SPRING 2025 MATH 540: QUIZ 8 SOLUTIONS

Name:

1. Find all odd primes primes $p \leq 37$ such that 5 is a square mod p. (3 points)

Solution. We first note that the only squares mod 5 are 1 and 4. Second, for any odd prime $p \leq 37$, we have $(\frac{5}{p}) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}}(\frac{p}{5}) = (\frac{p}{5})$.

Thus, $(\frac{3}{5}) = -1; (\frac{5}{5}) = 0; (\frac{7}{5}) = (\frac{2}{5}) = -1; (\frac{11}{5}) = (\frac{1}{5}) = 1; (\frac{13}{5}) = (\frac{3}{5}) = -1; (\frac{17}{5}) = (\frac{2}{5}) = -1; (\frac{19}{5}) = (\frac{4}{5}) = 1; (\frac{23}{5}) = (\frac{3}{5}) = -1; (\frac{29}{5}) = (\frac{4}{5}) = 1; (\frac{31}{5}) = (\frac{1}{5}) = 1; (\frac{37}{5}) = (\frac{2}{5}) = -1$.

Thus, 5 is a square mod: 11, 19, 29, 31.

2. Give an example to show that $(\frac{a}{n}) = 1$ need not imply that a is a quadratic residue mod n. Here $(\frac{a}{n})$ denotes the Jacobi symbol, $(\frac{a}{n}) := (\frac{a}{p_1})^{e_1} \cdots (\frac{a}{p_r})^{e_r}$, for $n = p_1^{e_1} \cdots p_r^{e_r}$. Be sure to provide all details. (3 points)

Solution. $(\frac{2}{15}) = (\frac{2}{3}) \cdot (\frac{2}{5}) = (-1) \cdot (-1) = 1$, but 2 is not a square mod 15. One can either verify this directly or use the fact that under the multiplicative map $\mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$ given by $\tilde{a} \to (\overline{a}, \hat{a})$, 2 is neither a square in $\mathbb{Z}_3$ nor $\mathbb{Z}_5$, so 2 is not a square mod 15.

3. Assuming $\gcd(a, n) = 1 = \gcd(b, n)$, prove the following properties of the Jacobi symbol:
(i) $(\frac{ab}{n}) = (\frac{a}{n}) \cdot (\frac{b}{n})$ and (ii) If $a \equiv b$ mod n, then $(\frac{a}{n}) = (\frac{b}{n})$. (4 points)

Solution. For (i), we use the property $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$, for the Legendre symbol $(\frac{c}{p})$, when p is prime. We have

$$\begin{aligned}
(\frac{ab}{n}) &= (\frac{ab}{p_1})^{e_1} \cdots (\frac{ab}{p_r})^{e_r} \\
&= \{(\frac{a}{p_1})(\frac{b}{p_1})\}^{e_1} \cdots \{(\frac{a}{p_r})(\frac{b}{p_r})\}^{e_r} \\
&= \{(\frac{a}{p_1})^{e_1}(\frac{b}{p_1})^{e_1}\} \cdots \{(\frac{a}{p_r})^{e_r}(\frac{b}{p_r})^{e_r}\} \\
&= \{(\frac{a}{p_1})^{e_1} \cdots (\frac{a}{p_r})^{e_r}\} \cdots \{(\frac{b}{p_1})^{e_1} \cdots (\frac{b}{p})^{e_r}\} \\
&= (\frac{a}{n})(\frac{b}{n}).
\end{aligned}$$

For (ii), we note that if $a \equiv b$ mod n, then $b = a + tn$, for some $t \in \mathbb{Z}$. Note that this shows $b \equiv a$ mod p_i, for each prime factor p_i of n. Thus, $(\frac{b}{n}) = (\frac{b}{p_i})^{e_1} \cdots (\frac{b}{p_r})^{e_r} = (\frac{a}{p_i})^{e_1} \cdots (\frac{a}{p_r})^{e_r} = (\frac{a}{n})$.