7-4 Some Properties of The Phi-Function

Note Title 11/2/2005

1. For a positive integer n, prove

$$\sum_{d|n} (-1)^{n/d} \phi(d) = \begin{cases} 0 & \text{if } n \text{ is even} \\ -n & \text{if } n \text{ is odd} \end{cases}$$

Pf: (1) If n is even, Then $n = 2^k N$, where $N = p_1^{k_1} \cdots p_r^{k_r}$, $p_i \neq 2$, and so N is odd.

Now break up The summation of $d|n$ into sums of divisors That always contain 2^k and all The other divisors. For divisors That always contain 2^k as a factor, This can be expressed as

$$\sum_{d|N} (-1)^{2^k N/2^k d} \phi(2^k d) = \sum_{d|N} (-1)^{N/d} \phi(2^k d)$$

But N is odd, so is d, so N/d is odd, and so $(-1)^{N/d} = -1$ $[d = p_1^{s_1} \cdots p_r^{s_r}, 0 \le s_i \le k_i, p_i \neq 2]$

$$\therefore \sum_{d|N} (-1)^{2^k N/2^k d} \phi(2^k d) = -\sum_{d|N} \phi(2^k d)$$

All The other divisors run over $2^{k-1} N$

$$\therefore \sum_{d|n} (-1)^{n/d} \phi(d) = \sum_{d|2^{k-1}N} (-1)^{2^k N/d} \phi(d) - \sum_{d|N} \phi(2^k d)$$

But as d runs over $2^{k-1}N$, $2^kN/d$ will always be even as the highest power of 2 for d is 2^{k-1}, so 2^kN will always have a factor of 2. $\therefore (-1)^{2^kN/d} = 1$

$$\therefore \sum_{d|n} (-1)^{n/d}\phi(d) = \sum_{d|2^{k-1}N} \phi(d) - \sum_{d|N} \phi(2^k d)$$

By Th. 7.6 from Gauss, $n = \sum_{d|n} \phi(d)$, so $\sum_{d|2^{k-1}N} \phi(d) = 2^{k-1}N$. Also, ϕ is multiplicative, so $\phi(2^k d) = \phi(2^k)\phi(d)$

$$\therefore \sum_{d|n} (-1)^{n/d}\phi(d) = 2^{k-1}N - \phi(2^k)\sum_{d|N}\phi(d)$$

$$= 2^{k-1}N - (2^k - 2^{k-1})(N)$$

$$= 2^{k-1}N - 2^kN + 2^{k-1}N$$

$$= 2\cdot 2^{k-1}N - 2^kN = 0$$

$$\therefore n \text{ even} \Rightarrow \sum_{d|n} (-1)^{n/d}\phi(d) = 0$$

(2) If n is odd, then $n = p_1^{k_1}\cdots p_r^{k_r}$, $p_i \neq 2$.
$\therefore d = p_1^{s_1}\cdots p_r^{s_r}$, $0 \le s_i \le k_i$, by Th. 6.1

$\therefore d$ is odd

$\therefore$ as d runs over n, n/d is odd, so $(-1)^{n/d} = -1$

$\therefore \sum_{d|n} (-1)^{n/d} \phi(d) = -\sum_{d|n} \phi(d) = -n$

$\therefore n$ odd $\Rightarrow \sum_{d|n} (-1)^{n/d} \phi(d) = -n$

2. Confirm That $\sum_{d|36} \phi(d) = 36$ and $\sum_{d|36} (-1)^{36/d} \phi(d) = 0$

The divisors, d, of 36 are: $1, 2, 3, 4, 6, 9, 12, 18, 36$
$\phi(d)$: $1, 1, 2, 2, 2, 6, 4, 6, 12$

$\therefore \sum_{d|36} \phi(d) = 1+1+2+2+2+6+4+6+12 = 36$

$\sum_{d|36} (-1)^{36/d} \phi(d) = 1+1+2-2+2+6-4+6-12 = 0$

3. For a positive integer n, prove That

$$\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(n)$$

Pf: By prob. #19, Sec. 6-1, if f and g are multiplicative, so is $f \cdot g$ and f/g.

