ,  $p \geq 5$  is

$$\Delta_E := 3^3 \Delta'_E$$



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points

## The Discriminant

Elliptic curves /  $\mathbb{F}_2$

Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## The discriminant of $E/\mathbb{F}_{2^\alpha}$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{F}_{2^\alpha}$$

If  $p = 2$ , the singularity condition becomes:

$$\begin{cases} \partial_x = 0 \\ \partial_y = 0 \end{cases} \longrightarrow \begin{cases} a_1y = x^2 + a_4 \\ a_1x + a_3 = 0 \end{cases}$$

## Classification of Weierstraß equations over $\mathbb{F}_{2^\alpha}$

- Case  $a_1 \neq 0$ :

```
El:=a6+a4x+a2x^2+x^3+a3y+a1xy+y^2;  
Simplify[ReplaceAll[El,{x->a3/a1,y->((a3/a1)^2+a4)/a1}]]
```

we obtain

$$\Delta_E := (a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_1^4 a_4^2 + a_1^3 a_3^3 + a_3^4) / a_1^6$$

- Case  $a_1 = 0$  and  $a_3 \neq 0$ : curve non singular ( $\Delta_E := a_3$ )
- Case  $a_1 = 0$  and  $a_3 = 0$ : **curve singular**  
 $(x_0, y_0), (x_0^2 = a_4, y_0^2 = a_2 a_4 + a_6)$  is the singular point!



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points

#### The Discriminant

Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## Special Weierstraß equation of $E/\mathbb{F}_{p^\alpha}$ , $p \neq 2$



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points

### The Discriminant

Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in \mathbb{F}_{p^\alpha}$$

If we “complete the squares” by applying the transformation:

$$\begin{cases} x \leftarrow x \\ y \leftarrow y - \frac{a_1x + a_3}{2} \end{cases}$$

the Weierstraß equation becomes:

$$E' : y^2 = x^3 + a'_2x^2 + a'_4x + a'_6$$

where  $a'_2 = a_2 + \frac{a_1^2}{4}$ ,  $a'_4 = a_4 + \frac{a_1a_3}{2}$ ,  $a'_6 = a_6 + \frac{a_3^2}{4}$

If  $p \geq 5$ , we can also apply the transformation

$$\begin{cases} x \leftarrow x - \frac{a'_2}{3} \\ y \leftarrow y \end{cases}$$

obtaining the equations:

$$E'' : y^2 = x^3 + a''_4x + a''_6$$

where  $a''_4 = a'_4 - \frac{a'_2{}^2}{3}$ ,  $a''_6 = a'_6 + \frac{2a'_2{}^3}{27} - \frac{a'_2a'_4}{3}$

# Special Weierstraß equation for $E/\mathbb{F}_{2^\alpha}$

Case  $a_1 \neq 0$

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad a_i \in \mathbb{F}_{2^\alpha}$$
$$\Delta_E := \frac{a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_1^4 a_4^2 + a_1^3 a_3^3 + a_3^4}{a_1^6}$$

If we apply the affine transformation:

$$\begin{cases} x \leftarrow a_1^2 x + a_3/a_1 \\ y \leftarrow a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^2 \end{cases}$$

we obtain

$$E' : y^2 + xy = x^3 + \left( \frac{a_2}{a_1^2} + \frac{a_3}{a_1^3} \right) x^2 + \frac{\Delta_E}{a_1^6}$$

Surprisingly  $\Delta_{E'} = \Delta_E / a_1^6$

With Mathematica

```
E1:=a6+a4x+a2x^2+x^3+a3y+a1xy+y^2;  
Simplify[PolynomialMod[ReplaceAll[E1,  
{x->a1^2 x+a3/a1, y->a1^3 y+(a1^2 a4+a3^2)/a1^3}],2]]
```



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Special Weierstraß equation for $E/\mathbb{F}_{2^\alpha}$

