Example: Checking for what p a quadratic form / $\mathbb{Q}$ has a non-zero solution in $\mathbb{Q}_p$.

Let $f(X,Y,Z) = X^2 - 13Y^2 + 17Z^2 \rightsquigarrow C_f \hookrightarrow \mathbb{P}^2$

$C_f(\mathbb{R}) \neq \emptyset$: $[\sqrt{13}, 1, 0]$. For primes p, we'll use Hensel's Lemma + analysis over $\mathbb{F}_p$.

For $p \neq 2, 13, 17$, $C_{f \bmod p}$ is non-singular, so it suffices to find a primitive solution mod p (for $p \neq 2, 13, 17$) — then Hensel forces a p-adic solution.

We've already seen (pigeonhole) that these primitive solutions exist — so $C_f(\mathbb{Q}_p) \neq \emptyset$ for $p \neq 2, 13, 17$.

$p=13$: (note $[0,1,0]$ is a singular point of $C_{f \bmod 13}$)

$f \bmod 13 = X^2 + 4Z^2$, so $[3,0,1]$ is a solution to $f \bmod 13$, and $\frac{\partial f}{\partial x}$ or $\frac{\partial f}{\partial z}$ at this point is $\neq 0$, so Hensel $\Rightarrow C_f(\mathbb{Q}_{13})$.

$p=17$: similarly $[8,1,0]$ lifts to a 17-adic solution

$p=2$: $f \bmod 8$ $f(2,1,1) \equiv 0 \bmod 8$ and $v_2\left(\frac{\partial f}{\partial y}(2,1,1)\right) = 1$, so we win again. **Conclusion:** $\forall p$, $C_f(\mathbb{Q}_p) \neq \emptyset$ and $C_f(\mathbb{R}) \neq \emptyset$.

Question: For this f, is $C_f(\mathbb{Q}) \neq \emptyset$? The 3-variable case of the Hasse-Minkowski thm says YES:

Thm (Legendre) Let $f \in \mathbb{Q}[X_0, \ldots, X_n]$ be a non-degenerate quadratic form. Then

$$\exists\, a \in \mathbb{Q}^{n+1} \setminus 0 : f(a) = 0 \iff \forall p,\ \exists\, a_p \in \mathbb{Q}_p^{n+1} \setminus 0 : f(a) = 0 \text{ and } \exists\, a_\infty \in \mathbb{R}^{n+1} \setminus 0 : f(a) = 0$$

Alternatively, write $C_f \hookrightarrow \mathbb{P}^n$ for the associated nonsingular projective hypersurface. Then

$$C_f(\mathbb{Q}) \neq \emptyset \iff \forall p,\ C_f(\mathbb{Q}_p) \neq \emptyset \text{ and } C_f(\mathbb{R}) \neq \emptyset$$

(we are only going to prove the $n=2$ case)

In particular, $\exists (a_0,a_1,a_2) \in \mathbb{Q}^3 \setminus 0 : a_0^2 - 13a_1^2 + 17a_2^2 = 0$

this is harder.

Rmk: ① The thm holds $\forall$ number field (- -)

② $n=1$ case is an exercise (HW)

③ We'll prove the $n=2$ case, which is elementary (but tricky)

④ $n=3$ (4 variables) is the hardest case; it uses quadratic reciprocity in a serious way. $n \geq 4$ is deduced by an inductive argument → see Serre, Course in Arithmetic

---

Now we'll prove the 3-variable thm.

The first key observation:

Lemma: Let k be any field w/ $\mathrm{char}(k) \neq 2$. Let $a, b \in k^\times$. Consider the field extension $k[\sqrt{b}]/k$ ($k[\sqrt{b}]$ is deg 2 $\iff b \notin (k^\times)^2$).

The equation $z^2 - ax^2 - by^2 = 0$ has a non-zero solution ($(x,y,z) \in k^3 \setminus 0$) if and only if

$$a \in N_{k[\sqrt{b}]/k}\left(k[\sqrt{b}]^\times\right) \subseteq k^\times.$$

Pf: Recall $N_{k[\sqrt{b}]/k}$ is the group homomorphism $k[\sqrt{b}]^\times \longrightarrow k^\times$ given by $N(\alpha) = \det(\alpha \text{ acting by multiplication on the } k\text{-vector space})$

Two cases: ① $b \in (k^\times)^2$: then any a is a norm,

and $(\sqrt{b})^2 - a\cdot 0^2 - b\cdot 1^2 = 0$ is a solution in k.

② $b \notin (k^\times)^2$. Suppose $a \in N(k[\sqrt{b}]^\times)$ so $\exists a_1, a_2 \in k$: $a = a_1^2 - b a_2^2$, so $(z,x,y) = (a_1, 1, a_2)$ is a solution.

