MTH 26001 - Elemantary Number Theory.
Name: Nguyen Minh Duc
Student ID: 20202026

ASSIGNMENT 6.

Sec 7.2

Problem 7.

(a) By definition, $\varphi(n) \le n$. —— ①

⊛ For $n=1$, $\varphi(n) = 1 \Rightarrow \frac{1}{2} = \frac{1}{2}\sqrt{1} < 1 = \varphi(1)$

⊛ For $n=2$, $\varphi(n) = 1 \Rightarrow \frac{1}{2}\sqrt{2} < 1 = \varphi(2)$

⊛ For $n = 2^k$, $k > 1$, $\varphi(n) = 2^{k-1}$

$$\frac{1}{2}\sqrt{2^{k-1}} = 2^{-1}2^{k/2} = 2^{\frac{k}{2}-1} < 2^{k-1} = \varphi(2^k)$$

$\Rightarrow \frac{1}{2}\sqrt{n} < \varphi(n)$

⊛ For $n = p^k$, $p > 2$ is prime, $k \geq 1$.

$\Rightarrow \varphi(n) = p^{k-1}(p-1)$.

Since $p \geq 3$, $p^2 \geq 3p \Rightarrow p^2 - 2p \geq p$

$\Rightarrow p^2 - 2p > p - 1$

$\Rightarrow p^2 - 2p + 1 > p$

$\Rightarrow (p-1)^2 > p$

$\Rightarrow p - 1 > \sqrt{p}$

Thus, $p^{k-1}(p-1) > p^{k-1}\sqrt{p} \geq p^{\frac{k-1}{2}} p^{1/2} = p^{k/2} = \sqrt{p^k}$.

$\Rightarrow \varphi(p^k) > \sqrt{p^k}$

⊛ For $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $k_i \geq 0 \ \forall i \in [0, r]$.

* For $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $k_i \geq 0 \ \forall i \in [0, r]$.
p_i is prime $\forall i \in [1, r]$

Since $\varphi(n)$ is multiplicative,
$\varphi(n) = \varphi(2^{k_0}) \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r})$.

$$\geq \left(\frac{1}{2}\sqrt{2^{k_0}}\right)\left(\sqrt{p_1^{k_1}}\right)\left(\sqrt{p_2^{k_2}}\right) \cdots \left(\sqrt{p_r^{k_r}}\right)$$
$$= \frac{1}{2}\sqrt{2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$
$$= \frac{1}{2}\sqrt{n} \quad \text{—— (2)}$$

* From (1) and (2), $\frac{1}{2}\sqrt{n} \leq \varphi(n) \leq n$

(b) Factorize $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, p_i is prime $\forall i \in [1, r]$
$k_i \geq 1 \ \forall i \in [1, r]$

Note that $p_i \geq 2 \Rightarrow \frac{1}{p_i} \leq \frac{1}{2} \Rightarrow -\frac{1}{p_i} \geq -\frac{1}{2}$
$\Rightarrow 1 - \frac{1}{p_i} \geq \frac{1}{2}$.

Now, we have
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$
$$\geq n\left(\frac{1}{2}\right)\left(\frac{1}{2}\right) \cdots \left(\frac{1}{2}\right)$$
$$= n\left(\frac{1}{2^r}\right)$$

$\Rightarrow \varphi(n) \geq \frac{n}{2^r}$.

(c) Factorize $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, p_i is prime $\forall i \in [1, r]$
$k_i \geq 1$

WLOG, assume that $p_1 < p_2 < \dots < p_r$.

Let $q = p_1^{k_1 - 1} p_2^{k_2} \dots p_r^{k_r}$, then $n = p_1 q$.

It is clear that $p_1 \leq q \Rightarrow p_1^2 \leq p_1 q = n \Rightarrow p_1 \leq \sqrt{n}$.

$\Rightarrow \frac{1}{\sqrt{n}} \leq \frac{1}{p_i} \Rightarrow \frac{\sqrt{n}}{n} \leq \frac{1}{p_i} \Rightarrow \sqrt{n} \leq \frac{n}{p_i} \Rightarrow -\sqrt{n} \geq -\frac{n}{p_i}$.

