3. $\phi(n) = \frac{n}{2}$ iff $n = 2^k \ \forall k \in \mathbb{Z}^+$

given $n = 2^k$ via theorem 7.1

$\phi(n) = \phi(2^k) = 2^k - 2^{k-1} = 2^k(1 - 1/2) = \frac{2^k}{2} = \frac{n}{2}$ ✓ the forward holds

$\therefore$ if $n = 2^k$ the proposition holds

Because $\phi(n) = \frac{n}{2}$, n must be even the only other possible form would be $n = 2^k M$ where M is odd. However this would mean that even numbers and those divisible by whichever prime factors M has (odd) would not be relatively prime anymore, and thus $\phi(n) < \frac{n}{2}$, prooving the reverse.

4. If $\phi(n) \mid n-1$ then n is square-free $\forall n \geq 2$

Trivially proovable for $n = p$ as theorem 7.1 gives

$\phi(n) = \phi(p) = p - 1 = n - 1$ $\therefore$ $n-1 \mid n-1$, $\phi(n) \mid n-1$

$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

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

$\phi(n) = \prod_{i \leq r} p_i^{k_i - 1}(p_i - 1)$ $\therefore$ if $p^2 \mid n$ then $p \mid \phi(n)$

and thus $\phi(n) \nmid p - 1$ and $\phi(n) \nmid n-1$

would be a contradiction.

5. $\phi(n^2) = n\phi(n)$

$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$n^2 = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^2$

Via 7.3 therm:

$\phi(n) = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})$

$\phi(n^2) = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^2 (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})$

$= n (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)$

$= n\,\phi(n)$ #

6. if $d = \gcd(n,m)$ then $\phi(n)\phi(m) = \phi(nm)\phi(d)/d$

lemma: if $d = \gcd(n,m)$ then $\phi\left(\frac{mn}{d}\right) = \phi(mn)/d$

let $d = \gcd(n,m) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

let $m \cdot n = p_1^{j_1} \cdot p_2^{j_2} \cdots p_r^{j_r}$

let $\frac{m \cdot n}{d} = p_1^{j_1-k_1} p_2^{j_2-k_2} \cdots p_r^{j_r-k_r}$

j_i will always be $> k_i$ as $d^2 \mid mn$

$$\phi\left(\frac{mn}{d}\right) = \prod_{i \le r} p_i^{j_i - k_i}\left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{i \le r} \frac{p_i^{j_i}}{p_i^{k_i}} \cdot \prod_{i \le r}\left(1 - \frac{1}{p_i}\right)$$

$$= \frac{\prod_{i \le r} p_i^{j_i}}{\prod_{i \le r} p_i^{k_i}} \cdot \prod_{i \le r}\left(1 - \frac{1}{p_i}\right)$$

$$= \frac{1}{d} \cdot mn \cdot \prod_{i \le r}\left(1 - \frac{1}{p_i}\right)$$

$$= \frac{1}{d} \cdot \phi(mn) \checkmark$$

We can assume WLOG that since $d = \gcd(m,n)$ that for at least one of the two given integers, lets say n, that $d \mid n$ but $d^2 \nmid n$.

Additionally, ϕ is multiplicative giving us

$$\phi(n)\phi(m) = \phi(d)\phi\left(\tfrac{n}{d}\right)\phi(m)$$ as $\gcd(n/d, m) = 1$

$$= \phi(d)\phi\left(\tfrac{nm}{d}\right)$$ via the lemma

$$= \phi(d)\tfrac{1}{d}\phi(nm)$$ commutative property

$$= \phi(nm)\phi(d)/d$$

#

8. if $\gcd(m,n)=1$ then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

equivalent to the simultaneous congruence

$$\cancel{m^{\phi(n)}} + n^{\phi(m)} \equiv 1 \pmod{m} \quad + \quad m^{\phi(n)} + \cancel{n^{\phi(m)}} \equiv 1 \pmod{n}$$

$$n^{\phi(m)} \equiv 1 \pmod{m} \checkmark \qquad m^{\phi(n)} \equiv 1 \pmod{n} \checkmark$$

Because both of these are proven by Euler's theorem, the original congruence holds and thus the proposition.

9. $\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\phi(n)} \quad \forall\, n \in \mathbb{Z}^+$

$\mu^2(d) = \begin{cases} 0 & \text{when } p^2 \mid d \text{ for some prime } p \\ 1 & \text{otherwise} \end{cases}$

lemma: $f(d) = \frac{\mu^2(d)}{\phi(d)}$ is a multiplicative function

- if given d is divided by a square p^2 or q^2

$f(p^2) = 0$ as $\mu^2(p^2) = 0$

$f(q)^2 = 0$ as $\mu^2(q^2) = 0$

$f(p^2)\, f(q^2) = 0$

$f(p^2 q^2) = 0$ as $\mu^2(p^2q^2) = 0$ is multiplicative

- if given d is squarefree, $\mu^2(d) = 1$ and thus

$f(d \text{ square free}) = \frac{1}{\phi(d)}$ which is also multiplicative as $\phi(d)$ is multiplicative

$f(a)\, f(b) = \frac{1}{\phi(a)} \cdot \frac{1}{\phi(b)} = \frac{1}{\phi(a \cdot b)} = f(ab)$ ✓

Therefore proving the proposition for all prime powers will prove it for all $n \in \mathbb{Z}$

LHS $\sum_{d|p^k} \frac{\mu^2(d)}{\phi(d)} = \frac{1}{\phi(1)} + \frac{1}{\phi(p)} = 1 + \frac{1}{(p-1)} = \frac{(p-1)+1}{(p-1)} = \frac{p}{p-1}$

RHS $\frac{n}{\phi(n)} = \frac{p^k}{\phi(p^k)} = \frac{\cancel{p^k}}{\cancel{p^k}(1-\frac{1}{p})} = \frac{1}{(1-\frac{1}{p})} = \frac{1}{\frac{p-1}{p}} = \frac{p}{p-1}$ ✓

Because it holds for a prime factor and the function is multiplicative the proposition must hold

10. The sum of integers from 1 to n that are relatively prime to n is congruent to 0 (mod n) $\forall\, n > 2$

$$\sum_{i=1}^{n} \left(\begin{cases} i & \text{if } \gcd(n,i)=1 \\ 0 & \text{else} \end{cases} \right) \equiv 0 \pmod{n}$$

<u>Theorem from class:</u> The sum of integers relatively prime to n $\in [1, n)$ is $\frac{1}{2} n \phi(n)$ $\forall\, n \geq 2$

via ↑

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

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

$$0 \equiv 0 \pmod{n} \quad \#$$