Counting points on algebraic stacks

Milan Lopuhaä-Zwakenberg[1]

[1]Security group, Technische Universiteit Eindhoven

October 15, 2018

This talk

Let T be a type of mathematical object.

Question

How many objects of type T exists?

This talk:

- We count certain objects found in algebraic geometry;
- We solve this counting problem using algebraic geometry.

Algebraic geometry

- Geometry described by polynomials over a field k
- $k = \mathbb{R}, \mathbb{C} \Rightarrow$ 'easier' and more intuitive geometry
- k finite $\Rightarrow$ finite counting problems

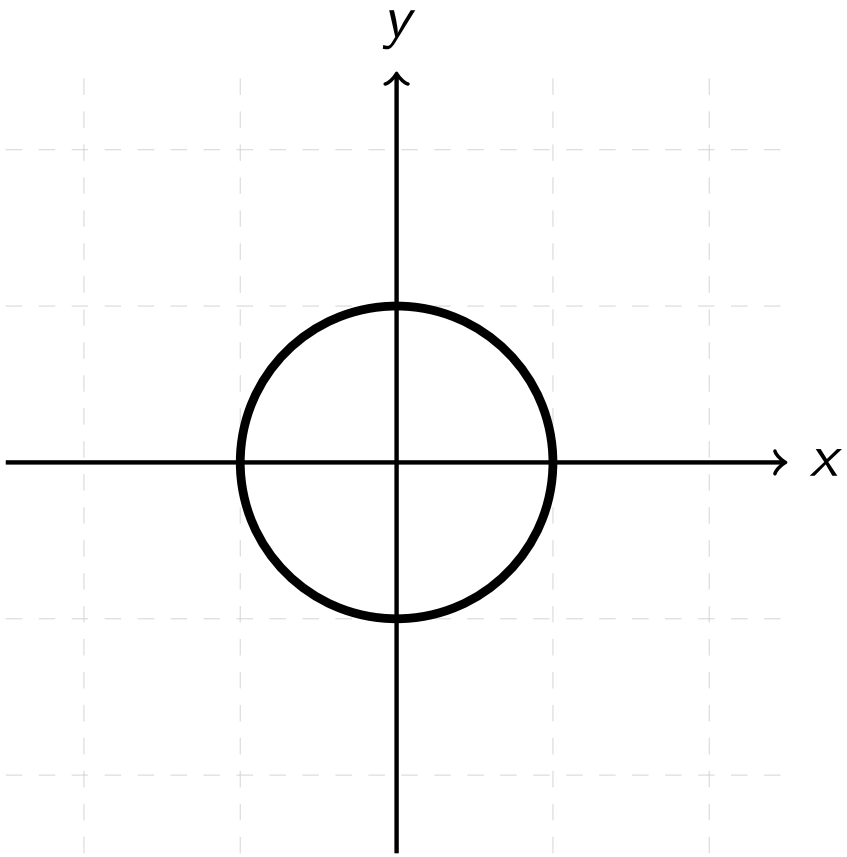
For now imagine $k = \mathbb{R}$, but pretend it is finite when needed!

What is algebraic geometry?

Let n and m be integers, and let $f_1, \ldots, f_m \in \mathbb{R}[X_1, \ldots, X_n]$ (i.e. polynomials with real coefficients). Then the *algebraic variety* V defined by $f_1, \ldots, f_m$ is

