$X^n + Y^n = Z^n$

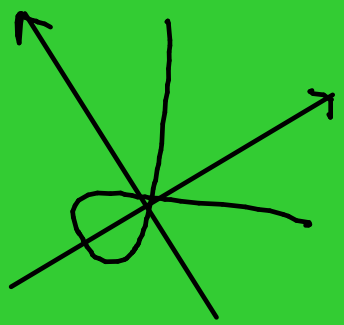
$\mathbb{F}_q \subseteq \overline{\mathbb{F}}_q$

A singular trip through the world of

ALGEBRAIC CURVES

over

FINITE FIELDS



$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right)$$

ANNAMARIA IEZZI

Dep. of Mathematics & Statistics

USF

$$\#X(\mathbb{F}_q) \leq q+1+g\lfloor 2\sqrt{q} \rfloor$$

Problem: Prove that $\sqrt{2}$ is an irrational number, that is $\sqrt{2}$ cannot be written as $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $y \neq 0$.

Traditional proof: Suppose $\sqrt{2}$ is rational, i.e. there exist $x, y \in \mathbb{Z}$ and $y \neq 0$ such that:

$$\sqrt{2} = \frac{x}{y}$$
$$\Downarrow$$
$$2 = \frac{x^2}{y^2}$$
$$\Downarrow$$
$$2y^2 = x^2$$

Use Fundamental Theorem of Arithmetic for getting a contradiction.

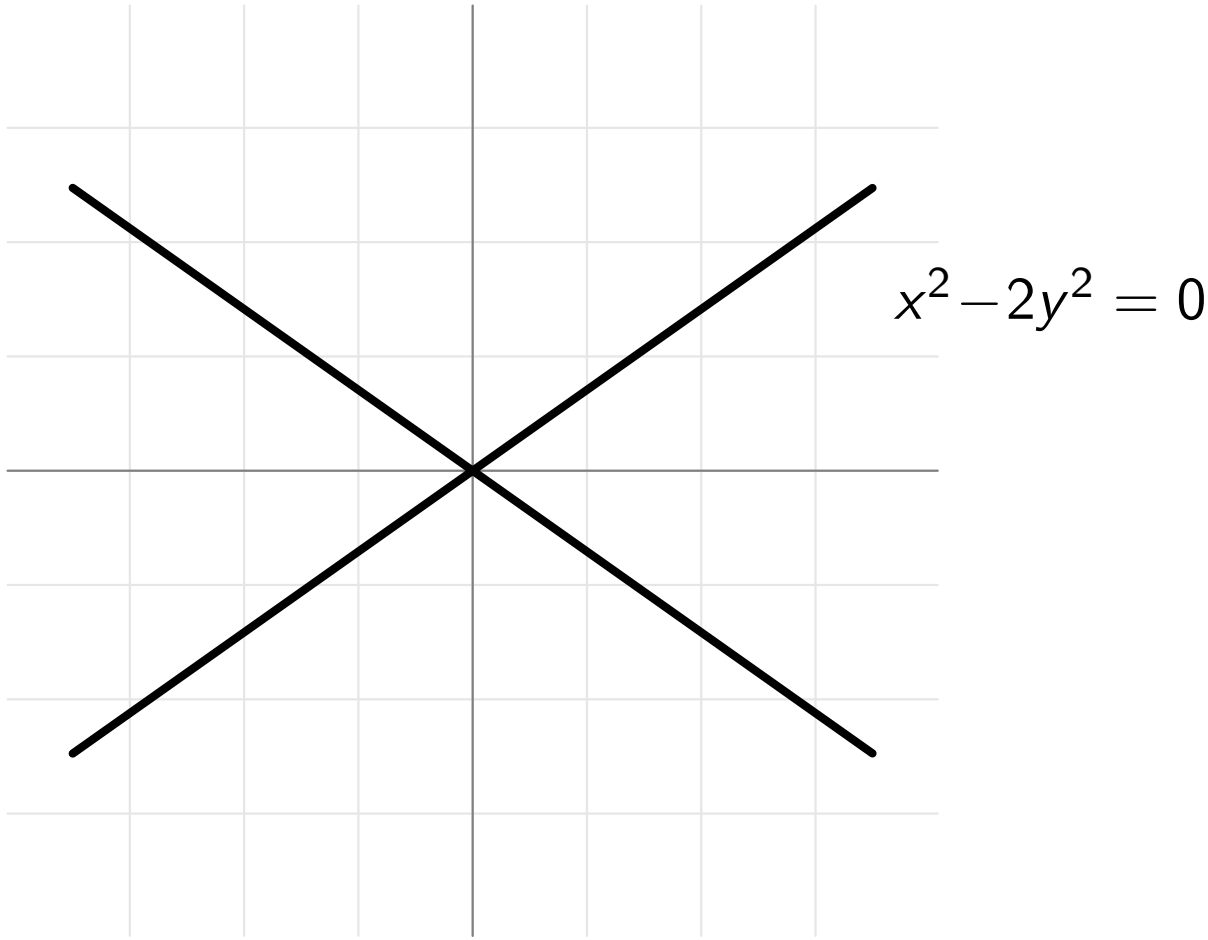
Problem: Prove that $\sqrt{2}$ is an irrational number, that is $\sqrt{2}$ cannot be written as $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $y \neq 0$.

