Elliptic Curves and Arithmetic Geometry. (MWF 1:10 – 2:00
Math 785. LC 310)

The topic is: Finding rational points on varieties.

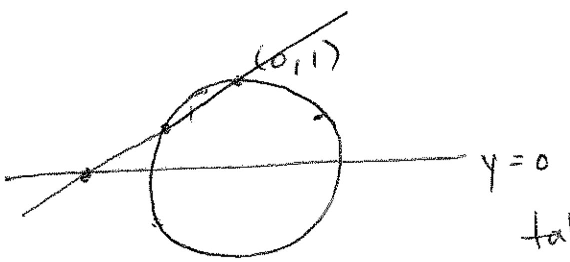
Example. A Pythagorean triple is a set $(x, y, z) \in \mathbb{Z}^3$ with $x^2 + y^2 = z^2$.

Can you find all? $(3, 4, 5), (5, 12, 13), \dots$

It is enough to find rational solutions (in bij. w/ primitive solutions) to $x^2 + y^2 = 1$.

So, if $V = V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$, find $V(\mathbb{Q})$.

We can write down all the solutions:



Consider the map

$\mathbb{A}^1 = \{y = 0\} \xrightarrow{\phi} V \setminus \{(0,1)\}$

Connect $(x, 0)$ with $(0,1)$ and take the point of intersection.

ϕ is "obviously" a bijection.
It is injective because two points determine a line.
It is surjective because every line between $(0,1)$ and another point on V goes through the line.

Indeed, get a bijection $\mathbb{A}^1(K) \longleftrightarrow V(K) - \{(0,1)\}$ for any subfield $K \subseteq \mathbb{R}$. (In fact any field K. Maybe you need char $K \neq 2$.)

If $z_1 \in \mathbb{A}^1 \longleftrightarrow z_2 \in V - \{(0,1)\}$ then TFAE.

(1) $z_1 \in \mathbb{A}^1(K)$
(2) $z_2 \in V(K)$
(3) The slope of the line is in K.

Here (1) → (3), (2) → (3), (3) → (1) all obvious.

Why (3) → (2)?

Solve $x^2 + y^2 = 1$

$y = mx + 1$

$x^2 + (mx+1)^2 = 1$

A quadratic equ with one solution over K.

So the other must be defined over K also.

Let's write down ϕ and its inverse.

Starting with $z \in \mathbb{A}^1$, $m = \frac{-1}{z}$.

$$x^2 + \left(1 - \frac{x}{z}\right)^2 = 1$$

$$x^2 - \frac{2x}{z} + \frac{x^2}{z^2} = 0 \qquad x^2\left(1 + \frac{1}{z^2}\right) - 2\frac{x}{z} = 0.$$

Don't want $x = 0$.

So: $x\left(1 + \frac{1}{z^2}\right) = \frac{2}{z}$

$$x\left(\frac{z^2+1}{z^2}\right) = \frac{2}{z}$$

$$x = \frac{2z}{z^2+1}$$

$$y = 1 - \frac{1}{z} \cdot \frac{2z}{z^2+1}$$

$$= \frac{z^2+1-2}{z^2+1} = \frac{z^2-1}{z^2+1}.$$

So ϕ is $z \longrightarrow \left(\frac{2z}{z^2+1}, \frac{z^2-1}{z^2+1}\right)$

a ~~morphism~~ ~~all~~ rational map.

The same is true also of ϕ^{-1}:

Given (x_0, y_0), slope is $\frac{1-y_0}{-x_0}$

so the intersection point is: $y = 0$
$$y = \frac{1-y_0}{-x_0} \cdot x + 1$$
$$\Rightarrow x = \frac{x_0}{1-y_0}.$$

So $\phi^{-1} : V \longrightarrow \mathbb{A}^1$ given by
$$(x_0, y_0) \longrightarrow \frac{x_0}{1-y_0}.$$

It is not defined at $(0,1)$ but it is everywhere else.

So: we've found all the rational points.

Exercises.

