MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2025, PROBLEMS 7

Return by Monday 13th October

1. Suppose that $a_1, \dots, a_k$ are non-zero integers and define the least common multiple, $\text{lcm}[a_1, \dots, a_k]$ of $a_1, \dots a_k$ to be the smallest positive integer ℓ such that $a_j | \ell$ for all j with $1 \le j \le k$. Suppose further that b is a positive integer such that $a_j | b$ for all j with $1 \le j \le k$.

(i) Prove that $\text{lcm}[a_1, \dots, a_k] | b$.

(ii) For each positive integer m the Carmichael function $\lambda(m)$ is defined to be the smallest positive number such that for every a with $(a, m) = 1$ and $1 \le a \le m$ we have $\text{ord}_m(a) | \lambda(m)$. Prove that $\lambda(m) | \phi(m)$.

2. Suppose that $k \in \mathbb{N}$. Prove that

$$1^k + 2^k + \cdots + (p-1)^k \equiv \left\{ \begin{array}{ll} 0 & \text{when } p-1 \nmid k, \\ -1 & \text{when } p-1 | k, \end{array} \right\} \pmod{p}$$

3. Prove that for any prime number $p \ne 3$ the product of its primitive roots lies in the residue class 1 modulo p.

4. Suppose that p is an odd prime and g is a primitive root modulo p. Prove that the conruence $x^2 \equiv g \pmod{p}$ is insoluble.

5. Find a complete set of quadratic residues r modulo 23 in the range $1 \le r \le 22$.