MATH 465 NUMBER THEORY, SPRING TERM 2025, PRACTICE EXAM 3, SOLUTIONS

Note: Mid-term Exam 3 will be 1:25 on Wednesday 9th April in room 216 Thomas.

1. Evaluate the following Legendre symbols, showing your working (i) $\left(\frac{-1}{103}\right)_L$, (ii) $\left(\frac{2}{103}\right)_L$, (iii) $\left(\frac{7}{103}\right)_L$.

(i) We have $\left(\frac{-1}{103}\right)_L = (-1)^{(102)/2} = -1$ by Euler's criterion. (ii) $\left(\frac{2}{103}\right)_L$. $103 \equiv 7 \pmod 8$, so $(103^2-1)/8$ is even and $\left(\frac{2}{103}\right)_L = 1$. (iii) By the law of quadratic reciprocity $\left(\frac{7}{103}\right)_L = -\left(\frac{103}{7}\right)_L = -\left(\frac{5}{7}\right)_L = -\left(\frac{7}{5}\right)_L = -\left(\frac{2}{5}\right)_L = +1$.

2. Given that 4999 is prime, determine the number of solutions of the congruence $x^2 \equiv 2021 \pmod{4999}$.

We have
$\left(\frac{2021}{4999}\right)_L = \left(\frac{4999}{2021}\right)_J = \left(\frac{957}{2021}\right)_J = \left(\frac{2021}{957}\right)_J = \left(\frac{107}{957}\right)_J$
$= \left(\frac{957}{107}\right)_J = \left(\frac{101}{107}\right)_J = \left(\frac{107}{101}\right)_J = \left(\frac{6}{101}\right)_J$
$= \left(\frac{2}{101}\right)_L \left(\frac{3}{101}\right)_L = -\left(\frac{101}{3}\right)_L = -\left(\frac{2}{3}\right)_L = +1.$
Hence the congruence has two solutions.

3. Suppose that $p \equiv 1 \pmod 6$. (i) Prove that the congruence $z^2 \equiv -3 \pmod p$ is soluble in z. (ii) Prove that there is an m with $m = 1$, 2 or 3 such that $x^2 + 3y^2 = mp$ is soluble in integers x and y. (iii) Deduce that there are integers x and y such that $x^2 + 3y^2 = p$.

(i) We have $\left(\frac{-3}{p}\right)_L = (-1)^{(p-1)/2}\left(\frac{3}{p}\right)_L = (-1)^{2(p-1)/2}\left(\frac{p}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1$. (ii) Choose a solution z to $z^2 \equiv -3 \pmod p$. Consider the $(1 + \lfloor\sqrt{p}\rfloor)^2 > p$ numbers $x + zy$ with $0 \le x < \sqrt{p}$, $0 \le y < \sqrt{p}$. Then at least one of the residue classes r modulo p contains at least two of these numbers, say $x_1 + zy_1$, $x_2 + zy_2$. Let $x = x_2 - x_1$, $y = y_2 - y_1$. Then $x + zy \equiv 0 \pmod p$ but $xy \not\equiv 0 \pmod p$ since the pairs x_1, y_1 and x_2, y_2 are different. Thus $x^2 + 3y^2 \equiv (-zy)2 + 3y^2 = y^2(z^2 + 3) \equiv 0 \pmod p$. Moreover $x^2 + 3y^2 < 4p$. Hence $x^2 + 3y^2 = mp$ with $m = 1$, 2 or 3. (iii) In (ii), if $m = 3$, then $3|x^2$ so $3|x$, and then $3(x/3)^2 + y^2 = p$ and we are done. If $m = 2$, then x and y are both even or both odd. But they cannot both be even, since then $4|2p$ which is impossible. If both are odd, then $x^2 + 3y^2 \equiv 1 + 3 = 4 \pmod 8$ and so we would again have $4|2p$.

4. Prove that for every positive integer n, $\sum_{m|n} \mu(m)d(m) = (-1)^{\omega(n)}$ where $\omega(n)$ is the number of different prime factors of n.

μ and d are multiplicative. Hence, so is $f(n) = \sum_{m|n} \mu(m)d(m) = (-1)^{\omega(n)}$. The for any prime p and positive integer k, $f(p^k) = 1 - d(p) = 1 - 2 = -1$.