M E T U
Department of Mathematics

	Elementary Number Theory I Midterm 2	
Code : *Math 365* Acad. Year : *2018-2019* Semester : *Fall* Instructor : *Tolga Karayayla* Date : *19.12.2018* Time : *17.40* Duration : *120 minutes*	Last Name : First Name : Student ID : Department : Signature : 7 Questions on 4 Pages SHOW DETAILED WORK!	

1	2	3	4	5	6	7		

1. (10+10 pts.) a) Show that $\phi(3n) = 3\phi(n)$ if and only if $3|n$.

Assume first that $3|n$, then $n = 3^k \cdot M$ for some $k \geq 1$ and $M \in \mathbb{Z}$ s.t. $\gcd(3, M) = 1$

Then $\phi(3n) = \phi(3 \cdot 3^k \cdot M) = \phi(3^{k+1} \cdot M) = \phi(3^{k+1}) \cdot \phi(M)$ (since $\gcd(3^{k+1}, M) = 1$)

$= (3^{k+1} - 3^k) \cdot \phi(M) = 3 \cdot (3^k - 3^{k-1}) \cdot \phi(M)$ ($k-1 \geq 0$ since $k \geq 1$)

$= 3 \cdot \phi(3^k) \cdot \phi(M) = 3 \cdot \phi(3^k \cdot M) = 3 \cdot \phi(n)$

Hence, $3|n \Rightarrow \phi(3n) = 3 \cdot \phi(n)$

Assume now $3 \nmid n$, then $\gcd(3, n) = 1$

Thus, $\phi(3n) = \phi(3) \cdot \phi(n) = (3^1 - 3^0) \cdot \phi(n) = 2\phi(n) \neq 3 \cdot \phi(n)$ (since $\phi(n) \neq 0$)

Therefore

$3 \nmid n \Rightarrow \phi(3n) \neq 3 \cdot \phi(n)$

Equivalently $\phi(3n) = 3 \cdot \phi(n) \Rightarrow 3|n$.

b) Show that $\sigma(n)$ is odd if and only if $n = k^2$ or $n = 2k^2$ for some integer k.

Let prime factorization of n be given by $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ ($\alpha_i \geq 1$ for all i)

Then $\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r})$

$\sigma(n)$ is odd iff each factor $(1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i})$ is odd.

If $p_i = 2$ for some i, $1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$ is odd for any value of $\alpha_i \geq 1$

For odd p_i, $1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} \equiv 1 + 1 + \cdots + 1 \equiv \alpha_i + 1 \pmod 2$, hence is odd if and only if α_i is even

Thus $\sigma(n)$ is odd if and only if

$n = 2^{2\beta_1} \cdot p_2^{2\beta_2} \cdots p_r^{2\beta_r}$ ($\beta_i \geq 0$) $\vee$ $n = 2^{2\beta_1 + 1} \cdot p_2^{2\beta_2} \cdots p_r^{2\beta_r}$ ($\beta_i \geq 0$)

$n = (2^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r})^2$ ($\beta_i \geq 0$) $\vee$ $n = 2 \cdot (2^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r})^2$ ($\beta_i \geq 0$)

$n = k^2 \vee n = 2k^2$

Note also if $n = 1$, $\sigma(1) = 1$ is odd and $1 = 1^2$ (statement holds for $n = 1$).

2. (5+10 pts.) Let ω be defined by $\omega(1) = 0$ and $\omega(n)$ is the number of distinct prime divisors of n for $n > 1$, $n \in \mathbb{Z}$.

a) Show that $f(n) = 2^{\omega(n)}$ is a multiplicative function from $\mathbb{Z}^+$ to $\mathbb{Z}$.

Let $\gcd(m,n) = 1$ $\quad m = 1$ (or $n = 1$) $\Rightarrow 2^{\omega(m\cdot n)} = 2^{\omega(n)} = 2^0 \cdot 2^{\omega(n)} = 2^{\omega(m)} \cdot 2^{\omega(n)}$

For $m > 1, n > 1$, $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ ($q_i \neq p_j$, p_i are distinct primes, q_j are distinct primes)

so $m \cdot n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$

$\omega(m \cdot n) = r + s = \omega(m) + \omega(n)$ $\quad \omega(m) = r$, $\omega(n) = s$

So $2^{\omega(m\cdot n)} = 2^{\omega(m)+\omega(n)} = 2^{\omega(m)} \cdot 2^{\omega(n)}$, hence $2^{\omega(n)}$ is a multiplic. fcn.

b) Show that $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$ for all $n \in \mathbb{Z}^+$.

