Title: An Algebraic Proof of Quadratic Reciprocity
Speaker: Rob Noble
Date: October 17^{th}, 2006

Abstract: (Outline)

Definition (Legendre Symbol)**.** If p is an odd prime, and $a \in \mathbb{Z}$ is relatively prime to p, we define the Legendre symbol as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a square modulo } p \\ -1, & \text{if } a \text{ is not a square modulo } p \end{cases}$$

Theorem (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

Proof. (Sketch) The proof is facilitated by the following diagram:

$$\begin{array}{ccccc} \mathbb{Q}(\zeta_q) & \longleftrightarrow & \{id\} & \cong & \{1\} \\ \cup & & \cap & & \cap \\ \mathbb{Q}(\sqrt{q^*}) & \longleftrightarrow & H & \cong & \left(\mathbb{F}_q^*\right)^2 \\ \cup & & \cap & & \cap \\ \mathbb{Q} & \longleftrightarrow & G & \cong & \mathbb{F}_q^* \end{array}$$

Here ζ_q is a primitive q^{th} root of unity, $G = Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, $H \leq G$ is the unique subgroup of G of index 2, and $q^* = (-1)^{\frac{q-1}{2}}q$. The Frobenius automorphism of p in $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ restricts to an element of $Gal(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$ which can be shown to correspond to both $\left(\frac{p}{q}\right)$ and $\left(\frac{q^*}{p}\right)$ modulo q. We therefore have

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right),$$

which proves the desired law of reciprocity once we apply Euler's criterion to evaluate $\left(\frac{-1}{p}\right)$. $\square$

Remarks:

- There are many many proofs! (http://www.rzuser.uni-heidelberg.de/ hb3/fchrono.html lists references for 221 different proofs)
- This theorem forms the basis for class field theory
- Reference: [Sam70] § 6.5.

References

[Sam70] Pierre Samuel, *Algebraic theory of numbers*, Hermann, Paris, 1970.