

MATH 465 NUMBER THEORY, SPRING 2009, PROBLEMS 13

Return by Monday 20th April

1. Evaluate the following Legendre symbols.

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

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. Show that for every prime p the congruence

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

is always soluble.

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