(1) This works identically for any K-rational point and any line not through it.

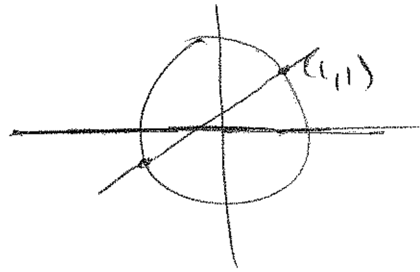
(2) In fact, if we write $\tilde{V} = V(x^2+y^2-z^2) \subseteq \mathbb{P}^2$,
$$\mathbb{P}^1(K) \longleftrightarrow \tilde{V}(K)$$
$$[x_0 : y_0] \longrightarrow [2x_0y_0 : x^2 - y^2 : x^2+y^2]$$
$$[x_0 : z_0 - y_0] \longleftarrow [x_0 : y_0 : z_0]$$
$$\shortparallel$$
$$[z_0 + y_0 : x_0],$$
we have an isomorphism $\mathbb{P}^1 \longrightarrow V$.

788/1.4.

What if we change it slightly?

Let $V = \{x^2 + y^2 = 2\}$.

Still okay!



$V = \{x^2 + y^2 = 3\}$

Still okay over $\mathbb{R}$, but $V(\mathbb{Q}) = \phi$.

Def. If $x \in \mathbb{Q}$ can be written as $x = p^n \cdot \frac{a}{b}$ for a prime p, with a, b coprime to $\mathbb{Q}$, we say $v_p(x) = n$

the p-adic valuation of x is n.

Also: $v_p(0) = \infty$ for all p.

Verify:

(1) $v_p(x \cdot y) = v_p(x) + v_p(y)$

(2) $v_p(x+y) = \min\{v_p(x), v_p(y)\}$ if $v_p(x) \neq v_p(y)$.

($\geq$ in general.)

Given (x,y) satisfying $x^2 + y^2 = 3$.

For $p = 3$:

Cannot have $v_p(x) \geq 1$ or $v_p(y) \geq 1$ by (2) above.

Indeed, must have $v_p(x) = v_p(y)$.

Clearing denominators, $x^2 + y^2 = a$, where $x, y \in \mathbb{Z}$ and:

$v_3(a) \geq 1$

$v_3(x) = v_3(y) = 0$.

Reduce it mod 3: $x^2 + y^2 \equiv 0 \pmod 3$

with $x, y \not\equiv 0 \pmod 3$.

No solutions! Issue is that -1 is not a quadratic residue.

How about $V = \{x^n + y^n = 1\}$.

<u>Theorem.</u> $V(\mathbb{Q}) = \{(0, \pm 1), (\pm 1, 0)\}$.

This is <u>Fermat's</u> <u>last</u> <u>theorem</u>, equivalent to:

$x^n + y^n = z^n$ has no integral solutions.

Proved by Wiles (w/ Taylor)

The trichotomy of <u>algebraic</u> <u>plane</u> <u>curves</u>.

<u>Genus 0</u>: These are conics. All work like you just saw.

Inf. many rational points (if any).

<u>Genus 1</u>: The elliptic curve case

Lots of structure. If there are any rational points then you can make them into a group.

<u>The Mordell-Weil Theorem.</u> This group is finitely generated.

<u>Genus ≥ 2.</u> <u>Faltings' Theorem.</u> These curves have only <u>finitely many</u> rational points.

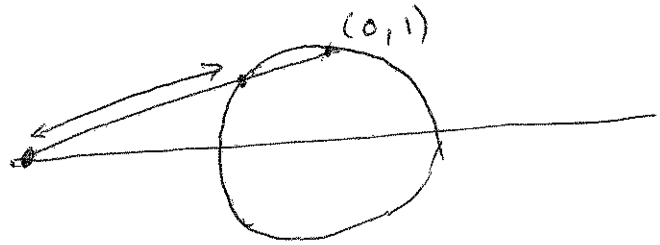
788, 2.1.

