Section 9. Euler's Theorem and Function

Note. In Section 6. Fermat's and Wilson's Theorems we saw:

Theorem 6.1. Fermat's Theorem. If p is prime and the greatest common divisor $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

In this section we explore what happens when we try to extend the result from primes p to nonprimes m.

Note. We consider the question: Given any integer m, is there a number $f(m)$ such that $a^{f(m)} \equiv 1 \pmod{m}$? Notice that if $(a, m) = d > 1$ then $d \mid a^k$ for any integer $k > 0$, so that $d \nmid (a^k - 1)$ and hence $m \nmid (a^k - 1)$. So if we want to generalize Fermat's Theorem to composite numbers m, we will still need to keep the greatest common divisor condition $(a, m) = 1$.

Example 6.A. Notice that with $m = 9$, each of $1, 2, 4, 5, 7, 8$ are relatively prime to $m = 9$, and we have:

$a \pmod{9}$	$a^2 \pmod{9}$	$a^3 \pmod{9}$	$a^4 \pmod{9}$	$a^5 \pmod{9}$	$a^6 \pmod{9}$
1	1	1	1	1	1
2	4	8	7	5	1
4	7	1	4	7	1
5	7	8	4	2	1
7	4	1	7	4	1
8	1	8	1	8	1

So it seems that the desired value of $f(9)$ is 6.

Note. Notice that there are 6 positive integers less than 9 which are relatively prime to 9. Dudley shows that this pattern also holds with $m = 6$ and $m = 10$ (where $f(6) = 2$ and $f(10) = 4$), and the pattern is to be established for $m = 14$ in Exercise 9.1 (where $f(14) = 6$). So enumerating the number of positive integers less than m which are relatively prime to m seems to be a useful thing. This inspires the following definition.

Definition. If m is a positive integer, then denote the number of positive integers less than or equal to m and relatively prime to m as $\varphi(m)$. We call $\varphi(m)$ *Euler's* φ*-function.*

Note. Notice that $\varphi(6) = 2$, $\varphi(9) = 6$, $\varphi(10) = 4$, and $\varphi(14) = 6$. In fact, the suspected pattern holds as is shown in the next theorem.

Theorem 9.1. Euler's Theorem. Suppose that $m \geq 1$ and $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Note 9.A. If $m = p$ is prime, then $\varphi(m) = p - 1$ so that Theorem 9.1 reduces to Fermat's Theorem (Theorem 6.1) when m is prime. We will prove Theorem 9.1 below. The key idea in the proof is that for prime p if $(a, p) = 1$ then the least residues (mod p) of $a, 2a, 3a, \ldots, (p-1)a$ are a permutation of $1, 2, 3, \ldots, p-1$, as shown in the following lemma.

Lemma 9.1. If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\varphi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues $(\text{mod } m)$ of $ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$ are a permutation of $r_1, r_2, r_3, \ldots, r_{\varphi(m)}$.

Note. We are now equipped to prove Theorem 9.1; the proof is similar to that of Fermat's Theorem.

Note. We now turn our attention to properties of Euler's φ-function. In particular, we will present a method for calculating $\varphi(n)$ based on the prime-power decomposition of n. A first step in this direction is the following.

Lemma 9.2. For prime p, $\varphi(p^n) = p^{n-1}(p-1)$ for all positive integers n.

Lemma 9.3. If $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$.

Corollary 9.A. If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then the list $r_1, r_2, \ldots, r_m$ contains exactly $\varphi(m)$ elements relatively prime to m.

Note. Recall from Section 7. The Divisors of an Integer that a function defined on the positive integers is *multiplicative* if and only if $(m, n) = 1$ implies $f(mn) = f(m)f(n)$. We next show that Euler's φ-function is multiplicative so that we can extend Lemma 9.2 to all positive integers using the Unique Factorization Theorem/Fundamental Theorem of Arithmetic (Theorem 2.2).

Theorem 9.2. Euler's φ-function is multiplicative.

Exercise 9.8. Calculate $\varphi(74)$, $\varphi(76)$, and $\varphi(78)$.

Solution. We have $\varphi(74) = \varphi(2 \cdot 37) = \varphi(2)\varphi(37) = (1)(36) = 36$, $\varphi(76) = \varphi(2^2 \cdot 19) = \varphi(2^2)\varphi(19) = (2)(18) = 36$, and $\varphi(78) = \varphi(2 \cdot 39) = \varphi(2)\varphi(39) = (1)(38) = 38$. $\square$

Note. We can now use Lemma 9.2 and Theorem 9.2 to find $\varphi(n)$ for all positive n.

Theorem 9.3. If n has a prime-power decomposition given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $\varphi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1)$.

Note. The proof of the following is straightforward and "left to the reader."

Corollary. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$.

Exercise 9.9(a). Calculate $\displaystyle\sum_{d \mid n} \varphi(d)$ for $n = 12$, 13, 14, 15, and 16.

Solution. With $n = 12$, the divisors are 1, 2, 3, 4, 6, and 12. We have $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(6) = 2$, and $\varphi(12) = 4$, so that

$$\sum_{d \mid 12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

With $n = 13$, the divisors are 1 and 13. We have $\varphi(1) = 1$ and $\varphi(13) = 12$, so that

$$\sum_{d \mid 13} \varphi(d) = \varphi(1) + \varphi(13) = 1 + 12 = 13.$$

With $n = 14$, the divisors are 1, 2, 7, and 14. We have $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(7) = 6$, and $\varphi(14) = 6$, so that

$$\sum_{d \mid 14} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(7) + \varphi(14) = 1 + 1 + 6 + 6 = 14.$$

With $n = 15$, the divisors are 1, 3, 5, and 15. We have $\varphi(1) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, and $\varphi(15) = 8$, so that

$$\sum_{d \mid 15} \varphi(d) = \varphi(1) + \varphi(3) + \varphi(5) = 1 + 2 + 4 + 8 = 15.$$

With $n = 16$, the divisors are 1, 2, 4, 8, and 16. We have $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(4) = 2$, $\varphi(8) = 4$, and $\varphi(16) = 8$, so that

$$\sum_{d \mid 16} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) + \varphi(16) = 1 + 1 + 2 + 4 + 8 = 16.$$

With these results, the next theorem (which will be useful in the next section) is not surprising. □

Theorem 9.4. If $n \geq 1$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Revised: 3/5/2022