"Diophantus's proof": Suppose $\sqrt{2}$ is rational, i.e. there exist $x, y \in \mathbb{Z}$ and $y \neq 0$ such that:

$$\sqrt{2} = \frac{x}{y}$$
$$\Downarrow$$
$$2 = \frac{x^2}{y^2}$$
$$\Downarrow$$
$$2y^2 = x^2 \quad \Rightarrow x^2 - 2y^2 = 0$$

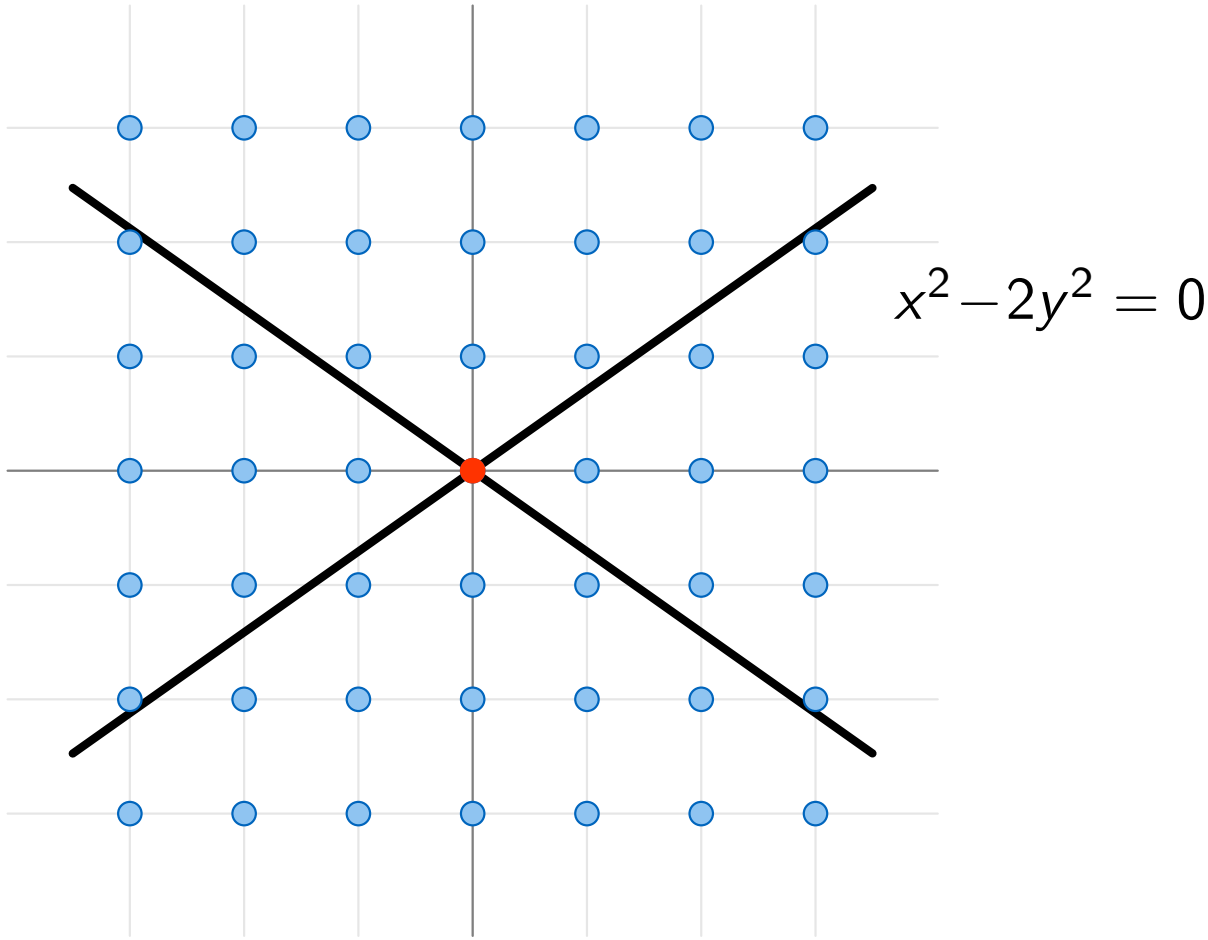
Equivalent problem: Prove that the polynomial equation $x^2 - 2y^2 = 0$ has no integral solution (x, y), except $(0, 0)$.