Conversely, suppose z,x,y is a solution in $k^3 \setminus 0$, $x \neq 0$, because otherwise $b \in (k^\times)^2$, so $a = \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2 \in N(k[\sqrt{b}]^\times)$. ∎

$k[\sqrt{b}])$

$= \prod \sigma(\alpha)$

$\sigma \in \mathrm{Hom}_k(k[\sqrt{b}], \bar{k})$

$= \begin{cases} \alpha & \text{if } k = k[\sqrt{b}] \\ a_1^2 - a_2^2 b & \text{if } k[\sqrt{b}]/k \\ & \text{is quadratic and} \\ & \alpha = a_1 + a_2\sqrt{b} \text{ for } a_i \in k. \end{cases}$

Pf of H-M for 3 variables: Necessity of having local solutions is clear. We'll show it is sufficient. Let $f \in \mathbb{Q}[X_0, X_1, X_2]$ be a non-degenerate quadratic form such that $C_f(\mathbb{Q}_p) \neq \emptyset$ $\forall p$ and $C_f(\mathbb{R}) \neq \emptyset$.

By linear COV, we may assume f is diagonal. We can rescale f so one coefficient is 1. Again by a linear COV we may assume $f(X_0, X_1, X_2) = X_0^2 - aX_1^2 - bX_2^2$ where $a, b \neq 0$ are square-free integers, and $|a| \leq |b|$.

Now carry out proof by induction on $|a|+|b| = m$

Base case: $m = 2$, so $|a| = |b| = 1$, and $f = X_0^2 \pm X_1^2 \pm X_2^2$. Any such f has a non-zero solution unless $f = X_0^2 + X_1^2 + X_2^2$, but this f has no solution $\in \mathbb{R}^3 \setminus 0$. ✓

Suppose $m > 2$, hence $|b| \geq 2$. Write $b = \pm p_1 \cdots p_r$ for distinct primes p_i.

Claim: **a is a square mod b**

Pf: By CRT, STP $\forall\, p \mid b$, $a \equiv \square \bmod p$. Clear if $p \mid a$, so assume $a \in \mathbb{Z}_p^\times$. By assumption, $\exists\, (z,x,y) \in \mathbb{Z}_p^3 \setminus (p\mathbb{Z}_p)^3$ such that $z^2 - ax^2 - by^2 = 0$.

As $p \mid b$, $z^2 \equiv ax^2 \bmod p$, so we win provided $x \not\equiv 0 \bmod p$

If $p \mid x$, then $p \mid z$, and $p^2 \mid by^2$, so since b is $\square$-free, $p \mid y$ $\longrightarrow$ contradicts primitivity of the solution.

Thus, $a \equiv \square \bmod p$.

Since $a \equiv \square \bmod b$, $\exists\ t \in \mathbb{Z} : |t| \le |b|/2$ such that $t^2 - a = b \cdot b'$ for some $b' \in \mathbb{Z}$.

Thus $bb' \in N_{k[\sqrt{a}]/k}(k[\sqrt{a}]^\times)$ $\quad (N(t+\sqrt{a}))$

for $k = \mathbb{Q}, \mathbb{Q}_p, \mathbb{R}$.

- For any such k, f has a non-zero solution in k^3 $\overset{\text{Lemma}}{\Longleftrightarrow}$ $b \in N_{k[\sqrt{a}]/k}(k[\sqrt{a}]^\times)$

$\Longleftrightarrow$ (N is mult.) $b' \in N_{k[\sqrt{a}]/k}(k[\sqrt{a}]^\times)$.

$\Longleftrightarrow$ $X_0^2 - aX_1^2 - b'X_2^2 = f'(X_0, X_1, X_2)$ has a non-zero solution in k^3

In particular, f' has local solutions in all $\mathbb{Q}_p, \mathbb{R}$.

But $|b'| = \left|\frac{t^2 - a}{b}\right| \le \frac{|b/2|^2}{|b|} + \frac{|a|}{|b|} \le \left|\frac{b}{4}\right| + 1 < |b|$. ($|b| \ge 2$)

(b' may not be square-free, but no matter:
if $b' = d^2 \cdot b''$ $(d \in \mathbb{Z}, b'' \in \mathbb{Z})$, then f' represents 0
$\Longleftrightarrow$ $X_0^2 - aX_1^2 - b''X_2^2$ represents 0.)