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

Let $n = p^k$

$$\therefore F(p^k) = \sum_{d|p^k} \frac{\mu^2(d)}{\phi(d)} = \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + \cdots + \frac{\mu^2(p^k)}{\phi(p^k)}$$

$$= 1 + \frac{1}{p-1} + \cdots + 0$$

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

as $\mu(p^k) = 0$ for $k \geq 2$

$\therefore$ if $n = p_1^{k_1} \cdots p_r^{k_r}$, then

$$F(n) = F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r})$$

$$= \frac{p_1}{p_1 - 1} \cdots \frac{p_r}{p_r - 1}$$

From Th. 7.3, $\phi(n) = n\left(\frac{p_1 - 1}{p_1}\right) \cdots \left(\frac{p_r - 1}{p_r}\right)$

$$\therefore \left(\frac{p_1 - 1}{p_1}\right) \cdots \left(\frac{p_r - 1}{p_r}\right) = \frac{\phi(n)}{n}$$

$$\therefore F(n) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$$

4. Use problem 4(c), Sec. 6.2, to give a proof of the fact that $n \sum_{d|n} \mu(d)/d = \phi(n)$.

Pf: Prob. 4(c) states $\sum_{d|n} \mu(d)/d = (1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r})$ if $n = p_1^{k_1}\cdots p_r^{k_r}$.

$$\therefore n \sum_{d|n} \mu(d)/d = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r})$$

$$= \phi(n) \quad \text{by Th. 7.3}$$

5. If $n>1$ has the prime factorization $n = p_1^{k_1}\cdots p_r^{k_r}$, establish each of the following:

(a) $\sum_{d|n} \mu(d)\phi(d) = (2-p_1)(2-p_2)\cdots(2-p_r)$

Pf: Since μ and ϕ are multiplicative, then $\mu\cdot\phi$ is multiplicative (prob. 19, Sec. 6.1).

$\therefore F(n) = \sum_{d|n} \mu(d)\phi(d)$ is multiplicative.

$$F(p^k) = \sum_{d|p^k} \mu(d)\,\phi(d)$$

$$= \mu(1)\cdot\phi(1) + \mu(p^1)\cdot\phi(p^1) + \dots + \mu(p^k)\cdot\phi(p^k)$$

$$= 1 + (-1)(p-1) + 0 + 0 + \dots + 0 = 2-p,$$

since $\mu(p^k) = 0$ for $k \geq 2$

$$\therefore F(n) = F(p_1^{k_1}\cdots p_r^{k_r}) = F(p_1^{k_1})\cdots F(p_r^{k_r})$$

$$= (2-p_1)\cdots(2-p_r)$$

=

Could also have used prob. 3, Sec. 6-2, which says,

$$\sum_{d|n} \mu(d) f(d) = (1-f(p_1))\cdots(1-f(p_r))$$

where f is multiplicative, not identically zero. But ϕ is multiplicative and not identically zero (e.g., $\phi(1)=1$, $\phi(p) = p-1$).

$$\therefore \sum_{d|n} \mu(d)\,\phi(d) = (1-\phi(p_1))\cdots(1-\phi(p_r))$$

$$= (1-(p_1-1))\cdots(1-(p_r-1))$$

$$= (2-p_1)\cdots(2-p_r)$$

(6) $\sum_{d|n} d\cdot\phi(d) = \left(\frac{p_1^{2k_1+1}+1}{p_1+1}\right)\cdots\left(\frac{p_r^{2k_r+1}+1}{p_r+1}\right)$

Pf: $f(x)=x$ is multiplicative, $\therefore f\cdot\phi$ is also.

$\therefore F(n) = \sum_{d|n} d\cdot\phi(d)$ is multiplicative.

(1) Consider $F(p^k) = \sum_{d|p^k} d\cdot\phi(d)$

$$= 1\cdot\phi(1) + p\cdot\phi(p) + p^2\cdot\phi(p^2) + \dots + p^k\cdot\phi(p^k)$$

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

$$= 1 + p^2 - p + p^4 - p^3 + p^6 - p^5 + \dots + p^{2k} - p^{2k-1}$$

$$= 1 + (-1)^1 p + (-1)^2 p^2 + (-1)^3 p^3 + \dots + (-1)^{2k} p^{2k}$$

But $(a^{2r+1}+1) = (a+1)(a^{2r} - a^{2r-1} + a^{2r-2} - a^{2r-3} + \dots + r^2 - r + 1)$

(i.e., coefficient of 1 for even exponents, -1 for odd exponents).

