MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2025, PROBLEMS 9

To be submitted by Monday 27th October

1. Evaluate the following Legendre symbols.

(i) $\left(\frac{2}{127}\right)_L$,

(ii) $\left(\frac{-1}{127}\right)_L$,

(iii) $\left(\frac{5}{127}\right)_L$,

(iv) $\left(\frac{11}{127}\right)_L$.

2. (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 $1 \pmod 6$.

3. Prove that if n is odd and $p|n$, then

$$\sum_{\substack{m=1 \\ (m,n)=1}}^{n} \left(\frac{m}{p}\right)_L = 0.$$

4A. Show that for every prime p the congruence

$$x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \pmod p$$

is always soluble.

4B. Find the number of solutions of the congruence (i) $x^2 \equiv 226 \pmod{563}$, (ii) $x^2 \equiv 429 \pmod{563}$.

5. Show that $(x^2 - 2)/(2y^2 + 3)$ is never an integer when x and y are integers.