CS688: Computational Arithmetic-Geometry

- Algebraic-geometry studies <u>algebraic equations</u> (like $y^2 = x^3$) from a <u>geometric perspective</u>. That means studying properties that one can visualize.

- Arithmetic-geometry studies the <u>counting qns.</u> Eg. how many points are there on $y^2 = x^3 \pmod{p}$?

- In this course we will also be interested in the <u>algorithmic</u> aspects.

- <u>Problem</u>: Given polys. $f_1, \ldots, f_m \in \mathbb{F}_p[x_1, \ldots, x_n]$. Check whether $\exists$ point $P \in \mathbb{F}_p^n$ s.t. $f_1(P) = \cdots = f_m(P) = 0$.
- How hard is this qn.?

- <u>Exercise</u>: This is NP-hard. (Even, when f_i's are quadratic & $p=2$.)

- So, efficient algos are unlikely here. However, this course is about curves, e.g. $n=2$, over finite fields. Much of modern maths arose from these objects!

- The first part of the course is solely about AG fundamentals. Once we have the necessary tools, we'll do CS applications.

- <u>Fundamentals</u>: • We'll study curves in the <u>modern</u> language of AG, i.e. varieties, morphisms, function fields etc. The guiding intuition here is that <u>geometric properties of a curve</u> are manifested in the <u>functions over it</u>.

- So, to study the roots of $y^2 = x^3$, we shall study the ring $\mathbb{F}[x,y]/\langle y^2 - x^3 \rangle$.
  - A highlight will be the <u>Riemann-Roch theorem</u> that defines/explains the <u>genus</u> of a curve (in <u>any</u> field).

  - Further, & more importantly, we'll prove an estimate for the #points on a curve over a finite field. (Called the <u>Riemann hypothesis for curves</u>!)

- <u>Applications</u>: Too many to cover:
  - Algos to count points on curves
  - integer factoring algos
  - computing $\sqrt[r]{1}$ in finite fields
  - cryptosystems
  - coding theory ...

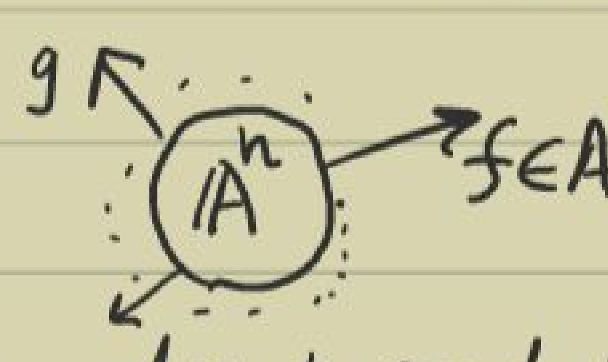
<u>Textbook</u>: Carlos Moreno (Algebraic curves over finite fields). <+ a number of online material>

Affine Varieties

- Let k be a field.
- Affine n-space over k is the set $\mathbb{A}^n_k := k^n$.
- If $P \in \mathbb{A}^n$ & $P = (a_1, \dots, a_n)$, then the $a_i \in k$ are coordinates of P.
- The polynomial ring $A := k[x_1, \dots, x_n]$.

▷ These two are related as: Any $f \in A$ defines a fn. $f : \mathbb{A}^n \to k$
$$P \mapsto f(P)$$

$\boxed{\text{Viewpoint:}}$



(f associates a value to each point in the space)

- The zeros of f, $Z(f) := \{P \in \mathbb{A}^n \mid f(P) = 0\}$.
- Generally, for $T \subseteq A$,
$$Z(T) := \{P \in \mathbb{A}^n \mid \forall f \in T,\ f(P) = 0\}.$$

- Eg. $Z(x_1^2, x_1+x_2) = \{(0,0)\}$ while
  $Z(x_1^2) = \{(0,t) \mid t \in k\}$.

- A subset $Y \subset \mathbb{A}^n$ is called <u>algebraic</u> (or <u>closed</u>) if $\exists T \subset A$ s.t. $Y = Z(T)$.

- Eg. $\mathbb{C}$ is trivially algebraic in $\mathbb{A}^1_{\mathbb{C}}$, but $\mathbb{C} \setminus \{0\}$ is <u>not</u> algebraic.

- For $Y \subseteq \mathbb{A}^n$ define an ideal
  <u>$I(Y)$</u> $:= \{ f \in A \mid \forall P \in Y, f(P) = 0 \}$.

- Now we have the associations:

$$
\begin{array}{rcl}
 & \mathbb{A}^n_k & & A \\
 & Y & \longrightarrow & I(Y) \leftarrow \text{ideal} \\
\text{algebraic} \rightarrow & Z(T) & \longleftarrow & T
\end{array}
$$

- Could we make these associations well-behaved, i.e. 1–1 ?

- For a closed set $Y \subset \mathbb{A}^n$ call the complement $\mathbb{A}^n \setminus Y$ <u>open</u>.
- It's easily seen that:

- <u>Proposition 1</u>: (a) ϕ & $\mathbb{A}^n$ are open.
  (b) If $\{Y_i\}_i$ are open, then $\bigcup_i Y_i$ is open.
  (c) If $\{Y_i\}_i$ are finitely many open subsets, then $\bigcap_i Y_i$ is open.

- Because of these properties we have the following geometry-inspired definition:

- <u>Defn</u>: The family of open subsets of $\mathbb{A}^n$ is called the <u>Zariski topology of $\mathbb{A}^n$</u>.

- If $Y \subseteq \mathbb{A}^n$ splits into two <u>proper</u> <u>closed</u> subsets, then we can (in a sense) reduce the study of Y to its parts. So,

- A $Y \subseteq \mathbb{A}^n$ is <u>irreducible</u> if $\nexists$ proper closed Y_1, Y_2 s.t. $Y = Y_1 \cup Y_2$.
  (Convention: $\underline{\phi}$ is reducible.)

- Eg. $\mathbb{A}^1_{\mathbb{C}}$ is irreducible.
  ($\because$ $\mathbb{A}^1_{\mathbb{C}} = Y_1 \cup Y_2 \Rightarrow$ some Y_i is infinite $\Rightarrow Y_i$ is not closed.)

- <u>Defn</u>: • An irreducible closed subset of $\mathbb{A}^n$ is called an <u>affine variety</u> (AV).
  • An AVs open subset is called a <u>quasi-affine variety</u>.

- Eg. • $Z(x_1^2)$ is an AV, but $Z(x_1 x_2)$ is not an AV (though closed).
  • $Z(x_1^2) \setminus Z(x_1^2, x_2)$ is quasi-affine.