MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2024, SOLUTIONS 7

1. Suppose that $a_1, \dots, a_k$ are non-zero integers and define the least common multiple, $\text{lcm}[a_1, \dots, l_k]$ 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 $\text{ord}_a(m)|\lambda(m)$. Prove that $\lambda(m)|\phi(m)$.

(i) For a given prime p, let $p^{r_j(p)}$ be the exact power of p dividing a_j. Then $\ell = \prod_p p^{\max_j r_j(p)}$, and for every prime p we also have $p^{\max_j r_j(p)}|b$. Hence $\ell|b$. (ii) We proved in class that for every a with $(a, m) = 1$ we have $\text{ord}_a(m)|\phi(m)$. Then the conclusion follows from (i) with $\ell = \lambda(m)$.

2. Suppose that $k \in \mathbb{N}$. Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 & \text{when } p-1 \nmid k, \\ -1 & \text{when } p-1|k. \end{cases}$

Let g be a primitive root modulo p. Then the residue classes g^h with $0 \le h \le p-2$ are a permutation of the reduced residue classes modulo p. Thus the sum in question is $\equiv (g^k)^0 + (g^k)^1 + \cdots + (g^k)^{p-2}$. When $p-1|k$ this is $\equiv p-1 \equiv -1 \pmod p$. When $p-1 \nmid k$, so that $g^k \not\equiv 1 \pmod p$ we have $(g^k-1)\big((g^k)^0 + (g^k)^1 + \cdots + (g^k)^{p-2}\big) = (g^k)^{p-1} - 1 \equiv 0 \pmod p$.

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

The case $p = 2$ is easy. When $p \ge 5$, so that $\phi(p) = p - 1 \ge 4$ the number of primitive roots modulo p, $\phi\big(\phi(p)\big) = \phi(p-1)$ is even. Moreover g is a primitive root modulo p iff and only if g^{-1} is, and $g^2 \not\equiv 1 \pmod p$. Thus the primitive roots can be paired off into $\phi(p-1)/2$ pairs g and g^{-1}.

4. Suppose that p is an odd prime and g is a primitive root modulo p. Prove that g is a quadratic non-residue modulo p.

If g were to be a quadratic residue there would be an x with $p \nmid x$ so that $x^2 \equiv g \pmod p$ and then $g^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod p$ contradicting the definition of primitive root.

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

$1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$.