The Euler-phi Function

Definition: An arithmetic function is a function that is defined for all positive integers.

Definition: An arithmetic function f is called multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n)=1$. It is called completely multiplicative if $f(mn) = f(m)f(n)$ for all $m,n \in \mathbb{Z}$.

Ex: $f(n)=1$ is completely multiplicative since $f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$.

Ex: $g(n)=n$ is also completely multiplicative since $g(mn) = mn = g(m)g(n)$.

Theorem 7.1: If f is a multiplicative function, and if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ is the prime power factorization of n, then

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_s^{\alpha_s}).$$

Proof: We use induction on s.
When $s=1$, $n = p_1^{\alpha_1}$ and then $f(n) = f(p_1^{\alpha_1})$ is trivially true.

Suppose the result is true for all positive integers n that has k distinct prime factors. Then, for any distinct primes $p_1, p_2, \ldots, p_k$,

$$f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}).$$

Now, let n be a positive integer with $k+1$ distinct positive prime factors.

Let

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k} \cdot q_{k+1}^{\beta_{k+1}}$$

Then,

$$\begin{aligned} f(n) &= f(q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k} \cdot q_{k+1}^{\beta_{k+1}}) \\ &= f(q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}) f(q_{k+1}^{\beta_{k+1}}) \\ &\quad (\because \gcd(q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}, q_{k+1}^{\beta_{k+1}}) = 1) \\ &= f(q_1^{\beta_1}) f(q_2^{\beta_2}) \cdots f(q_k^{\beta_k}) f(q_{k+1}^{\beta_{k+1}}) \\ &\quad \text{(by the induction hypothesis)} \end{aligned}$$

Hence the result.

<u>Theorem 7.2:</u> If p is prime, then $\varphi(p) = p-1$.

Conversely, if, for a positive integer $\varphi(p) = p-1$, then p is prime.

Proof: If p is prime, then every positive integer less than p is relatively prime to p. There are $p-1$ such integers. Hence,

$$\varphi(p) = p-1.$$

To prove the converse, suppose $\varphi(p) = p-1$. for a positive integer p, and that p is not prime. We derive a contradiction.

If p is not prime, then $p=1$ or p is composite.

If $p=1$ then $\varphi(p) \neq p-1$ because $\varphi(1)=1$.

Therefore, p is composite.

Then, $d \mid p$ for some $1<d<p$.

Then, $\gcd(d,p) > 1$. (Actually, $\gcd(d,p)$ should be greater than or equal to d.)

$\therefore \varphi(p) < p-1$, so $\varphi(p) \neq p-1$ again.

Hence the result.

Ex: $\varphi(7)=6$, $\varphi(11)=10$, $\varphi(97)=96$.

Ex: What is the value of $\varphi(p^2)$ when p is a prime? Let's investigate! Let's

list all integers k s.t. $1 \le k \le p^2$.

$$1, 2, 3, \dots, p-1, p, p+1, \dots, 2p, 2p+1, \dots, 3p, 3p+1, \dots, (p-1)p, (p-1)p+1, \dots, p^2.$$

The highlighted integers are the only integers that are <u>not</u> relatively prime to p.
There are p such integers.

$$\therefore \varphi(p^2) = p^2 - p = p^2\left(1 - \frac{1}{p}\right)$$

Ex: What is the value of $\varphi(p^3)$?
If we do as in the previous example, we see that

$$\varphi(p^3) = p^3 - p^2.$$

The following theorem generalizes these results.

<u>Theorem 7.3:</u> Let p be a prime and $\alpha \in \mathbb{Z}^+$.
Then,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Proof: The positive integers that are <u>not</u> relatively prime to p^α are the integers of the form kp where $1 \le k \le p^{\alpha-1}$.
Therefore, there are $p^{\alpha-1}$ such integers.

Therefore, there are $p^\alpha - p^{\alpha-1}$ integers that are relatively prime to p^α.

$$\therefore \quad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

<u>ex</u>: $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20.$

The integers relatively prime to 25 are

$1, 2, 3, 4, \cancel{5}, 6, 7, 8, 9, \cancel{10}, 11, 12, 13, 14, \cancel{15}, 16, 17, 18, 19, \cancel{20}, 21, 22, 23, 24, \cancel{25}$

<u>ex</u>: $\varphi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$

$\varphi(2^{10}) = 2^{10} - 2^9 = 2^9 = 512$

Next, we show that φ is multiplicative.