Last time: There is a bijection between

$\cancel{V(x^2+y^2-1)}$

$$\{(x,y) \in \underbrace{\mathbb{A}^2(K)}_{= K^2} : x^2+y^2-1=0\} \setminus (0,1) \qquad (K: \text{some subfield of } \mathbb{R})$$

and $\mathbb{A}^1(K)$, which is given by this picture.



We have the equations

$$\begin{array}{ccc} \text{Circle} & \longleftrightarrow & \mathbb{A}^1 \\ (x_0,y_0) & \longrightarrow & \dfrac{x_0}{1-y_0} \\ \left(\dfrac{2z_0}{z_0^2+1}, \dfrac{z_0^2-1}{z_0^2+1}\right) & \longleftarrow & z_0. \end{array}$$

We will see the definition of <u>projective space</u> shortly,

given

$$V = \{[x:y:z] \in \mathbb{P}^2 : x^2+y^2-z^2\},$$ these extend

to maps

$$\begin{array}{ccc} V(K) & \longleftrightarrow & \mathbb{P}^1(K) \\ [x_0 : y_0 : z_0] & \xrightarrow{\phi^{-1}} & [x_0 : z_0 - y_0] \\ [2x_0y_0 : x_0^2 - y_0^2 : x_0^2 + y_0^2] & \xleftarrow{\phi} & [x_0 : y_0]. \end{array}$$

These are inverse where they are bothe defined.

Now ϕ is defined everywhere.

If $[2x_0y_0 : x_0^2 - y_0^2 : x_0^2 + y_0^2] = [0:0:0]$

then $y_0 = 0$ and $x_0 = 0$

ϕ^{-1}, as written, is not:

$$[0:1:1] \longrightarrow [0:1-1].$$

So we have a pair of inverse <u>rational maps.</u>

They extend to isomorphisms because $[x_0 : z_0 - y_0]$

$= [z_0 + y_0 : x_0]$

(i.e. $x_0^2 = (z_0 - y_0)(z_0 + y_0)$

for $[x_0 : y_0 : z_0] \in V$.)

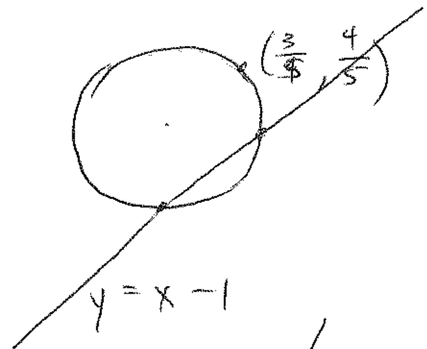
<u>Theorem.</u> (Sil, 2.2.1) Let C be a smooth curve and $V \in \mathbb{P}^N$ a variety. Then any rational map $C \to V$ is in fact a morphism.

Moreover, any morphism $\phi : C_1 \to C_2$ of curves is either constant or surjective.

(See Hartshorne, II.6.8 for a proof)

788, 2.3.

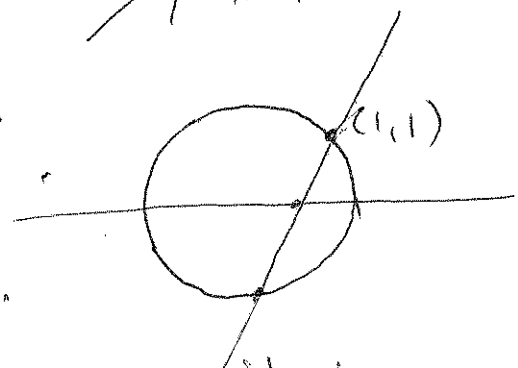
Fact. We could have started with any rational point and any line.



Exercise. Work out the details, e.g.

Do you see the mild complication and how to resolve it?

Or, let $V = \{(x,y) : x^2 + y^2 - 2\}$.



This gives a parametrization of $V(K)$.

Conclusion. If a circle has one K-rational point, it has infinitely many.

