9. Euler and Fermat Theorems

Theorem 9.1 (Euler's Theorem)**.** *If a and m are integers and $(a, m) = 1$ then*

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

Proof. Pick a reduced residue system $a_1, a_2, \dots, a_{\varphi(m)}$. By (8.10)

$$aa_1, aa_2, \dots, aa_{\varphi(m)}$$

is also a reduced residue system. It follows that both products are equal modulo m,

$$(aa_1)(aa_2)(aa_3)\dots(aa_{\varphi(m)}) \equiv a_1a_2a_3\dots a_{\varphi(m)} \mod m.$$

Rearranging, we get

$$a^{\varphi(m)}a_1a_2a_3\dots a_{\varphi(m)} \equiv a_1a_2a_3\dots a_{\varphi(m)} \mod m.$$

As we have a group, we can cancel $a_1a_2a_3\dots a_{\varphi(m)}$ from both sides, to get

$$a^{\varphi(m)} \equiv 1 \mod m.$$ □

Corollary 9.2 (Fermat's little Theorem)**.** *Let p be a prime and let a be an integer.*

If a is coprime to p then

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

In particular

$$a^p \equiv a \mod p.$$

Proof. $\varphi(p) = p - 1$ and so the first statement follows from (9.1). For the second statement there are two cases. If $(a, p) = 1$ multiply both sides of

$$a^{p-1} \equiv 1 \mod p$$

by a. If $(a, p) \neq 1$ then a is a multiple of p and $a \equiv 0 \mod p$. The equation

$$a^p \equiv a \mod p$$

is true as zero equals zero. □

Definition 9.3. *Let $m > 1$ be a natural number and let a be an integer coprime to m. The **order** of a is the smallest natural number t such that*

$$a^t \equiv 1 \mod m.$$

As

$$a^{\varphi(m)} \equiv 1 \mod m,$$

the order a is always at most $\varphi(m)$. Suppose we take $m = 9 = 3^2$. Then

$$\varphi(9) = 9 - 3 = 6.$$

In fact 1, 2, 4, 5, 7, 8 is a reduced residue system.

$$2^2 = 4 \qquad 2^3 = 8 \qquad 2^4 \equiv 7 \qquad 2^5 \equiv 5 \qquad \text{and} \qquad 2^6 \equiv 1 \mod 9.$$

Thus the order of 2 is 6. On the other hand,

$$5^2 \equiv 2 \qquad \text{and} \qquad 5^3 \equiv 1,$$

so that 5 has order 3, and

$$7^2 \equiv 1$$

so that 7 has order 2.

Theorem 9.4. *If $m > 1$ is a natural number and a is an integer such that $(a, m) = 1$ then the order of a divides $\varphi(m)$.*

Proof. Let t be the order of a. If we divide t into $\varphi(m)$ we get

$$\varphi(m) = qt + r,$$

where $0 \leq r < t$. We have

$$\begin{aligned} n &\equiv a^{\varphi(m)} \mod m \\ &= a^{qt+r} \\ &= (a^t)^q + a^r \\ &\equiv 1^q + a^r \mod m \\ &= a^r. \end{aligned}$$

As t is the smallest natural number such that $a^t \equiv 1 \mod m$, r is not a natural number, that is, $r = 0$.

It follows that the order of a divides $\varphi(m)$. □

Theorem 9.5. *If n is a natural number then*

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

Proof. If a is a natural number between 1 and n then the greatest common divisor d of a and n is a divisor d of n.

Therefore we can partition the natural numbers from 1 to n into parts

$$C_d = \{\, a \in \mathbb{N} \,|\, 1 \leq a \leq n, (a, n) = d \,\},$$

where d ranges over the divisors of n.

If $a \in C_d$ then let $b = a/d$. It follows that $(b, n/d) = 1$ and $1 \leq b \leq n/d$. Given b, note that $a = bd$. Thus

$$C_d = \{\, a \in \mathbb{N} \mid a = bd, 1 \leq b \leq n/d, (b, n/d) = 1 \,\}.$$

It follows that the cardinality of C_d is simply the number of integers between 1 and n/d coprime to n/d. We have

$$\begin{aligned} 1 &= |\{\, a \in \mathbb{N} \mid 1 \leq a \leq n \,\}| \\ &= \sum_{d|n} |C_d| \\ &= \sum_{d|n} \varphi(n/d) \\ &= \sum_{d|n} \varphi(d), \end{aligned}$$

where we used the fact the terms of third and fourth sums are rearrangements of each other. □

For example, consider $n = 10 = 2 \cdot 5$. The divisors of 10 are 1, 2, 5 and 10.

$$\varphi(1) = 1 \qquad \varphi(2) = 1 \qquad \varphi(5) = 4 \qquad \text{and} \qquad \varphi(10) = \varphi(2)\varphi(5) = 4.$$

As expected

$$1 + 1 + 4 + 4 = 10.$$