Now, $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right)$

$\leq n\left(1 - \frac{1}{p_i}\right) \quad \left(\because 1 - \frac{1}{p_i} < 1\right)$.

$= n - \frac{n}{p_i} \leq n - \sqrt{n}$

Thus, $\varphi(n) \leq n - \sqrt{n}$.

Problem 10.

- Let $p_1, p_2, \dots, p_r$ be primes that divide n also divide m.
- Factorize $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.

$m = (p_1^{t_1} p_2^{t_2} \dots p_r^{t_r})(q_1^{s_1} q_2^{s_2} \dots q_j^{s_j})$, q_i is prime and $q_u \neq p_v$ $\forall u, v$.

$\Rightarrow mn = p_1^{k_1+t_1} p_2^{k_2+t_2} \dots p_r^{k_r+t_r} q_1^{s_1} q_2^{s_2} \dots q_j^{s_j}$.

$\Rightarrow \varphi(mn) = p_1^{k_1+t_1} \dots p_r^{k_r+t_r} q_1^{s_1} \dots q_j^{s_j} \left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_r}\right)\left(1 - \frac{1}{q_1}\right)\dots\left(1 - \frac{1}{q_j}\right)$

$= \left[p_1^{t_1} p_2^{t_2} \dots p_r^{t_r} q_1^{s_1} \dots q_j^{s_j} \left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_r}\right)\left(1 - \frac{1}{q_1}\right)\dots\left(1 - \frac{1}{q_j}\right)\right](p_1^{k_1} \dots p_r^{k_r})$

$= \varphi(m)\, n$

$\Rightarrow \varphi(mn) = n\,\varphi(m)$.

Problem 18.

Problem 18.

Write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $d_i = p_i - 1$.

* For $\varphi(n) = 16 = 2^4$, from the hint, we have conditions for d_i.

(1) $d_i \mid 2^4 \Rightarrow d_i \in \{1, 2, 4, 8, 16\}$

$\Rightarrow p_i \in \{2, 3, 5, 9, 17\}$.

(2) p_i is prime, so $p_i \in \{2, 3, 5, 17\}$.

$\Rightarrow n = 2^{k_1} 3^{k_2} 5^{k_3} 17^{k_4}$, $k_i \geq 0 \ \forall i \in [1, 4]$.

$\Rightarrow \varphi(n) = (2^{k_1} - 2^{k_1 - 1})(3^{k_2} - 3^{k_2-1})(5^{k_3} - 5^{k_3-1})(17^{k_4} - 17^{k_4-1})$

$\Rightarrow 16 = 2^{k_1-1}(3^{k_2-1} \times 2)(5^{k_3-1} \times 4)(17^{k_4-1} \times 16)$

$\Rightarrow k_4 \leq 1,\ k_3 \leq 1,\ k_2 \leq 2,\ k_1 \leq 5$.

If $k_4 = 1$ then $17^{1-1} \times 16 = 16$.

$\Rightarrow k_1 = k_2 = k_3 = 0$

$\Rightarrow n = 17$.

If $k_4 = 0$, then $16 = 2^{k_1-1}(3^{k_2-1} \times 2)(5^{k_3-1} \times 4)$

If $k_3 = 1$ then $k_2 = 1, k_1 = 2 \Rightarrow n = 60$

or $k_2 = 0, k_1 = 3 \Rightarrow n = 40$.

If $k_3 = 0$ then $k_2 = 1, k_1 = 4 \Rightarrow n = 48$

$k_2 = 0, k_1 = 5 \Rightarrow n = 32$.

Thus, the solution for $\varphi(n) = 16$ is $n \in \{17, 32, 40, 48, 60\}$.

* For $\varphi(n) = 24 = 2^3 . 3$.

$\Rightarrow (p_i - 1) \mid 24 \Rightarrow p_i - 1 \in \{1, 2, 3, 4, 6, 8, 12, 24\}$.