<u>Theorem 7.4</u>: Let $m, n \in \mathbb{Z}^+$ and $\gcd(m,n) = 1$.

Then, $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof: Look at the following array.

1	$m+1$	$2m+1$	$\dots$	$(n-1)m+1$
2	$m+2$	$2m+2$	$\dots$	$(n-1)m+2$
3	$m+3$	$2m+3$	$\dots$	$(n-1)m+3$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
r	$m+r$	$2m+r$	$\dots$	$(n-1)m+r$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
m	$2m$	$3m$	$\dots$	mn

Suppose r is an integer s.t. $1 \le r \le m$ and $\gcd(m,r) = d > 1$.
Then, no number in the rth row is relatively prime to mn, i.e.,

$$\gcd(km+r,\ mn) > 1 \text{ for all } k = 1, 2, \ldots, n-1$$

Hence, if there are integers $km+r$ such that $\gcd(km+r, mn) = 1$, we should look at the rth rows such that $\gcd(m,r) = 1$.

We wish to determine the number of integers of the $km+r$ such that $\gcd(m,r) = 1$.

In other words, we will find the integers in the list

$$r,\ m+r,\ 2m+r,\ \ldots,\ (n-1)m+r$$

that are relatively prime to mn, where $\gcd(m,r) = 1$.

By Theorem 4.7, the n integers in the list form a complete system of residues modulo n.

Therefore, for each l with $0 \le l \le n-1$, there is a unique k such that

$$km + r \equiv l \pmod{n}. \quad \text{—} \circledast$$

Therefore,

$$\gcd(n, l) = 1 \iff \gcd(km+r, n) = 1.$$

(To prove this, suppose $\gcd(n, l) = 1$ and let $d = \gcd(km+r, n)$. Then,

$$d \mid (km+r) \text{ and } d \mid n.$$

By $\circledast$, $km + r = l + np$ for some $p \in \mathbb{Z}$.

$\therefore$ $d \mid (l + np)$ and $d \mid n$.

$\therefore$ $d \mid l$ and $d \mid n$ (Theorem 1.9).

$\therefore$ $d \mid \gcd(l, n) = 1$.

$\therefore$ $d = 1$.

The converse can also be proved in the same way.)

Therefore, the number of integers relatively prime to n is the same as the number of integers relatively prime to n in the list

$$r, m+r, 2m+r, \ldots, (n-1)m + r.$$

This number is $\varphi(n)$.

But, the number of such rows (i.e.,

with $\gcd(m, r) = 1$, $1 \le r \le m$) is $\varphi(m)$.

Hence, the total number of integers i with $1 \le i \le mn$ and $\varphi(mn) = 1$ is $\varphi(m)\varphi(n)$.

Hence,
$$\varphi(mn) = \varphi(m)\varphi(n)$$
and the theorem follows.

Ex: $\varphi(30) = \varphi(6 \cdot 5) = \varphi(6)\varphi(5) = 2 \cdot 4 = 8$

$\varphi(35) = \varphi(5 \cdot 7) = \varphi(5)\varphi(7) = 4 \cdot 6 = 24$

<u>Theorem 7.5:</u> Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime power factorization of $n \in \mathbb{Z}^+$. Then,
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Proof: $\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})$

$= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$

(since φ is multiplicative)

$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$

(by Theorem 7.3)

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)$$

$$= p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

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

Ex: $\varphi(100) = \varphi(2^2\cdot 5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$$= 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40$$

Ex: $\varphi(720) = \varphi(2^4\cdot 3^2\cdot 5) = 720\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$$= 192$$

<u>Theorem 7.6:</u> Let $n>2$. Then $\varphi(n)$ is even.

Proof: Exercise

For an arithmetic function f, we define the summatory function F by

$$F(n) = \sum_{d|n} f(d).$$

Thus, $F(n)$ is the sum of the values of f at all divisors of n.

Ex: Let $f(n) = n$. Then,

$$F(6) = \sum_{d|6} f(d)$$
$$= f(1) + f(2) + f(3) + f(6)$$
$$= 1 + 2 + 3 + 6$$
$$= 12$$

$$F(12) = \sum_{d|12} f(12)$$
$$= f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$$
$$= 1 + 2 + 3 + 4 + 6 + 12$$
$$= 28$$

Ex: Let $f(n) = n^2$.

