Lecture 34:

q a nondegen quad form on $\mathbb{Q}_p^n$, $d = \det(q)$, $\varepsilon = \varepsilon(q)$
$= \prod_{i<j} (a_i, a_j)$

Thm: q reps 0 iff: $n = 2$ and $d = -1$ (in $\mathbb{Q}_p^*/sqs$).
$n = 3$ and $(-1, -d) = \varepsilon$.
$n = 4$ and either $d \neq 1$ or
$n \geq 5$. ($d = 1$ and $\varepsilon = (-1,-1)$)

Cor: $a \in \mathbb{Q}_p^*/sqs$. Then q reps a iff
$n = 1$ and $a = d$.
$n = 2$ and $(a, -d) = \varepsilon$,
$n = 3$ and $a \neq -d$ or ($a = d$ and $(-1, -d) = \varepsilon$),
$n \geq 4$.

Pf: HW!

Pf of Thm:

$n = 4$: $q = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + a_4 x_4^2$ reps 0
$\iff \exists\, a \in \mathbb{Q}_p^*$ rep by both $a_1 x_1^2 + a_2 x_2^2$ and
$-a_3 x_3^2 - a_4 x_4^2$

[Can avoid $a = 0$ as the common value as then the two rank 2 forms are hyperbolic and rep all values.]

$\iff (a, -a_1 a_2) = (a_1, a_2)$ and $(a, -a_3 a_4) = (-a_3, -a_4)$

[Note that really there are only finitely many poss for a, a_i as can be thought of as cls of $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.]

The above eqns have no solutions iff

$$a_1 a_2 = a_3 a_4 \quad \text{and} \quad (a_1, a_2) = -(-a_3, -a_4)$$

(see Serre for this). The 1st cond says $d = 1$ and then

$$\varepsilon = \prod_{i<j} (a_i, a_j) = (a_1, a_2)(a_3, a_4) \prod_{\substack{i=1,2 \\ j=3,4}} (a_i, a_j)$$

$$= (a_1, a_2)(a_3, a_4)(a_1 a_2, a_3 a_4) = (a_1, a_2)(a_3, a_4)(-1, a_3 a_4)$$

$$= (a_1, a_2)(a_3, a_4)(-1, a_3)(-1, -a_4)(-1, -1)$$

$$= (a_1, a_2)(-a_3, -a_4)(-1, -1) = -(-1, -1).$$

$n \geq 5$: See Serre. ▨

Hasse-Minkowski Thm: q a quad form over $\mathbb{Q}$. Then q reps $0 \iff q_v$ reps 0 for every place v.

Proof: ($\Leftarrow$) Can assume q is nondegenerate and

$$q = x_1^2 + a_2 x_2^2 + \cdots + a_n x^n$$

Case $n=2$: $q = x^2 - ay^2$ reps $0 \iff a \in (\mathbb{Q}^\times)^2$.

As q_∞ reps 0, have $a > 0$. So $a = \prod_p p^{v(p)}$

As q_p reps 0, know $a \in (\mathbb{Q}_p^\times)^2 \Rightarrow |a|_p = p^{-v(p)} \in (\mathbb{Q}^\times)^2$,

i.e. $v(p)$ is even. So $a \in (\mathbb{Q}^\times)^2$.

Case $n=3$: $q = z^2 - ax^2 - by^2$ where $a, b \in \mathbb{Z}$ are squarefree with $0 < |a| \le |b|$.

Induct on $m = |a| + |b|$: Base case is $m=2$,

i.e. $q = z^2 \pm x^2 \pm y^2$. As q_∞ reps 0, have at least 1 negative sign $\Rightarrow q$ reps 0 over $\mathbb{Q}$.

So consider $m > 2 \Rightarrow |b| \ge 2$.

Claim: a is a square mod b. ($t^2 - a\cdot 1^2 - bb'\cdot 1^2 = 0$)

If so, $\exists t, b' \in \mathbb{Z}$ with $t^2 = a + bb'$ and $|t| \le \frac{b}{2}$. ⋆

$\Rightarrow (a, bb') = 1 \Rightarrow (a, b) = (a, b')$

Now

$$|b'| = \left| \frac{t^2 - a}{b} \right| \le \frac{|b|}{4} + 1 < |b|$$

and so we know inductively that HM holds for $q' = z^2 - ax^2 - by^2$. Now q'_v reps 0 for all v, as $(\star)$ holds for $\mathbb{Q}_v$ just as surely as it did for $\mathbb{Q}$. So q' reps 0 $\Rightarrow$ q does as well.

Pf of Claim: $b = \pm p_1 \cdots p_k$ where $k \geq 1$

As $\mathbb{Z}/b\mathbb{Z} \cong \bigoplus \mathbb{Z}/p_i\mathbb{Z}$, it's enough to show that a is a square mod p where $p = p_i > 2$.

True if $a \equiv 0 \bmod p$, so assume $a \in \mathbb{Z}_p^\times$.

By assumption, q_p reps 0, and so $\exists\, (x,y,z) \in (\mathbb{Z}_p)^3$ with at least one a unit where $z^2 - ax^2 - by^2 = 0$.

Now $z^2 - ax^2 \equiv 0 \bmod p$. Can't have $x \equiv 0 \bmod p$, as then $z \equiv 0 \bmod p$ and so $y \equiv 0 \bmod$ contradicting that one of x, y, z is a unit. So $a = \left(\frac{z}{x}\right)^2 \bmod p$ as needed to prove the claim and hence the theorem.

$n = 4, 5$ next time.