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

$$\therefore \frac{p^{2k+1}+1}{p+1} = p^{2k} - p^{2k-1} + \dots + p^2 - p + 1$$

$$\therefore F(p^k) = \frac{p^{2k+1}+1}{p+1}$$

(2) $$\therefore \sum_{d|n} d\cdot\phi(d) = F(n) = F(p_1^{k_1}\cdots p_r^{k_r})$$

$$= F(p_1^{k_1})\cdot\dots\cdot F(p_r^{k_r})$$

$$= \left(\frac{p_1^{2k_1+1}+1}{p_1+1}\right)\cdots\left(\frac{p_r^{2k_r+1}+1}{p_r+1}\right)$$

(C) $$\sum_{d|n} \frac{\phi(d)}{d} = \left(1+\frac{k_1(p_1-1)}{p_1}\right)\cdots\left(1+\frac{k_r(p_r-1)}{p_r}\right)$$

Pf: $f(x) = \frac{1}{x}$ is multiplicative.

$\therefore F(n) = \sum_{d|n} \frac{\phi(d)}{d}$ is multiplicative

(1) Consider $F(p^k) = \sum_{d|p^k} \phi(d)/d$

$$= \frac{\phi(1)}{1} + \frac{\phi(p)}{p} + \dots + \frac{\phi(p^k)}{p^k}$$

$$= 1 + \frac{p-1}{p} + \frac{p^2-p}{p^2} + \cdots + \frac{p^k-p^{k-1}}{p^k}$$

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

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

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

(2) $\therefore \sum_{d|n} \frac{\phi(d)}{d} = F(n) = F(p_1^{k_1} \cdots p_r^{k_r})$

$$= F(p_1^{k_1}) \cdots F(p_r^{k_r})$$

$$= \left(1 + \frac{k_1(p_1-1)}{p_1}\right) \cdots \left(1 + \frac{k_r(p_r-1)}{p_r}\right)$$

C. Verify the formula $\sum_{d=1}^{n} \phi(d) \left[\frac{n}{d}\right] = \frac{n(n+1)}{2}$, $n > 0$.

Pf: From Th. 7.6, if $n > 0$, $n = \sum_{d|n} \phi(d)$

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

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

But by Th. 6.11, $\sum_{d=1}^{N} F(d) = \sum_{d=1}^{N} \phi(d)\left[\frac{N}{d}\right]$

$$\therefore \sum_{d=1}^{N} \phi(d)\left[\frac{N}{d}\right] = \frac{N(N+1)}{2}$$

7. If n is square-free, prove $\sum_{d|n} \sigma(d^{k-1})\phi(d) = n^k$ for $k \geq 2$.

Pf: σ and ϕ are multiplicative, so

$$F(n) = \sum_{d|n} \sigma(d^{k-1})\phi(d) = \sum_{d|n} \underbrace{\sigma(d)\cdots\sigma(d)}_{k-1 \text{ times}} \cdot \phi(d) \quad (\text{since } k \geq 2)$$

is also multiplicative.

(1) Consider $n = p$ (n is square-free)

$$\therefore F(p) = \sum_{d|p} \sigma(d^{k-1})\phi(d)$$

$$= \sigma(1)\phi(1) + \sigma(p^{k-1})\phi(p)$$

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

(2) $\therefore$ if $n = p_1 p_2 \cdots p_r$, Then

$$\sum_{d|n} \sigma(d^{k-1})\phi(d) = F(n) = F(p_1)F(p_2)\cdots F(p_r)$$

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

8. For a square-free integer $n > 1$, show that $\tau(n^2) = n$ if and only if $n = 3$.

Pf: (1) If $n = 3$, then $\tau(n^2) = \tau(3^2) = 2+1 = 3$ by Th. 6.2

(2) Suppose n is square-free, $n > 1$, and $\tau(n^2) = n$

Let $n = p_1 p_2 \cdots p_r$, where $p_i \neq p_j$ since n is square-free.