Certainly $|a| + |b''| < |a| + |b|$, so we win by induction. ∎

The proof is effective: Suppose we want to solve $x^2 - 13y^2 + 17z^2 = 0$

($a = 13$, $b = -17$ square-free integers with $|a| \leq |b|$). The proof tells us:

- Solve $t^2 - a = b \cdot b'$ with $|t| \leq \frac{|b|}{2} = \frac{17}{2}$

$$8^2 - 13 = (-17) \cdot (-3)$$

($t = 8$, $b' = -3$)

so $(-17) \cdot (-3) = N_{\mathbb{Q}[\sqrt{13}]/\mathbb{Q}}(8 + \sqrt{13})$

Now, $-17 \in$ Norms $\Leftrightarrow$ $-3 \in$ Norms, so suffices to solve

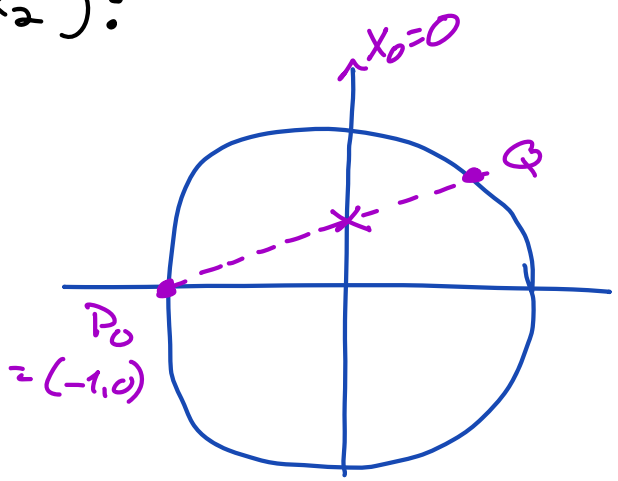
$x^2 + 3y^2 - 13z^2 = 0$

Etc — carrying this out is one of the PSet questions.

(solving this will realize $-3 = N_{\mathbb{Q}[\sqrt{13}]/\mathbb{Q}}(\alpha)$ so $-17 = N\left(\frac{8+\sqrt{13}}{\alpha}\right)$)

- We now understand how to determine when a nonsingular conic $C_f \hookrightarrow \mathbb{P}^2$ over k ($f \in k[x_0, x_1, x_2]$ homogeneous degree 2) has $C_f(k) \neq \emptyset$ for $k = \mathbb{R}, \mathbb{F}_p, \mathbb{Q}_p, \mathbb{Q}$.
- What about describing the full set $C_f(k)$? Recall the parametrization of "Pythagorean triples" ($f = x_0^2 + x_1^2 - x_2^2$):

$C_f(\mathbb{Q}) \ni P_0 = [-1, 0, 1]$.



$C_f \longrightarrow \{x_0 = 0\}$

$(P_0 \neq Q) \longmapsto$ the point of intersection of $\{x_0 = 0\}$ with the line $\overline{P_0 Q}$.

$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \longmapsto (0, t)$

try to extend this to a parametrization of the full projective curve C_f (or $C_f(\mathbb{Q})$)

where should P_0 go? P_0 should map to the intersection of the tangent line to C_f at P_0 with our fixed line ($x = 0$).

Generalization (PSet):

Prop: Let k be any field, and let $f \in k[x_0, x_1, x_2]$ be a homogeneous polynomial of degree 2. Assume $C_f \hookrightarrow \mathbb{P}^2$ is non-singular, and that $C_f(k) \neq \emptyset$. Then $X \cong \mathbb{P}^1$ (isomorphism of algebraic varieties).

More precisely, fix $P_0 \in C_f(k)$, and fix a linear form $L(x_0, x_1, x_2) \in k[x_0, x_1, x_2]$ such that $C_L \not\ni P_0$. Then the projection map

$$\pi : C_f \longrightarrow C_L$$

$$P_0 \neq Q \longmapsto C_L \cap \overline{P_0 Q}$$

$$P_0 \longmapsto C_L \cap \mathrm{Tan}_{C_f, P_0}$$

is an isomorphism of varieties over k.

In particular, $\forall$ fields $k' \supset k$, π induces a bijection $C_f(k') \xrightarrow{\sim} C_L(k')$

Moreover $C_L \cong \mathbb{P}^1$, so $C_f \cong \mathbb{P}^1$

("any nonsingular conic / k with a k-point is $\cong$ to $\mathbb{P}^1$").

(PSet).

Do this exercise!

Beyond Conics Recall our 4-step analysis for conics/$\mathbb{Q}$

1. Solve over $\mathbb{F}_p$ (by a counting argument)
2. Use 1. + Hensel's Lemma to solve over $\mathbb{Q}_p$ (and $\mathbb{R}$ easy)
3. Apply Hasse-Minkowski theorem to determine whether solutions exist over $\mathbb{Q}$
4. If $C_f(\mathbb{Q}) \neq \emptyset$, use a linear parametrization ($C_f \simeq \mathbb{P}^1$) to describe $C_f(\mathbb{Q})$.