Geometrically, $x^2 - 2y^2 = 0$ is the equation of a curve $\mathcal{C}$ in the plane.



Now, $\sqrt{2}$ is irrational if and only if the curve $\mathcal{C}$ has no points (x, y) with integral coordinates, a part $(0, 0)$.

Geometrically, $x^2 - 2y^2 = 0$ is the equation of a curve $\mathcal{C}$ in the plane.



Now, $\sqrt{2}$ is irrational if and only if the curve $\mathcal{C}$ has no points (x, y) with integral coordinates, a part $(0, 0)$.

$\sqrt{2}$ is irrational

$\Updownarrow$

The polynomial equation

$$x^2 - 2y^2 = 0$$

has no integral solution (x, y), except $(0, 0)$.

$\Uparrow$ homogeneous equation

There exist a prime number p such that the reduced equation mod p

$$x^2 + (p-2)y^2 = 0$$

has no solution (x, y) with $x, y \in \mathbb{Z}_p = \{0, \ldots, p-1\}$, except $(0, 0)$.

$\sqrt{2}$ is irrational

$\Updownarrow$

The curve defined by the equation

$$x^2 - 2y^2 = 0$$

has only one point with coordinates in $\mathbb{Z}$, given by $P(0,0)$.

$\Uparrow$

There exist a prime number p such that the reduced curve mod p defined by the equation

$$x^2 + (p-2)y^2 = 0$$

has only one point with coordinates in $\mathbb{Z}_p = \{0, \ldots, p-1\}$, given by $P(0,0)$.

For instance the reduced curve $\mathcal{C}_3$ mod 3 is defined by the equation:

$$\mathcal{C}_3 : x^2 + y^2 = 0.$$

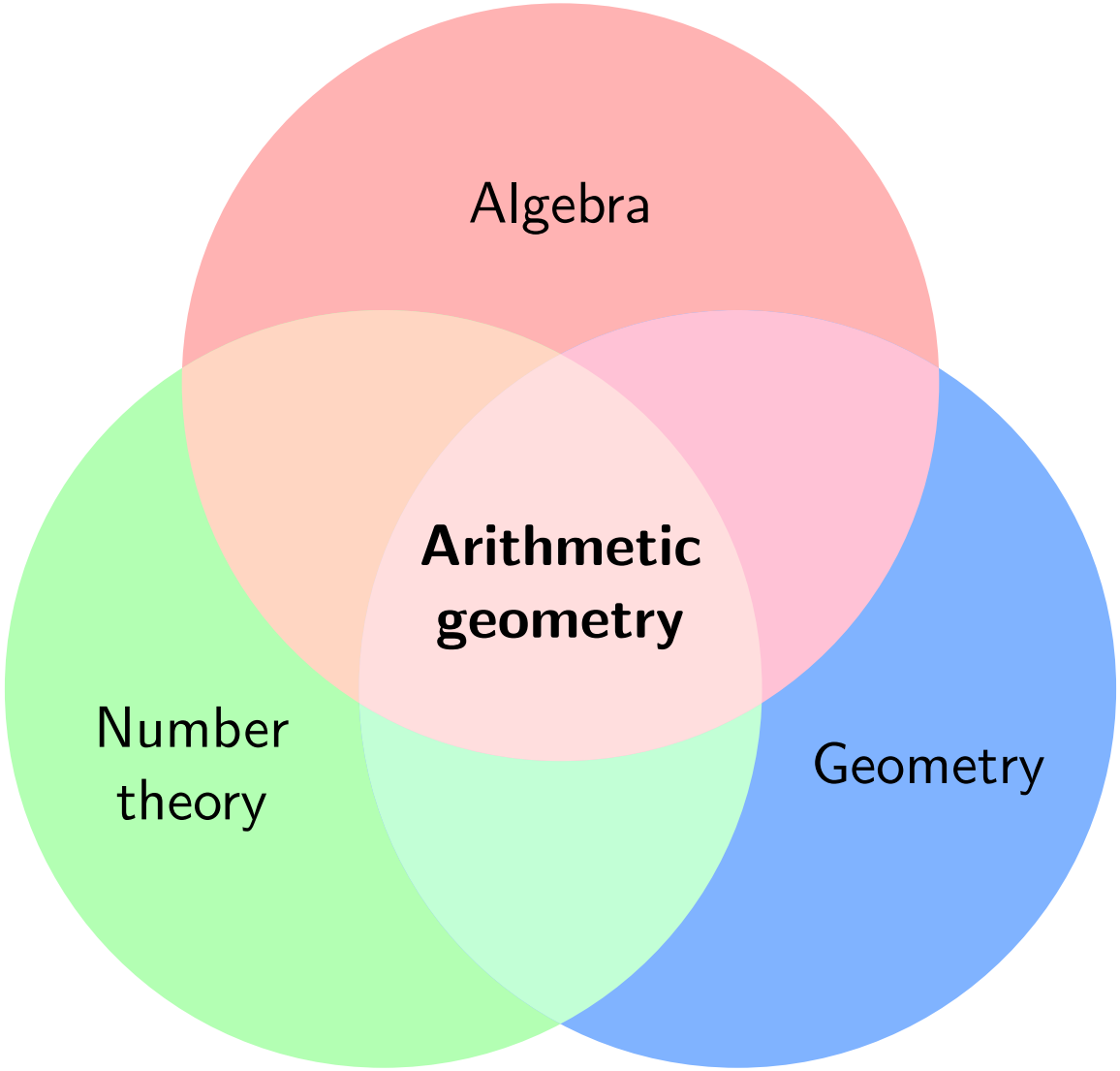
Question: Among the finite set

$$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\},$$

is $P(0,0)$ the only point whose coordinates verify the equation

$$x^2 + y^2 = 0 \mod 3?$$

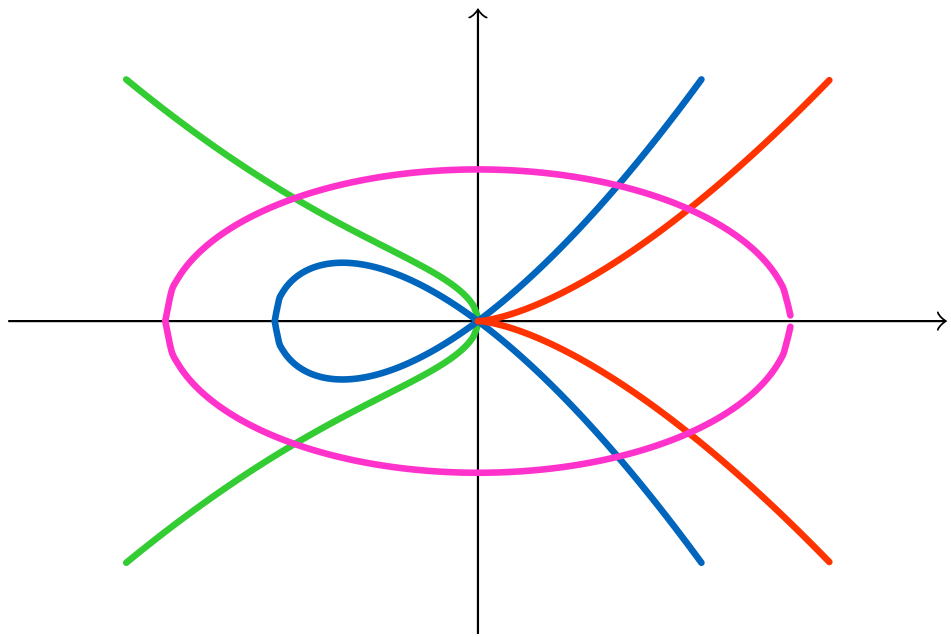
Yes, and this proves that $\sqrt{2}$ is an irrational number!


Algebra
Arithmetic geometry
Number theory
Geometry

Let's keep it simple!

It would be too much ambitious to describe the theory of algebraic curves (over finite fields) in the more general case in less than one hour.

We will give an overview of the fundamental concepts in the particular case of *plane curves*.



Affine/projective curves over $\mathbb{F}_q$

$\mathbb{F}_q$: *finite field* with q elements (q power of a prime number p)

$\overline{\mathbb{F}}_q$: algebraic closure of $\mathbb{F}_q$.

A *plane* **affine** *algebraic curve defined over* $\mathbb{F}_q$ is the geometric object

$$\mathcal{C} \subset \mathbb{A}^2(\overline{\mathbb{F}}_q) = \{(x, y) : x, y \in \overline{\mathbb{F}}_q\}$$

corresponding to the set of points whose coordinates are zeros of a polynomial in two variables with coefficients in $\mathbb{F}_q$:

$$\mathcal{C} : f(x, y) = 0, \quad f(x, y) \in \mathbb{F}_q[x, y].$$

We call *degree* of $\mathcal{C}$ the degree of $f(x, y)$.

Affine/projective curves over $\mathbb{F}_q$

$\mathbb{F}_q$: *finite field* with q elements (q power of a prime number p)

$\overline{\mathbb{F}}_q$: algebraic closure of $\mathbb{F}_q$.

A *plane* **projective** *algebraic curve defined* over $\mathbb{F}_q$ is the geometric object

$$\mathcal{C} \subset \mathbb{P}^2(\overline{\mathbb{F}}_q)$$

corresponding to the set of points whose coordinates are zeros of a *homogeneous* polynomial in three variables with coefficients in $\mathbb{F}_q$:

$$\mathcal{C} : F(X, Y, Z) = 0, \quad F \text{ homogeneous in } \mathbb{F}_q[X, Y, Z].$$

Example

- The equation
$$y^2 = x^3 + x$$
corresponds to a plane affine algebraic curve $\mathcal{C}$ defined over $\mathbb{F}_q$.

