Euler's Theorem

P. Reany

July 25, 2022

Abstract

Euler's Theorem is a generalization of Fermat's Little Theorem. Familiarity with modulo arithmetic is assumed.

1 Introduction

Fermat's Little Theorem states that for positive integer a and prime p,

$$a^p \equiv a \pmod{p}, \tag{1}$$

or

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2}$$

Euler's Theorem let's us generalize this by taking numbers modulo some positive integer n, but with a different exponent, given by

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{3}$$

Definition: One integer a is said to divide another integer b if there exists some other integer k such that $b = ka$. Symbolically, the statement that a divides b is represented as $a \mid b$. And if a does not divide b then we can write $a \nmid b$.

Definition: The symbol (a, b) shall mean the greatest common divisor of a and b. Some people write it as $\gcd(a, b)$, but I prefer the shorter version.

Definition: Two integers a and b are said to be *relatively prime* (to each other) or *coprime* if $(a, b) = 1$.

Definition: Let S be a set. Then the *order* of S is denoted by $|\, S \,|$. The order of a set 'counts' (or indicates) the number of elements in the set.

Definition: Pick a positive integer n. The number of positive integers less than or equal to n that are relatively prime to n is denoted by $\varphi(n)$. This function is

called *Euler's Totient Function.* (For our purposes here, we won't need to know the actual numerical value of $\varphi(n)$ because the n is arbitrary. All we care about is that $\varphi(n)$ exists and is finite.)

Definition: A Reduced Reductive System R modulo n: Choose a positive integer n. Let $\overline{R}$ be the set of all positive integers less than or equal to n that are relatively prime to n. Then

$$\overline{R} = \{r_1, r_2, \ldots, r_{\varphi(n)}\}\,, \tag{4}$$

where $(r_i, n) = 1$ for all $i \in [1, \ldots, \varphi(n)]$.

So, $\overline{R}$ is sort of a canonical choice for a Reduced Reductive System (RRS) where the elements are arranged in order of increasing value. But since the elements of $\overline{R}$ are taken modulo n, then any one of its elements can be replaced by any other element in the same equivalence class. For example, if $r = 4$ and $n = 25$, then r can be replaced by $4 + 25$, or $4 + 2 \times 25$, or $4 + m \times 25$, where m is any positive integer. Further, every element of $\overline{R}$ can be replaced by some equivalent element, independent of all other element of $\overline{R}$.

So, I'm letting the symbol R stand for any arbitrary RRS, including $\overline{R}$ as a special case. Furthermore, since R is a set, we don't care what the order of the elements are in this set. Therefore, under any permutation of its elements, an arbitrary R maps onto itself (as a set). Lastly, if R is an RRS, then

$$|\,R\,| = \varphi(n)\,. \tag{5}$$

Euclid's Lemma: If prime p divides the product of numbers s and t, then it must divide at least one of them. In other words, if $p \,|\, st$ then $p \,|\, s$ or $p \,|\, t$.

Lemma 1: If numbers s and t are each relatively prime to n then their product is also relatively prime to n. Thus, given that

$$(s, n) = 1 \quad \text{and} \quad (t, n) = 1\,, \tag{6}$$

then $(st, n) = 1$.

Proof of Lemma 1:

Proof by contradiction: Assume the conclusion is false. Then there is some integer m that divides both n and st. If m is a prime then call it p, else m is not prime but it has a prime factor, call it p. So, by Euclid's Lemma, either $p \,|\, s$, which contradicts the assumption that $(s, n) = 1$, or else $p \,|\, t$, which contradicts the assumption that $(t, n) = 1$. Therefore, the original conclusion is true.

2 Proof to Euler's Theorem:

Part 1: Fundamental to the manner of proof in this article is the ability to create an alternative RRS by acting on $\overline{R}$ by a one-to-one map (or function). Such a map would be just a permutation on $\overline{R}$, which is just another R. So, first, choose a number a such that $(a, n) = 1$, then we define a map $f_a : \overline{R} \to R$ given by

$$f_a \overline{r}_i = a\overline{r}_i, \quad \text{for all } i \in [1, \ldots, \varphi(n)]\,. \tag{7}$$

We need to prove two things about this map. First, that $(a\overline{r}_i, n) = 1$. In other words, the image of this map must be relativiely prime to n. We must also prove that f_a is one-to-one. If we can prove both of these, then we will have proven that the image of $\overline{R}$ under f_a is also an RRS, isomorphic to $\overline{R}$.

Okay, that $a\overline{r}_i$ in (7) is relatively prime to n was proven in Lemma 1.

To show that f_a is one-to-one, we assume that it is not. Then there are two elements of $a\overline{R}$, namely, $a\overline{r}_i$ and $a\overline{r}_j$, where $i \neq j$, such that

$$a\overline{r}_i \equiv a\overline{r}_j \pmod{n}\,, \tag{8}$$

from which it follows that

$$a(\overline{r}_i - \overline{r}_j) \equiv 0 \pmod{n}\,. \tag{9}$$

This means that $a(\overline{r}_i - \overline{r}_j)$ is a multiple of n. Well, a can't contain any of the prime factors of n since it's relatively prime to n; therefore, $n \nmid a$. So, we must conclude that $\overline{r}_i - \overline{r}_j$ is a multiple of n, and thus

$$\overline{r}_i - \overline{r}_j \equiv 0 \pmod{n}\,. \tag{10}$$

But this implies that

$$\overline{r}_i \equiv \overline{r}_j \pmod{n}\,, \tag{11}$$

which cannot be true for $i \neq j$, as the elements of $\overline{R}$ are distinct, hence, a contradiction. Thus, we conclude that f_a is one-to-one. But a function that maps a finite set one-to-one to itself is a permutation.

Part 2: We have shown that $R = a\overline{R}$ is a permutation of the elements of $\overline{R}$. Hence, the product of all the elements of $\overline{R}$ is equal to the product of all the elements of R:[1]

$$\prod_{i=1}^{\varphi(n)} (a\overline{r}_i) \equiv \prod_{i=1}^{\varphi(n)} \overline{r}_i \pmod{n}\,. \tag{12}$$

Therefore,

$$(a^{\varphi(n)} - 1) \prod_{i=1}^{\varphi(n)} \overline{r}_i \equiv 0 \pmod{n}\,. \tag{13}$$

[1] It may be natural to question how it is that these two products can be equal to each other when they look so disimilar to each other. The answer is that we have to trust what the mathematics says is true.

So, 1) at least one of the factors on the LHS of this is a multiple of n, that is, at least one of

$$a^{\varphi(n)} - 1 \qquad \text{or} \qquad \prod_{i=1}^{\varphi(n)} \overline{r}_i \tag{14}$$

is a multiple of n, or 2) all the prime factors of n are distributed between the two factors of (14). But $\prod_{i=1}^{\varphi(n)} \overline{r}_i$ can't contain any of the prime factors of n because each factor in it is relatively prime to n. That leaves $a^{\varphi(n)} - 1$ as a multiple of n, hence

$$a^{\varphi(n)} - 1 \equiv 0 \pmod{n}, \tag{15}$$

or, rather,

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{16}$$

which is what we were to show.