By Th. 6-2, $\tau(n^2) = \tau(p_1^2 p_2^2 \cdots p_r^2)$

$$= (2+1)(2+1)\cdots(2+1) = 3^r$$

$\therefore \tau(n^2) = n = p_1 p_2 \cdots p_r = 3^r$

By Th. 3.1 and its corollaries, all $p_i = 3$, which mean $n = 3$ and $r = 1$.

9. Prove that $3 \mid \sigma(3n+2)$ and $4 \mid \sigma(4n+3)$ for any positive integer n.

(a) $3 \mid \sigma(3n+2)$

Let $3n+2 = p_1^{k_1} \cdots p_r^{k_r}$

Since $3 \equiv 0 \pmod 3$ and $3n+2 \equiv 2 \pmod 3$,
Then $p_i^{k_i} \not\equiv 0 \pmod 3$ for $i = 1, 2, \ldots, r$

If all $p_i^{k_i} \equiv 1 \pmod 3$, Then $p_1^{k_1} \cdots p_r^{k_r} \equiv 1 \pmod 3$
Since $p_1^{k_1} \cdots p_r^{k_r} \equiv 2 \pmod 3$, There must
be one p_i s.t. $p_i^{k_i} \equiv 2 \pmod 3$
(and $\therefore$ $p_i \equiv 2 \pmod 3$, for if $p_i \equiv 0$, Then
$p_i^{k_i} \equiv 0$, and if $p_i \equiv 1$, Then $p_i^{k_i} \equiv 1$)

Since $p_i \equiv 2 \pmod 3$, Then

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

$\therefore$ if $p_i^r \equiv 2 \pmod 3$, Then r is odd.

$\therefore$ for $p_i^{k_1} \equiv 2 \pmod 3$, k_i is odd.

$$\therefore \sigma(p_i^{k_i}) = \frac{p_i^{k_i+1} - 1}{p_i - 1} = \frac{(p_i - 1)(p_i^{k_i} + p_i^{k_i-1} + \cdots + p_i + 1)}{p_i - 1}$$

$= p_i^{k_i} + p_i^{k_i-1} + \cdots + p_i + 1$, and k_i is odd.

Note $2 \equiv -1 \pmod 3$, so

if r is odd, $p_i^r \equiv -1 \pmod 3$
if r is even, $p_i^r \equiv 1 \pmod 3$

$$\therefore \sigma(p_i^{k_i}) = p_i^{k_i} + p_i^{k_i-1} + \dots + p_i + 1$$

$$\equiv (-1) + 1 + \dots + (-1) + 1 \pmod 3$$

$$\equiv 0 \pmod 3$$

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

$$\Rightarrow 3 \mid \sigma(p_1^{k_1} \cdots p_r^{k_r}) \quad [\sigma \text{ is multiplicative}]$$

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

(b) $4 \mid \sigma(4n+3)$

Let $4n+3 = p_1^{k_1} \cdots p_r^{k_r}$

$4n+3 \equiv 3 \equiv -1 \pmod 4$

As in (a), all $p_i^{k_i} \not\equiv 1 \pmod 4$, and $p_i^{k_i} \not\equiv 0 \pmod 4$
since if $p_i^{k_i} \equiv 0 \pmod 4 \Rightarrow 4n+3 \equiv 0 \pmod 4$

If $p_i^{k_i} \equiv 2 \pmod 4$ for any i, then

$p_1^{k_1} \cdots p_r^{k_r} \equiv 2$ or $3 \pmod 4$, $p_j \not\equiv p_i$, so

$$4n+3 = p_i^{k_i} p_1^{k_1} \cdots p_r^{k_r} \equiv 2\cdot 2 \text{ or } 2\cdot 3 \pmod 4$$
$$\equiv 0 \text{ or } 2 \pmod 4$$

$\therefore p_i^{k_i} \not\equiv 2 \pmod 4$ for any i.

