NUMBER THEORY

MATH 480

Dr. Alia Hamieh

Assignment 4

Deepak Jassal

Due Date:

November 20^{th}, 2025

Question 1 [2 marks]

Find all the primitive roots modulo 27.

Question 2 [2 marks]

Evaluate $\left(\frac{105}{1009}\right)$.

Question 3 [3 marks]

Let m be a positive integer with a primitive root. Suppose that $(a, m) = 1$. Prove that then the congruence $x^n \equiv a \mod m$ has exactly $(n, \phi(m))$ solutions if and only if $a^{\frac{\phi(m)}{(\phi(m),n)}} \equiv 1 \mod m$.

Question 4 [3 marks]

Let p be an odd prime number, and suppose that $h \geq 2$. Denote by g a primitive root modulo p^h.

(a) List all the solutions of the congruence $x^p \equiv 1 \pmod{p^h}$ using the primitive root g modulo p^h.

(b) List all the solutions of the congruence $x^{2p} \equiv 1 \pmod{p^h}$ using the primitive root g modulo p^h.

Question 5 [2 marks]

Let n be a positive integer with a primitive root. Using this primitive root, prove that the product of all positive integers less than n and relatively prime to n is congruent to -1 modulo n.

Question 6 [2 marks]

Let $p_1, p_2, \ldots, p_r$ be distinct prime numbers. Show that there exists an integer g such that g is a primitive root modulo p_i for all $1 \leq i \leq r$.

Question 7 [2 marks]

(a) Let a be an integer with $a \geq 2$, and suppose that $q \in \mathbb{N}$. What is the smallest positive integer d satisfying the property that $a^d \equiv 1 \pmod{a^q - 1}$? Deduce that q divides $\varphi(a^q - 1)$.

(b) Let q be a prime number. By considering the prime factorisation of the integer $N = a^q - 1$, show that either N is divisible by q, or else N is divisible by a prime number p with $p \equiv 1 \pmod q$.

Question 8 [3 marks]

Let q be a prime number. Prove that there are infinitely many prime numbers p with $p \equiv 1 \pmod q$.

Question 9 [3 marks]

Let $p \geq 5$ be an odd prime, show that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } \ p \equiv \pm 1 \mod 12 \\ -1 & \text{if } \ p \equiv \pm 5 \mod 12. \end{cases}$$

Question 10 [6 marks]

Let $n > 1$ be an odd integer. Write $n = p_1^{e_1} \cdots p_k^{e_k}$. Let a be an integer. We define the **Jacobi symbol** $\left(\frac{a}{n}\right)$ as follows:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

Prove the following properties:

(a) If $a \equiv b \mod n$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(b) If a and b are integers, then $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$.

(c) If $x^2 \equiv a \mod n$ has a solution, then $\left(\frac{a}{n}\right) = 1$. Provide an example that shows that the converse of this statement isn't always true.

(d) If m, n are relatively prime odd integers, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{n-1}{2}}.$$