Case  $a_1 = 0$  and  $\Delta_E := a_3 \neq 0$

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad a_i \in \mathbb{F}_{2^\alpha}$$

If we apply the affine transformation:

$$\begin{cases} x \longleftarrow x + a_2 \\ y \longleftarrow y \end{cases}$$

we obtain

$$E : y^2 + a_3 y = x^3 + (a_4 + a_2^2)x + (a_6 + a_2 a_4)$$

With Mathematica

```
E1:=a6+a4x+a2x^2+x^3+a3y+y^2;  
Simplify[PolynomialMod[ReplaceAll[E1,{x->x+a2,y->y}],2]]
```

## Definition

Two Weierstraß equations over  $\mathbb{F}_q$  are said (affinely) equivalent if there exists a (affine) change of variables that takes one into the other

## Exercise

Prove that necessarily the change of variables has form

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



## Introduction

- History
- length of ellipses
- why Elliptic curves?
- Fields

## Weierstraß Equations

- Singular points
- The Discriminant
- Elliptic curves  $/\mathbb{F}_2$
- Elliptic curves  $/\mathbb{F}_3$

## Point at infinity of $E$

- Projective Plane
- Homogeneous Polynomials
- Points at infinity
- Homogeneous Coordinates

## The sum of points

## Examples

- Structure of  $E(\mathbb{F}_2)$
- Structure of  $E(\mathbb{F}_3)$
- Further Examples

# 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)

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

### Definition (Elliptic curve)

An elliptic curve is 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



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points

#### The Discriminant

Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

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  $\mathbb{F}_2$



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant

## Elliptic curves / $\mathbb{F}_2$

Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples



## Elliptic curves in characteristic 3

Via a suitable transformation ( $x \rightarrow u^2x + r, y \rightarrow u^3y + u^2sx + t$ ) 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  $y^2 = x^3 - x^2 - 1$

### Exercise: Prove that

- ① Over  $\mathbb{F}_5$  there are 12 elliptic curves
- ② Compute all of them
- ③ How many are there over  $\mathbb{F}_4$ , over  $\mathbb{F}_7$  and over  $\mathbb{F}_8$ ?



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$

#### Elliptic curves / $\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples



## Definition (Projective plane)

$$\mathbb{P}_2(\mathbb{F}_q) = (\mathbb{F}_q^3 \setminus \{\mathbf{0}\}) / \sim$$

where  $\mathbf{0} = (0, 0, 0)$  and

$$\mathbf{x} = (x_1, x_2, x_3) \sim \mathbf{y} = (y_1, y_2, y_3) \iff \mathbf{x} = \lambda \mathbf{y}, \exists \lambda \in \mathbb{F}_q^*$$

## Basic properties of the projective plane

- 1  $P \in \mathbb{P}_2(\mathbb{F}_q) \Rightarrow P = [\mathbf{x}] = \{\lambda \mathbf{x} : \lambda \in \mathbb{F}_q^*, \mathbf{x} \in \mathbb{F}_q^3, \mathbf{x} \neq \mathbf{0}\}$
- 2  $\#[\mathbf{x}] = q - 1$ . Hence  $\#\mathbb{P}_2(\mathbb{F}_q) = \frac{q^3 - 1}{q - 1} = q^2 + q + 1$ ;
- 3  $P \in \mathbb{P}_2(\mathbb{F}_q)$ ,  $P =: [x, y, z]$  with  $(x, y, z) \in \mathbb{F}_q^3 \setminus \{\mathbf{0}\}$ ;
- 4  $[x, y, z] = [x', y', z'] \iff \text{rank} \begin{pmatrix} x & y & z \\ x' & y' & z' \end{pmatrix} = 1$
- 5  $\mathbb{P}_2(\mathbb{F}_q) \longleftrightarrow \{\text{lines through } \mathbf{0} \text{ in } \mathbb{F}_q^3\} = \{V \subset \mathbb{F}_q^3 : \dim V = 1\}$
- 6  $\mathbb{P}_2(\mathbb{F}_q) \longleftrightarrow \{\text{lines in } \mathbb{F}_q^2\}$ ,  $[a, b, c] \mapsto aX + bY + cZ = 0$

## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# The projective Plane

## Infinite and Affine points

- $P = [x, y, 0]$  *is a point at infinity*
- $P = [x, y, 1]$  *is an affine point*
- $P \in \mathbb{P}_2(\mathbb{F}_q)$  is either affine or at infinity
- $\mathbb{A}_2(\mathbb{F}_q) := \{[x, y, 1] : (x, y) \in \mathbb{F}_q^2\}$  *set of affine points*  
 $\#\mathbb{A}_2(\mathbb{F}_q) = q^2$
- $\mathbb{P}_1(\mathbb{F}_q) := \{[x, y, 0] : (x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\}$  *line at infinity*  
 $\#\mathbb{P}_1(\mathbb{F}_q) = q + 1$
- $\mathbb{P}_2(\mathbb{F}_q) = \mathbb{A}_2(\mathbb{F}_q) \sqcup \mathbb{P}_1(\mathbb{F}_q)$  *disjoint union*
- $\mathbb{P}_1(\mathbb{F}_q)$  can be thought as *set of directions of lines in  $\mathbb{F}_q^2$*

## General construction

- $\mathbb{P}_n(K)$ ,  $K$  field,  $n \geq 3$  is similarly defined;
- $\mathbb{P}_n(K) = \mathbb{A}_n(K) \sqcup \mathbb{P}_{n-1}(K)$
- $\#\mathbb{P}_n(\mathbb{F}_q) = q^n + \dots + q + 1$
- $\mathbb{P}_n(K) \longleftrightarrow \{\text{lines in } K^n\}$



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

#### Projective Plane

Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Homogeneous Polynomials

## Definition (Homogeneous polynomials)

$g(X_1, \dots, X_m) \in \mathbb{F}_q[X_1, \dots, X_m]$  is said *homogeneous* if all its monomials have the same degree. i.e.

$$g(X_1, \dots, X_m) = \sum_{j_1 + \dots + j_m = \partial g} a_{j_1, \dots, j_m} X_1^{j_1} \cdots X_m^{j_m}, a_{j_1, \dots, j_m} \in \mathbb{F}_q$$

## Properties of homogeneous polynomials - Projective Curves

- $\forall \lambda, F(\lambda X, \lambda Y, \lambda Z) = \lambda^{\partial F} F(X, Y, Z)$
- If  $P = [X_0, Y_0, Z_0] \in \mathbb{P}_2(\mathbb{F}_q)$ , then  $F(X_0, Y_0, Z_0) = 0$  depends only on  $P$ , not on  $X_0, Y_0, Z_0$
- $F(P) = 0 \Leftrightarrow F(X_0, Y_0, Z_0) = 0$  is well defined
- *Projective curve*  $F(X, Y, Z) = 0$  the set of  $P \in \mathbb{P}_2(\mathbb{F}_q)$  s.t.  $F(P) = 0$

## Example

Projective line  $aX + bY + cZ = 0$ ;  $Z = 0$ , line at infinity



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane

### Homogeneous Polynomials

Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Points at infinity of a plane curve

## Definition (Homogenized polynomial)

if  $f(x, y) \in \mathbb{F}_q[x, y]$ ,

$$F_f(X, Y, Z) = Z^{\partial f} f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

- $F_f$  is homogenous, **the homogenized of  $f$**
- $\partial F_f = \partial f$
- if  $f(x_0, y_0) = 0$ , then  $F_f(x_0, y_0, 1) = 0$
- the points of the curve  $f = 0$  are the affine points of the projective curve  $F_f = 0$

## Example (homogenized curves)

curve	affine curve	homogenized (projective curve)
line	$ax + by = c$	$aX + bY = cZ$
conic	$ax^2 + by^2 = 1$	$aX^2 + bY^2 = Z^2$

$Z = 0$  (line at infinity)

Not the homogenized of anything



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials

### Points at infinity

Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Points at infinity of a plane curve

## Definition

If  $f \in \mathbb{F}_q[x, y]$  then

$$\{[\alpha, \beta, 0] \in \mathbb{P}_2(\mathbb{F}_q) : F_f(\alpha, \beta, 0) = 0\}$$

is the set of *points at infinity* of  $f = 0$ .