$\Rightarrow p_i \in \{2, 3, 4, 5, 7, 9, 13, 25\}$

Since p_i is prime, $p_i \in \{2, 3, 5, 7, 13\}$.

$\Rightarrow n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4} 13^{k_5}$, $k_i \geq 0 \ \forall i \in [1, 5]$.

Since p_i is prime, ...

$\Rightarrow n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4} 13^{k_5}$, $k_i \geq 0 \; \forall i \in [1,5]$.

$\Rightarrow \phi(n) = (2^{k_1} - 2^{k_1-1})(3^{k_2} - 3^{k_2-1})(5^{k_3} - 5^{k_3-1})(7^{k_4} - 7^{k_4-1})(13^{k_5} - 13^{k_5-1})$

$\Rightarrow 24 = 2^{k_1-1}(3^{k_2-1} \cdot 2)(5^{k_3-1} \cdot 4)(7^{k_4-1} \cdot 6)(13^{k_5-1} \cdot 12)$

$\Rightarrow k_5 \leq 1,\; k_4 \leq 1,\; k_3 \leq 2,\; k_2 \leq 3,\; k_1 \leq 5.$

For $k_5 = 1$ then $k_4 = 0$, $k_3 = 0$ and $k_2 = 1, k_1 = 0 \Rightarrow n = 39$

or $k_2 = 1, k_1 = 1 \Rightarrow n = 78$

or $k_2 = 0, k_1 = 2 \Rightarrow n = 52$

For $k_5 = 0$, i.e. $n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4}$.

$\Rightarrow 24 = 2^{k_1-1}(3^{k_2-1} \cdot 2)(5^{k_3-1} \cdot 4)(7^{k_4-1} \cdot 6)$

If $k_4 = 1$, there will be 4 cases:

$k_3 = 0, k_2 = 0, k_1 = 3 \Rightarrow n = 56$

$k_3 = 0, k_2 = 1, k_1 = 2 \Rightarrow n = 84$

$k_3 = 1, k_2 = 0, k_1 = 1 \Rightarrow n = 70$

$k_3 = 1, k_2 = 0, k_1 = 0 \Rightarrow n = 35$

$k_3 = 1, k_2 = 0, k_1 = 0$

If $k_4 = 0$, i.e $n = 2^{k_1} 3^{k_2} 5^{k_3}$.

$\Rightarrow 24 = 2^{k_1-1}(3^{k_2-1} \cdot 2)(5^{k_3-1} \cdot 4)$

If $k_3 = 1$ then $6 = 2^{k_1-1}(3^{k_2-1} \cdot 2)$

$\Rightarrow k_2 = 2, k_1 = 0 \Rightarrow n = 45$

or $k_2 = 2, k_1 = 1 \Rightarrow n = 90.$

If $k_3 = 0$, i.e $n = 2^{k_1} 3^{k_2}$ $\Rightarrow 24 = 2^{k_1-1}(3^{k_2-1} \cdot 2)$

$\Rightarrow k_2 = 2, k_1 = 3$

$\Rightarrow n = 73$

Thus, the solution for $\phi(n) = 24$ is

$n \in \{35, 39, 45, 52, 56, 70, 72, 78, 84, 90\}$.

$\boxed{\text{Sec 7.3}}$

$\boxed{\text{Sec 7.3}}$

Problem 3.

- From the hint, $2^{15} - 2^3 = 5 \cdot 7 \cdot 8 \cdot 9 \cdot 13$.

$$= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13.$$

- Note that: $\varphi(2^3) = 4$, $\varphi(3^2) = 6$, $\varphi(5) = 4$, $\varphi(7) = 6$, $\varphi(13) = 12$.

If $2 \mid a \Rightarrow 2^3 \mid a^3 \Rightarrow 2^3 \mid a^3(a^{12}-1) \Rightarrow 2^3 \mid a^{15} - a^3$.