What about $\{x^2 + y^2 - 3\}$?

Claim. If $V = V(x^2 + y^2 - 3)$ then $V(\mathbb{Q}) = \phi$.

3.1. Affine and projective space.

Affine space $\mathbb{A}^n(K)$ (over a field K) is the set of n-tuples $(x_1, \ldots, x_n) \in K^n$.

(We can also say it is $\operatorname{Spec} K[x_1, \ldots, x_n]$ - not quite the same)

CAUTION. Silverman just says this is the set of K-rat'l pts of $\mathbb{A}^n(\bar{K})$.

If f is a polynomial in $x_1, \ldots, x_n$ then

$$V(f) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n(K) : f(x_1, \ldots, x_n) = 0\}$$

the vanishing set of f.

If S is a set of polynomials in $x_1, \ldots, x_n$ then

$$V(S) = \bigcap_{f \in S} V(f) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n(K) : f(x_1, \ldots, x_n) = 0 \text{ for all } f \in S\}$$

an affine variety. (Sometimes irreducibility is required.)

Example. $V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2(\mathbb{R})$.
$V(x^2 + y^2 + 1) \subseteq \mathbb{A}^2(\mathbb{R})$.

~~If $V = V(x^2 + y^2 + 1)$ then $V(\mathbb{R})$~~

If V is a variety then we write $V(K)$ for the set of its points with coordinates in K.

So, e.g. if $V = V(x^2 + y^2 + 1)$ then $V(\mathbb{R}) = \phi$
but $V(\mathbb{C}) \neq \phi$.

Projective space $\mathbb{P}^n(K)$ is the set of nonzero $n+1$-tuples $[x_1 : \cdots : x_{n+1}]$ subject to the equivalence relation

$$[x_1 : \cdots : x_{n+1}] \sim [\lambda x_1 : \cdots : \lambda x_{n+1}] \text{ for any } \lambda \in K.$$

3.2.

If f is a <u>homogeneous</u> polynomial in $x_1, \ldots, x_{n+1}$ then
(all terms of same degree)

$$V(f) = \{[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^{n+1}(K) : f(x_1, \ldots, x_{n+1}) = 0\}$$

and similarly if S is a set of homo polys.

These are <u>projective varieties</u>.

<u>Example</u>. Describe $V(y^2 z - x^3 + xz^2) \subseteq \mathbb{P}^2(\mathbb{R})$.

First of all, note that if for some $[x_0 : y_0 : z_0] \in \mathbb{P}^2$,

$y_0^2 z_0 - x_0^3 - x_0 z_0^2 = 0$, then

$(\lambda y_0)^2(\lambda z_0) - (\lambda x_0)^3 - (\lambda x_0)(\lambda z_0)^2 = 0$ so the condition <u>is</u> well defined. This is why we require homogeneity.

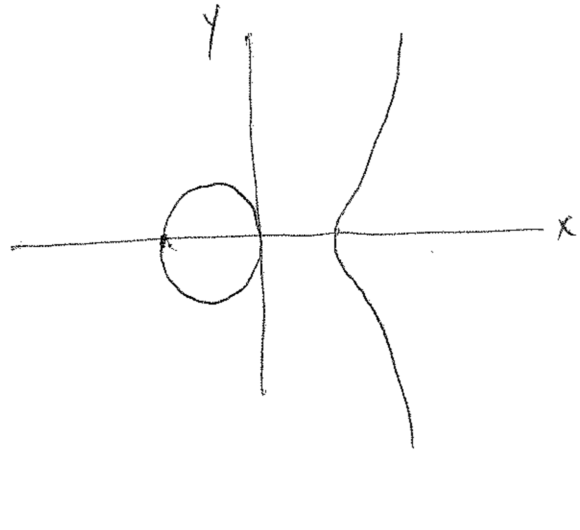
<u>Case 1</u>. $z \neq 0$. Since $[x : y : z] \sim [\frac{x}{z} : \frac{y}{z} : 1]$, and indeed every $[x : y : z] \in \mathbb{P}^2$ ~~[illegible]~~ with $z \neq 0$ can be written in a unique way with $z = 1$, WLOG assume $z = 1$.