(i.e. the intersection of the curve and  $Z = 0$ , the line at infinity)

The points of  $Z = 0$  are directions of lines in  $\mathbb{F}_q^2$

## Example (point at infinity)

- line:  $ax + by + c = 0 \rightsquigarrow [b, -a, 0]$
- hyperbola:  $x^2/a^2 - y^2/b^2 = 1 \rightsquigarrow [a, \pm b, 0]$
- parabola:  $y = ax^2 + bx + c \rightsquigarrow [0, 1, 0]$
- elliptic curve:  
 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \rightsquigarrow [0, 1, 0]$

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



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Projective lines

## tangent lines to projective curves

### Definition

If  $P = [x_1, y_1, z_1], Q = [x_2, y_2, z_2] \in \mathbb{P}_2(\mathbb{F}_q)$ , the projective line through  $P, Q$  is

$$r_{P,Q} : \det \begin{vmatrix} X & Y & Z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0$$

### Definition

The *tangent line* to a projective curve  $F(X, Y, Z) = 0$  at a non singular point  $P = [X_0, Y_0, Z_0]$  ( $F(X_0, Y_0, Z_0) = 0$ ) is

$$\frac{\partial F}{\partial X}(X_0, Y_0, Z_0)X + \frac{\partial F}{\partial Y}(X_0, Y_0, Z_0)Y + \frac{\partial F}{\partial Z}(X_0, Y_0, Z_0)Z = 0$$

### Exercise (Prove that)

- 1  $P$  belongs to its (projective) tangent line
- 2  $P$  affine  $\Rightarrow$  its tangent line is the homogenized of the affine tangent line
- 3 the tangent line to  $E/\mathbb{F}_q$  at  $\infty = [0, 1, 0]$  is  $Z = 0$  (line at infinity)



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## 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

- $E(\mathbb{F}_q) \subset \mathbb{P}_2(\mathbb{F}_q)$   $\rightarrow$  geometric advantages
  - $E(\mathbb{F}_q) \subset \mathbb{F}_q^2 \cup \{\infty\}$   $\rightarrow$  algebraic advantages
- $\infty$  might be thought as the “vertical direction”

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

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

- 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)  $\Rightarrow \infty = [0, 1, 0] \in r_{P,Q}$



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

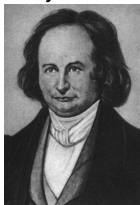
Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples



## History (from WIKIPEDIA)

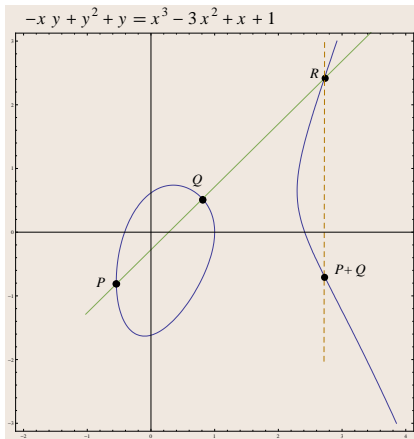
### Carl Gustav Jacob Jacobi

(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  
 $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$



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

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

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

$$-P := P'$$

## Elliptic curves over $\mathbb{F}_q$

F. Pappalardi



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# 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)**
- 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  $E(\mathbb{F}_{q^n})$



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## Computing the inverse $-P$