$$\text{homogenization}\downarrow \quad \uparrow\text{dehomogenization}$$

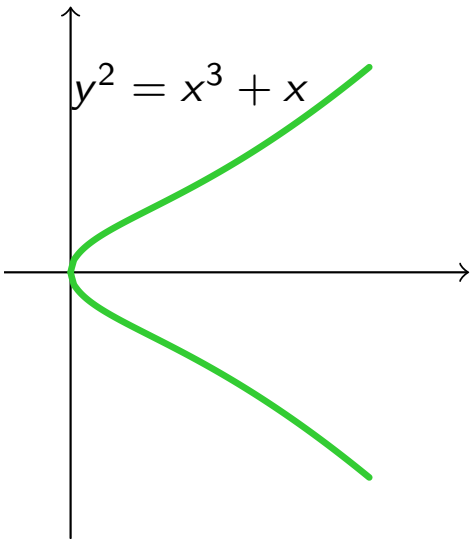
- The equation
$$Y^2Z = X^3 + XZ^2$$
corresponds to a plane projective algebraic curve $\overline{\mathcal{C}}$ defined over $\mathbb{F}_q$, which is the projective closure of $\mathcal{C}$ (note that the polynomial $Y^2Z = X^3 + XZ^2$ is the homogenization of $y^2 = x^3 + x$).

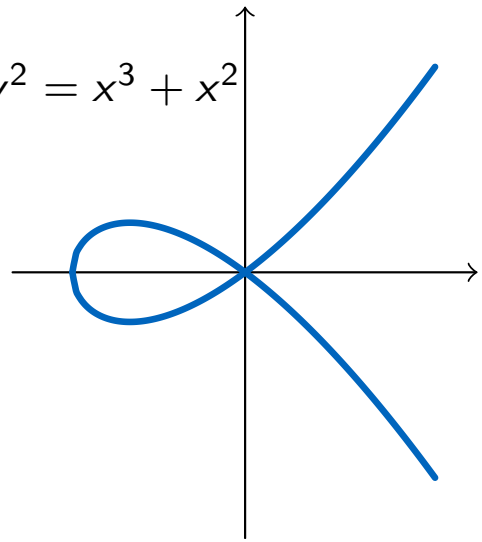
Irreducible curves over $\mathbb{F}_q$

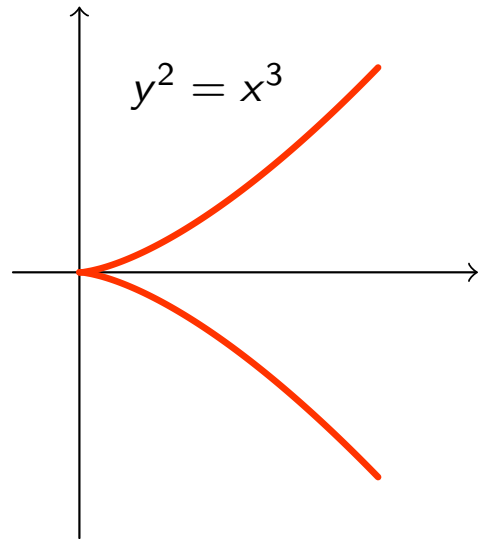
- A curve $\mathcal{C} : f(x, y) = 0$ is *irreducible* over $\mathbb{F}_q$ if the polynomial $f(x, y)$ is irreducible over $\mathbb{F}_q$.
- A curve $\mathcal{C} : f(x, y) = 0$ is *absolutely irreducible* over $\overline{\mathbb{F}}_q$ if the polynomial $f(x, y)$ is irreducible over $\overline{\mathbb{F}}_q$.

Example: The curve $x^2 + y^2 = 0$ is irreducible over $\mathbb{F}_3$ but it is not absolutely irreducible over $\overline{\mathbb{F}}_3$, because it is reducible over $\mathbb{F}_{3^2}$.

Smooth/singular curves and invariants







Invariants

- g: geometric genus (complexity of the curve)
  $g = 0$: projective line , $g = 1$: elliptic curve, etc.
- π: arithmetic genus $= g +$ (degree of singularity of the curve)

Note: $g \leq \pi$ and $g = \pi$ if and only if the curve is smooth.

Rational points

Let $\mathcal{C} : F(X, Y, Z) = 0$ be a plane projective algebraic curve defined over $\mathbb{F}_q$. A *rational point* (over $\mathbb{F}_q$) on $\mathcal{C}$ is a point $(x_0 : y_0 : z_0) \in \mathbb{P}^2(\mathbb{F}_q)$ such that $F(x_0, y_0, z_0) = 0$.

