CS681	**Computational Number Theory**

Lecture 19: Quadratic Reciprocity (contd.)

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Overview

Last class we proved one part of the Quadratic Reciprocity Theorem. We shall first finish the proof of the other part and then get to a generalization of the Legendre symbol - the Jacobi symbol.

1 Proof of Reciprocity Theorem (contd.)

Recall the statement of the theorem. If $p \neq q$ are odd primes, then

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

The idea of the proof is just the same. We choses $\tau = 1 + i$ last time and we got a $2^{\frac{p-1}{2}}$ term while computing τ^p. It would be the same here as well.

Let ζ be a principle q-th root of unity. We shall work with the field $\mathbb{F}_p(\zeta)$. Let

$$\tau = \sum_{a \in \mathbb{F}_q^\star} \left(\frac{a}{q}\right) \zeta^a$$

Just as before, we compute τ^2.

$$\begin{aligned}
\tau^2 &= \left(\sum_{a \in \mathbb{F}_q^\star} \left(\frac{a}{q}\right) \zeta^a\right)\left(\sum_{b \in \mathbb{F}_q^\star} \left(\frac{b}{q}\right) \zeta^b\right) \\
&= \sum_{a,b \in \mathbb{F}_q^\star} \left(\frac{a}{q}\right)\left(\frac{b}{q}\right) \zeta^{a+b} \\
&= \sum_{a,b \in \mathbb{F}_q^\star} \left(\frac{a}{q}\right)\left(\frac{b^{-1}}{q}\right) \zeta^{a+b} \\
&= \sum_{a,b \in \mathbb{F}_q^\star} \left(\frac{ab^{-1}}{q}\right) \zeta^{a+b}
\end{aligned}$$

Let us do a change of variable, by putting $c = ab^{-1}$

$$\begin{aligned}\tau^2 &= \sum_{c,b\in\mathbb{F}_q^\star}\left(\frac{c}{q}\right)\zeta^{bc+b}\\ &= \sum_{-1\neq c\in\mathbb{F}_q^\star}\left(\frac{c}{q}\right)\sum_{b\in\mathbb{F}_q^\star}(\zeta^{c+1})^b + \sum_{b\in\mathbb{F}_q^\star}\left(\frac{-1}{q}\right)\end{aligned}$$

Since both p and q are primes and $-1 \neq c \in \mathbb{F}_q^\star$, ζ^{c+1} is also a principle q-th root of unity. And therefore, $\sum_b(\zeta^{c+1})^b = -1$. Therefore,

$$\tau^2 = \sum_{-1\neq c\in\mathbb{F}_q^\star}\left(\frac{c}{q}\right) + (q-1)\left(\frac{-1}{q}\right)$$

Look at the first term. If one were to sum over all elements of $\mathbb{F}_q^\star$, then half of the $\left(\frac{c}{q}\right)$ would be 1 and the other would be -1 thus fully cancelling off. Since we are just excluding $c = -1$, the first term is just $\left(\frac{-1}{q}\right)$.

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

Now to evaluate τ^p.

$$\begin{aligned}\tau^p &= \sum_{a\in\mathbb{F}_q^\star}\left(\frac{a}{q}\right)\zeta^{ap}\\ &= \sum_{c\in\mathbb{F}_q^\star}\left(\frac{cp^{-1}}{q}\right)\zeta^c \qquad (c = ap)\\ &= \left(\frac{p^{-1}}{q}\right)\sum_{c\in\mathbb{F}_q^\star}\left(\frac{c}{q}\right)\zeta^c\\ &= \left(\frac{p}{q}\right)\tau\\ \tau^p &= \tau(\tau^2)^{\frac{p-1}{2}}\\ \implies \left(\frac{p}{q}\right)\tau &= \tau q^{\frac{p-1}{2}}\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\\ &= \tau\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\\ \implies \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad \square\end{aligned}$$

2 Jacobi Symbol

The legendre symbol $\left(\frac{m}{n}\right)$ can be naturally generalized to the case when m and n are odd and coprime numbers.

Definition 1. *Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Then the Jacobi symbol, also represented as $\left(\frac{m}{n}\right)$, is defined as follows*

$$\left(\frac{m}{n}\right) = \begin{cases} 0 & \text{if } (m,n) \neq 1 \\ \prod_{i=1}^{k} \left(\frac{m}{p_i}\right)^{\alpha_i} & \text{otherwise} \end{cases}$$

The Jacobi symbol also satisfies some nice multiplicative properties

- $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$
- $\left(\frac{m}{n_1 n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right)$

Using the above properties, we can get a generalize the theorem on the legendre symbol as well.

Theorem 1. *If m, n are odd numbers such that $(m,n) = 1$, then*

$$\begin{aligned} \left(\frac{2}{n}\right) &= (-1)^{\frac{n^2-1}{8}} \\ \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \end{aligned}$$

We shall prove this theorem in the next class. The proof will just be using induction on the factors of m and n.

WARNING: Please note that the Jacobi symbol $\left(\frac{m}{n}\right)$ doesn't say anything about whether or not m is a square modulo n. For example, if $n = p_1 p_2$ and m was chosen such that m is not a square modulo p_1 or p_2. Then the Jacobi symbol $\left(\frac{m}{p_1 p_2}\right) = (-1)(-1) = 1$ but m is not a square in $p_1 p_2$.