Homework 10
due on Wednesday, March 14

Solve the following problems.

Problem 1. Suppose that $m_1, m_2, \ldots m_k$ are positive integers such that a primitive root modulo m_i exists for each i. Prove that there is an integer a which is a primitive root modulo m_i for every i. Hint: Chinese Remainder Theorem should be useful.

Problem 2. Suppose that $p < q$ are odd prime numbers. Prove that pq is not a Carmicheal number. Hint: use a which is a primitive root modulo both p and q.

Problem 3. Let p be an odd prime number. Suppose a, b, c are integers and $p \nmid a$. Prove that the congruence $ax^2+bx+c \equiv 0 (\mod p)$ is solvable if and only if b^2-4ac is either congruent to 0 modulo p or it is a quadratic residue modulo p.

Problem 4. Prove that if a, b, c are non-zero integers then

$$\operatorname{lcm}(\gcd(a,b), \gcd(a,c)) = \gcd(a, \operatorname{lcm}(b,c).$$