Name Furqan Sajjad, ID 94983

MTH 313, Number Theory, Fall 2024, 1–3

Exam I

Ayman Badawi

Scores 44/44

QUESTION 1. (i) **(4 points)** Let $p \geq 2$ be a prime integer and $n \geq 1$ be an integer. Prove that $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Let $M = \{1 \leq a < p^n\}$, $|M| = p^n - 1 + 1 = p^n$

$D = \{1 \leq a < p^n \mid \gcd(a, p^n) \neq 1\} = \{pk \mid 1 \leq k < p^{n-1}\}$ (pk: multiples of p)

$|D| = p^{n-1} - 1 + 1 = p^{n-1}$

4

So $L = \{1 \leq a < p^n \mid \gcd(a, p^n) = 1\} = M - D$

$= p^n - p^{n-1}$

$= p^{n-1}(p-1)$ ✓

(ii) **(4 points)** Let $p \geq 2$ be a prime integer, prove that $\sum_{d \mid p^n} d = p^n$ for every $n \geq 1$.

$\sum_{d \mid p^n} \phi(d) = p^n$

If $d \mid p^n$, then d must be a power of p s.t. $d = p^k$, $0 \leq k \leq n$ (*) $p^0 = 1 \mid p^n$ also

So $\phi(d) = \phi(p^k) = (p-1)p^{k-1}$ so $\sum_{d \mid p^n} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p$

$= 1 + (p-1) + (p-1)p + \ldots + (p-1)p^{n-1}$

$= 1 + (p-1)[1 + p + p^2 + \ldots + p^{n-1}]$

$= 1 + (p-1)\left(\frac{1 - p^{n-1+1}}{1-p}\right) = 1 - (1 - p^n)$

$= p^n - 1 + 1$

$= p^n$ ✓

4

(iii) **(4 points)** Prove there are infinitely many prime numbers.

Deny and therefore assume (finite number of primes)

Assume that there is a largest prime P

Let $X = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot P$ (product of finitely many primes)

is larger than P $(X > P)$

4

$X+1$ is larger than P but no prime divides $X+1$ since

$\forall p \in \underbrace{\text{primes}}_{\{2,3,5,\ldots,P\}}$, $X \pmod p = 0$ so $(X+1) \pmod p = 1$

so $X+1$ is a prime larger than P ↯ So there are infinitely many prime

(iv) **(4 points)** Prove that there are 2^{2024} consecutive positive integers such that none of them is prime.

Let $N = 2^{2024}$

Let $M = (N+1)!$ ← product of all numbers from 2 to (N+1) inclusive
$\Rightarrow \forall k \in \{2 \le k \le N+1\}$, $M \bmod k = 0$

$M+2$ is not prime since $M \pmod 2 = 0$ so $(M+2) \pmod 2 = 0$
$M+3$ is not prime since $M \pmod 3 = 0$ so $(M+3) \pmod 3 = 0$
$M+4$ is not prime since $M \pmod 4 = 0$ so $(M+4) \pmod 4 = 0$
⋮

$M+(N+1)$ is not prime since $M \pmod{N+1} = 0$ so $(M+(N+1)) \pmod{N+1} = 0$

So we have $(N+1)-2+1 = N = 2^{2024}$ consecutive +ve int. s.t. none are prime

4

QUESTION 2. (6 points) Let $x \in Z$ such that (a) $3x \pmod{12} = 6$, (b) $2x \pmod{10} = 8$. Find all values of x over planet Z.

