MAT 115B Number Theory	**Winter 2025**
	January 24, 2025

Lecture 8

Lecturer: Elena Fuchs *Scribe: Avery Li*

Lecture 7 Recap

Theorem 8.1. *Let p be an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, 2 is a quadratic residue mod p iff $p \equiv 1, 7 \pmod 8$, and is not when $p \equiv 3, 5 \pmod 8$.*

Lecture 8

Example 8.2. $p = 17$, $\left(\frac{2}{17}\right) = 1$ because $17 \equiv 1 \pmod 8$, $6^2 \equiv 2 \pmod 1 7$.

Proof of Theorem 8.1. We count the values of $2k > \frac{p}{2}$ iff $k > \frac{p}{4}$. There are $n = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ total k. Then, Gauss's lemma gives us that $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}$. Now, we want to show that $n = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = \frac{p^2-1}{8} \pmod 2$. We know that p can be $1, 3, 5, 7 \pmod 8$. We will consider 5, the other cases can be shown similarly. Suppose $p = 8k + 5$ for some $k \in \mathbb{Z}$. Then we have

$$\begin{aligned}
LHS &= \frac{8k+5-1}{2} - \lfloor \frac{8k+5}{4} \rfloor \\
&= 4k + 2 - \lfloor 2k + \frac{5}{4} \rfloor \\
&= 4k + 2 - 2k - 1 \\
&\equiv 1 \pmod 2 \\
RHS &= \frac{(8k+5)^2 - 1}{8} \\
&= \frac{64k^2 + 80k + 25 - 1}{8} \\
&= 8k^2 + 10k + 3 \\
&\equiv 1 \pmod 2 \\
\implies LHS &\equiv RHS \pmod 2.
\end{aligned}$$

□

Quadratic Reciprocity

Theorem 8.3 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes, then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

$$= \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Equivalently, $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$, *i.e.*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \textit{if } p \equiv 1 \pmod 4 \textit{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \textit{otherwise.} \end{cases}$$

How is this theorem useful?

Example 8.4. We can now switch large "denominators" to the numerator, and vice versa. $\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = \left(\frac{2}{3}\right)$ because $101 \equiv 1 \pmod 4$ and $101 \equiv 2 \pmod 3$.

Example 8.5. When is $\left(\frac{5}{p}\right) = 1$? We have that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by the theorem. $\left(\frac{p}{5}\right) = 1$ iff $p \equiv 1, 4 \pmod 5$ by observation, therefore, $\left(\frac{5}{p}\right) = 1$ iff $p \equiv 1, 4 \pmod 5$.

Example 8.6. When is $\left(\frac{3}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = -1$? We have that $p = 2$ works. if p is odd, $p \neq 3$. Then, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ iff $p \equiv 1 \pmod 4$. We have that $\left(\frac{3}{p}\right) = 1$ iff $p \equiv 1 \pmod 3$, so $\left(\frac{3}{p}\right) = 1$ iff $p \equiv 1 \pmod{12}$ by Chinese remainder theorem. This can be computed similarly for $\left(\frac{3}{p}\right) = -1$ to get $p \equiv 11 \pmod{12}$.

Remark 8.7. Note that 8.3 does not work for $p = 2$.

Example 8.8. *Compute* $\left(\frac{-57}{103}\right)$.

$$\begin{aligned}
\left(\frac{-57}{103}\right) &= \left(\frac{-1}{103}\right)\left(\frac{3}{103}\right)\left(\frac{19}{103}\right) \\
&= -1 \cdot -\left(\frac{103}{3}\right) \cdot -\left(\frac{103}{19}\right) && 8.3 \\
&= -1 \cdot \left(\frac{1}{3}\right) \cdot \left(\frac{8}{19}\right) && \text{By LOGIC (using mod)} \\
&= -1 \cdot 1 \cdot \left(\frac{2}{19}\right)^3 && \text{Properties of legendre symbol} \\
&= -1 \cdot \left(\frac{2}{19}\right)^3 \\
&= -1 \cdot -1 && 8.1 \\
&= 1.
\end{aligned}$$