Interest: a curve defined over a finite field has always a **finite** number of rational points.

Indeed

$$\sharp\mathcal{C}(\mathbb{F}_q) \leq \sharp\mathbb{P}^2(\mathbb{F}_q) = \frac{q^3 - 1}{q - 1} = q^2 + q + 1.$$

$\Rightarrow$ Applications to information theory:

- cryptography: elliptic-curve cryptography, etc.
- coding theory: error-correcting codes (Goppa codes), etc.

From now on...

Let X be a curve defined over a finite field $\mathbb{F}_q$:

- algebraic;
- projective;
- absolutely irreducible.

Notation

- q: cardinality of $\mathbb{F}_q$;
- $\sharp X(\mathbb{F}_q)$: number of rational points over $\mathbb{F}_q$;
- $\sharp X(\mathbb{F}_{q^n})$: number of points with coordinates in $\mathbb{F}_{q^n}$;
- g: geometric genus of X;
- π: arithmetic genus of X;
- $\tilde{X}$: normalization of X.

The zeta function, a tool for counting rational points

To study $\sharp X(\mathbb{F}_{q^n})$, we consider the *zeta function* of X:

$$Z_X(T) := \exp\left(\sum_{n=1}^{\infty} \sharp X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right),$$

which is the natural generalisation of the Riemann zeta function to curves over finite fields.

Example: the case of the projective line $\mathbb{P}^1$.

The Riemann Hypothesis for curves over finite field

Theorem (Weil, 1948)

If X is a smooth curve defined over $\mathbb{F}_q$ of genus g, then

$$Z_X(T) = \frac{P(T)}{(1-T)(1-qT)},$$

where

$$P(T) = \prod_{i=1}^{2g}(1-\omega_i T) \in \mathbb{Z}[T]$$

and $\omega_i \in \mathbb{C}$ are algebraic integers of absolute value $\sqrt{q}$.

The polynomial $P(T)$ contains a lot of information about the curve. In particular we have

$$\sharp X(\mathbb{F}_q) = q + 1 - \sum_{n=1}^{2g} \omega_i.$$

The smooth case

Theorem (Serre-Weil-Hasse bound)

If X is a smooth curve defined over $\mathbb{F}_q$ of genus g,

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}].$$

Let us denote by

$$N_q(g)$$

the maximum number of rational points on a smooth curve defined over $\mathbb{F}_q$ of genus g.

Clearly we have:

$$N_q(g) \leq q + 1 + g[2\sqrt{q}].$$

Furthermore $N_q(g)$ is explicit for $g = 0, 1, 2$.

The singular case

In 1996, Aubry and Perret found relations between a curve and its normalization.

Let X be a curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π, with normalization map $\nu : \tilde{X} \to X$. They proved that:

- $Z_X(T) = Z_{\tilde{X}}(T) \prod_{P \in \operatorname{Sing} X} \left(\frac{\prod_{Q \in \nu^{-1}(P)} (1 - T^{\deg Q})}{1 - T^{\deg P}} \right)$;
- $|\sharp \tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \pi - g$.

Theorem (Aubry-Perret bound)

If X is a curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π, then:

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}] + \pi - g.$$

The quantity $N_q(g, \pi)$

We introduce an analogous quantity of $N_q(g)$ for singular curves:

Definition

For q a power of a prime, g and π non negative integers such that $\pi \geq g$, let us define the quantity

