Last time: introduced the field $\mathbb{Q}_p$ for a prime number p.

This is a complete nonarchimedean field (w/ absolute value $|\cdot|_p$).

Last time: can expand elements of $\mathbb{Q}_p$ via p-adic expansion

$$\sum_{i \gg -\infty}^{\infty} a_i p^i \qquad a_i \in \{0, 1, \ldots, p-1\}.$$

Over $\mathbb{R}$, given $f(x) \in \mathbb{R}[x]$, can detect existence of roots by looking at signs.

Hensel's lemma:

Let $f(x) \in \mathbb{Z}_p[x]$.

Let $\alpha \in \mathbb{Z}_p$ s.t.

$|f(\alpha)|_p < 1$ & $|f'(\alpha)|_p = 1$.

Then $\exists!$ $\beta \in \mathbb{Z}_p$ such that

$|\alpha - \beta|_p < 1$ and $f(\beta) = 0$.

(Another formulation:

If $\overline{f}(x) \in \mathbb{F}_p[x]$ has a simple root $\overline{\alpha} \Rightarrow$ this lifts uniquely to a root $\beta \in \mathbb{Z}_p$ of f.)

Pf sketch: Use Newton's method to refine α to the root β.

Define a sequence of p-adic integers $\alpha_0, \alpha_1, \alpha_2, \ldots$

such that $\alpha_0 = \alpha$

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

Then $|f(\alpha_n)|_p \longrightarrow 0 \quad n \to \infty$

$\{\alpha_n\}$ is a Cauchy sequence which is going to converge to limit β.

$|f(\alpha_{n+1})|_p \leq |f(\alpha_n)|^2 \rightsquigarrow$ use Taylor approximation of f near α_n.

$$f(\alpha_{n+1}) = f(\alpha_n) + f'(\alpha_n)\left(-\frac{f(\alpha_n)}{f'(\alpha_n)}\right) + O\left(\frac{f(\alpha_n)}{f'(\alpha_n)}\right)^2$$

$$= O\left(\frac{f(a_n)^2}{f'(a_n)}\right)$$

Pf by successive approximation

Want: β s.t. $f(\beta) = 0$.

β has a p-adic expansion

Observation: first n p-adic digits of $f(\beta)$ depend on the first n p-adic digits of β. Inductively solve for the p-adic digits of β.

Example) $p > 2$

Consider $x^{p-1} - 1 \in \mathbb{Z}_p[x]$

Recall that $u^{p-1} = 1$ if $u \in \mathbb{F}_p^\times$.

So any $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \text{ s.t. } |x|_p = 1\}$.

has $|x^{p-1} - 1|_p < 1$.

But $(p-1)x^{p-2}$ is a p-adic unit.

$\Rightarrow$ In each congruence class of $\mathbb{Z}_p$ (except zero) mod p there is a $(p-1)$st root of unity.

i.e.

Conclusion: $\mathbb{Q}_p$ contains $(p-1)$st roots of unity.

(On problem set: $x \in \mathbb{Z}_p^\times$

Consider $x, x^p, x^{p^2}, \ldots$

converges p-adically to a $(p-1)$st root of unity which is $\equiv$ mod p to x :)

Ex) Let $p \equiv 1 \mod 4$.
Then $\sqrt{-1} \in \mathbb{Q}_p$.
(Special case of the above)
Consider x^2+1 in $\mathbb{F}_p$ has a root
$\Rightarrow$ apply Hensel's lemma.

Hensel's lemma gives a complete determination of which elements of $\mathbb{Q}_p^\times$ are squares & determines

$$\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}.$$

Ex) $p > 2$.
Given $u \in \mathbb{Z}_p^\times$ then
Hensel's lemma implies that

u admits a square root

$\iff$ $\overline{u} \in \mathbb{F}_p^\times$ admits a square root.

Apply Hensel's lemma to $x^2 - u$.

In general, if we've given an element of $\mathbb{Q}_p^\times$, can always write it as $p^i u$ where $i \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$.

This is a square in $\mathbb{Q}_p^\times$

$\iff$ i even & $\overline{u} \in \mathbb{F}_p^\times$ is a square.

Conclusion:

$$\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

p $\quad$ $u \in \mathbb{Z}_p^\times$ s.t. $\overline{u} \in \mathbb{F}_p^\times$

not a square.

$$\mathbb{Z}_p / p\mathbb{Z}_p \simeq \mathbb{F}_p$$

Any p-adic integer

$$\sum_{i=0}^{\infty} a_i p^i \longrightarrow a_0$$

It's a little trickier for $p = 2$.

Can show $u \in \mathbb{Z}_2^\times$ s.t. $u - 1$ is divisible by 8 is necessarily a square.

Conclusion:

$$\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2} \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$$

$$2 \quad -1 \quad 5$$

Now let's apply to quadratic forms over $\mathbb{Q}_p$.

Fix a quadratic form $\langle a_1, \dots, a_n \rangle$ over $\mathbb{Q}_p$ so $a_i \in \mathbb{Q}_p^\times$.