(a) $3x = 6 \pmod{12}$ (a, b, n)

$\gcd(a,n) = 3 \mid 6$ so 3 solutions, $d = \frac{12}{3} = 4$

$x \in \{2, 6, 10\}$ in Z_{12} so $x \in \{2+4k \mid k \in Z\}$ in Z

Verify (a): $2(3+4k) \pmod{12}$
$= 6+12k \pmod{12}$
$= 6+0 = 6$ ✓

(b) $2x = 8 \pmod{10}$

$\Rightarrow 2(2+4k) = 8 \pmod{10}$

$\Rightarrow 4+8k = 8 \pmod{10}$

$\Rightarrow 8k = 4 \pmod{10}$ (a, b, n)

$\gcd(8,10) = 2 \mid 4$ so 2 solutions, $d = \frac{10}{2} = 5$

$k \in \{3, 8\}$ in Z_{10}

$x = 2+4k$: $k=3 \rightarrow 2+4(3) = 14$; $k=8 \rightarrow 2+4(8) = 34$

$x \in \{14+20m \mid m \in Z\}$ in Z

6

QUESTION 3. (8 points) Find all ordered triplets (x, y, z) over Z_4 such that $x + 2y + 2z = 3$ in Z_4 (i.e., $x, y, z \in Z_4$)

$x+2y+2z = 3$ in Z_4

- x must be a multiple of $\gcd(1,4) = 1$ so $x \in \{0,1,2,3\}$ in Z_4 (a) (b) (c) (d)

(a) $x = 0 \Rightarrow 2y+2z = 3$ in Z_4
sum even cannot be odd so no solutions for (a)

(b) $x = 1 \Rightarrow 2y+2z = 2$ in Z_4

$2y$ must be a mul. of 2 in Z_4	$2z$ must be a mul. of 2 in Z_4
0	0
2	2

Pairs are (0,2) & (2,0)

for (0,2): $2y = 0 \Rightarrow y = 0, y = 2$ in Z_4; $2z = 2 \Rightarrow z = 1, z = 3$ in Z_4

for (2,0): $2y = 2 \Rightarrow y = 1, y = 3$ in Z_4; $2z = 0 \Rightarrow z = 0, z = 2$ in Z_4

S.S for (b) is $\{(1,0,1), (1,0,3), (1,2,1), (1,2,3), (1,1,0), (1,1,2), (1,3,0), (1,3,2)\}$

(c) $x = 2 \Rightarrow 2y+2z = 1$ for (c), no solutions

(d) $x = 3 \Rightarrow 2y+2z = 0$

$2y$ must be a mul. of 2 in Z_4	$2z$ must be a mul. of 2 in Z_4
0	0
2	2

Pairs are (0,0) & (2,2)

for (0,0): $2y = 0 \Rightarrow y = 0, y = 2$ in Z_4; $2z = 0 \Rightarrow z = 0, z = 2$ in Z_4

for (2,2): $2y = 2 \Rightarrow y = 1, y = 3$ & $2z = 2 \Rightarrow z = 1, z = 3$ in Z_4

S.S for (d) is $\{(3,0,0), (3,0,2), (3,2,0), (3,2,2), (3,1,1), (3,1,3), (3,3,1), (3,3,3)\}$

S.S overall = ↓ ∪ ↑

QUESTION 4. (6 points) What are the smallest positive integer and the largest negative integer that satisfy (i) $x\ (mod\ 9) = 2, (ii) x\ (mod\ 3) = 2, (iii) x\ (mod\ 7) = 3$,

$\begin{cases} x\ (\text{mod } 9) = 2 \\ x\ (\text{mod } 3) = 2 \\ x\ (\text{mod } 7) = 3 \end{cases}$ reduced $\Longrightarrow$ $\begin{cases} x\ (\text{mod } \overset{m_1}{9}) = 2^{r_1} \\ x\ (\text{mod } \overset{m_2}{7}) = 3^{r_2} \end{cases}$

6 ✓

$x\ (\text{mod } 9) = 2 \Rightarrow x\ (\text{mod } 3) = 2$

$x = n_1 c_1 r_1 + n_2 c_2 r_2\ (\text{mod } m) = \boxed{38}$ in $\mathbb{Z}_{63}$

