Euler's Theorem

1. Definition: The Euler ϕ Function is defined for natural num. m: $\phi(m)$ is equal to the number of integers in $\{1, 2, \dots, m-1\}$ that R.P. to m.

   e.g. $\phi(16) = 8$. $\{1, 2, 3, \dots, 16\}$: $1, 3, 5, 7, 9, 11, 13, 15$

2. Thm 7.2.14.: If p is prime. $\phi(p) = p-1$.

   proof: Considering set $S = \{1, 2, \dots, p-1\}$.

   Since p is prime, it's only divisor are 1 and p.

   $\forall n \in S$. $\gcd(p, n) = 1$. $\Rightarrow \phi(p) = p-1$.

3. Thm 7.2.15.: If p and q are distinct primes. then $\phi(pq) = (p-1)(q-1)$.

   proof: Assume. p, q be prime numbers.

   WLOG. Assume $p < q$.

   Let $N = p \cdot q$.

   WTS: $\phi(N) = (p-1)(q-1)$.

   Consider $S = \{1, 2, \dots. N-1\}$.

   $= \{1, 2, \dots, p, \dots, q, \dots, p \cdot q - 1\}$.

   Let $x \in S$.

   Since p, q are prime. $N = p \cdot q$ is the only factorization by FTA.

   If $\underbrace{\gcd(N, x) \neq 1}_{x \text{ must contain } p \cdot q}$. then $\underbrace{\gcd(p, x) \neq 1}_{p \mid x}$ or $\underbrace{\gcd(q, x) \neq 1}_{q \mid x}$. or both.

   Since $x < p \cdot q$.

   If $p \mid x$ and $p \mid x$. Then $p \cdot q \mid x$, which is impossible, gives. p and q can't divide x at same time. as $p \cdot q > x$ (we exclude the both cond.).

   Thus. $\phi(N) = |S| -$ num of multiples of p $-$ num of multiples of q.

   ① # of p: $p.\ 1 \cdot p, 2 \cdot p, \dots, (q-1) \cdot p$. $\longrightarrow q-1$

   ② # of q: $q,\ 1 \cdot q, 2 \cdot q, \dots, (p-1) \cdot q$. $\longrightarrow p-1$.

$\therefore \phi(N) = p\cdot q - 1 - (p-1) - (q-1)$.

$$= p\cdot q - p - q + 1 = p(q-1) - (q-1) = (p-1)(q-1).$$

e.g. Let p be a prime number. Prove. $\phi(p^2) = p^2 - p$.

WTS: $\phi(p^2) = p^2 - p$.

pf: Considering set $S = \{1, 2, \ldots, p^2 - 1\}$.

$\forall s \in S$. $s < p^2$.

Since p is a prime, if $\gcd(p, s) \neq 1$. then $\gcd(p^2, s) \neq 1$. (as $p | s$ when $\gcd(p, s) \neq 1$).

Thus. $\phi(p^2) = |S| -$ num of multiples of p. i.e. $\gcd(p, s) \neq 1$. $= \gcd(p^2, s) \neq 1$.

$$= p^2 - 1 - (p-1) = p^2 - p.$$

$\hookrightarrow p, 2p, 3p, \ldots, (p-1)p$.

4. Cancellation Law: If a is R.P. to m and $ax \equiv ay \pmod m$, then $x \equiv y \pmod m$.

proof: Assume a is R.P. to m. i.e. $\gcd(a, m) = 1$.

Assume. $ax \equiv ay \pmod m$.

WTS: $x \equiv y \pmod m$.

Since $ax \equiv ay \pmod m$. $m | (ax - ay)$. $\Rightarrow m | a(x - y)$

By Thm. 7.2.9., since a is R.P. to m, gives. $m | x - y$, i.e. $x \equiv y \pmod m$

$\blacksquare$.

5. Euler's Theorem: If m is a natural num. greater than 1 and a is a natural num R.P. to m, then $a^{\phi(m)} \equiv 1 \pmod m$.

proof: Let $a, m \in \mathbb{N}$. $m > 1$.

Assume. $\gcd(a, m) = 1$.

WTS: $a^{\phi(m)} \equiv 1 \pmod m$.

Considering set $S = \{1, 2, \ldots, m-1\}$.

Let $S' = \{r_1, \dots, r_{\phi(m)}\}$ be the num in S that is R.P. to m.

Thus. we have. $(ar_1)\cdot \dots \cdot (ar_{\phi(m)}) \equiv r_1 \cdot \dots \cdot r_{\phi(m)} \pmod m$.

$$\Rightarrow a^{\phi(m)} \cdot r_1 \cdot \dots \cdot r_{\phi(m)} \equiv r_1 \cdot \dots \cdot r_{\phi(m)} \pmod m.$$

Since. $\gcd(r_i, m) = 1$. $\forall i \in \{1, 2, \dots, \phi(m)\}$. gives. $a^{\phi(m)} \equiv 1 \pmod m$ by Thm. 7.2.16.

1). FLT is its special form when p is prime $p \nmid a$. i.e. $\gcd(p, a) = 1$.

Thus. $\phi(p) = p - 1$, gives. $a^{p-1} \equiv 1 \pmod p$.