Otherwise, $2 \nmid a \Rightarrow \gcd(2^3, a) = 1$ ($\because$ 2 is prime)

By Euler's theorem, $a^{\varphi(2^3)} \equiv 1 \pmod{2^3}$

$$\Rightarrow a^4 \equiv 1 \pmod{2^3}$$
$$\Rightarrow a^{12} \equiv 1 \pmod{2^3}$$
$$\Rightarrow a^{15} \equiv a^3 \pmod{2^3}$$
$$\Rightarrow 2^3 \mid a^{15} - a^3.$$

Thus, $2^3 \mid a^{15} - a^3 \quad \forall a \in \mathbb{Z}$. —— ①

Similarly for 3^2, 5, 7 and 13, we obtain

$$\left.\begin{array}{l} 3^2 \mid a^{15} - a^3 \\ 5 \mid a^{15} - a^3 \\ 7 \mid a^{15} - a^3 \\ 13 \mid a^{15} - a^3 \end{array}\right\} \forall a \in \mathbb{Z}. \text{ —— ②}$$

From ① and ②, we have $(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13) \mid a^{15} - a^3 \quad \forall a \in \mathbb{Z}$.

$$\Rightarrow (2^{15} - 2^3) \mid (a^{15} - a^3) \quad \forall a \in \mathbb{Z}.$$

Problem 4

Since $\gcd(a, n) = 1$, by Euler's theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$

$$\Rightarrow a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$$

Note that $a^{\varphi(n)} - 1 = (a-1)(a^{\varphi(n)-1} + a^{\varphi(n)-2} + \dots + a + 1)$

Hence, $(a-1)(a^{\varphi(n)-1} + a^{\varphi(n)-2} + \dots + a + 1) \equiv 0 \pmod{n}$

Since $\gcd(a-1, n) = 1$, we obtain
$$a^{\varphi(n)-1} + a^{\varphi(n)-2} + \dots + a + 1 \equiv 0 \pmod n.$$

Problem 7.

Note that $\gcd(10,3) = 1$, then by Euler's theorem,

$$3^{\varphi(10)} \equiv 1 \pmod{10}$$
$$\Rightarrow 3^4 \equiv 1 \pmod{10}$$
$$\Rightarrow (3^4)^{25} \equiv 1 \pmod{10}$$
$$\Rightarrow 3^{100} \equiv 1 \pmod{10}$$
$\Rightarrow$ Unit digit of 3^{100} is 1

Problem 10.

- If $2|a \Rightarrow 2|a^{4n+1} \Rightarrow 2|(a^{4n+1}-a) \Rightarrow a^{4n+1} \equiv a \pmod 2$

  If $2 \nmid a \Rightarrow a \equiv 1 \pmod 2 \Rightarrow a^{4n} \equiv 1 \pmod 2 \Rightarrow a^{4n+1} \equiv a \pmod 2$

  $\Rightarrow a^{4n+1} \equiv a \pmod 2 \ \forall a \in \mathbb{Z}$ —— (1)

- If $5|a \Rightarrow 5|a^{4n+1} \Rightarrow 5|(a^{4n+1}-a) \Rightarrow a^{4n+1} \equiv a \pmod 5$

  If $5 \nmid a \Rightarrow \gcd(5,a) = 1$, by Euler's theorem,

  $$a^{\varphi(5)} \equiv 1 \pmod 5 \Rightarrow a^4 \equiv 1 \pmod 5$$
  $$\Rightarrow a^{4n} \equiv 1 \pmod 5$$
  $$\Rightarrow a^{4n+1} \equiv a \pmod 5$$

  $\Rightarrow a^{4n+1} \equiv a \pmod 5 \ \forall a \in \mathbb{Z}$ —— (2)

From (1) and (2), $\begin{cases} a^{4n+1} \equiv a \pmod 2 \\ a^{4n+1} \equiv a \pmod 5 \end{cases} \Rightarrow a^{4n+1} \equiv a \pmod{10}$

$\Rightarrow a^{4n+1}$ and a has the same last digit.

$\boxed{\text{Sec 7.4}}$

Problem 3.

