MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2024, PROBLEMS 8

Return by Monday 21st October

1. Evaluate the following Legendre symbols.

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

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. (i) Prove that if p is an odd prime $a, b \in \mathbb{Z}$ and $(a, p) = 1$, then

$$\sum_{n=1}^{p} \left(\frac{an+b}{p}\right)_L = 0.$$

(ii) Prove that if p is an odd prime, then $\displaystyle\sum_{r=1}^{p-1} \left(\frac{r(r+1)}{p}\right)_L = \sum_{s=1}^{p-1} \left(\frac{1+s}{p}\right)_L = -1.$

Hint: Observe that for every reduced residue class r modulo p there is a unique reduced residue class s_r modulo p such that $rs_r \equiv 1 \pmod p$, and that for every reduced residue class s modulo p one has $s_r \equiv s \pmod p$ for some r.

(iii) Prove that if p is an odd prime, then the number of residues r modulo p for which both r and $r+1$ are quadratic residues is $\dfrac{p - (-1)^{\frac{p-1}{2}}}{4} - 1$. Note that with our definitions 0 is neither a quadratic residue nor a quadratic non–residue.

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

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

5. Write computer programs to implement **LJ** and **QC**, and use them to evaluate the Legendre symbols

$$\left(\frac{a}{p}\right)_L$$

when $a = 40000000003$ and $a = 400000000031$, and $p = 100000000019$ and $p = 100000000057$, and when it is 1 to solve $x^2 \equiv a \pmod p$.