8. Euler φ-function

We have already seen that $\mathbb{Z}_m$, the set of equivalence classes of the integers modulo m, is naturally a ring. Now we will start to derive some interesting consequences in number theory.

It is clear that the equivalence classes are represented by the integers from zero to $m-1$, $[0]$, $[1]$, $[2]$, $[3]$, ..., $[m-1]$. Indeed, if a is any integer we may divide m into a to get a quotient and a remainder,

$$a = mq + r \qquad \text{where} \qquad 0 \leq r \leq m-1.$$

In this case

$$[a] = [r].$$

From the point of view of number theory it is very interesting to write down other sets of integers with the same properties.

Definition 8.1. *A set S of integers is called a* ***complete residue system****, modulo m, if every integer $a \in \mathbb{Z}$ is equivalent, modulo m, to exactly one element of S.*

We have already seen that

$$\{\, r \in \mathbb{Z} \,|\, 0 \leq r \leq m-1 \,\} = \{\, 0, 1, 2, \dots, m-2, m-1 \,\}$$

is a complete residue system. Sometimes it is convenient to shift so that 0 is in the centre of the system

$$\{\, r \in \mathbb{Z} \,|\, -m/2 < r \leq m/2 \,\} = \{\, \dots, -2, -1, 0, 1, 2, \dots \}.$$

For example if $m = 5$ we would take -2, 1, 0, 1 and 2 and if $m = 8$ we would take -3, -2, -1, 0, 1, 2, 3 and 4.

Fortunately it is very easy to determine if a set S is a complete residue system:

Lemma 8.2. *Let $S \subset \mathbb{Z}$ be a subset of the integers and let m be a non-negative integer. If any two of the following two conditions hold then so does the third, in which case S is a complete residue system.*

1. *S has m elements.*
2. *No two different elements of S are congruent.*
3. *Every integer is congruent to at least one element of S.*

Proof. We have already seen that

$$S_0 = \{\, r \in \mathbb{Z} \,|\, 0 \leq r \leq m-1 \,\} = \{\, 0, 1, 2, \dots, m-2, m-1 \,\}$$

is a complete residue system. Clearly S_0 has m elements.

Note that there is a natural map

$$f \colon S \longrightarrow S_0,$$

which sends an element a of S to its residue modulo m.

Note that (1) holds if and only if S and S_0 have the same number of elements; (2) holds if and only if f is injective and (3) holds if and only if f is surjective.

It is then easy to see that any two of (1), (2) and (3) imply the third. $\square$

We can use (8.2) to prove a nice:

Theorem 8.3. *Let m be a positive integer and let $a_1, a_2, \dots, a_m$ is a complete residue system, modulo m. Suppose that b and $k \in \mathbb{Z}$ and $(k, m) = 1$.*

Then

$$ka_1 + b, \qquad ka_2 + b, \qquad \dots, \qquad ka_m + b,$$

is also a complete residue system, modulo m.

Proof. Note that if $ka_i + b = ka_j + b$ then $a_i = a_j$. Thus

$$ka_1 + b, \qquad ka_2 + b, \qquad \dots, \qquad ka_m + b,$$

is a sequence of m distinct integers. We check that (2) of (8.2) also holds.

Suppose that

$$ka_i + b \equiv ka_j + b \mod m.$$

Then certainly

$$ka_i \equiv ka_j \mod m.$$

As $(k, m) = 1$, it follows by (7.11) that

$$a_i \equiv a_j \mod m. \qquad \square$$

We shall start dropping any reference to equivalence classes when we work in the ring $\mathbb{Z}_m$. This is purely a matter of notational convenience. The ring $\mathbb{Z}_m$ has two operations, addition and multiplication. Note that

$$\begin{aligned}
&1 \\
&2 = 1 + 1 \\
&3 = 2 + 1 = 1 + 1 + 1 \\
&4 = 3 + 1 = 1 + 1 + 1 + 1,
\end{aligned}$$

and so on, give all the elements of $\mathbb{Z}_m$ under addition. The group $\mathbb{Z}_m$ under addition is called **cyclic** and 1 is called a generator.

It is more interesting to figure out what happens under multiplication. If p is a prime then the non-zero elements of $\mathbb{Z}_p$ are a group under multiplication. We will see that it is always cyclic.

