Wiktor Sierakowski

Eulers Totient Function

$\phi(n)$ = Number of positive integers less than n, which are coprime to n

2 numbers are co-prime if $\gcd(a,b) = 1$

(1) Show that $\phi(15) = 8$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

adding all coprimes we get 8

(2) investigate $\phi(p)$, where p is prime.

7 : 1 2 3 4 5 6 7
11 : 1 2 3 4 5 6 7 8 9 10
13 : 1 2 3 4 5 6 7 8 9 10 11 12

Since p is prime, its only factors are 1 and p. all the numbers less than p will share no factors other than 1, making every number less than p a coprime to p.

larger cases:
$\phi(547) = 546$
$\phi(557) = 556$

Hence, it can be said that $\phi(p)$ for p(prime) will evaluate to p-1 coprimes.

$\therefore \quad \phi(p) = p - 1$

(3) Investigate $\phi(2^n)$ where $n = 1, 2, 3$, $\phi(3^n)$ and $\phi(p^n)$

$\phi(2^n) \rightarrow$

$\phi(2) = 1$
$\phi(4) = 2$
$\phi(8) = 4$
$\phi(16) = 8$
$\vdots$
$\phi(256) = 128.$

$\phi(3^n) \rightarrow$

$\phi(3) = 2$
$\phi(9) = 6$
$\phi(27) = 18$
$\phi(81) = 54$
$\phi(243) = 162$

By observing both cases of $\phi(3^n)$ and $\phi(2^n)$ we can see that the pattern for $\phi(2^n)$ is 2^{n-1}.
However for $\phi(3^n)$ we have $3^n - 3^{n-1}$. If we look at the $\phi(2^n)$ sequence, the same sequence occurs just in a less obvious form
Hence:

$$\phi(p^n) = p^n - p^{n-1}, \text{ where } p \text{ is prime}$$

(4) what are $\phi(3)$ and $\phi(5)$. It is true that $\phi(15) = \phi(5) \times \phi(3)$ under which conditions is it true that $\phi(nm) = \phi(n) \times \phi(m)$?

$\phi(15) = 8$

$\phi(5) = 4$

$\phi(3) = 2$

$\therefore \phi(15) = \phi(5) \times \phi(3)$

Further Tests

$\phi(32) = 16$

$\phi(8) = 4$ $\quad 16 \neq 4 \times 2$

$\phi(4) = 2$

$\phi(77) = 60$

$\phi(7) = 6$ $\quad 60 = 6 \times 10$

$\phi(11) = 10$

$\phi(21) = 12$

$\phi(7) = 6$ $\quad 12 = 6 \times 2$

$\phi(3) = 2$

$\phi(143) = 120$

$\phi(13) = 12$ $\quad 120 = 12 \times 10$

$\phi(11) = 10$

$\phi(64) = 32$

$\phi(16) = 8$ $\quad 32 \neq 8 \times 2$

$\phi(4) = 2$

at first it may seem as if $\phi(mn) = \phi(m) \times \phi(n)$ if both m and n are both prime, however;

$$\phi(140) = \phi(20) \times \phi(7)$$
$$48 = 8 \times 6$$

where 20 is not prime.

The property that (20,7), (13,11) and (7,11) all share are the fact they are coprimes. 2 numbers have the coprime property if $\gcd(a,b) = 1$

Hence, it can be said that $\phi(mn) = \phi(m) \times \phi(n)$ if m and n are coprime to each other.

(5) Can you find a general Expression for $\phi(n)$

Every real number has a unique prime factorization.

consider the prime factorisation of n to be;

$$n = a_1^{b_1} \cdot a_2^{b_2} \cdot a_3^{b_3} \cdot a_4^{b_4}.$$

then from part (3) we know $\phi(p^n) = p^n - p^{n-1}$

so we will obtain

$$\left(a_1^{b_1} - a^{b_1-1}\right) \cdot \left(a_2^{b_2} - a_2^{b_2-1}\right) \cdot \ldots \cdot \left(a_4^{b_4} - a_4^{b_4-1}\right)$$

factorising:

$$a_1^{b_1}\left(1 - \frac{1}{a_1}\right) \cdot a_2^{b_2}\left(1 - \frac{1}{a_2}\right) \ldots \cdot a_4^{b_4}\left(1 - \frac{1}{a_4}\right)$$

$$= a_1^{b_1} a_2^{b_2} \ldots a_4^{b_4}\left(1 - \frac{1}{a_1}\right)\left(1 - \frac{1}{a_2}\right) \ldots \left(1 - \frac{1}{a_4}\right)$$

$a_1^{b_1} a_2^{b_2} \ldots a_4^{b_4}$ is the prime factorisation of n

$$\underbrace{a_1^{b_1} a_2^{b_2} \dots a_n^{b_n}}\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\dots\left(1-\frac{1}{a_n}\right)$$

prime factorisation of n

Simplifying obtains

$$\phi(n) = n\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\dots\left(1-\frac{1}{a_n}\right)$$

where a_1, a_2, a_n are distinct prime factors of n.

