Problem Set IV

1. If p, q are prime numbers such that Z_{pq}^* is cyclic, what are the possible values for p and q? ☐
2. Let p, q be odd prime numbers. Characterize all natural numbers which are roots of the equation $x^2 = 1 \mod p$ in terms of p and q using Chinese remainder theorem. ☐
3. Find all ideals in the ring $\mathbf{Z}_{30}$. For each ideal I, give an example for a ring homomorphism from $\mathbf{Z}_{30}$ (to any ring) which has I as the kernel. ☐
4. Let R be any ring. the characterisitic of the ring is defined as the least positive integer k such that $1 + 1 + \cdots + 1$ (k times) is zero. Show that the characterisitic of a finite field must be prime. Give an example for an infinite field whose characterisitic is not a prime. ☐
5. Consider the map $f : \mathbf{Z}_6 \times \mathbf{Z}_4 \mapsto \mathbf{Z}_{12}$ defined by $f(x, y) = x + y \mod 12$. Is f a ring homomorphism? If so, find the kernel, image and all cosets of the kernel. ☐
6. Consider the map $f : \mathbf{Z}_{12} \mapsto \mathbf{Z}_6 \times \mathbf{Z}_4$ defined by $f(x) = (x \mod 6, x \mod 4)$. Is f a ring homomorphism? If so, find the kernel, image and all cosets of the kernel. ☐
7. If m, n and postive numbers such that GCD$(m, n) \neq 1$. Show that the map $f : Z_{mn} \mapsto \mathbf{Z}_m \times \mathbf{Z}_n$ defined by $f(x) = (x \mod m, x \mod n)$ is a homomorphism, but not an isomorphism. Find the kernel and image of f. ☐
8. Find all generators of $\mathbf{Z}_{25}^*$. ☐
9. Find all $a \in \mathbf{Z}_{25}^*$ such that the Miller Rabin test with a chosen as the random test element returns composite. ☐
10. Let p, q be distinct odd prime numbers. Let $n = pq$. Let $p - 1$ divide $n - 1$, but $q - 1$ does not divide $n - 1$. Characterize all $a \in \mathbf{Z}_p^* \times \mathbf{Z}_q^*$ such that $a^{n-1} \equiv 1 \mod n$. ☐
11. Let p, q, r be prime numbers. Let g_1, g_2, g_3 be generators of $\mathbf{Z}_p^*, \mathbf{Z}_q^*$ and $\mathbf{Z}_r^*$ respectively. What will be the order of the element $(g_1, g_2, g_3) \in \mathbf{Z}_p^* \times \mathbf{Z}_q^* \times \mathbf{Z}_r^*$ (in terms of p, q and r)? ☐
12. Find all generators $g \in \mathbf{Z}_{11}^*$ that are not generators for $\mathbf{Z}_{121}^*$. ☐
13. Consider the homomorphism $f(x) = x \mod 6$ from $\mathbf{Z}_{24}$ to $\mathbf{Z}_6$. Let $a \in \mathbf{Z}_{24}$ and $b \in \mathbf{Z}_6$ satisfy $f(a) = b$. Characterize all solutions for $f(a) = b$. ☐
14. Let p be an odd prime. Let g be a generator of $\mathbf{Z}_{p^2}^*$. Show that g is a generator of $\mathbf{Z}_{p^3}^*$ as well. ☐
15. Show that a Carmichael number must have at least 3 distinct prime factors. ☐
16. Let α, β be non-zero distinct real numbers. Let $f(x) = a \mod (x - \alpha)$ and $f(x) = b \mod (x - \beta)$. Find the Chinese remainder theorem solution for $f(x)$ in terms of α, β and f. ☐
17. Using Chinese remainder theorem, find the polynomial $f(x)$ of minimum degree satisfying $f(x) = 1 \mod (x - 2)$, $f(x) = 2 \mod (x - 3)$ and $f(x) = 3 \mod (x - 4)$. ☐
18. If p is an odd prime such that $p^2 | n$, show that n is not a Carmichael number. ☐