Since $\mu(n)$ and $\varphi(n)$ are multiplicative, $\dfrac{\mu^2(n)}{\varphi(n)}$ is also multiplicative

Since $\mu(n)$ and $\varphi(n)$ are multiplicative, $\frac{\quad}{\varphi(n)}$ is also multiplicative

$$\Rightarrow F(n) = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} \text{ is multiplicative as well}$$

For $n = p^k$, p is prime and $k \geq 1$.

$$F(p^k) = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{\mu^2(1)}{\varphi(1)} + \frac{\mu^2(p)}{\varphi(p)} + \dots + \frac{\mu^2(p^k)}{\varphi(p^k)}$$

$$= 1 + \frac{1}{p-1} + 0 + \dots + 0.$$

$$= \frac{p}{p-1}$$

For $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, p_i is prime and $k_i \geq 1$ $\forall i \in [1, r]$,

$$F(n) = F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r})$$

$$= \frac{p_1}{p_1 - 1} \cdot \frac{p_2}{p_2 - 1} \dots \frac{p_r}{p_r - 1}$$

Note that $\varphi(n) = n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right) \dots \left(\frac{p_r}{p_r-1}\right)$

Thus, $F(n) = \frac{n}{\varphi(n)}$

$$\Rightarrow \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}.$$

Problem 6.

From theorem 7.6, $n = \sum_{d|n} \varphi(d)$

Let $F(n) = \sum_{d|n} \varphi(d)$.

Since $F(n) = n$, $\sum_{d=1}^{n} F(d) = \frac{n(n+1)}{2}$. — ①

By theorem 6.11, $\sum_{d=1}^{n} F(d) = \sum_{d=1}^{n} \varphi(d)\left[\frac{n}{d}\right]$ — ②

$n \qquad n(n+1)$

$d=1 \qquad d=1$

From ① and ②, $\sum_{d=1}^{n} \varphi(n)\left[\frac{n}{d}\right] = \frac{n(n+1)}{2}$.

Problem 7.

$$F(n) = \sum_{d|n} \sigma(d^{k-1})\,\varphi(d) = \sum_{d|n} \underbrace{\sigma(d)\sigma(d)\dots\sigma(d)}_{k-1 \text{ times}}\varphi(d)$$

Since $\sigma(n)$ and $\varphi(n)$ are multiplicative, $F(n)$ is also multiplicative.

⊗ For $n=p$, p is prime.

$$F(p) = \sum_{d|n} \sigma(d^{k-1})\,\varphi(p) = \sigma(1)\varphi(1) + \sigma(p^{k-1})\varphi(p)$$
$$= 1 + \frac{p^{k-1+1}-1}{p-1}\cdot(p-1)$$
$$= 1 + p^k - 1 = p^k.$$

⊗ For $n = p_1 p_2 \cdots p_r$, p_i is prime $\forall i \in [1, r]$

$$F(n) = F(p_1 p_2 \cdots p_r) = F(p_1)F(p_2)\cdots F(p_r)$$
$$= p_1^k\, p_2^k \cdots p_r^k$$
$$= n^k.$$

Therefore, $\sum_{d|n} \sigma(d^{k-1})\,\varphi(n) = n^k$ for all square-free integer n and $k \geq 2$.

Problem 9.

⊗ Factorize $3n+2 = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.

Since $3n+2 \equiv 2 \pmod 3$, $\exists\, p_i$ such that $p_i^{k_i} \equiv 2 \pmod 3$.

$\Rightarrow p_i \equiv 2 \pmod 3$ $\Big($ $\because$ if $p_i \equiv 0 \pmod 3 \Rightarrow p_i^{k_i} \equiv 0 \pmod 3$
and if $p_i \equiv 1 \pmod 3 \Rightarrow p_i^{k_i} \equiv 1 \pmod 3$ $\Big)$

$p_i^1 \equiv 2 \pmod 3$, $p_i^2 \equiv 4 \equiv 1 \pmod 3$.

Notice that $p_i^0 \equiv 1 \pmod 3$, $p_i^1 \equiv 2 \pmod 3$, $p_i^2 \equiv 4 \equiv 1 \pmod 3$.

It can be seen that $p_i^{k_i} \equiv 2 \pmod 3 \iff k_i$ is odd.

