Note 7 Supplement: Euler's Totient Function

Computer Science 70
University of California, Berkeley

Summer 2018

1 Euler's Totient Function

1.1 Introduction

First, we establish some notation. For this note, $m \geq 2$ is a positive integer representing the modulus. Then, $\mathbb{Z}/m\mathbb{Z}$ is the set of numbers $\{0, 1, \ldots, m-1\}$ where the operations of addition and multiplication are taken modulo m. The notation $(\mathbb{Z}/m\mathbb{Z})^\times$ is the set of numbers in $\mathbb{Z}/m\mathbb{Z}$ which have multiplicative inverses. We have seen then that $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ is equivalent to $\gcd(a, m) = 1$.

We define **Euler's totient function** as the function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ (where $\mathbb{Z}^+$ denotes the positive integers) by $\varphi(1) := 1$, and for all positive integers $m \geq 2$, $\varphi(m) := |(\mathbb{Z}/m\mathbb{Z})^\times|$. Equivalently, for positive integers $m \geq 2$, $\varphi(m)$ is the number of elements in $\{0, 1, \ldots, m-1\}$ which are coprime with m.

Example 1. We list the values of φ for the first 10 integers.

m	$(\mathbb{Z}/m\mathbb{Z})^\times$	$\varphi(m)$
1		1
2	$\{1\}$	1
3	$\{1, 2\}$	2
4	$\{1, 3\}$	2
5	$\{1, 2, 3, 4\}$	4
6	$\{1, 5\}$	2
7	$\{1, 2, 3, 4, 5, 6\}$	6
8	$\{1, 3, 5, 7\}$	4
9	$\{1, 2, 4, 5, 7, 8\}$	6
10	$\{1, 3, 7, 9\}$	4

Example 2. When p is prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ consists of all of the numbers $\{1, \ldots, p-1\}$ since any integer strictly between 1 and p must be coprime with p. Thus, $\varphi(p) = p - 1$.

1.2 Euler's Theorem

Recall the following result:

Theorem 1. *For $a \in \mathbb{Z}/m\mathbb{Z}$, the map $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $f(x) := ax \bmod m$ is a bijection if and only if $\gcd(a, m) = 1$.*

So, if $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $f(x) := ax \bmod m$ is a bijection. What happens if $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ as well? Then, both a^{-1} and x^{-1} exist, and $a^{-1}x^{-1}$ is the inverse of ax, so $ax \in (\mathbb{Z}/m\mathbb{Z})^\times$ as well. This fact can be expressed as saying that $(\mathbb{Z}/m\mathbb{Z})^\times$ is *closed under multiplication*.

Therefore, we can also think of f as a function $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$. Since f is one-to-one when we think of it as a function $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, then it remains one-to-one when we think of it as a function $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$, and since the domain and codomain have the same size, then we can conclude that f is a *bijection* $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$.

As a consequence, the sets $(\mathbb{Z}/m\mathbb{Z})^\times$ and $\{ax : x \in (\mathbb{Z}/m\mathbb{Z})^\times\}$ are the same modulo m. Think of the latter set as a rearranged version of the former set (although this is purely for intuition's sake, since sets are not inherently ordered). From this fact we can deduce:

Theorem 2 (Euler's Theorem)**.** *If $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Proof. Since the sets $(\mathbb{Z}/m\mathbb{Z})^\times$ and $\{ax : x \in (\mathbb{Z}/m\mathbb{Z})^\times\}$ are the same modulo m, then when we multiply the elements in each set, we should obtain the same result: $\prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} x \equiv \prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} ax \pmod{m}$. Since each $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ has a multiplicative inverse, we can cancel out the x from both sides of the equation to get $\prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} a \equiv 1 \pmod{m}$. Finally, since there are $\varphi(m)$ elements in $(\mathbb{Z}/m\mathbb{Z})^\times$, we get $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

In the specific case when the modulus is a prime p, we have:

Corollary 1 (Fermat's Little Theorem)**.** *If $a \in (\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots, p-1\}$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Euler's Theorem can be used to speed up exponentiation in modular arithmetic.

Example 3. Let us compute $5^{1000000} \bmod 12$. Since $\gcd(5, 12) = 1$, then by Euler's Theorem we have $5^{\varphi(12)} \equiv 5^4 \equiv 1 \pmod{12}$. So, we can write $5^{1000000} \equiv (5^4)^{250000} \equiv 1 \pmod{12}$.

