# 8 Euler's $\varphi$-function

The function $\varphi$ introduced above is called Euler's totient function. Note: If $m$ is a prime $p$, then $\varphi(p) = p - 1$.

**Theorem**. Fix any $m \geq 1$. Then, for any integer $a$ relatively prime to $m$, we have

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

**Corollary (Fermat's Little Theorem)**. For any prime $p$, and for any $a$ not divisible by $p$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is *very* useful for computations.

**Example**: Compute $11^{470} \pmod{37}$.

**Idea**: Since 37 is a prime, by Fermat's little theorem,

$$a^{36} \equiv 1 \pmod{37}.$$

Hence

$$a^{r+36b} \equiv a^r \pmod{37}.$$

Write, using the Euclidean algorithm,

$$\begin{aligned} 470 &= 36b + r, \;\; 0 \leq r < 37 \\ &= 36 \cdot 13 + 2 \\ \Rightarrow 11^{470} &\equiv 11^2 \pmod{37} \\ &\equiv 10 \pmod{37}. \end{aligned}$$

**Proof of Theorem**. Let

$$\mathrm{S} = \{r_0, \dots, r_{n-1}\}$$

be a set of reps. for $\mathbb{Z}/m$, and let $(a, m) = 1$. Consider

$$\mathrm{S}' = \{ar_0, ar_1, \dots, ar_{m-1}\}.$$

**Claim**. $\mathrm{S}'$ is another set of reps for $\mathbb{Z}/m$.

To show the claim, we need to prove

$$ar_i \neq ar_j \pmod m, \text{ for } i \neq j.$$

Suppose $ar_i = ar_j$, for some $i \neq j$. Then

$$a(r_i - r_j) \equiv 0 \pmod m,$$

i.e., $m|a(r_i - r_j)$. Since $(a, m) = 1$, $m|(r_i - r_j)$, but this contradicts the fact that S is a set of reps. for $\mathbb{Z}/m$. Hence the claim.

So S and S$'$ are both sets of reps for $\mathbb{Z}/m$. In other words, for each congruence class $B_i$ and $m$, $\exists!$ number in $B_i \cap$ S and in $B_i \cap$ S$'$. Consequently, the product of all the numbers in S coprime to $m$ will be congruent (mod $m$) to the product of all the numbers in S$'$ coprime to $m'$.

Moreover, if $r_i$ is coprime to $m$, so is $ar_i$. So

$$\prod_{\substack{r_i \in \mathrm{S} \\ (r_i,m)=1}} (ar_i) \equiv \prod_{\substack{r_i \in \mathrm{S} \\ (r_i,m)=1}} r_i \bmod m)$$

$$\Rightarrow a^{\varphi(m)} \underbrace{\left( \prod_{\substack{r_i \in s \\ (r_i,m)=1}} r_i \right)}_{=b, \text{ say}} \equiv \left( \prod_{\substack{r_i \in s \\ (r_i,m)=1}} r_i \right) \pmod m$$

$$\Rightarrow a^{\varphi(m)} b \equiv b \pmod m, \text{ with } (b, m) = 1.$$

$$\Rightarrow m \mid (a^{\varphi(m)} - 1)b.$$

Since $(b, m) = 1$,

$$m|a(^{\varphi(m)} - 1), \text{ i.e., } a^{\varphi(m)} \equiv 1 \pmod m.$$

**Warning**: Little Fermat says that $a^{p-1} \equiv 1 \pmod p$, for any prime $p$ **and** $1 \leq a < p$. It might happen that $\exists m \geq 1$ which is **not** a prime and $a$ such that

$$a^{m-1} \equiv 1 \pmod m.$$

For example, consider $m = 340 = (11)(31)$, and $a = 2$.

$$2^{340} \equiv 2^{11-1} 34 \equiv 1 \pmod{11}$$

by Little Fermat. Also

$$2^{340} \equiv 2^{(31-1)11} \cdot 2^{10} \equiv 2^{10} \pmod{31}$$

Clearly, if $m$ is a prime $p$, then $\varphi(m) = p - 1$. It is of great importance to have a formula for computing $\varphi(m)$ even when $m$ is not a prime. To this end we prove the following

