Definition 1. *The **Euler Totient Function** is defined for $n \geq 1$ as the number of positive integers not exceeding n which are relatively prime to n.*

That is to say:

$$\varphi(n) := \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1. \tag{1}$$

Remark 1. *Most of the following results are a more detailed explanation of what is contained in [1].*

Theorem 1 (Euler-Fermat theorem)**.** *Assume $(a, m) = 1$. Then we have:*

$$a^{\varphi(m)} \equiv 1 \mod m. \tag{2}$$

To prove this theorem we first need to understand the following definition:

Definition 2. *Given a positive integer m, a **reduced residue system modulo** m is any set of $\varphi(m)$ integers that are incongruent modulo m and relatively prime to m.*

We will also make use of the following lemma:

Lemma 1. *If $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ is a reduced residue system modulo m and if $(k, m) = 1$, then $\{ka_1, ka_2, \cdots, ka_{\varphi(m)}\}$ is also a reduced residue system modulo m.*

Proof. Since $(a_i, m) = (k, m) = 1$ we have $(ka_i, m) = 1$ for $i = 1, \cdots, \varphi(m)$. Also, given that no two a_i are congruent modulo m, no two ka_i are congruent modulo m. □

Remark 2. *Notice that there are exactly $\varphi(m)$ different residue classes modulo m of numbers relatively prime to m, therefore any reduced residue system modulo m contains exactly $\varphi(m)$ representatives of different residue classes modulo m*

Proof of the Euler-Fermat theorem. Let $\{b_1, b_2, \cdots, b_{\varphi(m)}\}$ be a reduced residue system modulo m. Since $(a, m) = 1$, lemma 1 implies that $\{ab_1, ab_2, \cdots, ab_{\varphi(m)}\}$ is also a reduced residue system. Hence the product of all the integers in the first set is congruent to the product of those in the second set (this is because the sets contain the same residue classes modulo m).

Therefore:

$$b_1, \cdots, b_{\varphi(m)} \equiv a^{\varphi(m)} b_1, \cdots, b_{\varphi(m)} \mod m.$$

Each b_i is relatively prime to m so we can cancel each one to obtain the theorem. □

References

[1] Tom M Apostol. *Introduction to analytic number theory.* Springer Science & Business Media, 2013.