In general, if $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $a^k \equiv a^{k \bmod \varphi(m)} \pmod{m}$.

1.3 A Formula for Euler's Totient Function

The following is a consequence of the Chinese Remainder Theorem.

Theorem 3 (Chinese Remainder Theorem)**.** *If $m_1, m_2 \geq 2$ are coprime integers, then the function $g : \mathbb{Z}/m_1m_2\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ given by $g(x) := (x \bmod m_1,\ x \bmod m_2)$ is an isomorphism, i.e., g is a bijection and*

$$g(x + y) = g(x) + g(y),$$
$$g(xy) = g(x)g(y)$$

for all $x, y \in \mathbb{Z}/m_1m_2\mathbb{Z}$, where addition and multiplication of elements in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ is defined componentwise:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2 \bmod m_1,\ b_1 + b_2 \bmod m_2),$$
$$(a_1, b_1)(a_2, b_2) = (a_1a_2 \bmod m_1,\ b_1b_2 \bmod m_2).$$

Here is a consequence of the isomorphism. If $x \in (\mathbb{Z}/m_1m_2\mathbb{Z})^\times$, then x^{-1} exists, and $g(x \cdot x^{-1}) = g(1) = (1, 1)$. On the other hand, we also have $g(x \cdot x^{-1}) = g(x) \cdot g(x^{-1})$. So, $g(x) \cdot g(x^{-1}) = (1, 1)$, which means the first component of $g(x)$ and the first component of $g(x^{-1})$ multiply to be 1. Therefore, the first component of $g(x)$ has a multiplicative inverse in $\mathbb{Z}/m_1\mathbb{Z}$. Similarly, the second component of $g(x)$ also has a multiplicative inverse in $\mathbb{Z}/m_2\mathbb{Z}$. So, $g(x) \in (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$.

Conversely, if $g(x) \in (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$, then there exists a tuple $(a, b) \in (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$ such that $g(x) \cdot (a, b) = (1, 1) = g(1)$, but then $g(x \cdot g^{-1}(a, b)) = g(1)$. Since g is one-to-one, we must have $x \cdot g^{-1}(a, b) = 1$, i.e., $x \in (\mathbb{Z}/m_1m_2\mathbb{Z})^\times$.

We can now think of g as a function

$$(\mathbb{Z}/m_1m_2\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$$

and the inverse function g^{-1} as a function

$$(\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times \to (\mathbb{Z}/m_1m_2\mathbb{Z})^\times.$$

We already know that g and g^{-1} are one-to-one, so g must be a *bijection* $(\mathbb{Z}/m_1m_2\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$.

In particular, we must have

$$|(\mathbb{Z}/m_1m_2\mathbb{Z})^\times| = |(\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times| = |(\mathbb{Z}/m_1\mathbb{Z})^\times| \cdot |(\mathbb{Z}/m_2\mathbb{Z})^\times|.$$

Another way to read the above equation is $\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$. Thus, φ is called a **multiplicative** function. (Note: For functions $h : \mathbb{Z}^+ \to \mathbb{Z}^+$, the word *multiplicative* specifically means that for coprime m_1 and m_2, then $h(m_1m_2) = h(m_1)h(m_2)$. It does *not* mean that $h(xy) = h(x)h(y)$ for *any* positive integers x and y.)

Now consider an integer $n \geq 2$ and let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be its prime factorization. So, k is a positive integer, $p_1, \ldots, p_k$ are distinct prime numbers, and $\alpha_1, \ldots, \alpha_k$ are positive integers. Then, $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$. It remains to compute $\varphi(p^\alpha)$ for p prime and a positive integer α.

Since $\varphi(p^\alpha)$ is the number of elements in $\{0, 1, \ldots, p^\alpha - 1\}$ which are coprime with p^α, we turn to a counting argument. There are p^α numbers total in $\mathbb{Z}/p^\alpha\mathbb{Z}$, and among these, the numbers which are *not* coprime with p^α are $0, p, 2p, \ldots, p^\alpha - p = (p^{\alpha-1} - 1)p$. So, there are $p^{\alpha-1}$ numbers in $\mathbb{Z}/p^\alpha\mathbb{Z}$ which are *not* coprime with p^α, which leaves $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. Finally, we have our desired formula for $\varphi(n)$:

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