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.
$27 = 3^3$. $\varphi(3) = 2$, by *lemma 2.8.13* the number of integers less than 3 of order 2 do not exceed $\varphi(2) = 1$. Also, by *theorem 2.8.9* we know that 3 has a primitive root. Since $2^1 \not\equiv 1 \mod 3$ and $2^2 \equiv 1 \mod 3$ we have 2 as a primitive root of 3. By *theorem 2.8.15* we know that either 2 or $2 + 3 = 5$ is a primitive root(s) for 9. $\varphi(9) = 6$, so we need to check to see if the order of 2 or 5 are 6 in modulo 9.

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 7,\ 2^5 = 32 \equiv 5 \mod 9,\ 2^6 \equiv 5 \times 2 \equiv 1 \mod 9,$$

and

$$5^1 = 5,\ 5^2 = 25 \equiv 7,\ 5^3 \equiv 7 \times 5 = 35 \equiv 8 \mod 9,\ 5^4 \equiv 8 \times 5 \equiv 4,$$
$$5^5 \equiv 4 \times 5 \equiv 2 \mod 9, 5^6 \equiv 2 \times 5 \equiv 1 \mod 9.$$

So, both 2 and 5 are primitive roots of 9. From *theorem 2.8.16* we know that both 2 and 5 are primitive roots of 27. The other primitive roots of 27 are of the form 2^a where a is any integer mod 27 such that $\gcd(a, \phi(27)) = \gcd(a, 18) = 1$. These integers are 1,5,7,11,13,17.

$$\begin{aligned}
2^1 &\equiv 2 \\
2^5 &\equiv 32 \equiv 5 \\
2^7 &\equiv 2^5 \cdot 2^2 \equiv 5 \cdot 4 = 20 \\
2^{11} &= 2^9 \cdot 2^2 \equiv (-1) \cdot 4 \equiv 23 \\
2^{13} &= 2^9 \cdot 2^4 \equiv (-1) \cdot 16 \equiv 11 \\
2^{17} &= 2^9 \cdot 2^8 \equiv (-1) \cdot 13 \equiv 14
\end{aligned}$$

So the primitive roots of 27 are 2,5,20,23,11,14.

Question 2 [2 marks]

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

$$\left(\frac{105}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)\left(\frac{7}{1009}\right)$$

By *theorem 3.2.1* we have

$$\left(\frac{105}{1009}\right) = \left(\frac{1009}{3}\right)\left(\frac{1009}{5}\right)\left(\frac{1009}{7}\right)$$

$$\left(\frac{105}{1009}\right) = \left(\frac{1}{3}\right)\left(\frac{4}{5}\right)\left(\frac{1}{7}\right)$$

$$\left(\frac{105}{1009}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{5}\right)\left(\frac{1}{7}\right)$$

$$\left(\frac{105}{1009}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right)(-1)(-1)\left(\frac{-1}{7}\right)\left(\frac{-1}{7}\right)$$

$$\left(\frac{105}{1009}\right) = (-1)(-1)(-1)(-1)(-1)(-1) = 1$$

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 $a^{\frac{\phi(m)}{(\phi(m),n)}} \equiv 1 \mod m$.

Proof. ($\Rightarrow$) $x^n \equiv a \mod m$ has $\gcd(n, \varphi(m))$ solutions. Let $y = \gcd(n, \varphi(m))$. We know that $a^{\varphi(m)} \equiv 1 \mod m$. Let r be the primitive root, then $a \equiv r^k \mod m$, and $x^n \equiv r^k l \mod m$ for some $k, l \in \mathbb{Z}$. So

$$r^{nl} \equiv r^k \mod m$$

then

$$nl \equiv k \mod \varphi(m)$$

this implies that

$$y | k$$

then $k/y \in \mathbb{Z}$. So

$$r^k \equiv r^{k \cdot \frac{\varphi(m)}{y}} \equiv a^{\frac{\phi(m)}{y}}.$$

($\Leftarrow$) $a^{\frac{\varphi m}{y}} \equiv 1$. Let $a \equiv r^k \mod m$, and $x^n \equiv r^k l \mod m$ for some $k, l \in \mathbb{Z}$. then

$$r^{\frac{k\varphi(m)}{y}} \equiv 1 \mod m.$$

$$r^{\frac{k}{y}\varphi(m)} \equiv 1 \mod m.$$

So $k|y$. Then $ln \equiv k \mod m$ has y solutions. Then

$$r^{ln} \equiv r^k \Leftrightarrow x^n \equiv a \mod m$$ □

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.