Note that $p_i \equiv 2 \equiv -1 \pmod 3 \Rightarrow p^{k_i} \equiv -1 \pmod 3$ ($\because k_i$ is odd)

Now, $\sigma(p_i^{k_i}) = p_i^{k_i} + p_i^{k_i - 1} + \dots + p_i + 1 \equiv (-1)^{k_i} + (-1)^{k_i - 1} + \dots + (-1) + 1 \pmod 3$

$\equiv 0 \pmod 3$ ($\because k_i$ is odd)

$\Rightarrow 3 \mid \sigma(p_i^{k_i})$

$\Rightarrow 3 \mid \sigma(p_1^{k_1}) \dots \sigma(p_i^{k_i}) \dots \sigma(p_r^{k_r})$

$\Rightarrow 3 \mid \sigma(p_1^{k_1} \dots p_r^{k_r})$

$\Rightarrow 3 \mid \sigma(3n+2)$.

- Factorize $4n+3 = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.

$4n+3 \equiv 3 \pmod 4$.

If all $p_i^{k_i} \equiv 0 \pmod 4 \Rightarrow 4n+3 \equiv 0 \not\equiv 3 \pmod 4$

If all $p_i^{k_i} \equiv 1 \pmod 4 \Rightarrow (4n+3) \equiv 1 \not\equiv 3 \pmod 4$.

If all $p_i^{k_i} \equiv 2 \pmod 4 \Rightarrow 4n+3 \equiv 0$ or $2 \not\equiv 3 \pmod 4$

There must exists $p_i^{k_i} \equiv 3 \pmod 4$ for some i.

For $p_i \equiv 0 \pmod 4 \Rightarrow p_i^{k_i} \equiv 0 \pmod 4$

$p_i \equiv 1 \pmod 4 \Rightarrow p_i^{k_i} \equiv 1 \pmod 4$

$p_i \equiv 2 \pmod 4 \Rightarrow p_i^{k_i} \equiv 2^{k_i} \equiv 2 \pmod 4$

$\Rightarrow p_i \equiv 3 \pmod 4$.

$\Rightarrow p_i \equiv -1 \pmod 4$.

If k_i is even, $p_i^{k_i} \equiv 1 \pmod 4$

If k_i is odd, $p_i^{k_i} \equiv -1 \equiv 3 \pmod 4$

$\hookrightarrow k_i$ is odd.

Then, $\sigma(p_i^{k_i}) = p_i^{k_i} + p_i^{k_i - 1} + \dots + p + 1 \pmod 4$

$= (-1)^{k_i} + (-1)^{k_i - 1} + \dots + (-1) + 1 \pmod 4$

$\equiv 0 \pmod 4$ ($\because k_i$ is odd)

$\Rightarrow 4 \mid \sigma(p_i^{k_i}) \Rightarrow 4 \mid \sigma(p_1^{k_1}) \dots \sigma(p_i^{k_i}) \dots \sigma(p_r^{k_r})$

$\Rightarrow 4 \mid \sigma(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})$

$\Rightarrow 4 \mid \sigma(4n+3)$.

Problem 15.

Firstly, let's prove $f(d) = \varphi(\frac{n}{d})$ is multiplicative.

Let $G(n) = \sum_{d \mid n} \varphi(d)$, then $G(n)$ is multiplicative.

$\Rightarrow G(n) = \sum_{d \mid n} \phi(\frac{n}{d}) = \sum_{d \mid n} f(d) \Rightarrow f(d)$ is multiplicative.

$\Rightarrow \sum_{d \mid n} \sigma(d) f(d)$ is multiplicative.