Let $f(n) = 2^{\omega(n)}$, from above f is multiplicative, thus $F(n) = \sum_{d|n} f(d)$ is also multiplic.

$\tau(n)$ is multiplicative, then if $\gcd(m,n) = 1$, we have $\gcd(m^2, n^2) = 1$, hence

$G(n) = \tau(n^2) \Rightarrow G(m\cdot n) = \tau((m\cdot n)^2) = \tau(m^2 \cdot n^2) = \tau(m^2) \cdot \tau(n^2) = G(m) \cdot G(n)$

Therefore, $G(n) = \tau(n^2)$ is also multiplicative.

To prove two multiplicative functions $F(n)$ and $G(n)$ are equal for all $n \geq 1$, it suffices to prove $F(p^\alpha) = G(p^\alpha)$ for any prime p and $\alpha \geq 1$.

$G(p^\alpha) = \tau(p^{2\alpha}) = 2\alpha + 1$.

$F(p^\alpha) = \sum_{d|p^\alpha} 2^{\omega(d)} = 2^0 + 2^1 + 2^1 + \cdots + 2^1 = 1 + \alpha \cdot 2 = 2\alpha + 1$

$d | p^\alpha \Rightarrow d \in \{1, p, p^2, \ldots, p^\alpha\}$ and $\omega(1) = 0$, $\omega(p^i) = 1$ for $i \geq 1$

Thus $F(p^\alpha) = G(p^\alpha)$ ⊛

3. (10 pts.) Find a formula for $\sum_{d|n} \frac{(\mu(d))^2}{\phi(d)}$ in terms of the prime factorization of n.

$\mu(n)$ and $\phi(n)$ are multiplicative, then $f(n) = \frac{(\mu(n))^2}{\phi(n)}$ is also multiplicative.

Thus $F(n) = \sum_{d|n} f(d) = \sum_{d|n} \frac{(\mu(n))^2}{\phi(n)}$ is also multiplicative.

$n = 1 \Rightarrow F(1) = 1$

$n > 1 \Rightarrow$ Let prime factorization of n be $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ (p_i distinct primes, $\alpha_i \geq 1$)

Then

$F(n) = F(p_1^{\alpha_1}) \cdot F(p_2^{\alpha_2}) \cdots F(p_r^{\alpha_r})$

$= \left(1 + \frac{1}{p_1 - 1}\right) \cdot \left(1 + \frac{1}{p_2 - 1}\right) \cdots \left(1 + \frac{1}{p_r - 1}\right) = \frac{p_1}{p_1 - 1} \cdot \frac{p_2}{p_2 - 1} \cdots \frac{p_r}{p_r - 1}$

Since for any i,

$F(p_i^{\alpha_i}) = \sum_{d|p_i^{\alpha_i}} \frac{(\mu(d))^2}{\phi(d)} = \frac{(\mu(1))^2}{\phi(1)} + \frac{(\mu(p_i))^2}{\phi(p_i)} + 0 + \cdots + 0 = \frac{1}{1} + \frac{1}{p_i - 1}$

$(\mu(p_i^k))^2 = 0^2 = 0$ if $k \geq 2$

4. (10+10 pts.) a) Find the largest $k \in \mathbb{Z}$ such that $9^k \mid \frac{300!}{(100!)^3}$.

Largest r such that $3^r \mid 300!$

$r = \sum_{k=1}^{\infty} \left[\frac{300}{3^k}\right] = 100 + 33 + 11 + 3 + 1 = 148$

Largest s such that $3^s \mid 100!$: $s = \sum_{k=1}^{\infty} \left[\frac{100}{3^k}\right] = 33 + 11 + 3 + 1 = 48$

$\Rightarrow (3^{48})^3 = 3^{144}$ is the largest ~~expo~~ power of 3 that divides $(100!)^3$

Then $3^{148-144} = 3^4$ is the highest power of 3 that divides $\frac{300!}{(100!)^3}$

$3^4 = 9^2 \Rightarrow$ Answer is $\underline{\underline{2}}$

b) Find the largest $k \in \mathbb{Z}$ such that $175^k \mid 365 \cdot 364 \cdot 363 \cdots 102 \cdot 101$.