Proof. Let $x \equiv g^k \mod p^h$ for some $k \in \mathbb{Z}$. Then $g^{kp} \equiv 1 \mod p^h$ and $\varphi(p^h) = p^(h-1)(p-1)$. So

$$k = t(p^{h-2}(p-1)),\ 1 \leq t \leq p-1. \qquad \square$$

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

Proof. Let $x \equiv g^k \mod p^h$ for some $k \in \mathbb{Z}$. Then $g^{2kp} \equiv 1 \mod p^h$ and $\varphi(p^h) = p^(h-1)(p-1)$. So

$$k = \frac{t}{2}(p^{h-2}(p-1)),\ 1 \leq t \leq p-1. \qquad \square$$

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.

Proof. There are $\varphi(n)$ integers that are less than n and relatively prime to n. Let these integers be

$$\{m_1, m_2, \ldots, m_{\varphi(n)}.\}$$

We can rewrite these using the primitve root

$$\{g^{k_1}, g^{k_2}, \ldots, g^{k_{\varphi(m)}}.\}$$

These can be further rewritten as

$$\{g^0, g^1, \ldots, g^{\varphi(n)-1}.\}$$

So this product is

$$\prod_{r=0}^{\varphi(n)-1} g^r = g^{1+2+\cdots+\varphi(n)-1} = g^{\frac{(\varphi(n)-1)\varphi(n)}{2}}$$

This is an element of order 2, so we have

$$\prod_{r=0}^{\varphi(n)-1} g^r = g^{1+2+\cdots+\varphi(n)-1} = g^{\frac{(\varphi(n)-1)\varphi(n)}{2}} \equiv -1 \mod n. \qquad \square$$

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 $1 \leq i \leq r$.

Proof. Let g_i be a primitive root modulo p_i for $1 \leq i \leq r$. By CRT there exists

$$g \equiv g_i \mod p_i \quad 1 \leq i \leq r.$$

And this g is a primitive root for all moduli because $g \equiv g_i \mod p_i$ for all i. $\square$

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 $\varphi(a^q - 1)$.

Proof. $a^d \equiv 1 \pmod{a^q - 1} \Leftrightarrow a^d - 1 \equiv 0 \pmod{a^q - 1} \Leftrightarrow a^q - 1 | a^d - 1 \Leftrightarrow q | d$. The smallest d is $d = q$. $\gcd(a^q - 1, a) = 1$ so $a^{\varphi(a^q-1)} \equiv 1 \mod a^q - 1$ and $a^q \equiv 1 \mod a^q - 1$ so $\varphi(a^q - 1) = wq$ for some $w \in \mathbb{Z}$. Therefore, $q | \varphi(a^q - 1)$. □

(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 $p \equiv 1 \pmod{q}$.

Proof.

$$\varphi(N) = \prod_{p^e | N} p^{e-1}(p - 1).$$

Assume for contradiction that no prime divisor of N is of the form $p = q$ or $p \equiv 1 \mod q$. Then for all p that divide N we habe $q \nmid p - 1$ which shows that $q \nmid \varphi(N)$. But in 7a we shows that $q | \varphi(N)$, this is a contradiction. So either $p = q$ or $p \equiv 1 \mod q$. □

Question 8 [3 marks]

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

Proof. Assume there are finitely many primes p with $p \equiv 1 \mod q$. Let these primes be

$$p_1, p_2, \ldots, p_n.$$

Let

$$a = \prod_{i=1}^{n} p_i,\ N = a^q - 1.$$

Then $a \equiv 0 \mod q$, and $a \equiv 0 \mod p_i$ $(1 \leq i \leq n)$. Since $N > 1$ we have $\exists p$ prime such that $p|N$.
Then $N \equiv -1 \mod q$ and $N \equiv -1 \mod p_i$ $(1 \leq i \leq n)$. So we have $p \neq q$ and $p \notin \{p_1, p_2, \ldots, p_n\}$. In 7b we showed that all prime divisors of N are of the form $p = q$ or $p \equiv 1 \mod q$. Since $p \neq q$ it must be that $p \equiv 1 \mod q$. But $p \notin \{p_1, p_2, \ldots, p_n\}$, so the assumption is false. □