Alternate form using product notation

$$\phi(n) = n \prod_{a|n} \left(1-\frac{1}{a}\right)$$, where a is a distinct prime factor of n. ($n \bmod a \equiv 0$)

Checking:

$\phi(40) = 16$

$= 2^3 \times 5$

$= 40(1-1/2)(1-1/5)$

$= 40 \times \frac{1}{2} \times \frac{4}{5} = \frac{160}{10} = \underline{16}$

$\phi(250) = 100$

$250 = 5^3 \times 2$

$= 250\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$= 250 \times \frac{1}{2} \times \frac{4}{5}$

$= \frac{1000}{10} = \underline{100}$

$\phi(770) = 240$

$770 = 2 \times 5 \times 7 \times 11$

$= 770\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)$

$= 770\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\left(\frac{10}{11}\right)$

$= \frac{770 \times 240}{770}$

$= \underline{240}$

⑥ Extension: Euler-Fermat Theorem

Evaluate $x^{\phi(n)} \bmod n$ for different values of n and x under which conditions is it true that

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

$x = 12$
$n = 16$ $\quad 12^8 \bmod 16 = 0$
$\phi(n) = 8$

$x = 11$
$n = 13$ $\quad 11^{12} \bmod 13 = \underline{1}$
$\phi(n) = 12$

$x = 15$
$n = 18$ $\quad 15^6 \bmod 18 = 9$
$\phi(18) = 6$

$x = 17$
$n = 19$ $\quad 17^{18} \bmod 19 = 1$
$\phi(n) = 18$

$x = 23$
$n = 37$ $\quad 23^{36} \bmod 37 = 1$
$\phi(n) = 36$

proof of the Euler-Fermat Theorem;

Picking a residue system:

$a_1, a_2, a_3, a_4, a_5 \ldots a_k$

It follows the reduced residue system will be

$a_1, a_2, a_3, a_4, a_5 \ldots a_{\phi(x)}$

It can be proved that;

$ka_1, ka_2, ka_3, ka_4 \ldots ka_{\phi(x)}$

is also a reduced residue system

if and only if $\gcd(k, x) = 1$

It follows that both reduced residue systems' products are equal in modulo x.

$$(ka_1)(ka_2)\ldots(ka_{\phi(x)}) = (a_1)(a_2)(a_3)(a_{\phi(x)})$$

$$k^{\phi(x)}(a_1)(a_2)(a_3)\ldots(a_{\phi(x)}) = (a_1)(a_2)(a_3)\ldots(a_{\phi(x)}) \pmod{x}$$

(factoring out k)

$$k^{\phi(x)} = \frac{(a_1)(a_2)(a_3)\ldots(a_{\phi(x)})}{(a_1)(a_2)(a_3)\ldots(a_{\phi(x)})} \pmod{x}$$

$$k^{\phi(x)} \equiv 1 \pmod{x}$$

This is the same as $x^{\phi(n)} \equiv 1 \bmod n$

However for the second reduced residue system to be equivalent to the first, $\gcd(k, x)$ had to be 1, making them coprime.

Hence, for the Euler-Fermat theorem to $\equiv 1$, x and n must be coprimes.

going back to the examples;

$X = 12$ $\quad 12^8 \bmod 16 = 0$

$n = 16$

$\phi(n) = 8$ $\quad$ 12 and 16 are not coprime

$X = 11$ $\quad 11^{12} \bmod 13 = 1$

$n = 13$

$\phi(n) = 12$ $\quad$ 11 and 13 are coprimes

$X = 17$ $\quad 17^{18} \bmod 19 = 1$

$n = 19$

$\phi(n) = 18$ $\quad$ 17 and 19 are coprimes

As shown, for $X^{\phi(n)} \bmod n \equiv 1$ $\quad$ x and n must be coprimes.