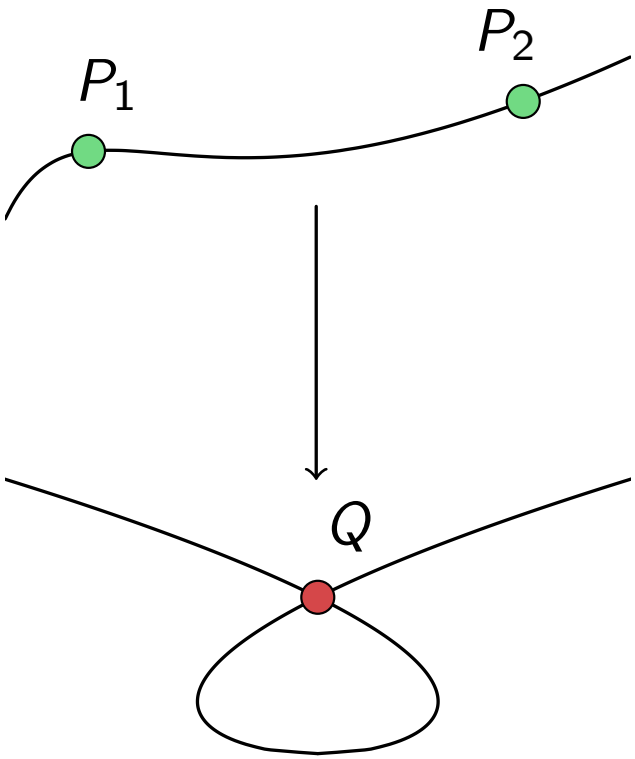
$$N_q(g, \pi)$$

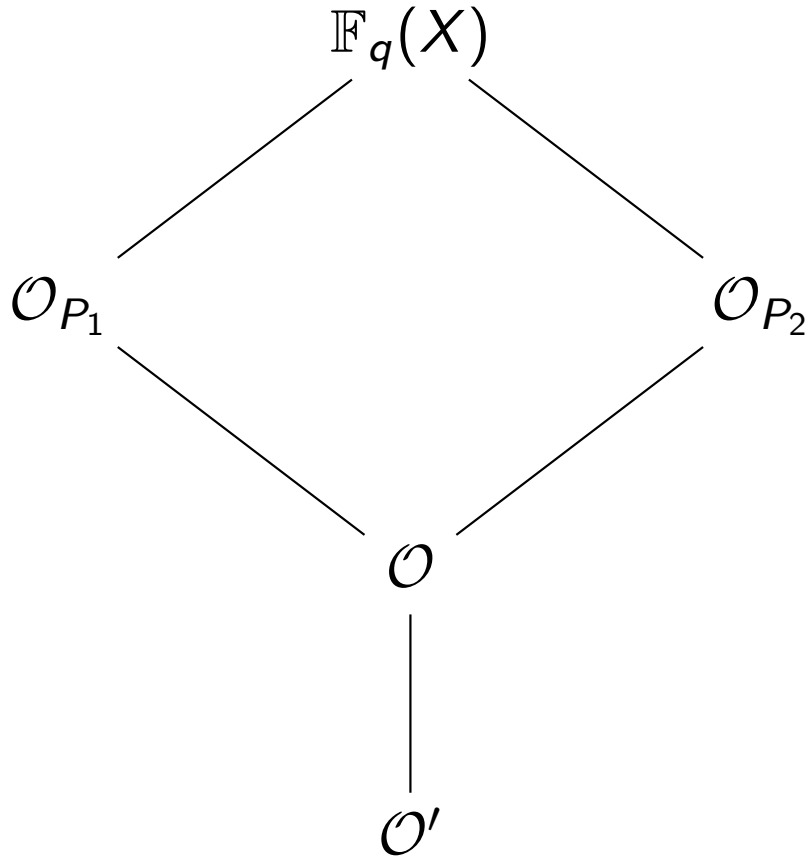
as the maximum number of rational points over $\mathbb{F}_q$ on a curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π.

Obviously we have:

- $N_q(g, g) = N_q(g)$,
- $N_q(g, \pi) \leq N_q(g) + \pi - g$.
- $N_q(g, \pi) \leq q + 1 + g[2\sqrt{q}] + \pi - g$,

How to determine $N_q(g, \pi)$?





Theorem

$$N_q(g,\pi) = N_q(g) + \pi - g \quad \Longleftrightarrow \quad g \leq \pi \leq g + \mathcal{B}_q(g),$$

where $\mathcal{B}_q(g)$ denotes the maximum number of points of degree 2 on a curve with $N_q(g)$ points.