SPRING 2025 MATH 540: QUIZ 7 SOLUTIONS

Name:

1. State Euler's Quadratic Residue Theorem. (2 points)

Solution. For an odd prime p, and $a \in \mathbb{Z}$ such that $\gcd(a,p) = 1$, a is a quadratic residue mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

2. Find the roots of $p(x) = 3x^2 + 4x + 4 \bmod 11$. Check your answers. (4 points)

Solution. For $p(x)$, $a = 3, b = 4, c = 4$, if we want to apply the quadratic formula to $ax^2 + bx + c$. We need to check if $b^2 = 4ac$ is a square mod 11. In this case, $b^2 - 4ac = -32 \equiv 1 \bmod 11$, which is a square mod 11. Thus, 1, -1 are the square roots of 1 mod 11. In this case, 2a = 6, which has multiplicative inverse 2, mod 11. Thus, the roots of $p(x)$ mod 11 are: 2(-4+1) = -6 and 2(-4-1) = -10. Reducing modulo 11, the roots are 5 and 1.

To check:

$p(5) \equiv 3 \cdot 25 + 4 \cdot 5 + 4 \equiv 9 + 9 + 4 \equiv 22 \equiv 0 \bmod 11.$

$p(1) \equiv 3 + 4 + 4 \equiv 11 \equiv 0 \bmod 11.$

3. Use Quadratic Reciprocity to show that $(\frac{3}{p}) = \begin{cases} 1, & \text{if } p \equiv 1, 11 \bmod 12 \\ -1, & \text{if } p \equiv 5, 7 \bmod 12 \end{cases}$. (4 points)

Solution. Suppose $p = 12n + 1$. Then $(\frac{3}{12n+1}) = (-1)^{1 \cdot 6n}(\frac{12n+1}{3}) = (\frac{1}{3}) = 1$.

Suppose $p = 12n + 11$. Then $(\frac{3}{12n+11}) = (-1)^{1 \cdot (6n+5)}(\frac{12n+11}{3}) = -1 \cdot (\frac{11}{3}) = -1 \cdot (\frac{2}{3}) = (-1) \cdot (-1) = 1$, since 2 is not a square mod 3.

Suppose $p = 12n + 5$. Then $(\frac{3}{12n+5}) = (-1)^{1 \cdot (6n+2)}(\frac{12n+5}{3}) = 1 \cdot (\frac{5}{3}) = 1 \cdot (\frac{2}{3}) = 1 \cdot (-1) = -1$

Suppose $p = 12n + 7$. Then $(\frac{3}{12n+7}) = (-1)^{1 \cdot (6n+3)}(\frac{12n+7}{3}) = (-1) \cdot (\frac{7}{3}) = (-1) \cdot (\frac{1}{3}) = (-1) \cdot 1 = -1$