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

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

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

Write  $P' = (x'_1, y'_1)$ . Since  $r_{P, \infty} : x = x_1 \Rightarrow x'_1 = x_1$  and  $y_1$  satisfies

$$y^2 + a_1x_1y + a_3y - (x_1^3 + a_2x_1^2 + a_4x_1 + a_6) = (y - y_1)(y - y'_1)$$

So  $y_1 + y'_1 = -a_1x_1 - a_3$  (both coefficients of  $y$ ) and

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

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

**Definition:**  $P_1 +_E P_2 = -P_3$  where  $r_{P_1, P_2} \cap E(\mathbb{F}_q) = \{P_1, P_2, P_3\}$

Finally, if  $P_3 = (x_3, y_3)$ , then

$$P_1 +_E P_2 = -P_3 = (x_3, -a_1x_3 - a_3 - y_3)$$



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Lines through points of $E$

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

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

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

$$\textcircled{1} P_1 \neq P_2 \text{ and } x_1 \neq x_2 \implies r_{P_1, P_2} : y = \lambda x + \nu$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - x_1y_2}{x_2 - x_1}$$

$$\textcircled{2} P_1 \neq P_2 \text{ and } x_1 = x_2 \implies r_{P_1, P_2} : x = x_1$$

$$\textcircled{3} P_1 = P_2 \text{ and } 2y_1 + a_1x_1 + a_3 \neq 0 \implies r_{P_1, P_2} : y = \lambda x + \nu$$

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

$$\textcircled{4} P_1 = P_2 \text{ and } 2y_1 + a_1x_1 + a_3 = 0 \implies r_{P_1, P_2} : x = x_1$$

$$\textcircled{5} r_{P_1, \infty} : x = x_1 \quad r_{\infty, \infty} : z = 0$$



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## Intersection between a line and $E$

We want to compute  $P_3 = (x_3, y_3)$  where  $r_{P_1, P_2} : y = \lambda x + \nu$ ,

$$r_{P_1, P_2} \cap E(\mathbb{F}_q) = \{P_1, P_2, P_3\}$$

We find the intersection:

$$r_{P_1, P_2} \cap E(\mathbb{F}_q) = \left\{ \begin{array}{l} E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ r_{P_1, P_2} : y = \lambda x + \nu \end{array} \right.$$

Substituting

$$(\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3(\lambda x + \nu) = x^3 + a_2x^2 + a_4x + a_6$$

Since  $x_1$  and  $x_2$  are solutions, we can find  $x_3$  by comparing

$$\begin{aligned} x^3 + a_2x^2 + a_4x + a_6 - ((\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3(\lambda x + \nu)) &= \\ x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + \dots &= \\ (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \dots \end{aligned}$$

Equating coefficients of  $x^2$ ,

$$x_3 = \lambda^2 - a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu$$

Finally

$$P_3 = (\lambda^2 - a_1\lambda - a_2 - x_1 - x_2, \lambda^3 - a_1\lambda^2 - \lambda(a_2 + x_1 + x_2) + \nu)$$



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# 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  $P_1 \neq P_2$

- $x_1 = x_2$
- $x_1 \neq x_2$

$$\Rightarrow P_1 +_E P_2 = \infty$$

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

- If  $P_1 = P_2$

- $2y_1 + a_1x + a_3 = 0$
- $2y_1 + a_1x + a_3 \neq 0$

$$\Rightarrow P_1 +_E P_2 = 2P_1 = \infty$$

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

Then

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



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# 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  $P_1 \neq P_2$

- $x_1 = x_2$
- $x_1 \neq x_2$

$$\Rightarrow P_1 +_E P_2 = \infty$$

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

- If  $P_1 = P_2$

- $y_1 = 0$
- $y_1 \neq 0$

$$\Rightarrow P_1 +_E P_2 = 2P_1 = \infty$$

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

Then

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



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## A Finite Field Example

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

### Example

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

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

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

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

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

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

### Exercise

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



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples



## Theorem (Classification of finite abelian groups)

If  $G$  is *abelian and finite*,  $\exists n_1, \dots, n_k \in \mathbb{N}^{>1}$  such that