**Theorem** Let $m > 1$. Write $m = \prod_{i=1}^{r} p_i^{a_i}$, with $p_1, \cdots, p_r$ primes and $a_1, \cdots, a_r$ positive integers. Then

$$\varphi(m) = \prod_{i=1}^{r} p_i^{a_i - 1}\,(p_i - 1) \tag{a}$$

and

$$m = \sum_{d|m} \varphi(d). \tag{b}$$

**Proof**: (a) **Step 1:** *Show $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ if $n_1, n_2$ are relatively prime.*

**Proof of Step 1:**

$$\begin{aligned}\varphi(n_1 n_2) &= \#\{y \in \{1, 2, \cdots, n_1 n_2 - 1\} \mid (y,\, n_1 n_2) = 1\} \\ &= \#\{a_i n_1 + b_j n_2 \mid (a_i n_1 + b_j n_2,\, n_1 n_2) = 1, a_i \bmod n_2,\, b_j \bmod n_1\}.\end{aligned}$$

But since $(n_1, n_2) = 1$, we have

$$(a_i n_1 + b_j n_2,\, n_1 n_2) = 1 \Longleftrightarrow \begin{pmatrix} (a_i n_1 + b_j n_2,\, n_1) = 1 \\ \text{and} \\ (a_i n_1 + b_j n_2,\, n_2) = 1 \end{pmatrix}$$

Also, $(a_i n_1 + b_j n_2, n_1) = 1$ iff $(b_j n_2, n_1) = 1$, that is iff $(b_j, n_1) = 1$.

Similarly, $(a_i n_1 + b_j n_2, n_2) = 1$ iff $(a_i, n_2) = 1$.

Consequently,

$$\begin{aligned}\varphi(n_1 n_2) &= \#\{a_i n_1 + b_j n_2 \mid (a_i, n_2) = 1, (b_j, n_1) = 1\} \\ &= \varphi(n_1)\,\varphi(n_2).\end{aligned}$$

Hence we have achieved Step 1.

**Step 2**: *If $p$ is a prime and $a > 0$, then show:* $\varphi(p^a) = p^{a-1}(p-1)$.
**Proof of Step 2**:

$$\varphi(p^a) = \#\{b \in \{0, \cdots, p^a - 1\} \mid p \nmid b\} = p^a - \#\{b \in \{0, 1, \cdots, p^a\} \mid p \mid b\} = p^a - p^{a-1},$$

which proves the assertion.

**Step 3**: *Proof of the general case.*

By step 1, we have

$$\text{If} \quad m = \prod_{i=1}^{r} p_i^{a_i}, \text{then} \quad \varphi(m) = \prod_{i=1}^{r} \varphi\left(p_i^{a_i}\right)$$

This is so because $(p_i^{a_i}, p_j^{a_j}) = 1$ if $i \neq j$. Now part (a) of the Theorem follows by Step 2.

(b): $m = \prod_{d|m}^{r} p_r^{a_i}$. So every positive divisor $d$ of $m$ is of the form $m = \prod_{i=1}^{r} p_i^{b_i}$ with $0 \leq b_i \leq a_i$. So

$$\sum_{d|m} \varphi(d) = \sum_{\{(b_1, \ldots, b_r) | 0 \leq b_i \leq a_i, \forall i\}} \varphi\left(\prod_{i=1}^{r} p_i^{b_i}\right).$$

By part (a) this equals

$$\sum_{\{(b_1, \ldots, b_r) | 0 \leq b_i \leq a_i, \forall i\}}^{r} \varphi(p_i^{b_i}),$$

with $\varphi(p_i^{b_i})$ being $p^{b_i} - p_i^{b_i - 1}$ (resp. 1) if $b_i > 0$ (resp. $b_i = 0$). Exchanging the sum and the product, and noting that

$$\sum_{\{(b_1, \ldots, b_r) | 0 \leq b_i \leq a_i, \forall i\}}^{r} \varphi(p_i^{b_i}) = p_i^{a_i},$$

we get

$$\sum_{d|m} \varphi(d) = \prod_{i=1}^{r} p_i^{a_i} = m.$$