$\therefore p_i^{k_i} \equiv 3 \equiv -1 \pmod 4$ for some i,

and $\therefore p_i \equiv 3 \pmod 4$

for $p_i \equiv 0 \Rightarrow p_i^{k_i} \equiv 0 \pmod 4$
$p_i \equiv 1 \Rightarrow p_i^{k_i} \equiv 1 \pmod 4$
$p_i \equiv 2 \Rightarrow p_i^{k_i} \equiv 2 \pmod 4$

$\therefore p_i^2 \equiv 9 \equiv 1 \pmod 4 \Rightarrow p_i^{2K} \equiv 1 \pmod 4$
for all K

$\therefore$ if s is even, $p_i^s \equiv 1 \pmod 4$

$\therefore p_i^{k_i} \equiv -1 \pmod 4 \Rightarrow k_i$ is odd

As in (a) $\sigma(p_i^{k_i}) = p_i^{k_i} + p_i^{k_i - 1} + \cdots + p_i + 1$

$$\equiv (-1) + 1 + \cdots + (-1) + 1$$

$$\equiv 0 \pmod 4$$

$\therefore 4 \mid \sigma(p_i^{k_i})$

$\therefore 4 \mid \sigma(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) \Rightarrow 4 \mid \sigma(4n+3)$

10. (a) Given $k > 0$, establish that there exists a sequence of k consecutive integers $n+1, n+2, \ldots, n+k$ satisfying

$$\mu(n+1) = \mu(n+2) = \ldots = \mu(n+k) = 0$$

Pf: Use the author's hint. Let p_k be the kth prime.

$\therefore \gcd(p_i^2, p_j^2) = 1$ for $i \neq j$.

$\therefore$ By the Chinese Remainder Th., there is a solution to :

$$x \equiv -1 \pmod{p_1^2}$$
$$x \equiv -2 \pmod{p_2^2}$$
$$\vdots$$
$$x \equiv -k \pmod{p_k^2}$$

where $p_1 = 2$, $p_2 = 3$, $\ldots$, $p_k = k$th prime

By the discussion on p. 138, if $n = p_1 p_2 \cdots p_k$ and $N_i = n/p_i$, then a simultaneous solution is:

$$x = (-1)N_1^{\phi(p_1^2)} + (-2)N_2^{\phi(p_2^2)} + \ldots + (-k)N_k^{\phi(p_k^2)}$$

$\therefore x = -N_1^{\phi(2^2)} - 2N_2^{\phi(3^2)} - \dots - kN_k^{\phi(p_k^2)}$

$\therefore x + i \equiv 0 \pmod{p_i^2}$ for $i = 1, 2, \dots, k$

$\therefore x + i = a p_i^2$, some a

so $\mu(x+i) = 0$, $i = 1, 2, \dots, k$

(b) Find four consecutive integers for which $\mu(n) = 0$

By (a), consider
$$x \equiv -1 \pmod{2^2}$$
$$x \equiv -2 \pmod{3^2}$$
$$x \equiv -3 \pmod{5^2}$$
$$x \equiv -4 \pmod{7^2}$$

Let $s = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 = 44100$

$N_1 = s/2^2 = 3^2 \cdot 5^2 \cdot 7^2 = 11025$

$N_2 = s/3^2 = 2^2 \cdot 5^2 \cdot 7^2 = 4900$

$N_3 = s/5^2 = 2^2 \cdot 3^2 \cdot 7^2 = 1764$

$N_4 = s/7^2 = 2^2 \cdot 3^2 \cdot 5^2 = 900$

Also, $\phi(2^2) = 2$, $\phi(3^2) = 6$, $\phi(5^2) = 20$, $\phi(7^2) = 42$

$\therefore$ a simultaneous solution is:

$$x = -(11025)^2 - 2(4900)^6 - 3(1764)^{20} - 4(900)^{42}$$

$\therefore \mu(x+1) = \mu(x+2) = \mu(x+3) = \mu(x+4) = 0$

But This is a rather awkward number.
$\therefore$ solve by method developed in proof of Chinese Remainder Th. in sec. 4.4.