In higher degree, every step except 2. becomes much more difficult.

Example: 1. Consider $3X_0^3 + 4X_1^3 + 5X_2^3 = f(X_0, X_1, X_2)$ defining $C_f \hookrightarrow \mathbb{P}^2$. For $p \equiv 1 \bmod 3$,

$$C_f(\mathbb{F}_p) = \bigcup_{i=0}^{2} \left(C_f(\mathbb{F}_p) \cap \{X_i \neq 0\} \right) = \{3x^3 + 4y^3 + 5 = 0\} \cup \{3x^3 + 4 + 5z^3 = 0\} \cup \{3 + 4y^3 + 5z^3 = 0\}$$

An equation like $3x^3 = 5 - 4y^3$ does not have solutions by a simple counting argument, since $\left| (\mathbb{F}_p^\times)^3 \right| = \frac{p-1}{3}$.

There is in this case an elementary argument to show $\exists$ solution, but
- how many solutions?
- higher degree, more complicated polys?

(3) The analogue of the H-M theorem fails ("most of the time", in fact!). We'll do an example next.

(4) Even if we know $C_f(\mathbb{Q}) \neq \emptyset$, describing $C_f(\mathbb{Q})$ is extremely difficult and even when $\deg(f) = 3$ the subject of deep open problems. We'll spend much of the course starting to study this $\deg(f) = 3$ case.

Goal:
Failure of the local-global principle for genus 1 curves (e.g. nonsingular cubic in $\mathbb{P}^2$).

Example: $f(X_0, X_1, X_2) = 3X_0^3 + 4X_1^3 + 5X_2^3 \in \mathbb{Q}[X_0, X_1, X_2]$

$C_f(\mathbb{R}) \neq \emptyset$, and $\forall p \; C_f(\mathbb{Q}_p) \neq \emptyset$, but $C_f(\mathbb{Q}) = \emptyset$

↑ checking these statements is a good exercise

↑ tricky. (see Keith Conrad's note on this for details)

We'll do the details of an easier example.

Let $p \equiv 1 \bmod 8$ such that $\left(\frac{2}{p}\right)_4 \neq 1$ ($x^4 = 2 \bmod p$ not solvable in $\mathbb{F}_p$)

(eg $p = 17$)

Consider the affine curve $C^0 \hookrightarrow \mathbb{A}^2$ over $\mathbb{Q}$.

//

$\{w^2 = 2 - 2pz^4\}$.

C^0 is nonsingular (check this), but the projective closure $\overline{C^0} = \{W^2T^2 = 2T^4 - 2pZ^4\} \hookrightarrow \mathbb{P}^2$ is singular on $\overline{C^0} \cap \{T=0\} = \{[0,1,0]\}$ (T, w, Z). (check)

Fact: Let C^0 be any nonsingular affine curve. Then there is a nonsingular projective curve (maybe in higher-dim $\mathbb{P}^n$) C such that $C^0 \cong C \setminus \{\text{finite set}\}$.

In our example, we can see this explicitly:

Define $C \hookrightarrow \mathbb{P}^3$ as the intersection of two quadrics $X_0X_3 - X_1^2 = 0$ and $X_2^2 - 2X_0^2 + 2pX_3^2 = 0$.

$$C^0 \xrightarrow{f} U_0 = \{X_0 \neq 0\} \cong \mathbb{A}^3$$

$$f: (w,z) \longmapsto [1, z, w, z^2]$$

So we see $f: C^0 \longrightarrow C \cap U_0$, and this map has inverse

$$C \cap U_0 \longrightarrow C^0$$
$$= \{(y_1,y_2,y_3) \in \mathbb{A}^3 \mid y_3 = y_1^2,\ y_2^2 - 2 + 2py_3^2 = 0\}$$

given by $g(y_1,y_2,y_3) = (y_2, y_1)$

So we find $C^0 \xrightarrow{\sim} C \cap U_0$ (iso of varieties).

Note: $C \setminus C^0 = C \cap \{X_0 = 0\} = \{[0,0,\pm\sqrt{-2p},1]\}$.

→ Check that C is nonsingular also at these points

Theorem: For this $C \hookrightarrow \mathbb{P}^3$,

$C(\mathbb{Q}_p) \neq \emptyset \ \forall p$, but $C(\mathbb{Q}) = \emptyset$.

$C(R) \neq \phi$

Next time: we'll start by very quickly defining nonsingularity for general varieties, and then we'll prove the theorem. — see Gaurav's talk video

PSet post tomorrow a.m.