We have an <u>affine patch</u> $\mathbb{A}^2 \subseteq \mathbb{P}^2$

$$(x, y) \longrightarrow [x : y : 1]$$

Set $z = 1$: $y^2 - x^3 + x = 0$ $\quad y^2 = x^3 - x$

$$= x(x-1)(x+1)$$



Case 2. $z = 0$. Then since $y^2 z - x^3 + xz^2 = 0$,

$$-x^3 = 0 \Rightarrow x = 0.$$

So the only remaining point is $[0 : 1 : 0]$.

If we think of V in terms of its affine patch $y^2 = x^3 - x$, this is the "point at infinity".

Def. A projective plane curve is $V(f) \subseteq \mathbb{P}^2$ where f is a single nonzero homogeneous polynomial.

If C is such a curve, defined with coefficients in a field k, then for each field K/k, we write

$$C(K) := \{ [x : y : z] \in \mathbb{P}^2(K) : f(x, y, z) = 0 \}.$$

C is (geometrically) irreducible if f does not factor over $\bar{k}$.

It is degenerate if it factors and has a repeated root.

(Example: $V((x+y-z)^2)$ is a conic.
$V((x+y-z)(x+y+z))$ is a pair of lines, reducible but nondegenerate.)

It is singular at a point $P = [x_0 : y_0 : z_0]$ if

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0.$$

It is smooth (nonsingular) if there are no singular points in $C(\bar{k})$.

3.4.

Components of a curve.

If k is algebraically closed, and f's factorization in $k[x, y, z]$ is $f = f_1 f_2 \cdots f_n$, the f_i are the *irreducible components* of f.

Bezout's Theorem. If $V(f_1)$ and $V(f_2)$ are projective plane curves with no common components, then they intersect in $(\deg f_1)(\deg f_2)$ points, counted with multiplicity.

Example. Suppose

$$f_1 = a_1 x + a_2 y + a_3 z$$
$$f_2 = b_1 x + b_2 y + b_3 z,$$

are distinct lines.

They intersect in exactly one point.

Middlebrow Proof. The intersection consists of all $[x : y : z]$ with

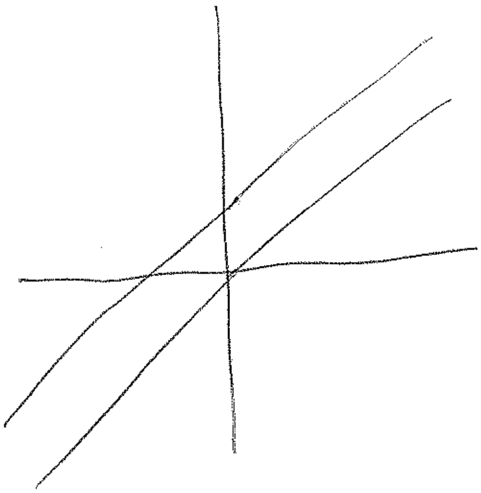
$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \operatorname{Ker} \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}.$$

If the lines are different the matrix has rank 2, hence nullity 1.

As $\mathbb{P}^2 = \{\text{lines through } A^3\}$, the intersection is one point.

3.5.

<u>Example</u>. Projectivize $y = x$, $y = x+1$ and determine their unique point of intersection.



$$y = x$$
$$y = x + z$$
$\Longrightarrow$ $x = y$ and $z = 0$.

So $[1 : 1 : 0]$.

Our "affine patch" is
$\{[x : y : 1] : (x,y) \in \mathbb{A}^2\}$
so we don't see it.

Informally, think of $[1 : 1 : 0]$ as close to
$$[1 : 1 : \varepsilon] = \left[\frac{1}{\varepsilon} : \frac{1}{\varepsilon} : 0\right].$$

A point far off in the direction of both lines.