Using N_1, N_2, N_3, N_4 as above, and
$a_1 = -1,\ a_2 = -2,\ a_3 = -3,\ a_4 = -4$

$11025 x_1 \equiv 1 \pmod 4$
$\therefore 11025 x_1 - 11024 x_1 \equiv 1$
$x_1 \equiv 1 \pmod 4$

$4900 x_2 \equiv 1 \pmod 9$
$4900 x_2 - 9 \cdot 544 x_2 \equiv 1$
$4 x_2 \equiv 1 + 3 \cdot 9 = 28$
$x_2 \equiv 7 \pmod 9$

$1764 x_3 \equiv 1 \pmod{25}$
$\therefore 1764 x_3 - 1750 x_3 \equiv 1$
$14 x_3 \equiv 1,\ 28 x_3 \equiv 2$
$3 x_3 \equiv 2 + 25 = 27$
$\therefore x_3 \equiv 9 \pmod{25}$

$900 x_4 \equiv 1 \pmod{49}$
$900 x_4 - 18 \cdot 49 x_4 \equiv 1$
$18 x_4 \equiv 1,\ 54 x_4 \equiv 3$
$54 x_4 - 49 x_4 \equiv 3$
$5 x_4 \equiv 3,\ 50 x_4 \equiv 30$
$\therefore x_4 \equiv 30$

$\therefore x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4$

$= -11025(1) - 2(4900)(7) - 3(1764)(9) - 4(900)(30)$
$= -11025 - 68600 - 47628 - 108000$

$= -235253$

$\therefore x = -235{,}253$ is a solution.

Can make this number smaller noting that the solution is unique modulo $2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 = 44{,}100$.

$\therefore x = -235{,}253 + 6(44{,}100) = 29{,}347$

$$\begin{aligned} \therefore\ x+1 &= 29{,}348 = 2^2 \cdot 11 \cdot 23 \cdot 29 \\ x+2 &= 29{,}349 = 3^3 \cdot 1087 \\ x+3 &= 29{,}350 = 2 \cdot 5^2 \cdot 587 \\ x+4 &= 29{,}351 = 7^2 \cdot 599 \end{aligned}$$

$\therefore \mu(x+1) = \mu(x+2) = \mu(x+3) = \mu(x+4) = 0$

11. Modify the proof of Gauss's Th. to establish

$$\sum_{k=1}^{n} \gcd(k,n) = \sum_{d \mid n} d \cdot \phi\left(\frac{n}{d}\right) = n \sum_{d \mid n} \frac{\phi(d)}{d}, \text{ for } n \geq 1$$

Pf: Let d be a divisor of n. Create set S_d s.t.

$$S_d = \{m : \gcd(m,n) = d;\ 1 \leq m \leq n\}$$

Let $N = \{1, 2, \ldots, n\}$

If $a \in N$, then if $\gcd(a,n) = 1$, then $a \in S_1$
If $\gcd(a,n) = c > 1$, then $a \in S_c$.
$\therefore$ $a \in N$ is in at least one set S_i

But every $a \in N$ is in at most one set S_i.
For if $a \in S_i$, $a \in S_j$, $i \neq j$, then
$\gcd(a,n) = i = j$.

$\therefore$ The sets S_d partition N into a finite number of sets.

$$\gcd(m,n) = d \iff \gcd(m/d, n/d) = 1 \qquad [1]$$

Pf: (a) By corollary 1 to Th. 2.4 in Sec. 2.2,
$\gcd(m,n) = d \Rightarrow \gcd(m/d, n/d) = 1$
(b) Suppose $\gcd(m/d, n/d) = 1$
$\therefore$ There are integers x, y s.t.
$\frac{m}{d} x + \frac{n}{d} y = 1$, $\therefore$ $mx + ny = d$
Suppose $\gcd(m,n) = c$. $\therefore$ $m = ac$, $n = bc$

$\therefore$ $(ac)x + (bc)y = d \Rightarrow c \mid d$
$\therefore$ By Th. 2.5, Sec. 2.2, $d = \gcd(m,n)$

Also, for S_d, $1 \le m \le n$, so $m/d \le \frac{n}{d}$.

$\therefore$ From [1], # elements in S_d = # positive integers, $\le n/d$, that are relatively prime to n/d, and this is $\phi(n/d)$.

