EULER TOTIENT FUNCTION.

$\phi(n)$ = Number of integers between 1 and n whose gcd with n is 1

$$\phi(n) = \left|\{x : 1 \leq x \leq n,\ gcd(x, n) = 1\}\right|$$

$\phi(41) = ?$
$\phi(32) = ?$
$\phi(35) = ?$
$\phi(600) = ?$

Rule 1:
If p is prime then $\phi(p) = p-1$

- 41 is prime, by definition 41 has only two factors - 1, 41.
$\therefore \phi(41) = 41-1 = 40$

Rule 2
If $a = p^n$ where p is prime then

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

- $32 = 2^5$,

$$\phi(32) = \phi(2^5) = 2^5 - 2^4 = 32-16 = 16$$

Rule 3

If $\gcd(m, n) = 1$, then

$$\phi(mn) = \phi(m)\,\phi(n)$$

- $\phi(35)$
$= \phi(5 \times 7)$
$= \phi(5) \cdot \phi(7)$
$= (5-1) \cdot (7-1)$
$= 4 \cdot 6 = 24$

- $\phi(600) = \phi(2^3 \times 3 \times 5^2)$

$= \phi(2^3) \times \phi(3) \times \phi(5^2)$

$= (2^3 - 2^2) \times (3-1) \times (5^2 - 5^1)$

$= (8-4) \times 2 \times (25-5)$

$= 4 \times 2 \times 20$

$= 160$.

Formula for $\phi(n)$
(Euler's Totient theorem)

If $p_1, p_2, \cdots p_k$ are the prime divisors of n

Then,

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$$\phi(600) = 600\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 600 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$$

$$= 160$$

(SAME ANSWER!)

EULER'S THEOREM

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

Show by calculation that Euler's Theorem is true for $n=10$, and all $a<n$.

$\phi(n) = 4 \quad \{1,3,7,9\}$.

$\therefore 1^4 = 1 \bmod 10$.

$3^4 = 81 \bmod 10 = 1 \bmod 10$

$7^4 = 2401 \bmod 10 = 1 \bmod 10$.

$9^4 = 6561 \bmod 10 = 1 \bmod 10$.

$\therefore$ Proved.

Use Euler's theorem to calculate $7^{133} \bmod 26$.

$(\mathbb{Z}_{26} = \bmod 26)$

Note that $\phi(26) = \phi(2\times13) = (2-1)(13-1)$
$= 1\times12 = 12$.

So $7^{12} \equiv 1 \bmod 26$

$7^{133} \bmod 26 = 7^{132+1} = 7^{12\cdot11+1} = (7^{12})^{11}\cdot 7$

$= ((7^{12})^{11}\cdot 7) \pmod{26}$

$= 1^{11}\cdot 7 = 7 \pmod{26}$

Let p and q be distinct primes.
Let a be a positive integer such
that $a < p$, and $a < q$
Let k be any positive integer
Prove that

$$a^{k(p-1)(q-1)+1} \equiv a \ (\text{mod } p \cdot q)$$

using Euler's theorem.

$$a^{\phi(n)} \equiv 1 \bmod n$$

$$a^{\phi(pq)} = 1 \bmod (pq)$$

Since $a < p$, $a < q$, $\gcd(a, p \cdot q) = 1$
using Euler's theorem

$$a^{\phi(pq)} \equiv 1 \bmod (pq)$$

Raising both sides to the power k

$$\left[a^{\phi(pq)}\right]^k \equiv 1^k \bmod (pq)$$

$$a^{k \cdot \phi(pq)} = 1 \bmod (pq)$$

$$a^{k \cdot \phi(pq)} \cdot a = a \bmod (pq)$$

$$a^{(k \cancel{+1}) \phi(pq)+1} = a \bmod (pq)$$

But

$$\phi(pq) = (p-1)(q-1)$$

$$a^{k(p-1)(q-1)+1} \equiv a \bmod (pq)$$