Then, $$F(8) = \sum_{d|8} f(d)$$
$$= f(1) + f(2) + f(4) + f(8)$$
$$= 1^2 + 2^2 + 4^2 + 8^2$$
$$= 85$$

<u>Theorem 7.7:</u> Let $n \in \mathbb{Z}^+$. Then,

$$\sum_{d|n} \varphi(d) = n$$

Proof: Let C_d be the set of all integers m such that $\gcd(m, n) = d$, i.e.,

$$C_d = \{ m \mid \gcd(m,n) = d,\ 1 \le m \le n \}$$

It is easy to see that

$$\gcd(m,n) = d \iff \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1.$$

Hence, $\gcd(m,n) = d$ with $1 \le m \le n$

$$\iff$$

$$\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1 \quad \text{with} \quad \frac{m}{d} \le \frac{n}{d}$$

Hence, the number of elements in C_d is equal to the number of elements relatively prime to $\frac{n}{d}$ and not exceeding $\frac{n}{d}$, i.e., $\varphi\left(\frac{n}{d}\right)$.

The sets C_d are disjoint because the gcd is unique.

Hence,

$$n = \sum_{d \mid n} \# C_d$$

$$= \sum_{d \mid n} \varphi\left(\frac{n}{d}\right)$$

$$= \sum_{d \mid n} \varphi(d)$$

because when d runs through the divisors of n then $\frac{n}{d}$ runs through the same divisors.

Ex: Let $n = 18$.

Divisors of 18 are 1, 2, 3, 6, 9 and 18.

$C_1 = \{1, 5, 7, 11, 13, 17\}$

$C_2 = \{2, 4, 8, 10, 14, 16\}$

$C_3 = \{3, 15\}$

$C_6 = \{6, 12\}$

$C_9 = \{9\}$

$C_{18} = \{18\}$

Note that $\varphi\left(\frac{18}{1}\right) = \varphi(18) = 6$

$\varphi\left(\frac{18}{2}\right) = \varphi(9) = 6$

$\varphi\left(\frac{18}{3}\right) = \varphi(6) = 2$

$\varphi\left(\frac{18}{6}\right) = \varphi(3) = 2$

$\varphi\left(\frac{18}{9}\right) = \varphi(2) = 1$

$\varphi\left(\frac{18}{18}\right) = \varphi(1) = 1$

Finally, $18 = 6 + 6 + 2 + 2 + 1 + 1$

Now we see how to find the inverse images of an integer under φ. That is, we see, given $k \in \mathbb{Z}^+$, how to find $n \in \mathbb{Z}^+$ such that

$$\varphi(n) = k.$$

There may be many solutions for n. We

can also write

$$\varphi^{-1}\{k\}$$

to denote the set of all n such that $\varphi(n) = k$.

We can use the formula

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

where $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

Let's look at the following example.

Ex: Find the solutions of $\varphi(n) = 8$.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Then,

$$8 = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

Then, $p_i \leq 9 \ \forall i$.

Also, $p_i \neq 7$ because $(7-1) \nmid 8$.

$\therefore$ possible values for p_i are 2, 3 and 5.

$\therefore$ $n = 2^a 3^b 5^c$ for some a, b, c.

Moreover, $b, c \leq 1$ because, otherwise 3 or 5 should divide 8.

Case 1: $b = c = 0$.

Then, $n = 2^a$ with $a \geq 1$.

Then,

$$8 = 2^a - 2^{a-1}$$

$$\therefore 8 = 2^{a-1}$$

$$\therefore a - 1 = 3 \implies a = 4$$

$$\therefore n = 16$$

Case 2: $b = 0$, $c = 1$

Then, $n = 2^a \cdot 5$; $a \geq 1$.

$$\therefore 8 = 2^{a-1} \cdot 4$$

$$\therefore 2^{a-1} = 2 \implies a = 2$$

$$\therefore n = 20.$$

Case 3: $b = 1$, $c = 0$

Then, $n = 2^a \cdot 3$

$$\therefore 8 = 2^{a-1} \cdot 2 \implies a = 3$$

$$\therefore n = 24$$

Case 4: $b = 1$, $c = 1$

Then, $n = 2^a \cdot 3 \cdot 5$.

$$\therefore 8 = 2^{a-1} \cdot 2 \cdot 4. \implies a = 1$$

$$\therefore n = 30$$

Also, if $a = 0$, then $n = 15$

Hence, $n = 15, 16, 20, 24, 30$.