$\Rightarrow x \in \{38 + 63k \mid k \in \mathbb{Z}\}$ in $\mathbb{Z}$

$m = m_1 m_2 = \boxed{63}$

$n_1 = \frac{m}{m_1} = m_2 = \boxed{7}$, $n_2 = \frac{m}{m_2} = m_1 = \boxed{9}$

$\overset{7}{n_1} \text{ mod } \overset{9}{m_1} = 7$ $\qquad$ $\overset{9}{n_2} \text{ mod } \overset{7}{m_2} = 2$

and 7^{-1} in $\mathbb{Z}_9$ is $\overset{c_1}{\boxed{4}}$ $\qquad$ and 2^{-1} in $\mathbb{Z}_7$ is $\overset{c_2}{\boxed{4}}$

So 38 is the smallest +ve integer and $(38-63) = -25$ is the Largest -ve integer that satisfies the System

QUESTION 5. 1. **(4 points)** Find $7^{266}\ (mod\ 45)$.

$\overset{a}{7}^{\overset{m}{266}}\ (\text{mod } \overset{n}{45}) = 7^{266 \text{ mod } 24}\ (\text{mod } 45) = 7^2\ (\text{mod } 45)$
$= \boxed{4}$

$\gcd(a,n) = 1$ so $a^{\phi(n)} = 1\ (\text{mod } n)$

$\Rightarrow 7^{24} = 1\ (\text{mod } 45)$

4

$n = 45 = 5 \cdot 3^2$

$\phi(n) = \phi(5) \cdot \phi(3^2) = 4 \cdot 2 \cdot 3 = 24$

2. **(4 points)** Find two positive integers $x > 0$ and $y > 0$ such that $2024 = x^2 - y^2$.

$\underset{n}{2024} = 4 \cdot \underset{m}{506}$ so $x = (m+1) = 507$
&
$y = (m-1) = 505$

X

Verify: $2024 \overset{?}{=} 507^2 - 505^2$ ✓

Name Joud Hamdan, ID 95608

MTH 313, Number Theory, Fall 2024, 1–3

Exam I

Ayman Badawi

Scores 44/44

QUESTION 1. (i) **(4 points)** Let $p \geq 2$ be a prime integer and $n \geq 1$ be an integer. Prove that $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Let $A = \{1 \leq a \leq p^n\}$ $|A| = p^n$

Let $B = \{1 \leq b \leq p^n \mid gcd(b, p^n) \neq 1\} = \{pk \mid 1 \leq k \leq p^{n-1}\}$

$\Rightarrow |B| = p^{n-1}$

$C = A - B = \{1 \leq c \leq p^n \mid gcd(c, p^n) = 1\}$

$\phi(p^n) = |C| = |A| - |B| = p^n - p^{n-1}$

✗

(ii) **(4 points)** Let $p \geq 2$ be a prime integer, prove that $\sum_{d|p^n} d = p^n$ for every $n \geq 1$.

$\sum_{d|p^n} \phi(d) = p^n$

(1) $n = 1$: $\sum_{d|p} \phi(d) = \phi(1) + \phi(p)$

$= 1 + p - 1 = p$

(2) Assume $\sum_{d|p^k} \phi(d) = p^k$ $\exists$ $k \geq 1$

✗

from Question 1 ✓

(4) $\sum_{d|p^{k+1}} \phi(d) = \left(\sum_{d|p^k} \phi(d)\right) + \phi(p^{k+1}) = p^k + p^{k+1} - p^k$

$= p^{k+1}$

(iii) **(4 points)** Prove there are infinitely many prime numbers.

Deny. $\exists$ finitely many prime numbers $p_1, p_2, p_3, \ldots, p_k$.

Let $x = p_1 p_2 p_3 \ldots p_k + 1$ and let d be a prime factor of x

$\Rightarrow d \in \{p_1, p_2, p_3, \ldots, p_k\} \Rightarrow d \mid p_1 p_2 p_3 \ldots p_k$ and

$d \mid x \Rightarrow d \mid 1$ which is a contradiction

✗

(iv) **(4 points)** Prove that there are 2^{2024} consecutive positive integers such that none of them is prime.