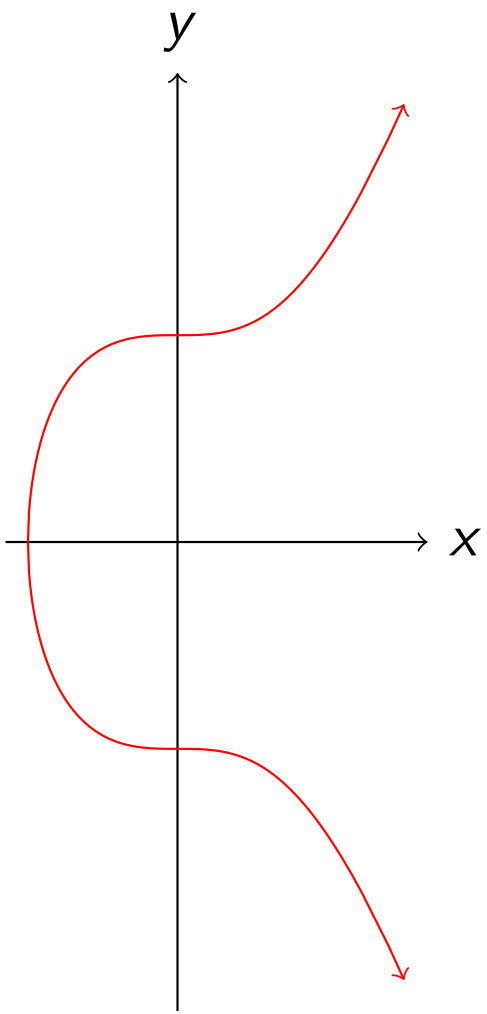
$$V = \left\{ \vec{v} = (v_1, \ldots, v_n) \in \mathbb{R}^n : f_1(\vec{v}) = \ldots = f_m(\vec{v}) = 0 \right\}.$$

Examples



$$X^2 + Y^2 - 1 = 0$$

Examples



$$Y^2 = X^3 + 7$$

Examples

- Circle: $X^2 + Y^2 - 1 = 0$.
- Elliptic curve: $Y^2 = X^3 + a \cdot X + b$.
- Line: $n = 1$, no equations.
- 2×2-matrices with determinant 1:

$$\left\{ \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} : X_1X_4 - X_2X_3 - 1 = 0 \right\}.$$

Remark

Many geometric properties of algebraic varieties (tangent spaces, intersections,...) can be expressed in polynomials, e.g. algebraically!

Set of elliptic curves

Question

What does the set of all real elliptic curves (conics, abelian varieties,...) look like?

- Every elliptic curve is of the form $Y^2 = X^3 + aX + b$, so

$$\{\text{Ell. curves}\} = \left\{(a,b) \in \mathbb{R}^2 : 4a^3 + 27b^2 \neq 0\right\}?$$

- NO! because some pairs give the same curve:

$$\begin{array}{ccc} \{(x,y) : y^2 = x^3 + 16x + 64\} & \xrightarrow{\sim} & \{(x',y') : y'^2 = x'^3 + x' + 1\} \\ (x,y) & \mapsto & (4x', 8y') \end{array}$$

Problem

Determining the set of elliptic curves (or other objects) is difficult.

Counting elliptic curves over finite fields

Now $k =$ finite. Let $\mathrm{Ell}(k)$ be the set of elliptic curves over k; this is a finite set. Its *point count* $\#\mathrm{Ell}(k)$ is

$$\sum_{E \in \mathrm{Ell}(k)} \frac{1}{\#\mathrm{Aut}(E)}.$$

Weights because of relation between point counts and geometry:
The 'function'

$$\mathrm{Ell}\colon \{\mathrm{Fields}\} \to \{\mathrm{Sets}\}$$

is an *algebraic stack*. It is itself a geometrical object!

Main result

Theorem (MLZ 2018)

Let C *be an algebraic stack. Suppose* C *is a* quotient stack $[G\backslash X]$. *If* G *and* X *are sufficiently nice, then we can explicitely find a function* P *such that* $\#\mathsf{C}(k) = P(\#k)$ *for all finite fields* k.

Remark

- Many stacks are quotient stacks, e.g. stacks of elliptic curves, abelian varieties, curves...
- Main examples of sufficiently nice quotient stacks:
  - torsion groups of abelian varieties
  - quotients under unipotent groups

To do:

- What is a quotient stack?
- What is 'sufficiently nice'?

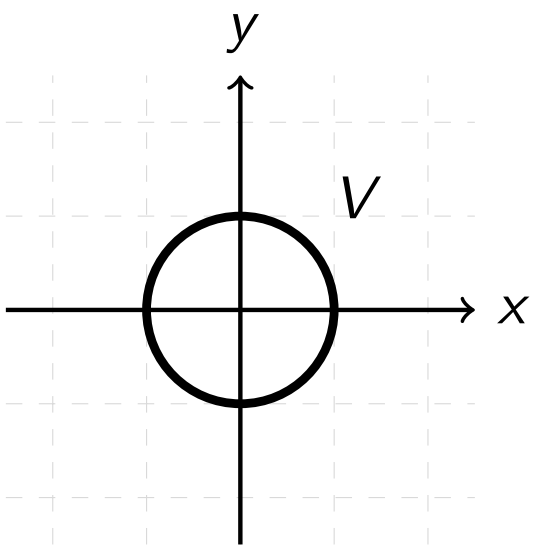
Intermezzo: twists

Let $V = \left\{ \vec{x} \in \mathbb{R}^n : f_1 \vec{x}) = \ldots = f_m(\vec{x}) = 0 \right\}$; then

