Lecture 35: The Hilbert Symbol Revisited.

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

[Last time: Proved when $n \leq 3$. Cases $n = 4, \geq 5$ are harder. This theorem really encompasses a lot of stuff... refer to HW.]

Hilbert symbol, revisited. $(a,b) = \begin{cases} +1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a non-trivial sol'n.} \\ -1 & \text{otherwise.} \end{cases}$

$a, b \in K^\times$

- $(\ ,\ ): K^\times/_{sqs} \times K^\times/_{sqs} \longrightarrow \{\pm 1\}$
- $(1, a) = (a, -a) = (a, 1-a) = 1$ etc.

From now on, focus on $K = \mathbb{Q}_p$.

Bilinear: $(a, b_1 b_2) = (a, b_1)(a, b_2)$

Pf: Equivalently, for each $a \in \mathbb{Q}_p^\times$, the map $\mathbb{Q}_p^\times \longrightarrow \{\pm 1\}$, $b \longmapsto (a,b)$ is a homomorphism. Clear if a is a square, so assume not. Let $H_a = \{ b \in \mathbb{Q}_p^\times \mid (a,b) = 1 \}$ [If all is well, this is a subgp of index 2.] First, H_a is a subgp as $H_a = N_{L/\mathbb{Q}_p}(L)$ where $L = \mathbb{Q}(\sqrt{a})$.

Case p odd: ($p = 2$ omitted)

Claim: $(\mathbb{Q}_p^\times)^2 \subsetneq H_a \subsetneq \mathbb{Q}_p^\times$

If so, then as $[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2] = 4$ we have $[\mathbb{Q}^\times : H_a] = 2$, which forces $b \mapsto (a,b)$ to be a homomorphism, as desired.

<u>Pf of Claim</u>:

<u>$(\mathbb{Q}_p^\times)^2 \subsetneq H_a$</u>: $-a \in H_a$, so if $-a \notin (\mathbb{Q}_p^\times)^2$ we're done. If $-a$ is a square, then $z^2 - ax^2 - by^2 \sim z^2 + x^2 - by^2$. Pick $b \in \mathbb{Z}$ a non-sq mod p, and hence $b \notin (\mathbb{Q}_p^\times)^2$. Now $z^2 + x^2 = b$ has a sol'n in $\mathbb{F}_p$ and hence $\mathbb{Z}_p$ (like HW). So $b \in H_a \setminus (\mathbb{Q}_p^\times)^2$.

<u>$H_a \subsetneq \mathbb{Q}_p^\times$</u>: Really only 3 choices for a, namely $\varepsilon, p, \varepsilon p$ where $\varepsilon \in \mathbb{Z}_p^\times \setminus (\mathbb{Z}_p^\times)^2$.
If $a = \varepsilon$, then $p \notin H_a$ as

$z^2 - \varepsilon x^2 - py^2 = 0$ has a sol'n $/\mathbb{Q}_p$
$\Rightarrow$ has a sol'n over $\mathbb{Z}_p \Rightarrow z^2 - \varepsilon x^2 = 0$ has a sol'n over $\mathbb{F}_p \Rightarrow \varepsilon \in \mathbb{F}_p^\times$

If $a = p$ or εp, then $\varepsilon \notin H_a$. $\blacksquare$

Computing (a,b) in general: $a = p^k \varepsilon \quad b = p^l \eta$ with $\varepsilon, \eta \in \mathbb{Z}_p^\times$. Now $(c,c) = (c,-c)(c,-1) = (c,-1)$.

Thus

$$(a,b) = (p^k, p^l)(p^k, \eta)(\varepsilon, p^l)(\varepsilon, \eta)$$
$$= (p,-1)^{kl}(p,\eta)^k (p,\varepsilon)^l (\varepsilon,\eta)$$

Thm: For $p \neq 2$, $(p,\varepsilon) = \left(\frac{\varepsilon}{p}\right)$ and $(\varepsilon,\eta) = 1$

$(2,\varepsilon) = (-1)^{(\varepsilon^2-1)/8} \quad (\varepsilon,\eta) = (-1)^{\left(\frac{\varepsilon-1}{2}\right)\left(\frac{\eta-1}{2}\right)}$

Pf: $(p,\varepsilon) = \left(\frac{\varepsilon}{p}\right)$ clear from above discussion.

$1 - \varepsilon X^2 - \eta y^2 = 0$ has a nontrivial sol'n over $\mathbb{F}_p$ and hence $\mathbb{Z}_p$.

Case $p=2$ omitted as always. To make sense of the statement, the exponents are in $\mathbb{Z}_2$ and so their residue class in $\mathbb{F}_2$ determines whether $(-1)^{\text{blah}} = 1$ or -1.

Hibert Product Formula: $a, b \in \mathbb{Q}^\times$. Then $(a,b)_v = 1$ for all but finitely many places v and $\prod_v (a,b)_v = 1$. [In other words, the # of v where $(a,b)_v = -1$ is even.]

Pf: The first part is clear since a and $b \in \mathbb{Z}_p^\times$ for almost all p. Since Hilbert symbols don't see squares, reduce to the case where a, b are squarefree integers, i.e. $a = \pm p_1 \cdots p_k$
$b = \pm q_1 \cdots p_l$

Bilinearity then reduces to the cases

$$(-1,-1), \; (p,-1), \; (p,q) \quad \text{distinct}$$

E.g. ⓐ $\prod_v (-1,-1)_v = (-1,-1)_\infty (-1,-1)_2 = (-1)(-1) = 1$

ⓑ p, q odd

$$\prod_v (p,q)_v = (p,q)_p (p,q)_q (p,q)_2$$
$$= \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = 1$$

$\blacksquare$

In fact, Hilbert's Prod. formula is equiv. to quad. reciprocity.

Note: $(\ ,\ )$ is bilinear on $\mathbb{Q}^\times$ as a consequence of Hasse-Minkowski.