Homework 10, solutions

Problem 1. Suppose that $m_1, m_2, \dots m_k$ 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.

Solution. We may assume that $m_1 = 4$ and $m_i = p_i^{k_i}$ or $m_i = 2p_i^{k_i}$ for some odd prime p_i for $i > 1$.

Recall that we proved that there is is a primitive root b modulo an odd prime p such that $p^2 \nmid (b^{p-1} - 1)$ and any such b is a primitive root modulo p^t for every positive integer t. Replacing b by $b + p^2$ if necessary, we may assume that b is odd and then b is also a primitive root modulo $2p^t$ for very $t > 0$. Choose any such b and call it a_p.

By the Chinese Remainder Theorem, we can find and integer a such that

$$a \equiv -1(\mod 4), \text{ and } a \equiv a_{p_i}(\mod p_i^2)$$

for $i = 2, 2 \dots k$. Then a is a primitive root modulo 4, p_i^t, $2p_i^t$ for every $t > 0$ and $i = 2, \dots k$. Thus a has the required proprty.

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.

Solution. By the first problem, there is an integer a which is a primitive root modulo p and a primitive root modulo q. In particular, a is relatively prime to pq. Suppose pq is a Carmichael number. Then $a^{pq} \equiv a(\mod pq)$ and therefore $a^{pq-1} \equiv 1(\mod pq)$ (since $\gcd(a, pq) = 1$). We may assume that $p < q$. Since $a^{pq-1} \equiv 1(\mod q)$ and the order of a modulo q is $q - 1$ we have $(q - 1)|(pq - 1)$. However, $pq - 1 = p(q - 1) + p - 1$, so $(q - 1)|(p - 1)$. This is howver impossible since $p < q$. The contradiction shows that pq is not a Carmichael number.

Remark. The suggestion in the hint is in fact unnecessary as in the above argument it suffices to choose a which is a primitive root modulo 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.

Solution. Since p is odd and $p \nmid a$, we have $\gcd(p, 4a) = 1$. Thus the congruence $ax^2 + bx + c \equiv 0(\mod p)$ is equivalent to the congruence $4a(ax^2 + bx + c) \equiv 0(\mod p)$. Note that

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$$

Thus, if x is a solution to our congruence then $y = 2ax + b$ satisfies

$$y^2 \equiv b^2 - 4ac(\mod p)$$

so $b^2 - 4ac$ is either divisible by p or a quadratic residue modulo p. Conversely, if $b^2 - 4ac$ is either divisible by p or a quadratic residue modulo p then the congruence $y^2 \equiv b^2 - 4ac(\mod p)$ has a solution y. The congruence $2ax + b \equiv y(\mod p)$ is also solvable (since $\gcd(2a, p) = 1$)) and any solution x satisfies our original congruence $ax^2 + bx + c \equiv 0(\mod p)$.

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

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

Solution. We will use the following simple fact: if u, w are positive integers then $u = w$ if and only if $e_p(u) = e_p(w)$ for every prime number p. Recall also, that if $e_p(u) = s$ and $e_p(w) = t$ then $e_p(\gcd(u, w)) = \min(s, t)$ and $e_p(\operatorname{lcm}(u, w)) = \max(s, t)$.

Let p be a prime number and let $e_p(a) = \alpha$, $e_p(b) = \beta$, $e_p(c) = \gamma$. We may assume that $\beta \leq \gamma$ (replacing the roles of b and c if necessary).

There are three case to consider:

1. case 1. $\alpha < \beta \leq \gamma$
2. case 2. $\beta \leq \alpha \leq \gamma$
3. case 3 $\beta \leq \gamma < \alpha$.

In case 1 we have $e_p(\gcd(a, b)) = \alpha$, $e_p(\gcd(a, c)) = \alpha$, $e_p(\operatorname{lcm}(b, c)) = \gamma$. Thus

$$e_p(\operatorname{lcm}(\gcd(a, b), \gcd(a, c))) = \alpha, \text{ and } e_p(\gcd(a, \operatorname{lcm}(b, c))) = \alpha.$$

In case 2 we have $e_p(\gcd(a,b)) = \beta$, $e_p(\gcd(a,c)) = \alpha$, $e_p(\operatorname{lcm}(b,c)) = \gamma$. Thus

$$e_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))) = \alpha, \text{ and } e_p(\gcd(a, \operatorname{lcm}(b,c))) = \alpha.$$

Finally, in case 3 we have $e_p(\gcd(a,b)) = \beta$, $e_p(\gcd(a,c)) = \gamma$, $e_p(\operatorname{lcm}(b,c)) = \gamma$. Thus

$$e_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))) = \gamma, \text{ and } e_p(\gcd(a, \operatorname{lcm}(b,c))) = \gamma.$$

In every case, we have

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

and therefore

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