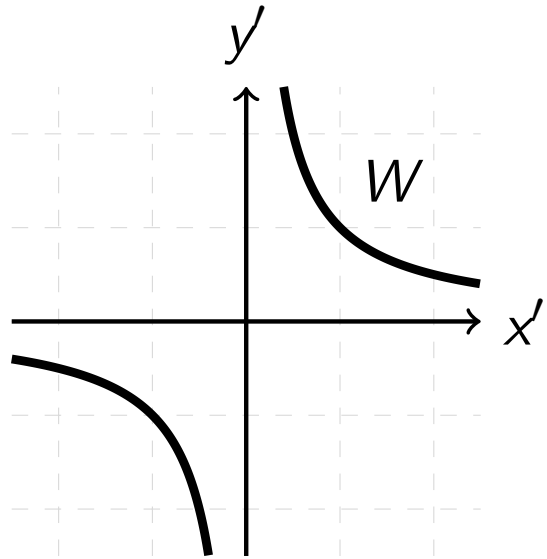
$$V_{\mathbb{C}} = \left\{ \vec{x} \in \mathbb{C}^n : f_1 \vec{x}) = \ldots = f_m(\vec{x}) = 0 \right\}.$$

Problem: sometimes $V_{\mathbb{C}}$ and $W_{\mathbb{C}}$ are isomorphic while V and W are not.

Intermezzo: twists



$$X^2 + Y^2 = 1$$



$$X'Y' = 1$$

These are not isomorphic, but the complex varieties $V_{\mathbb{C}}$ and $W_{\mathbb{C}}$ are:

$$\begin{array}{ccc} V_{\mathbb{C}} & \xrightarrow{\sim} & W_{\mathbb{C}} \\ (X, Y) & \mapsto & (X + iY, X - iY) \end{array}$$

W is called a *twist* of V.

Intermezzo: twists

Let $V = \left\{\vec{x} \in \mathbb{R}^n : f_1\vec{x}) = \ldots = f_m(\vec{x}) = 0\right\}$. Then we have a map

$$\begin{array}{rcl} \sigma\colon V_{\mathbb{C}} & \to & V_{\mathbb{C}} \\ (v_1, \ldots, v_n) & \mapsto & (\bar{v}_1, \ldots, \bar{v}_n) \end{array}$$

and $V = V_{\mathbb{C}}^{\sigma} := \{\vec{v} : \sigma(\vec{v}) = \vec{v}\}$. We can make twists of V as follows:

- Take $z\colon V_{\mathbb{C}} \xrightarrow{\sim} V_{\mathbb{C}}$;
- Let σ_z be the composition $V_{\mathbb{C}} \xrightarrow{z} V_{\mathbb{C}} \xrightarrow{\sigma} V_{\mathbb{C}}$;
- Define $V_z := V_{\mathbb{C}}^{\sigma_z}$.

Many $z \in \mathrm{Aut}(V)$ give the same V_z; the set of twists is $\mathrm{H}^1(\mathbb{R}, \mathrm{Aut}(V))$.

Quotient stacks

Let X be a real algebraic variety. Let G be (a subgroup of) $\mathrm{Aut}(X)$ that is itself an algebraic variety. Examples:

- $X = \mathbb{R}^n$, $G = \mathrm{GL}_n(\mathbb{R})$.
- $X = \mathbb{R}$, $G = \mathbb{R}$ (translations).
- $X =$circle, $G = \{\pm \mathrm{id}\}$.

Then the stack $[G\backslash X]\colon \{\mathrm{fields}\} \to \{\mathrm{sets}\}$ is defined as follows. We take $[G\backslash X](\mathbb{C})$:

- Objects: G-orbits in X (i.e. $x \cong x'$ if $x = g(x')$ for some $g \in G$);
- Automorphisms: $\mathrm{Aut}(x) = \{g \in G : g(x) = x\}$.

