13. Euler Theorem

Theorem 13.1. *The units U of $\mathbb{Z}_n$ are precisely the set G_n of elements of $\mathbb{Z}_n$ coprime to n.*

In particular G_n is a group under multiplication.

Proof. The product of two numbers coprime to n is coprime to n so that G_n is closed under multiplication. Pick a nonzero element $a \in G_n$ and define a map

$$f \colon G_n \longrightarrow G_n \qquad \text{by the rule} \qquad b \longrightarrow ab.$$

Suppose that $f(b_1) = f(b_2)$. Then $ab_1 = ab_2$. As a is coprime to n, it is not a zero-divisor. Hence the cancellation law holds and so $b_1 = b_2$. It follows that f is one to one.

As G_n is finite, f is onto. Therefore we may find $b \in G_n$ such that $1 = f(b)$ and so $ab = 1$. Therefore a is a unit. Thus $G_n \subset U$. Every unit is not a zero-divisor and so every unit is coprime to n. Thus $U = G_n$.

But then G_n is a group as U is a group. □

Definition 13.2 (Euler's phi-function)**.** *If n is positive integer, $\varphi(n)$ is the number of integers between 1 and $n-1$ coprime to n.*

We already know that if p is prime then $\varphi(p) = p - 1$.

Example 13.3. *What is $\varphi(15)$?*

We want to count the integers between 1 and 14 coprime to $15 = 3 \cdot 5$. These are the integers which are neither a multiple of 3 nor a multiple of 5. These are

$$1 \qquad 2 \qquad 4 \qquad 7 \qquad 8 \qquad 11 \qquad 13 \qquad 14.$$

Thus

$$\varphi(15) = 8.$$

Later on we will see a much more efficient way to compute $\varphi(n)$.

Theorem 13.4 (Euler's Theorem)**.** *If a is relatively prime to n then*

$$a^{\varphi(n)} = 1 \mod n.$$

Proof. If r is the remainder when you divide n into a then

$$a^{\varphi(n)} = r^{\varphi(n)} \mod n.$$

So we might as well assume that $a \in \mathbb{Z}_n$. As a is coprime to n, $a \in G_n$ a group of order $\varphi(n)$. Thus

$$a^{\varphi(n)} = 1 \in \mathbb{Z}_n,$$

and so

$$a^{\varphi(n)} = 1 \mod n. \qquad \square$$

Example 13.5. *What is the remainder when you divide 11^{60} by 15?*

11 is prime and so it is coprime to 15. We already computed $\varphi(15) = 8$, so that by Euler's Theorem we know:

$$11^8 = 1 \mod 15.$$

Therefore

$$\begin{aligned} 11^{60} &= 11^{56} \cdot 11^4 \\ &= (11^8)^7 \cdot 11^4 \\ &= 11^4 \\ &= (-4)^4 \\ &= 2^8 \\ &= 1 \mod 15, \end{aligned}$$

by another application of Euler's Theorem, using the fact that 2 is coprime to 15.

One potential drawback of Euler's Theorem is that it seems hard work to compute $\varphi(n)$ if n is large. Not so.

Definition 13.6. *Let*

$$f : \mathbb{N} \longrightarrow \mathbb{N}$$

*be a function from the natural numbers to the natural numbers. We say that f is **multiplicative** if*

$$f(mn) = f(m)f(n)$$

whenever m and n are coprime.

Proposition 13.7. *The Euler phi-function is multiplicative.*

Proof. We want to count the number of elements of $\mathbb{Z}_{mn}$ coprime to mn. This is the same as the number of units. Now by the Chinese remainder Theorem, the two rings

$$\mathbb{Z}_{mn} \qquad \text{and} \qquad \mathbb{Z}_m \times \mathbb{Z}_n$$

are isomorphic (this is where we use the fact that m and n are coprime). So the number of units in the first ring is the same as the number of units in the second ring.

Suppose that $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. This is a unit if and only if we can find $(c, d) \in \mathbb{Z}_m \times \mathbb{Z}_n$ such that

$$(a, b)(c, d) = (ab, cd) = (1, 1).$$

It follows that $ab = 1$ and $cd = 1$, so that a and b are units. Thus $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is a unit if and only if $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$ is a unit. The number of possibilities for a is $\varphi(m)$ and the number of possibilities for b is $\varphi(n)$. Thus the number of units in $\mathbb{Z}_m \times \mathbb{Z}_n$ is $\varphi(m)\varphi(n)$.

Putting all of this together we get

$$\varphi(mn) = \varphi(m)\varphi(n). \qquad \square$$

(13.7) already gets us quite far:

$$\begin{aligned}\varphi(15) &= \varphi(3 \cdot 5)\\ &= \varphi(3)\varphi(5)\\ &= (3-1)(5-1)\\ &= 8,\end{aligned}$$

the same answer we got as the slow way of eliminating all multiples of 3 and 5.

Unfortunately we get stuck if n is slighly more complicated:

$$\begin{aligned}\varphi(24) &= \varphi(3 \cdot 8)\\ &= \varphi(3)\varphi(8)\\ &= (3-1)\varphi(8).\end{aligned}$$

What we are missing is how to compute $\varphi(8)$ or more generally $\varphi(p^k)$ where p is prime.

Proposition 13.8. *If p is a prime and k is a natural number then*

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

Proof. We want to know the number of integers between 1 and p^k coprime to p. These are simply the number of integers between 1 and p^k which are not multiples of p. The multiples of p are

$$1 \quad p \quad 2p \quad 3p \quad 4p \quad \dots \quad p^{k-1}p = p^k.$$

So there are p^{k-1} multiples of p between 1 and p^k. Hence there are

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

integers between 1 and p^k which are coprime to p. $\square$

Using (13.8) we see that

$$\varphi(8) = 8 - 4 = 4.$$

Thus

$$\varphi(24) = 8.$$

Theorem 13.9. *If $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ is the prime factorisation of the natural number n then*

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_m^{k_m} - p_m^{k_m-1}).$$

Proof. We simply apply (13.7) and (13.8):

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}) \\
&= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_m^{k_m}) \\
&= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_m^{k_m} - p_m^{k_m-1}).
\end{aligned}$$

□