Question 9 [3 marks]

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

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

Proof. By *theorem 3.1.8* we know that

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } \ p \equiv 1 \mod 4 \\ -1 & \text{if } \ p \equiv 3 \mod 4. \end{cases}$$

Since $p \geq 5$ we have $p \not\equiv 0 \mod 3$.
For p modulo 12 we have $p \equiv 1, 5, 7, 11 \mod 12$. So we have

p mod 12	p mod 4	p mod 3	$\left(\frac{3}{p}\right)$
1	1	1	1
5	1	2	-1
7=-5	3	1	-1
11=-1	3	2	1

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

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 $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

Proof. $a \equiv b \mod n \Leftrightarrow a \equiv b \mod p_i$, where $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, with p_i distinct primes and $e_i \in \mathbb{Z}$ $(1 \leq i \leq k)$. That is to say that

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$$

So,

$$\left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_i}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k} = \left(\frac{b}{p_1}\right)^{e_1} \left(\frac{b}{p_i}\right)^{e_2} \cdots \left(\frac{b}{p_k}\right)^{e_k}.$$

Therefore if $a \equiv b \mod n$

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

□

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

Proof. Using the prime factorization of n given in part (a) we have

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_i}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k},$$

and

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)^{e_1} \left(\frac{b}{p_i}\right)^{e_2} \cdots \left(\frac{b}{p_k}\right)^{e_k}.$$

So

$$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_i}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k} \left(\frac{b}{n}\right) \left(\frac{b}{p_1}\right)^{e_1} \left(\frac{b}{p_i}\right)^{e_2} \cdots \left(\frac{b}{p_k}\right)^{e_k} = \left(\frac{ab}{n}\right).$$

□

(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.

Proof. Given that $x^2 \equiv a \mod n$ has a solution we have $x^2 \equiv 1 \mod p_i$ where p_i is from the prime factorization of n given in part (a). We can then see that

$$\left(\frac{a}{p_i}\right) = 1 \quad \text{for all } 1 \leq i \leq k.$$

Then

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_i}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k} = 1^{e_1} 1^{e_2} \cdots 1^{e_k}.$$

□

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

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

Proof. Let $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ for distinct primes p_i and $e_i \in \mathbb{Z}$ for $(1 \leq i \leq r)$, and $n = q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$ for distinct primes q_i and $f_i \in \mathbb{Z}$ for $(1 \leq i \leq r)$.
Then,

$$\left(\frac{m}{n}\right) \prod_{i=1}^{k} \prod_{j=1}^{r} \left(\frac{p_i^{e_i}}{q_j^{f_j}}\right),$$

and

$$\left(\frac{n}{m}\right) \prod_{i=1}^{r} \prod_{j=1}^{k} \left(\frac{q_i^{f_i}}{p_j^{e_j}}\right),$$

Taking their product we obtain

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k} \prod_{j=1}^{r} \left[\left(\frac{p_i^{e_i}}{q_j^{f_j}}\right)\left(\frac{q_i^{f_i}}{p_j^{e_j}}\right)\right]$$

this can be rearranged to give

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k} \prod_{j=1}^{r} (-1)^{e_i f_j \left(\frac{p_i - 1}{2}\right)\left(\frac{q_i - 1}{2}\right)}$$

Moving the product into the exponent we obtain

$$\sum_{i=1}^{k} \sum_{j=1}^{r} e_i f_j \left(\frac{p_i - 1}{2}\right)\left(\frac{q_i - 1}{2}\right)$$

another rearrangement yields

$$\sum_{i=1}^{k} e_i \left(\frac{p_i - 1}{2}\right) \sum_{j=1}^{r} f_j \left(\frac{q_i - 1}{2}\right).$$

Put

$$a = \sum_{i=1}^{k} e_i \left(\frac{p_i - 1}{2}\right) \sum_{j=1}^{r} f_j \left(\frac{q_i - 1}{2}\right),$$

then

$$(-1)^a = (-1)^{\sum_{i=1}^{k} e_i \left(\frac{p_i - 1}{2}\right) \sum_{j=1}^{r} f_j \left(\frac{q_i - 1}{2}\right)}.$$

This is as far as I got before class started, I'm not so sure that the last step is the right direction to finish the proof. □