Thus, # elements in $S_d = \phi(n/d)$

$$\therefore \sum_{k \in S_d} \gcd(k,n) = d \cdot \phi(n/d), \text{ since } \gcd(k,n) = d$$

As mentioned above, S_d exactly partitions N.

$$\therefore \sum_{k=1}^{n} \gcd(k,n) = \sum_{d|n} d \cdot \phi(n/d)$$

Now when $d|n$, there is a d' s.t. $d \cdot d' = n$, so that $\{d : d|n\} = \{d' : d|n\}$

$$\therefore \sum_{d|n} d \cdot \phi(n/d) = \sum_{d'|n} d' \cdot \phi(n/d')$$

$$= \sum_{\frac{n}{d}|n} \frac{n}{d} \cdot \phi\left(\frac{n}{n/d}\right) = n \sum_{d|n} \frac{\phi(d)}{d}$$

12. For $n > 2$, establish $\phi(n^2) + \phi((n+1)^2) \le 2n^2$

Pf: Relation does work for $n = 2$

$$\phi(2^2) + \phi((2+1)^2) = \phi(4) + \phi(9) = 2 + 6 = 8 \le 2 \cdot 2^2 = 8$$

By problem 7(c), Sec. 7.2, if K is composite, $\phi(K) \le K - \sqrt{K}$

n^2 is composite, so is $(n+1)^2$

$$\therefore \phi(n^2) \le n^2 - \sqrt{n^2} = n^2 - n$$

$$\phi((n+1)^2) \le (n+1)^2 - \sqrt{(n+1)^2}$$
$$= n^2 + 2n + 1 - (n+1)$$
$$= n^2 + n$$

$$\therefore \phi(n^2) + \phi((n+1)^2) \le n^2 - n + n^2 + n = 2n^2$$

13. Given integer n, prove there exists at least one K for which $n \mid \phi(K)$.

Pf: If $K = p_1^{k_1} \cdots p_r^{k_r}$ so that

$$\phi(K) = p_1^{k_1 - 1} \cdots p_r^{k_r - 1}(p_1 - 1) \cdots (p_r - 1)$$

We want $n = p_1^{k_1 - 1} \cdots p_r^{k_r - 1}$

$\therefore$ Let $n = q_1^{a_1} \cdots q_s^{a_s}$

Then choose $K = q_1^{a_1+1} \cdots q_s^{a_s+1}$

$\therefore \phi(K) = q_1^{a_1} \cdots q_s^{a_s} (q_1 - 1) \cdots (q_s - 1)$

and clearly $n \mid \phi(K)$

14. Show that if n is the product of twin primes, say $n = p(p+2)$, then $\phi(n)\sigma(n) = (n+1)(n-3)$

Pf: $\gcd(p, p+2) = 1$, so

$$\phi(n) = \phi(p) \cdot \phi(p+2) = (p-1)(p+2-1) = (p-1)(p+1)$$

But $\sigma(n) = \sigma(p)\,\sigma(p+2) = (p+1)(p+3)$

$$\therefore \phi(n)\sigma(n) = (p-1)(p+1)^2(p+3)$$

Now $(n+1)(n-3) = (p^2 + 2p + 1)(p^2 + 2p - 3)$

$$= (p+1)^2 (p+3)(p-1)$$

$$\therefore \phi(n)\sigma(n) = (n+1)(n-3)$$

15. Prove (a) $\sum_{d|n} \sigma(d)\phi(n/d) = n\tau(n)$ and

(b) $\sum_{d|n} \tau(d)\phi(n/d) = \sigma(n)$

Lemma: if $d|n$, then $F(d) = \phi(\frac{n}{d})$ is multiplicative

Pf: For any number theoretic function f,

$$\sum_{d|n} f(d) = \sum_{d|n} f(\tfrac{n}{d})$$

$\therefore$ Let $F(n) = \sum_{d|n} \phi(d)$

Since ϕ is multiplicative, by Th. 6.4, F is multiplicative.