By rescaling, can write it in the form

$$\langle u_1, \dots, u_r \rangle \oplus \langle pv_1, \dots, pv_s \rangle$$

$u_i, v_i \in \mathbb{Z}_p^\times$.

If $p > 2$, can use this to completely classify quadratic forms over $\mathbb{Q}_p$. (in terms of forms over $\mathbb{F}_p$).

In fact, $W(\mathbb{Q}_p) \simeq W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$.

Construction (reverse the above)

Let $\langle \bar{u}_1, \dots, \bar{u}_r \rangle$ be a quadratic form over $\mathbb{F}_p$. Can produce a quadratic over $\mathbb{Q}_p$ by lifting $\bar{u}_i$ to a p-adic unit u_i

$$\langle \bar{u}_1, \dots, \bar{u}_r \rangle \rightsquigarrow \langle u_1, \dots, u_r \rangle$$

There is non-uniqueness in the choice of the u_i, but up to scaling by squares.

In fact, this gives a well-defined map

$$\left\{ \begin{array}{c} \text{iso classes of} \\ \text{quadratic forms over} \\ \mathbb{F}_p \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{iso classes} \\ \text{of forms} \\ \text{over } \mathbb{Q}_p \end{array} \right\}$$

Can see this using Witt's
Chow equivalence theorem.

This produces a map of $p>2$.
commutative rings

$$GW(\mathbb{F}_p) \xrightarrow{\varphi} GW(\mathbb{Q}_p)$$

$$\langle \bar{u}_1, \dots, \bar{u}_r \rangle \longmapsto \langle u_1, \dots, u_r \rangle$$

Can also produce the map $\langle p \rangle \varphi$
sending

$$\langle \bar{u}_1, \dots, \bar{u}_r \rangle \longmapsto \langle pu_1, \dots, pu_r \rangle$$

so obtains a map $(\varphi, p\varphi)$

$$GW(\mathbb{F}_p) \oplus GW(\mathbb{F}_p) \longrightarrow GW(\mathbb{Q}_p)$$

This map is surjective-

Not injective b/c

$\langle 1, -1 \rangle = \langle p, -p \rangle$

$= H_2$.

Theorem (Springer): This is the only redundancy: ($p > 2$).

$$GW(\mathbb{Q}_p) \cong \frac{GW(\mathbb{F}_p) \oplus GW(\mathbb{F}_p)}{\langle H, -H \rangle}$$

$$W(\mathbb{Q}_p) \cong W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$$

An anisotropic quadratic form over $\mathbb{Q}_p \rightsquigarrow$ a pair of anisotropic quadratic forms over $\mathbb{F}_p$.

Cor: Any quadratic form over $\mathbb{Q}_p$ in ≥ 5 variables is isotropic. There is an anisotropic quadratic form of dim 4, so $u(\mathbb{Q}_p) = 4$.

Pf: Follows the previous arguments. Explicitly say

$$\langle u_1, u_2, \underbrace{pv_1, pv_2, pv_3}_{u_i, v_i \in \mathbb{Z}_p^\times} \rangle.$$

Want: this is isotropic.

In fact, $\langle pv_1, pv_2, pv_3 \rangle$ is isotropic $\iff \langle v_1, v_2, v_3 \rangle$

is isotropic. To see this,

need a solution

of $V_1 x_1^2 + V_2 x_2^2 + V_3 x_3^2 = 0.$

This eqn has a nonzero solution over $\mathbb{F}_p$ $(\bar{x}_1, \bar{x}_2, \bar{x}_3)$

b/c forms in ≥ 3 vars over $\mathbb{F}_p$ are isotropic. Can lift to a solution over $\mathbb{Z}_p$ using Hensel's lemma. (fix 2 of the variables).

Works similarly for

$\underbrace{(u_1, u_2, u_3)}_{\text{isotropic not } p}, pv_1, pv_2$

Ex) Let $\langle 1, \bar{u} \rangle$ is anisotropic over $\mathbb{F}_p$.
(i.e. $1, -\bar{u}$ not a square).

Lift $\bar{u}$ to $u \in \mathbb{Z}_p^\times$

Then: form $\langle 1, u, p, pu \rangle$ is anisotropic over $\mathbb{Q}_p$.

Why? Suppose

(*) $x_1^2 + u x_2^2 + p x_3^2 + pu x_4^2 = 0$ over $\mathbb{Q}_p$.

Wlog, can assume $\{x_i \in \mathbb{Z}_p\}$ & not all the x_i are divisible by p.
(x_1, x_2, x_3, x_4). Suppose $x_1 \in \mathbb{Z}_p^\times$.
or $x_2 \in \mathbb{Z}_p^\times$

Reduce mod p
$\bar{x}_1^2 + u \bar{x}_2^2 = 0$

Conversely, suppose x_1, x_2 are div by p
but one of $x_3, x_4 \in \mathbb{Z}_p^\times$.

Then LHS of $(*)$ div by p
but not zero mod p^2.