Math 115. Slides from the Lecture of October 29 (corrected)

This handout contains the slides from the lecture of October 29.

It has been updated to reflect the following corrections (relative to the version handed out in class):

- The date was corrected from October 24 to October 29.
- In the definition of Jacobi symbol, $\left(\frac{P}{Q}\right)$ should have been $\left(\frac{a}{Q}\right)$ in three places.
- In the definition of Jacobi symbol, a (the number on top) is not required to be odd.
- The property $\left(\frac{P}{Q_1Q_2}\right) = \left(\frac{P}{Q_1}\right)\left(\frac{P}{Q_2}\right)$ was added to the list of properties of the Jacobi symbol (alongside the property $\left(\frac{P_1P_2}{Q}\right) = \left(\frac{P_1}{Q}\right)\left(\frac{P_2}{Q}\right)$).
- Corrected two missing right brackets in the list of properties of the Jacobi symbol.

An Example of Quadratic Reciprocity

Example. For which primes p (including $p = 2$) is 7 a quadratic residue modulo p?

Special cases: $p = 2$: yes, $p = 7$: no (by definition).

For all other p: $$\left(\frac{7}{p}\right) = \begin{cases} \left(\frac{p}{7}\right) & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{7}\right) & \text{if } p \equiv -1 \pmod 4\ . \end{cases}$$

$$\text{Therefore } \left(\frac{7}{p}\right) = 1 \iff \begin{cases} \left(\frac{p}{7}\right) = 1 & \text{if } p \equiv 1 \pmod 4 \\ \left(\frac{p}{7}\right) = -1 & \text{if } p \equiv -1 \pmod 4\ . \end{cases}$$

$$\iff \begin{cases} p \equiv 1, 2, 4 \pmod 7 & \text{if } p \equiv 1 \pmod 4 \\ p \equiv 3, 5, 6 \pmod 7 & \text{if } p \equiv -1 \pmod 4\ . \end{cases}$$

$$\iff \begin{cases} p \equiv 1, 9, 25 \pmod{28} & \text{or} \\ p \equiv 3, 19, 27 \pmod{28}\ . \end{cases}$$

So 7 is a quadratic residue modulo p if and only if:

$$p = 2 \text{ or } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$$

or (equivalently) $p = 2$ or $p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$.

Theorem 3.5 (see the book) gives another way, but I think that this way is easier.

§ 3.3. Jacobi Symbols

Definition. Let Q be an odd positive integer, with prime factorization $Q = q_1 \cdots q_s$ (with q_i prime for all i, repeated as necessary). Then for all $a \in \mathbb{Z}$, the **Jacobi Symbol** $\left(\frac{a}{Q}\right)$ is defined by

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q_1}\right) \cdots \left(\frac{a}{q_s}\right)$$

(where $\left(\frac{a}{Q}\right)$ is a Jacobi symbol and $\left(\frac{a}{q_1}\right), \dots, \left(\frac{a}{q_s}\right)$ are Legendre symbols).

Note: When Q is prime, the Jacobi and Legendre symbols $\left(\frac{a}{Q}\right)$ are equal, so it's OK to use the same notation.

Basics about Jacobi symbols: Let $P, P_1, P_2, Q, Q_1, Q_2 \in \mathbb{Z}$ with Q, Q_1, Q_2 odd and positive. Then:

- $\left(\frac{P}{Q}\right) \in \{-1, 0, 1\}$
- $\left(\frac{P}{Q}\right) \neq 0 \iff \gcd(P, Q) = 1$
- If P is a quadratic residue modulo Q, then $\left(\frac{P}{Q}\right) = 1$. [*Proof:* If $P \equiv x^2 \pmod{Q}$ and $\gcd(P, Q) = 1$ then $P \equiv x^2 \pmod{q_i}$ and $\gcd(P, q_i) = 1$ for all i, so $\left(\frac{P}{q_i}\right) = 1$ for all i.]
- The converse of the above is *false.*
  [*Example:* $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, but 2 is not a quadratic residue modulo 15, because it's not one mod 3.]
- $\left(\frac{P_1 P_2}{Q}\right) = \left(\frac{P_1}{Q}\right)\left(\frac{P_2}{Q}\right)$ and $\left(\frac{P}{Q_1 Q_2}\right) = \left(\frac{P}{Q_1}\right)\left(\frac{P}{Q_2}\right)$
- If $\gcd(P, Q) = 1$ then $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$.
- If $P_1 \equiv P_2 \pmod{Q}$ then $\left(\frac{P_1}{Q}\right) = \left(\frac{P_2}{Q}\right)$.
- $\left(\frac{a}{Q}\right) \equiv a^{\frac{Q-1}{2}} \pmod{Q}$ is *false.*
  [*Examples:* (1) $a = 2$, $Q = 15$;
  $\left(\frac{a}{Q}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ but $2^7 = 128 \equiv 8 \pmod{15}$;
  (2) $a = 2$, $Q = 9$: $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = (-1)^2 = 1$ but $2^4 = 16 \equiv 7 \pmod{9}$.]

Theorem (Quadratic Reciprocity for Jacobi Symbols, Thms. 3.7 and 3.8). *Let Q be an odd positive integer. Then:*

(a). $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$;

(b). $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$; *and*

(c). *if P is an odd positive integer, then*

$$\left(\frac{P}{Q}\right) = (-1)^{\left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right)} \left(\frac{Q}{P}\right).$$

Lemma 1. *For all odd integers* a *and* b*, we have*

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2} ;$$

therefore

$$(-1)^{\frac{ab-1}{2}} = (-1)^{\frac{a-1}{2}}(-1)^{\frac{b-1}{2}} .$$

Proof.

$$\begin{aligned}\frac{ab-1}{2} - \frac{a-1}{2} - \frac{b-1}{2} &= \frac{ab-a-b+1}{2} \\ &= \frac{(a-1)(b-1)}{2} = 2\left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right) ,\end{aligned}$$

and this is even because $\frac{a-1}{2}$ and $\frac{b-1}{2}$ are integers. □

Lemma 2. *For all odd integers* a *and* b*, we have*

$$\frac{(ab)^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod{2} ;$$

therefore

$$(-1)^{\frac{(ab)^2-1}{8}} = (-1)^{\frac{a^2-1}{8}}(-1)^{\frac{b^2-1}{8}} .$$

Proof.

$$\begin{aligned}\frac{(ab)^2-1}{8} - \frac{a^2-1}{8} - \frac{b^2-1}{8} &= \frac{a^2b^2-a^2-b^2+1}{8} \\ &= \frac{(a^2-1)(b^2-1)}{8} = 8\left(\frac{a^2-1}{8}\right)\left(\frac{b^2-1}{8}\right) ,\end{aligned}$$

and this is even because $\frac{a^2-1}{8}$ and $\frac{b^2-1}{8}$ are integers. □

Proof of the theorem. (a). Write $Q = q_1 \cdots q_s$ as before. Then

$$\left(\frac{-1}{Q}\right) = \prod \left(\frac{-1}{q_i}\right) = \prod (-1)^{\frac{q_i-1}{2}} = (-1)^{\frac{Q-1}{2}} .$$

(b). As above,

$$\left(\frac{2}{Q}\right) = \prod \left(\frac{2}{q_i}\right) = \prod (-1)^{\frac{q_i^2-1}{8}} = (-1)^{\frac{Q^2-1}{8}} .$$

(c). First note that if P and Q are not relatively prime, then the equation is true because $\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) = 0$, so both sides are zero.

Otherwise, write $P = p_1 \cdots p_r$ with p_i prime for all i (and also $Q = q_1 \cdots q_s$ as before).

Then we have

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}\left(\frac{q_j}{p_i}\right)$$
$$= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)$$
$$= (-1)^{\left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right)}\left(\frac{Q}{P}\right),$$

where the last step is true because, by repeated application of Lemma 1,

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right) = \left(\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\right)\left(\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right)\right)$$
$$\equiv \left(\frac{\prod_{i=1}^{r}p_i-1}{2}\right)\left(\frac{\prod_{j=1}^{s}q_j-1}{2}\right) \pmod 2$$
$$= \left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right),$$

$\square$