Lecture 34:

Let $g$ be a quadric form on $\mathbb{Q}_p^n$, $d = \text{disc}(g)$, $\varepsilon = \varepsilon(g)$

$$d = \prod_{i<j} (a_i, a_j)$$

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

**Cor:** $a \in \mathbb{Q}_p^*/\text{sqfs}$, then $g$ reps $a$ iff:
- $n = 1$ and $a = d$,
- $n = 2$ and $(a, -d) = \varepsilon$,
- $n = 3$ and $a \neq -d$ or $(a = d$ and $(-1, -d) = \varepsilon$),
- $n > 4$.

**Ref:** HW!

**Ref of Thm:**

$n = 4$:

$$g = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + a_4 x_4^2 \text{ reps 0}$$

$$\iff \exists a \in \mathbb{Q}_p^* \text{ reps by both } a_1 x_1^2 + a_2 x_2^2 \text{ and } -a_3 x_3^2 - a_4 x_4^2$$

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

$$\iff (a_1, -a_2) = (a_1, a_2) \text{ and } (a_3, -a_4) = (-a_3, -a_4)$$
Note that really there are only finitely many possibilities for \( a, a_i \) as can be thought of as sets of \( \mathbb{Q}_p \). The above systems have no solutions iff

\[
a_1a_2 = a_3a_4 \quad \text{and} \quad (a_1, a_2) = (-a_3, -a_4)
\]

(see above for this). The 1st cond. says \( d = 1 \) and then

\[
\epsilon = \prod_{i < j} (a_i, a_j) = (a_1, a_2)(a_3, a_4) \prod_{l=1,2}^{j=3,4} (a_l, a_j)
\]

\[
= (a_1, a_2)(a_3, a_4) (a_1a_2, a_3a_4) = (a_1, a_2)(a_3, a_4)(-1, a_3a_4)
\]

\[
= (a_1, a_2)(a_3, a_4)(-1, a_3)(-1, -a_4)(-1, -1)
\]

\[
= (a_1, a_2)(-a_3, -a_4)(-1, 1) = -(-1, 1).
\]

\( \hfill \boxed{\text{\textcolor{green}{n > 5: see above.}} \quad \hfill} \)

\underline{Hurwitz-Minkowski Thm.:} \quad \text{\textcolor{green}{q a quad form over } } \mathbb{Q}.

Then \( q \) reps \( 0 \iff q_v \) reps \( 0 \) for every place \( v \).

\underline{Proof:} \( (\Leftarrow) \) can assume \( q \) is nondegenerate and

\[
q = x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2
\]
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 \( a = \prod_p \nu(p) \).

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

i.e. \( \nu(p) \) 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 \( 0 < |a| \leq |b| \).

Clearest case is \( m = 1a1 + 1b1 \): 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 on \( \mathbb{Q} \).

So consider \( m > 2 \Rightarrow |b| > 2 \).

Claim: \( a \) is a square mod \( b \).

\( t^2 - a \cdot t^2 - bb' \cdot 1^2 = 0 \)

If so, \( \exists t, b' \in \mathbb{Z} \) with \( t^2 = a + b b' \) and \( |t| \leq \frac{b}{2} \).

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

Now \( |b'| = \left| \frac{t^2 - a}{b} \right| \leq \frac{|b|}{4} + 1 < |b| \)
and so we know inductively that HM holds for \( q' = z^2 - ax^2 - by^2 \). Now \( q' \) reps 0 for all \( r \), so HM holds for \( Q_r \) just as surely as it did for \( Q \). So \( q' \) reps 0 \( \implies q \) does as well.

\[ \text{Pf of claim: } b = \pm p \cdots p^k \text{ where } k \geq 1 \]

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 \( a \equiv 0 \mod p \), so assume \( a \in \mathbb{Z}_p^x \).

By assumption, \( q \) reps 0, and so \( \exists (x, y, z) \in (\mathbb{Z}/p) \times \mathbb{Z}/p^i \mathbb{Z} \) with at least one a unit where \( z^2 - ax^2 - by^2 = 0 \).

Now \( z^2 - ax^2 \equiv 0 \mod p \). Can't have \( x \equiv 0 \mod p \), so then \( z \equiv 0 \mod p \) and \( x \equiv 0 \mod p \) contradicting that one of \( x, y, z \) is a unit. So \( a = (\frac{z}{x})^2 \mod p \) as needed.

To prove the claim and hence the theorem, \( n = 4, 5 \) next time.