Lecture 7

Lecturer: Elena Fuchs *Scribe: Avery Li*

Fact 7.1. *The product of two quadratic residues is a quadratic residue and the product of two quadratic non-residues is a quadratic residue.*

Fact 7.2. *We have that -1 is a quadratic residue mod p when $p \equiv 1 \mod 4$.*

Example 7.3. $p = 11$, quadratic residues are $1, 3, 4, 5, 9$. Look at $a, 2a, 3a, \dots \frac{p-1}{2}a \mod p$

a	1	2	3	4	5	6	7	8	9	10	11
1	*	*	*	*	*						
2		*		*		*		*		*	
3			*	*		*	*		*		
4	*			*	*			*	*		
5	*	*				*	*	*			
6	*	*				*	*	*			
7		*	*			*	*			*	
8		*			*		*	*		*	
9	*		*		*		*		*		
10					*	*	*	*	*	*	

We'll now count how many how many dots are past the middle line.

Lemma 7.4. *Let p be an odd prime, let $p \not| a$. Let $n = |\{\frac{p+1}{2} \le x \le p-1 | k \equiv ka \mod p$ for some $1 \le k \le \frac{p-1}{2}\}|$. Then $\left(\frac{a}{p}\right) = (-1)^n$.*

Proof. Let $r_1, r_2, \dots, r_n$ be the x's that we count above. Let $s_1, s_2, \dots, s_m$ be the other $ka \mod p$. Compare $\{p - r_1, p - r_2, \dots, p - r_n, s_1 s_2, \dots, s_m\}$ to $\{1, 2, \dots, \frac{p-1}{2}\}$, we will show that these are in fact the same sets. If they are the same, then

$$
\begin{aligned}
&(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_m && = \left(\frac{p-1}{2}\right)! \\
&\equiv (-r_1)(-r_2) \cdots (-r_n) s_1 s_2 \cdots s_m \mod p && \\
&\equiv (-1)^n r_1 \cdot r_2 \cdots r_n s_1 s_2 \cdots s_m \mod p && \\
&\equiv (-1)^n a \cdot 2a \cdot 3a \cdots \frac{p-1}{2} a && \equiv \left(\frac{p-1}{2}\right)! \\
&\equiv (-1)^n a^{\frac{p-1}{2}} && \equiv 1 \mod p \\
&\equiv (-1)^n \left(\frac{a}{p}\right) && \equiv 1 \mod p \\
&\equiv \left(\frac{a}{p}\right) && \equiv (-1)^n \mod p
\end{aligned}
$$

Now we need to show that these sets are in fact the same. Note that each of the differences $p - r_i \leq \frac{p-1}{2}$, then $\{p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m\} \subseteq \{1, 2, \ldots, \frac{p-1}{2}\}$. Assume towards a contradiction that $r_i = s_j$ for some i, j. Then

$$\begin{aligned}
&p - r + i \equiv s_j \mod p \\
&\Rightarrow -r_i \equiv s_j \mod p \\
&\Rightarrow r_i + s_j \equiv 0 \mod p \\
&\Rightarrow p | r_i + s_j \equiv ka + la = (k + l)a
\end{aligned}$$

Then, because $k, \ell \leq \frac{p-1}{2}$, we have that $k + l \leq p - 1$. so we have $p | (k + \ell)a \Rightarrow p | a$. This is a contradiction because we assumed that $p \not| a$. Therefore, $r_i \neq s_j$. Similarly, $p - r_i \neq p - r_j$ if $i \neq j$ because if this were true, then $p | r_i - r_j \Rightarrow p | sa - ta \Rightarrow p | (s - t)a \Rightarrow p | a$, which is a contradiction.

$\square$

Theorem 7.5. *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 if and only if $p \equiv 1, 7 \mod 8$.*