$N_2 = (2^{2024}+1)! + 2$ is not prime since $2 \mid N_2$.

$N_3 = (2^{2024}+1)! + 3$ is not prime since $3 \mid N_3$

$N_4 = (2^{2024}+1)! + 4$ is not prime since $4 \mid N_4$

4

$N_{2^{2024}+1} = (2^{2024}+1)! + (2^{2024}+1)$ is not prime since $2^{2024}+1 \mid N_{2^{2024}+1}$

$\Rightarrow$ We have 2^{2024} consecutive non-prime integers

QUESTION 2. (6 points) Let $x \in Z$ such that (a) $3x \pmod{12} = 6$, (b) $2x \pmod{10} = 8$. Find all values of x over planet Z.

Solve $3x \pmod{12} = 6$ over Z.

$SS = \{2 + 4k \mid k \in Z\}$

Find smallest $k \in Z$ s.t $2(2+4k) \pmod{10} = 8$

$4 + 8k \pmod{10} = 8$

$8k \pmod{10} = 4$

$k = 3$

6

$x = 2 + 4(3) = 14$ is the smallest solution to (a) and (b).

Solution over $Z = \{14 + 20m \mid m \in Z\}$

QUESTION 3. (8 points) Find all ordered triplets (x, y, z) over Z_4 such that $x + 2y + 2z = 3$ in Z_4 (i.e., $x, y, z \in Z_4$)

x must be a multiple of 1	$2y$ must be a multiple of 2 (+2)	$2z$ must be a multiple of 2 (+2)	$2y+2z$
0 X	$0 \to 0,2$	$0 \to 0,2$	3 X
1			2
2 X	$2 \to 1,3$	$2 \to 1,3$	1 X
3			0

$4 \pmod 4 = 0$

$2 \pmod 4 = 2$

$0 \pmod 4 = 0$

16 triplets

9/8

$(1,0,1), (1,2,3), (1,3,0)$
$(1,0,3), (1,1,0), (1,3,2)$
$(1,2,1), (1,1,2)$

$(3,0,0), (3,1,3), (3,3,1)$
$(3,0,2), (3,1,1), (3,3,3)$
$(3,2,0), (3,2,2)$

QUESTION 4. (6 points) What are the smallest positive integer and the largest negative integer that satisfy (i) $x \pmod 9 = 2, (ii) x \pmod 3 = 2, (iii) x \pmod 7 = 3$,

Since $9 \mid (x-2) \Rightarrow 3 \mid (x-2)$, we only need to

solve $x \pmod 9 = 2$

$x \pmod 7 = 3$

Smallest positive $x = \left(7\left(7 \pmod 9\right)^{-1}(2) + 9\left(2 \pmod 7\right)^{-1}(3)\right) \pmod{63}$

$= \left((7)(4)(2) + 9(4)(3)\right) \pmod{63}$

$= 164 \pmod{63} = 38$ ✓ SS over $Z = \{38 + 63k \mid k \in Z\}$ ✓

Largest negative integer $= 38 + 63(-1) = -25$ ✓

QUESTION 5. 1. **(4 points)** Find $7^{266} \pmod{45}$.

$\phi(45) = \phi(3^2 \times 5) = 3(2) \times 4 = 24$

$7^{266} \pmod{45} = 7^{24(11)+2} \pmod{45}$ By Euler

$= (7^{24})^{11} \pmod{45} \cdot 7^2 \pmod{45} = 1 \cdot 7^2 \pmod{45}$

$= 4$

2. **(4 points)** Find two positive integers $x > 0$ and $y > 0$ such that $2024 = x^2 - y^2$.

$2024 = 4m \Rightarrow m = 506$ ✓

Let $x = 506 + 1 = 507$, $y = 506 - 1 = 505$ ✓