NT Notes 6

They're supposed to turn in some problems to me.

1. Find the quadratic residues of 3.

$0 \xrightarrow{x^2} 0$, $1 \xrightarrow{x^2} 1$, $2 \xrightarrow{x^2} 1$ so $\{0,1\}$ are them.

2. Find the quadratic residues of 19

$0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 16 \equiv -2 \equiv 17$, $5^2 \equiv 11$, ...

3. Find the value of $\left(\frac{j}{7}\right)$ for $j \in \{1,2,3,4,5,6\}$.

$$\left(\frac{j}{7}\right) = \begin{cases} 0 & \text{if } 7 \mid j \\ 1 & \text{if } j \text{ is a quad residue mod } 7 \\ -1 & \text{" nonresidue "} \end{cases}$$

4. Evaluate $\left(\frac{7}{11}\right)$ using Euler's criterion.

$\left(\frac{a}{p}\right) \equiv_p a^{\frac{1}{2}(p-1)}$ ← helpful

$$\left(\frac{7}{11}\right) = 7^{\frac{1}{2}(11-1)} = 7^5 = 7 \cdot (49)^2 \equiv_{11} 7 \cdot 5^2 \equiv_{11} 7 \cdot 3 \equiv_{11} -1$$

5. For ints a, b not divisible by p, show that either one, or all three of a, b, ab are quadratic residues of p.

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ Duh?!

Use Euler's criterion to prove $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv_4 1 \\ -1 & p \equiv_4 3 \end{cases}$

(do $p=2$ separately)

6. For prime p and quadratic residue a of p. Show that if $p \equiv_4 1$, then $-a$ is also a quadratic residue of p, whereas if $p \equiv_4 3$, then $-a$ is a nonresidue of p.

If $p \equiv_4 3$ then only $2 \mid p-1$, whereas $4 \mid p-1$ if $p \equiv_4 1$.

7. If p is odd prime and $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$.

$(a^2)^{\frac{1}{2}p-1} = a^{p-1} \equiv_p 1$ Fermat