Feb 1st

Euler Function

if n - natural number > 1

define $\varphi(n)$ = number of natural numbers $\leq n$ which are relatively prime to n

$\varphi(6) = 2$ — 1, 2, 3, 4, 5, 6

$\varphi(7) = 6$

if p is prime $\Rightarrow \varphi(p) = p-1$ — any $1 \leq a < p-1 \Rightarrow \gcd(a,p) = 1$

$\varphi(5) = 4$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = 2$

$\varphi(6) = 2$

$\varphi(7) = 6$

$\varphi(8) = 4$

$\varphi(p^k) = ?$

p - prime

$\varphi(9) = 6$

1, 2, 3, 4, 5, 6, 7, 8, 9

Which numbers are NOT relatively prime to p?

= all numbers divisible by p.

if $\gcd(a, p^k) \neq 1 \Rightarrow \gcd(a, p^k) = p^l \Rightarrow p \mid a$

$1p, 2p, 3p, \cdots, p^k$

$\frac{p^k}{p} = p^{k-1}$ numbers (need to get rid of these)

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

$\varphi(pq) = ?$ p, q primes $p \neq q$

$1, 2, 3, \cdots, pq$

Sps $1 \leq a < pq$ $\gcd(a, pq) \neq 1 \Rightarrow p \mid a$ or $q \mid a$

how many numbers are divisible by p? $\leq pq$

$p, 2p, 3p, \cdots qp$ — q numbers

numbers divisible by q

$q, 2q, 3q, \cdots pq$ — p numbers

But we double counted pq (the only # that divisible by p & q and $\leq pq$ is pq)

so $\boxed{\varphi(pq) = pq - p - q + 1}$

So we find $\varphi(10) = (2-1)(5-1) = 1 \cdot 4 = 4$

$10 - 2 - 5 + 1 = 4$

$\varphi(21) = 21 - 3 - 7 + 1 = 12$

$(3-1)(7-1) = 12$

$$\boxed{\varphi(p^k q^l) = (p^k - p^{k-1})(q^l - q^{l-1}) = p^k q^l - p^{k-1} q^l - p^k q^{l-1} + p^{k-1} q^{l-1}}$$

how many divisible by p?

$p \cdot 1, p \cdot 2, \cdots, p^k q^l$

$\frac{p^k q^l}{p} = p^{k-1} q^l$

divisible by q?

$\frac{p^k q^l}{q} = p^k q^{l-1}$

$\varphi(p^k q^l) = p^k q^l - p^{k-1} q^l - p^k q^{l-1} + 1$ (again one of the $p^k q^l$ number is double counted)

How many divisible by pq?

$pq \cdot 1, pq \cdot 2, \ldots, pq \frac{p^k q^l}{pq}$ $\Rightarrow p^{k-1} q^{l-1}$ numbers

$\varphi(12) = \varphi(2^2 3^1) = (2^2 - 2^1)(3^1 - 3^0) = (4-2)(3-1) = 4$

$\varphi(p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \cdots (p_l^{k_l} - p_l^{k_l - 1})$

n $= p_1^{k_1}(1 - \frac{1}{p_1}) p_2^{k_2}(1 - \frac{1}{p_2}) \cdots p_l^{k_l}(1 - \frac{1}{p_l})$

$= p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_l})$

$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_l})$

Theorem: Let a, n be relatively prime numbers

then $a^{\varphi(n)} \equiv 1 \pmod{n}$

if $n = p$ prime $\varphi(p) = p - 1$
$\gcd(a, p) = 1$ just means $p \nmid a$
$\Rightarrow$ if $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$
Fermat's Little Theorem $\longrightarrow$ special case of Eulers theorem when $n = p$ prime

Ex: $a = 5$, $n = 6$, $\varphi(6) = \varphi(2, 3) = 1 \cdot 2 = 2$
$5^{\varphi(6)} \equiv 5^2 \equiv 1 \bmod 6$

$a = 3$, $n = 20$, $\gcd(3, 20) = 1$
$\Rightarrow$ E theorem applies $3^{\varphi(20)} \equiv 1 \bmod 20$
$\varphi(20) = \varphi(2^2 \cdot 5^1) = (2^2 - 2^1)(5^1 - 5^0) = 2 \cdot 4 = 8$

$3^8 \equiv 1 \bmod 20$

$3^4 = 81 \equiv 1 \bmod 20$
$3^8 = (3^4)^2 = (81)^2 \equiv 1^2 \equiv 1 \bmod 20$

if $\gcd(a, n) \neq 1$, $a^{\varphi(n)} \not\equiv 1 \bmod n$

Ex: Find the last digit of 7^{102}
$7^{102} \bmod 10 = ?$

gcd.(7, 10) = 1 ⇒ Euler's Theorem applies

$7^{\varphi(10)} \equiv 1 \pmod{10}$

$\varphi(10) = \varphi(5 \cdot 2) = 4$

$7^4 \equiv 1 \mod 10$

Check $7^2 \equiv 49 \equiv -1 \mod 10$

$7^4 \equiv (-1)^2 \mod 10 \equiv 1 \mod 10$

$\Rightarrow 7^{4k} \equiv 1 \mod 10$

$7^{102} \equiv 9 \mod 10$