And we take $[G\backslash X](\mathbb{R}) = \{V : V_{\mathbb{C}} \in [G\backslash X](\mathbb{C})\}$.

Counting points on quotient stacks

Theorem (MLZ 2018)

Let $[G\backslash X]$ be a quotient stack, and let k be a finite field. Then

$$\#[G\backslash X](k) = \sum_{z \in \mathrm{H}^1(k,G)} \frac{\#X_z(k)}{\#G_z(k)}.$$

Problems:

- $\#X(k)$ might be difficult to determine;
- $\mathrm{H}^1(k, G)$ might be difficult to determine;
- $\#X_z(k), \#G_z(k)$ will change if we change z;
- All of these depend on k.

“Sufficiently nice”

Problems:

- $\#X(k)$ might be difficult to determine;
- $\mathrm{H}^1(k, G)$ might be difficult to determine;
- $\#X_z(k), \#G_z(k)$ will change if we change z;
- All of these depend on k.

Solutions:

- Choose X such that computing $\#X(k)$ is easy (e.g. $X = k^n$);
- Choose G such that X_z does not depend on z.
- Choose G such that $\#G(k)$ is easy (e.g. $\#\mathrm{GL}_2(k) = (k^2 - 1)(k^2 - k)$).

"Sufficiently nice"

Theorem (Lang 1956, Serre 1963)

Let G be an algebraic group and let k be a finite field.

- *If G is finite, then $\sum_{z \in \mathrm{H}^1(k,G)} \frac{1}{\#G_z(k)} = 1$.*
- *Let $\pi(G)$ be the finite set of connected components of G. Then $\mathrm{H}^1(k, G) = \mathrm{H}^1(k, \pi(G))$.*

Corollary

Let G^0 be the component of G containing id. *Suppose G_z^0 does not depend on $z \in \mathrm{H}^1(k, G)$. Then*

$$\sum_{z \in \mathrm{H}^1(k,G)} \frac{1}{\#G_z(k)} = \sum_{z \in \mathrm{H}^1(k,G)} \frac{1}{\#\pi(G_z)(k) \cdot \#G_z^0(k)} = \frac{1}{\#G^0(k)}.$$

Counting points

Corollary

If G_z^0 does not depend on $z \in \mathrm{H}^1(k, G)$, then

$$\sum_{z \in \mathrm{H}^1(k,G)} \frac{1}{\#G_z(k)} = \sum_{z \in \mathrm{H}^1(k,G)} \frac{1}{\#\pi(G_z)(k) \cdot \#G_z^0(k)} = \frac{1}{\#G^0(k)}.$$

Theorem

Suppose G_z^0 and X_z do not depend on z. Then

$$[G\backslash X](k) = \sum_{z \in \mathrm{H}^1(k,G)} \frac{\#X_z(k)}{\#G_z(k)} = \frac{\#X(k)}{\#G^0(k)}.$$

Examples where this is true:

- $X = k^n$;
- G^0 unipotent (e.g. k^n), or $G = \Gamma \times G^0$ with Γ finite.

Application: Torsion groups on elliptic curves

Let p be a prime number. Let k be a finite field of characteristic p (i.e. $\#k = p^m$). Let E be an elliptic curve over k.

Fact

Let E be an elliptic curve over k.

- There is a natural addition law, written $+$, on E, and a $0 \in E$ such that $0 + x = x$.
- $E[p] := \left\{ x \in E : \underbrace{x + \ldots + x}_{p \text{ times}} = 0 \right\}$ is an algebraic variety.

Torsion groups on elliptic curves

- $E[p]$ is an important characteristic of E (ordinary vs supersingular)
- Can be generalised to *abelian varieties* ('multidimensional elliptic curves').
- $\mathrm{BT}^d = \{A[p] : A \text{ } d\text{-dim. abelian variety}\}$ is a stack.

Counting torsion groups

Question

What is $\#\mathrm{BT}^d(k)$?

Answer

By expressing BT^d as a sufficiently nice quotient stack, we can calculate $\#\mathrm{BT}^d(k)$ as a polynomial in $\#k$.

Remark

Loads of room for generalisations! (e.g. p^n-torsion, given endomorphism group, flags,...)