$175 = 7 \cdot 25 = 5^2 \cdot 7$ $\quad 365 \cdot 364 \cdots 102 \cdot 101 = \frac{365!}{100!}$

$\sum_{k=1}^{\infty} \left[\frac{365}{5^k}\right] = 73 + 14 + 2 = 89$, $\sum_{k=1}^{\infty} \left[\frac{100}{5^k}\right] = 20 + 4 = 24$

$5^{89-24} = 5^{65}$ is the highest power of 5 dividing $\frac{365!}{100!}$

$\sum_{k=1}^{\infty} \left[\frac{365}{7^k}\right] = 52 + 7 + 1 = 60$, $\sum_{k=1}^{\infty} \left[\frac{100}{7^k}\right] = 14 + 2 = 16$

$7^{60-16} = 7^{44}$ is the highest power of 7 that divides $\frac{365!}{100!}$

$(175)^k = (5^2 \cdot 7)^k = 5^{2k} \cdot 7^k \mid \frac{365!}{100!} \iff 2k \le 65 \wedge k \le 44$

$k \le 32 \wedge k \le 44$

Thus $k \le 32 \iff 175^k \mid \frac{365!}{100!}$ Answer: $\underline{\underline{32}}$

5. (10 pts.) If $n > 1$ is a composite integer, show that $\phi(n) \le n - \sqrt{n}$. (Hint: Consider the smallest prime divisor p of n.) Assume n is composite and p is the smallest prime divisor of n.

$n = p \cdot a$ for some $a \in \mathbb{Z}^+$ and $1 < a < n$. If q is a prime div. of a, then $q \mid a \wedge a \mid n \Rightarrow q \mid n$, hence $p \le q$, so $p \le a$.

$n = p \cdot a \ge p \cdot p \Rightarrow n \ge p^2 \Rightarrow \sqrt{n} \ge p$.

The number of integers from 1 to n, which are divisible by p is $\left[\frac{n}{p}\right] \ge \left[\frac{n}{\sqrt{n}}\right]$

There $\lceil \sqrt{n} \rceil$ integers are not relatively prime to n since p divides them and n. $= \lceil \sqrt{n} \rceil$

So $\phi(n) \le n - \lceil \sqrt{n} \rceil$ ~~###~~ But if $\sqrt{n} \notin \mathbb{Z}$, then $n - \sqrt{n} < n - \lceil \sqrt{n} \rceil$, so this is not a complete proof. The correct proof is:

$n = p_1^{\alpha} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ ($r \ge 0$, $\alpha_i \ge 1$, p_i distinct primes)

$\varphi(n) = n \cdot \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \le n\left(1 - \frac{1}{p}\right) = n - \frac{n}{p} \le n - \sqrt{n}$

$=$ equality if only prime factor is p

6. (10 pts.) Find $0 \le x \le 359$ such that $7^{9700} \equiv x \pmod{360}$.

By Euler's Thm, $7^{\varphi(360)} \equiv 1 \pmod{360}$ since $\gcd(7, 360) = 1$

$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2)(3^2 - 3^1)(5^1 - 5^0) = 96$

Then $7^{96} \equiv 1 \pmod{360}$

$9700 = 96 \cdot 101 + 4$

$7^{9700} \equiv 7^{96 \cdot 101 + 4} \equiv (7^{96})^{101} \cdot 7^4 \equiv 1^{101} \cdot 7^4 = 49^2 \equiv 2401 \equiv 241 \pmod{360}$

7. (3×5 pts.) State whether the following statements are True or False. Give brief explanation for each case.

a) Let $n > 1$. If $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$, then n is a prime.

False. There are absolute pseudo prime numbers which are non-prime integers satisfying this given condition.

b) Let $n > 1$. If $(n-1)! \equiv -1 \pmod{n}$, then n is a prime.

True.

If $n = a \cdot b$ is composite (where $1 < a < n$, $1 < b < n$), then

Case 1: $a \neq b \Rightarrow a \cdot b \mid 1 \cdot 2 \cdot 3 \cdots (n-1) = (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod{n}$

$a = b \Rightarrow$

Case 2: $a = b$, $n = a^2$ $1 < a < n$.

$a \mid (n-1)! \Rightarrow a^2 = n \mid ((n-1)!)^2 \Rightarrow ((n-1)!)^2 \equiv 0 \pmod{n}$

Hence $(n-1)! \not\equiv -1 \pmod{n}$ otherwise $((n-1)!)^2 \equiv (-1)^2 \equiv 1 \not\equiv 0 \pmod{n}$

$0 \not\equiv 1 \pmod{n}$ since $n > 1$.

c) If $\sum_{d \mid n} f(d) = \sum_{d \mid n} g(d)$ for all $n \in \mathbb{Z}^+$, then $f(n) = g(n)$ for all $n \in \mathbb{Z}^+$.

True. Let $F(n) = \sum_{d \mid n} f(d) = \sum_{d \mid n} g(d)$, then by Mobius Inversion Formula:

$$f(n) = \sum_{d \mid n} F(d) \cdot \mu\left(\frac{n}{d}\right) = g(n) \quad \text{for all } n \in \mathbb{Z}^+$$