MATH 465 NUMBER THEORY, SPRING 2025, SOLUTIONS 08

1. Evaluate the following Legendre symbols.

$$\text{(i)} \quad \left(\frac{2}{127}\right)_L, \quad \text{(ii)} \quad \left(\frac{-1}{127}\right)_L, \quad \text{(iii)} \quad \left(\frac{5}{127}\right)_L, \quad \text{(iv)} \quad \left(\frac{11}{127}\right)_L.$$

(i) $127 \equiv 7 \pmod 8$, so 2 is a QR modulo 127. (ii) $127 \equiv 3 \pmod 4$, so -1 is a QNR modulo 127. (iii) $5 \equiv 1 \pmod 4$ so, by law of QR, $\left(\frac{5}{127}\right)_L = \left(\frac{127}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1$. (iv) $11 \equiv 127 \equiv 3 \pmod 4$ so, by law of QR, $\left(\frac{11}{127}\right)_L = -\left(\frac{127}{11}\right)_L = -\left(\frac{6}{11}\right)_L = 1$.

2. Given that 5003 is prime, determine the solubility of $x^2 \equiv 2021 \pmod{5003}$.

$$\left(\frac{2021}{5003}\right)_L = \left(\frac{5003}{2021}\right)_J = \left(\frac{961}{2021}\right)_J.$$

Now $961 = 31^2$ is a perfect square so $\left(\frac{2021}{5003}\right)_L = 1$.

3. (i) Prove that 3 is a QR modulo p when $p \equiv \pm 1 \pmod{12}$ and is a QNR when $p \equiv \pm 5 \pmod{12}$. (ii) Prove that -3 is a QR modulo p for primes p with $p \equiv 1 \pmod 6$ and is a QNR for primes $p \equiv -1 \pmod 6$. (iii) By considering $4x^2 + 3$ show that there are infinitely many primes in the residue class $1 \pmod 6$.

(i) By law of QR, $\left(\frac{3}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)_L$. The Legendre symbol here is $\left(\frac{1}{3}\right)_L = 1$ when $p \equiv 1$ or $7 \pmod{12}$ and is -1 otherwise. The desired conclusion follows. (ii) From (i) $\left(\frac{-3}{p}\right)_L = \left(\frac{-1}{p}\right)_L \left(\frac{3}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right)_L = \left(\frac{p}{3}\right)_L$ and this is 1 when $p \equiv 1 \pmod 3$ and -1 otherwise. (iii) Suppose there are only a finite number of such primes, say $p_1, \ldots, p_n$ and let $x = p_1 \ldots p_n$. Since $x > 0$ and $3 \nmid x$ there is a prime p such that $p | 4x^2 + 3$ and $p > 3$. Hence -3 is a QR modulo p and so by (ii) $p \equiv 1 \pmod 3$. Thus $p | x$ and $p | 3 = (4x^2 + 3) - 4x^2$ which is impossible.

4. Show that for every prime p the congruence $x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \pmod p$ is always soluble.

We have $x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$. If $p = 2$ or 3 we may take $x = p$. Suppose $p > 3$. If either 2 or 3 is a QR modulo p, then we are done. If they are both QNR, then 6 is a QR and we are done once more.

5. Decide the solubility of (i) $x^2 \equiv 219 \pmod{383}$, (ii) $x^2 \equiv 226 \pmod{562}$, (iii) $x^2 \equiv 429 \pmod{563}$, (iv) $x^2 \equiv 105 \pmod{317}$.

(i) $\left(\frac{219}{383}\right)_J = 1$ and 383 is prime, (ii) This is equivalent to $2y^2 \equiv 113 \pmod{281}$ and so $z^2 \equiv 226 \pmod{281}$, and $\left(\frac{226}{281}\right)_J = -1$. (iii) $\left(\frac{429}{563}\right)_J = 1$ and 563 is prime. (iv) $\left(\frac{105}{317}\right)_J = 1$ and 317 is prime.