Euler's Phi Function

An *arithmetic* function is any function defined on the set of positive integers.

Definition. An arithmetic function f is called *multiplicative* if $f(mn) = f(m)f(n)$ whenever m, n are relatively prime.

Theorem. *If f is a multiplicative function and if $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ is its prime-power factorization, then $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_s^{a_s})$.*

Proof. (By induction on the length, s, of the prime-power factorization.) If $n = p_1^{a_1}$ then there is nothing to prove, as $f(n) = f(p_1^{a_1})$ is clear. If $n = p_1^{a_1} p_2^{a_2}$ then $f(n) = f(p_1^{a_1}) f(p_2^{a_2})$ since $\gcd(p_1^{a_1}, p_2^{a_2}) = 1$, so the result holds for all numbers with prime-power factorization of length 2.

Assuming as the inductive hypothesis that the result holds for all numbers with prime-power factorization of length s, we consider a number $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} p_{s+1}^{a_{s+1}}$ with prime-power factorization of length $s+1$. Then we have

$$f(n) = f(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) f(p_{s+1}^{a_{s+1}})$$

since $\gcd(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}, p_{s+1}^{a_{s+1}}) = 1$. Thus by the inductive hypothesis we get $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_s^{a_s}) \cdot f(p_{s+1}^{a_{s+1}})$. $\square$

Now we apply this to the Euler phi function. Recall that $\varphi(n)$ is, by definition, the number of congruence classes in the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of *invertible* congruence classes modulo n.

Theorem. *Euler's phi function φ is multiplicative. In other words, if $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.*

To prove this, we make a rectangular table of the numbers 1 to mn with m rows and n columns, as follows:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
m & 2m & 3m & \cdots & nm
\end{array}$$

The numbers in the rth row of this table are of the form $km + r$ as k runs from 0 to $m - 1$.

Let $d = \gcd(r, m)$. If $d > 1$ then no number in the rth row of the table is relatively prime to mn, since $d \mid (km + r)$ for all k. So to count the residues relatively prime to mn we need only to look at the rows indexed by values of r such that $\gcd(r, m) = 1$, and there are $\varphi(m)$ such rows.

If $\gcd(r, m) = 1$ then every entry in the rth row is relatively prime to m, since $\gcd(km + r, m) = 1$ by the Euclidean algorithm. It follows from Theorem 4.7 of Rosen that the entries in such a row form a complete residue system modulo n. Thus, exactly $\varphi(n)$ of them will be relatively prime to n, and thus relatively prime to mn.

We have shown that there are $\varphi(m)$ rows in the table which contain numbers relatively prime to mn, and each of those contain exactly $\varphi(n)$ such numbers. So there are, in total, $\varphi(m)\varphi(n)$ numbers in the table which are relatively prime to mn. This proves the theorem.

Theorem. *For any prime p we have that $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1 - \frac{1}{p})$.*

The proof is an easy exercise. Just make a list of the numbers from 1 to p^a and count how many numbers in the list are not relatively prime to p^a. You will find that you are just counting the multiples of p, and there are p^{a-1} such multiples.

Theorem. *For any integer $n > 1$, if $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ is the prime-power factorization, then*

$$\begin{aligned} \varphi(n) &= n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_s}) \\ &= p_1^{a_1-1} p_2^{a_2-1} \cdots p_s^{a_s-1} (p_1 - 1)(p_2 - 1) \cdots (p_s - 1). \end{aligned}$$

This is proved by simply putting together all the results of this lecture. Since φ is multiplicative, we get

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_s^{a_s}) \\ &= p_1^{a_1}(1 - \tfrac{1}{p_1}) p_2^{a_2}(1 - \tfrac{1}{p_2}) \cdots p_s^{a_s}(1 - \tfrac{1}{p_s}) \end{aligned}$$

and the result follows after rearranging the order of the factors.

Comment. The result of the preceding theorem can be written as $\varphi(n) = n \prod_{p \mid n}(1 - \frac{1}{p})$, where it must be understood that in the product, p ranges over the *prime* divisors of n.

Example. Since $1000 = 10^3 = 2^3 5^3$ we have $\varphi(1000) = 1000(1-\frac{1}{2})(1-\frac{1}{5}) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$.

In other words, there are exactly 400 congruence classes in the group $(\mathbb{Z}/1000\mathbb{Z})^\times$ of multiplicative units.

By Euler's theorem, it follows that if $\gcd(a, 1000) = 1$ then

$$a^{400} \equiv 1 \pmod{1000}.$$

Equivalently, $[a]^{400} = [1]$ in $\mathbb{Z}/1000\mathbb{Z}$ whenever $\gcd(a, 1000) = 1$.