13 Theorems of Euler, Fermat and Carmichael

Definition 13.1. A function f defined on the positive integers is said to be **multiplicative** if

$$f(m)f(n) = f(mn), \quad \forall m, n \in \mathbb{Z}^+, \tag{9}$$

where $\gcd(m, n) = 1$.

If

$$f(m)f(n) = f(mn), \quad \forall m, n \in \mathbb{Z}^+, \tag{10}$$

then f is **completely multiplicative**. Every completely multiplicative function is multiplicative.

Euler's φ-function

Definition 13.2. Let n be a positive integer. Euler's φ-function, $\varphi(n)$, is defined to be the number of positive integers k less than n which are relatively prime to n:

$$\varphi(n) = |\{k \mid 0 \leq k < n, \gcd(k, n) = 1\}|.$$

Example 13.1. By Definition 13.2, we have the following values of $\varphi(n)$:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	40	100	32	102

Lemma 13.1. For any positive integer n,

$$\sum_{d|n} \varphi(d) = n.$$

Theorem 13.1. *Let n be a positive integer and* $\gcd(m, n) = 1$. *Then:*

1. *Euler's φ-function is multiplicative. That is,*

$$\varphi(mn) = \varphi(m)\varphi(n),$$

where $\gcd(m, n) = 1$.

2. *If n is a prime, say p, then*

$$\varphi(p) = p - 1.$$

(Conversely, if p is a positive integer with $\varphi(p) = p - 1$, then p is prime.)

3. *If n is a prime power p^α with $\alpha > 1$, then*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

4. *If n is composite and has the standard prime factorization form, then*

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right).$$

Equivalently,

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

Carmichael's λ-function

Definition 13.3. Carmichael's λ-function, $\lambda(n)$, is defined as follows:

$$\lambda(p) = \varphi(p) = p - 1 \quad \text{for prime } p,$$

$$\lambda(p^\alpha) = \varphi(p^\alpha) \quad \text{for } p = 2 \text{ and } \alpha \leq 2,$$

$$\lambda(p^\alpha) = \varphi(p^\alpha) \quad \text{for } p \geq 3,$$

$$\lambda(2^\alpha) = \frac{1}{2}\varphi(2^\alpha) \quad \text{for } \alpha \geq 3,$$

$$\lambda(n) = \operatorname{lcm}\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\right) \quad \text{if } n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Example 13.2. By Definition 13.3, we have the following values for $\lambda(n)$:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\lambda(n)$	1	1	2	2	4	2	6	2	6	4	20	100	16	102

Example 13.3. Let $n = 65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$, and $a = 11$. Then, $\gcd(65520, 11) = 1$ and we have

$$\varphi(65520) = 8 \cdot 6 \cdot 4 \cdot 6 \cdot 12 = 13824,$$

$$\lambda(65520) = \text{lcm}(4, 6, 4, 6, 12) = 12.$$

The number of multiplicative inverses

Theorem 13.2. *The number of multiplicative inverses b^{-1} modulo n is $\varphi(n)$, where $\varphi(n)$ is Euler's totient function. Specifically, the number of integers b such that $\gcd(b, n) = 1$ (i.e., the number of integers that have a multiplicative inverse modulo n) is given by $\varphi(n)$.*

Example 13.4. et $n = 21$. Since $\varphi(21) = 12$, there are twelve values of b for which the multiplicative inverse $b^{-1} \pmod{21}$ exists. In fact, the multiplicative inverse modulo 21 only exists for each of the following values of b:

$$b : 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.$$

The corresponding values of $b^{-1} \pmod{21}$ are:

$$b^{-1} \pmod{21} : 1, 11, 16, 17, 8, 19, 2, 13, 4, 5, 10, 20.$$

Euler's Theorem

Theorem 13.3. *If $m > 0$ and a is relatively prime to m, then*

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

Fermat's Little Theorem

Theorem 13.4. *If p is prime and a is relatively prime to p, then*

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

Let's look at some examples. Take $m = 12$, then

$$\varphi(m) = \varphi(2^2 \cdot 3) = (2^2 - 2)(3 - 1) = 4.$$

The positive integers $a < m$ with $\gcd(a, m) = 1$ are $1, 5, 7$, and 11.

$$14 \equiv 1 \pmod{12} \quad \text{is clear.}$$

$$5^2 \equiv 1 \pmod{12} \quad \text{since} \quad 12 \mid 5^2 - 1.$$

Therefore,

$$5^4 \equiv 1 \pmod{12}.$$

Now, since $7 \equiv -5 \pmod{12}$ and 4 is even, we have:

$$7^4 \equiv (-5)^4 \equiv 5^4 \pmod{12}.$$

Thus,

$$7^4 \equiv 1 \pmod{12}.$$

Next, $11 \equiv -1 \pmod{12}$, and since 4 is even, we get:

$$11^4 \equiv (-1)^4 \equiv 1 \pmod{12}.$$

Corollary 13.1 (Converse of Fermat's Little Theorem)**.** Let n be an odd positive integer. If $\gcd(a, n) = 1$ and

$$a^{n-1} \equiv 1 \pmod{n},$$

then n is composite.

Carmichael's Theorem

Theorem 13.5. *Let a and n be positive integers with $\gcd(a, n) = 1$. Then,*

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

where $\lambda(n)$ is Carmichael's function.

The Order of an Element

The order of an element

Definition 13.4. For integers $a, m \neq 0$ with $\gcd(a, m) = 1$, the order of $a \mod m$ is its order in the multiplicative group $\mathbb{Z}_m$, that is,

$$\text{ord}_m(a) = \min \{\gamma \in \mathbb{N} \mid a^\gamma \equiv 1 \pmod{m}\}.$$

Example 13.5. The powers of 2 modulo 7 yield the following congruences:

$$2^1 \equiv 2 \pmod{7},$$

$$2^2 \equiv 4 \pmod{7},$$

$$2^3 \equiv 1 \pmod{7},$$

$$2^4 \equiv 2 \pmod 7,$$

$$2^5 \equiv 4 \pmod 7,$$

$$2^6 \equiv 1 \pmod 7.$$

This means that the integer 2 has order 3 modulo 7, as the smallest integer γ such that $2^\gamma \equiv 1 \pmod 7$ is $\gamma = 3$.

Remark 13.1. $\lambda(n)$ will never exceed $\varphi(n)$ and is often much smaller than $\varphi(n)$; it is the value of the largest order it is possible to have.

Example 13.6. Let $a = 11$ and $n = 24$. Then $\varphi(24) = 8$, $\lambda(24) = 2$. So,

$$11^{\varphi(24)} = 11^8 \equiv 1 \pmod{24},$$

$$11^{\lambda(24)} = 11^2 \equiv 1 \pmod{24}.$$

That is, $\text{ord}_{24}(11) = 2$.

Lemma 13.2. If $a^n \equiv 1 \pmod m$, then $\text{ord}_m(a) \mid n$. In particular, $\text{ord}_m(a) \mid \varphi(m)$.

Primitive Root

Theorem 13.6. *If $\text{ord}_m(a) = \varphi(m)$, then a is called a primitive root modulo m.*

The primitive root of 7 is 3 because the following holds: $\varphi(7) = 6$, and $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1 \pmod 7$.

Exercises

1. Find $\varphi(8)$, $\varphi(19)$ and $\varphi(101)$.
2. Find $\lambda(8)$, $\lambda(19)$ and $\lambda(101)$.
3. Compute the order of 2 with respect to the prime modulo 3, 5, 7, 11, 13, 17, and 19.
4. Compute the order of -7 modulo 13