①  $n_1 \mid n_2 \mid \dots \mid n_k$

②  $G \cong C_{n_1} \oplus \dots \oplus C_{n_k}$

Furthermore  $n_1, \dots, n_k$  (*Group Structure*) are unique

## Example (One can verify that:)

$$C_{2400} \oplus C_{72} \oplus C_{1440} \cong C_{12} \oplus C_{60} \oplus C_{15200}$$

Shall show Wednesday that

$$E(\mathbb{F}_q) \cong C_n \oplus C_{nk} \quad \exists n, k \in \mathbb{N}^{>0}$$

(i.e.  $E(\mathbb{F}_q)$  is either cyclic ( $n = 1$ ) or the product of 2 cyclic groups)



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

# Proof of the associativity

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

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

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

## Mathematica code

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

- runs in 2 seconds on a PC
- For an elementary proof: "An Elementary Proof of the Group Law for Elliptic Curves."  
Department of Mathematics: Rice University. Web. 20 Nov. 2009.  
<http://math.rice.edu/~friedl/papers/AAELLIPTIC.PDF>
- More cases to check. e.g.  $P +_E 2Q = (P +_E Q) +_E Q$



## Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

## Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

## Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

## The sum of points

## Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## 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  $C_2 \oplus C_2$ .

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



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves  $/\mathbb{F}_2$   
Elliptic curves  $/\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## 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	$y^2 = x^3 - x$	$\{\infty, (0, 1), (0, 2), (0, 0)\}$	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:

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

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



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves  $/\mathbb{F}_2$   
Elliptic curves  $/\mathbb{F}_3$

#### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$

Structure of  $E(\mathbb{F}_3)$

Further Examples

## EXAMPLE: Elliptic curves over $\mathbb{F}_5$ and $\mathbb{F}_4$

$\forall E/\mathbb{F}_5$  (12 elliptic curves),  $\#E(\mathbb{F}_5) \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ .

$\forall n, 2 \leq n \leq 10 \exists! E/\mathbb{F}_5 : \#E(\mathbb{F}_5) = n$  with the exceptions:

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

- $E_1 : y^2 = x^3 + 1$  and  $E_2 : y^2 = x^3 + 2$  both order 6

$$\begin{cases} x \leftarrow 2x \\ y \leftarrow \sqrt{3}y \end{cases}$$

$E_1$  and  $E_2$  affinely equivalent  
over  $\mathbb{F}_5[\sqrt{3}] = \mathbb{F}_{25}$  (*twists*)

- $E_3 : y^2 = x^3 + x$  and  $E_4 : y^2 = x^3 + x + 2$  order 4

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

- $E_5 : y^2 = x^3 + 4x$  and  $E_6 : y^2 = x^3 + 4x + 1$  both order 8

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

- $E_7 : y^2 = x^3 + x + 1$  order 9 and  $E_7(\mathbb{F}_5) \cong C_9$

**Exercise:** Classify all elliptic curves over  $\mathbb{F}_4 = \mathbb{F}_2[\xi], \xi^2 = \xi + 1$



#### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

#### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

#### Point at infinity of $E$










Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

#### The sum of points

#### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$   
Further Examples

## 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.



### Introduction

History  
length of ellipses  
why Elliptic curves?  
Fields

### Weierstraß Equations

Singular points  
The Discriminant  
Elliptic curves /  $\mathbb{F}_2$   
Elliptic curves /  $\mathbb{F}_3$

### Point at infinity of $E$

Projective Plane  
Homogeneous Polynomials  
Points at infinity  
Homogeneous Coordinates

### The sum of points

### Examples

Structure of  $E(\mathbb{F}_2)$   
Structure of  $E(\mathbb{F}_3)$

### Further Examples