⊛ For $n = p^k$, p is prime and $k \geq 1$.

$$\sum_{d \mid p^k} \sigma(d) \varphi(\frac{p^k}{d}) = \sigma(1)\varphi(\frac{p^k}{1}) + \sigma(p)\varphi(\frac{p^k}{p}) + \dots + \sigma(p^k)\varphi(\frac{p^k}{p^k}).$$

$$= 1(p^k - p^{k-1}) + (p+1)(p^{k-1} - p^{k-2}) + \dots + \frac{p^{k+1}-1}{p-1} \cdot 1$$

$$= (p^k - p^{k-1}) + (p^k - p^{k-1} + p^{k-1} - p^{k-2}) + \dots + (p^k - 1) + (p^k + p^{k-1} + \dots + p + 1).$$

$$= (p^k - p^{k-1}) + (p^k - p^{k-2}) + \dots + (p^k - 1) + (p^k + p^{k-1} + \dots + p + 1)$$

$$= (k+1) p^k$$

$$= \tau(p^k) p^k$$

For $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, p_i is prime and $k_i \geq 1 \ \forall i \in [1, r]$.

Since $\sum_{d \mid n} \sigma(d)\varphi(\frac{n}{d})$ is multiplicative, we have:

$$F(n) = \sum_{d \mid n} \sigma(d)\varphi(\frac{n}{d}) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r})$$

$$= p_1^{k_1} \tau(p_1^{k_1}) \, p_2^{k_2} \tau(p_2^{k_2}) \dots p_r^{k_r} \tau(p_r^{k_r})$$

$$= (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})\, \tau(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})$$
$$= n\,\tau(n)$$

⊗ Similar to above, $F(n) = \sum_{d|n} \tau(n)\varphi(\frac{n}{d})$ is multiplicative

For $n = p^k$, p is prime and $k \geq 1$.

$$F(p^k) = \sum_{d|p^k} \tau(d)\varphi\left(\frac{p^k}{d}\right) = \tau(1)\varphi\left(\frac{p^k}{1}\right) + \tau(p)\varphi\left(\frac{p^k}{p}\right) + \cdots + \tau(p^k)\varphi\left(\frac{p^k}{p^k}\right)$$

$$\Rightarrow F(p^k) = 1(p^k - p^{k-1}) + 2(p^{k-1} - p^{k-2}) + \cdots + (k+1)\cdot 1$$
$$= p^k - p^{k-1} + 2p^{k-1} - 2p^{k-2} + \cdots + k+1$$
$$= p^k + p^{k-1} + \cdots + 1$$
$$= \frac{p^{k+1} - 1}{p - 1} = \sigma(p^k)$$

For $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, p_i is prime and $k_i \geq 1$ $\forall i \in [1, r]$

Since $F(n)$ is multiplicative,

$$F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r})$$
$$= \sigma(p_1^{k_1})\, \sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r})$$
$$= \sigma(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})$$
$$= \sigma(n)$$

$$\Rightarrow \sum_{d|n} \tau(n)\varphi\left(\frac{n}{d}\right) = \sigma(n).$$

Problem 16.

Let $b_1, b_2, \ldots, b_{\varphi(n)}$ be positive integers that are coprime with n.

$\Rightarrow b_1 + b_2 + \cdots + b_{\varphi(n)} = \frac{1}{2} n\phi(n)$ for $n \geq 2$.

Note that $\varphi(n)$ is even for $n > 2$, so $\frac{1}{2}\varphi(n)$ is an integer.

$$\Rightarrow \frac{1}{2} n\phi(n) \equiv 0 \pmod{n}$$

$$\Rightarrow b_1 + b_2 + \cdots + b_{\varphi(n)} \equiv 0 \pmod{n}$$

Also, $b_i \not\equiv b_j \pmod{n}$ $\forall i \neq j$.

Since $a_1, a_2, \dots a_{\varphi(n)}$ form a reduced set of residues mod n,

$$\begin{cases} a_1 \equiv b'_1 \pmod{n} \\ a_2 \equiv b'_2 \pmod{n} \\ \vdots \\ a_{\varphi(n)} \equiv b'_{\varphi(n)} \pmod{n} \end{cases}$$

, where $b'_1, b'_2, \dots, b'_{\varphi(n)}$ is the sequence b in some order.

$$\Rightarrow a_1 + a_2 + \dots + a_{\varphi(n)} \equiv b'_1 + b'_2 + \dots + b'_{\varphi(n)} \equiv b_1 + b_2 + \dots + b_{\varphi(n)} \equiv 0 \pmod{n}$$