Let $g(d) = \phi(\frac{n}{d})$

$$\therefore F(n) = \sum_{d|n} \phi(d) = \sum_{d|n} \phi(\tfrac{n}{d}) = \sum_{d|n} g(d)$$

By Th. 6.8, $g(d) = \phi(\frac{n}{d})$ is multiplicative

$\therefore$ if $\gcd(r,s)=1$ and $rs|n$, then

$g(rs) = \phi(\frac{n}{rs}) = g(r)g(s) = \phi(\frac{n}{r})\phi(\frac{n}{s})$

(a) Since $F(n) = \sum_{d|n} \sigma(d)\phi\left(\frac{n}{d}\right)$ is multiplicative

by Lemma above and prob. 19, Sec. 6.1,

it suffices to show for $n = p^k$, p prime, That

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

because if $n = p_1^{k_1} \cdots p_r^{k_r}$, Then

$$F(n) = F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) =$$

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

$$= n\,\tau(n)$$

The divisors of p^k are $1, p, p^2, \ldots, p^{k-1}, p^k$
$(k+1)$ divisors $= \tau(p^k)$

$$\therefore F(p^k) = \sum_{d|p^k} \sigma(d)\phi\left(\frac{p^k}{d}\right)$$

$$= \sigma(1)\phi\left(\frac{p^k}{1}\right) + \sigma(p)\phi\left(\frac{p^k}{p}\right) + \ldots + \sigma(p^{k-1})\phi\left(\frac{p^k}{p^{k-1}}\right) + \sigma(p^k)\phi\left(\frac{p^k}{p^k}\right)$$

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

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

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

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

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

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

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

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

$$\therefore \sum_{d|n}\tau(d)\phi\left(\frac{n}{d}\right)=n\tau(n)$$

(b) Since, as in (a), $F(n)=\sum_{d|n}\tau(d)\phi\left(\frac{n}{d}\right)$ is multiplicative, it suffices to show, for p prime, $F(p^k)=\sigma(p^k)$, for then $\sum_{d|n}\tau(d)\phi\left(\frac{n}{d}\right)=\sigma(n)$

$$\therefore F(p^k)=\sum_{d|p^k}\tau(d)\phi\left(\frac{p^k}{d}\right)$$

$= \tau(1)\phi\left(\frac{p^k}{1}\right) + \tau(p)\phi\left(\frac{p^k}{p}\right) + \dots + \tau(p^{k-1})\phi\left(\frac{p^k}{p^{k-1}}\right) + \tau(p^k)\phi\left(\frac{p^k}{p^k}\right)$

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

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

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

$= \dfrac{p^{k+1} - 1}{p-1} = \sigma(p^k)$

$\therefore F(p^k) = \sigma(p^k)$

$\therefore \sum_{d|n} \tau(d)\phi\left(\frac{n}{d}\right) = \sigma(n)$

16. If $a_1, a_2, \dots, a_{\phi(n)}$ is a reduced set of residues modulo n, show $a_1 + a_2 + \dots + a_{\phi(n)} \equiv 0 \pmod{n}$, $n > 2$

Pf: Let $b_1, b_2, \dots, b_{\phi(n)}$ be the positive integers, less than n, that are relatively prime to n. Then by Th. 7-7,

for $n \geq 2$, $b_1 + b_2 + \dots + b_{\phi(n)} = \frac{1}{2} n \phi(n)$

But $n \equiv 0 \pmod{n}$. For $n > 2$, $\phi(n)$ is even, so $\frac{1}{2}\phi(n)$ is an integer, so

$$b_1 + \dots + b_{\phi(n)} = \frac{1}{2} n \phi(n) \equiv 0 \pmod{n}$$

Also, $b_i \not\equiv b_j \pmod{n}$ since $1 \le b_i, b_j < n$

Now, $a_1, a_2, \dots, a_{\phi(n)}$ are congruent, not necessarily in order of appearance, to $b_1, b_2, \dots, b_{\phi(n)}$, since both are reduced sets of residues.

$$\therefore \quad a_1 \equiv b_1' \pmod{n}$$
$$a_2 \equiv b_2' \pmod{n}$$
$$\vdots$$
$$a_{\phi(n)} \equiv b'_{\phi(n)} \pmod{n}$$

where $b_1', \dots, b'_{\phi(n)}$ are the integers $b_1, \dots, b_{\phi(n)}$ in some order.

$$\therefore a_1 + \dots + a_{\phi(n)} \equiv b_1' + \dots + b'_{\phi(n)} = b_1 + \dots + b_{\phi(n)} \equiv 0 \pmod{n}$$

$$\therefore a_1 + \dots + a_{\phi(n)} \equiv 0 \pmod{n} \qquad (n > 2)$$