For example, suppose we take $p = 7$. We have

$$2^2 = 4 \qquad 2^3 = 8 \equiv 1 \mod 7.$$

Thus

$$\begin{aligned} 2^4 &= 2 \cdot 2^3 \\ &= 2 \cdot 1 \\ &= 2. \end{aligned}$$

If we keep going we will just get 1, 2 and 4 (there is a reason it is called cyclic). Thus 2 is not a generator.

Now consider 3 instead of 2. We have

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

Thus the non-zero elements of $\mathbb{Z}_7$ is a cyclic group with generator 3 (but not 2).

For general m, the non-zero elements of $\mathbb{Z}_m$ do not form a group under multiplication. We have already seen that the product of two elements might be zero, so that the set of non-zero elements is not closed under multiplication.

Definition 8.4. *Let $m > 1$ be an integer. U_m is the set of units of $\mathbb{Z}_m$.*

It is not hard to check that U_m is a group under multiplication.

Definition 8.5. *The Euler φ-function*

$$\varphi \colon \mathbb{N} \longrightarrow \mathbb{N}$$

just sends m to the cardinality of U_m.

If p is a prime then every non-zero element of $\mathbb{Z}_p$ is a unit, so that

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

Lemma 8.6. *Let $m > 1$ and $a \in \mathbb{Z}$ be integers.*

Then $[a]$ is a unit if and only if $(a, m) = 1$.

Proof. If $(a, m) = 1$ then we can find integers λ and μ such that

$$1 = \lambda a + \mu m.$$

In this case

$$\begin{aligned} 1 &= [1] \\ &= [\lambda a + \mu m] \\ &= [\lambda][a] + [\mu][m] \\ &= [\lambda][a]. \end{aligned}$$

Thus $[\lambda]$ is the inverse of $[a]$.

Conversely, suppose that $[a]$ is a unit. Then we can find an integer b such that

$$[a][b] = 1.$$

It follows that $ab \equiv 1 \mod m$, that is, $ab - 1$ is divisible by m. Thus

$$ab - 1 = km,$$

for some integer k. Rearranging, we get

$$1 = (-b)a + km.$$

Thus $(a, m) = 1$. □

Lemma 8.7. *If m is a natural number then $\varphi(m)$ is the number of integers a from 0 to $m - 1$ coprime to m.*

Proof. The elements of $\mathbb{Z}_m$ are represented by the integers a from 0 to $m - 1$ and $[a]$ is a unit if and only if it is coprime to m. □

This gives an easy way to compute the Euler φ-function, at least for small values of m. Suppose $m = 6$. Of the integers 0, 1, 2, 3, 4 and 5, only 1 and 5 are coprime to 6. Thus $\varphi(6) = 2$.

Definition 8.8. *A set S of integers is called a* ***reduced residue system****, modulo m, if every integer coprime to m is equivalent to exactly one element of m.*

Lemma 8.9. *Let $S \subset \mathbb{Z}$ be a subset of the integers and let m be a non-negative integer. If any two of the following two hold conditions then so does the third, in which case S is a reduced residue system.*

(1) S has $\varphi(m)$ elements.
(2) No two different elements of S are congruent.
(3) Every is congruent to at least one element of S.

Proof. A simple variation of the proof of (8.2) □

Theorem 8.10. *Let m be a positive integer and let $a_1, a_2, \dots, a_{\varphi(m)}$ is a reduced residue system, modulo m.*

If $k \in \mathbb{Z}$ is the coprime to m then $ka_1, ka_2, \dots, ka_{\varphi(m)}$ is also a reduced residue system, modulo m.

Proof. Similar, and simpler, than the proof of (8.3). □

Definition 8.11. *We say that a function*

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

is multiplicative if $f(mn) = f(m)f(n)$, whenever m and n coprime.

Theorem 8.12. *φ is multiplicative.*

Proof. Suppose that $m = 1$. Then $mn = 1 \cdot n = n$ so that

$$\begin{aligned}\phi(m)\phi(n) &= \phi(1)\phi(n)\\ &= \phi(n)\\ &= \phi(1 \cdot n)\\ &= \phi(mn).\end{aligned}$$

Thus the result holds if $m = 1$. Similarly the result holds if $n = 1$. Thus we may assume that m and $n > 1$. Consider the array

$$\begin{array}{ccccc} 0 & 1 & 2 & \dots & m-1 \\ m & m+1 & m+2 & \dots & m+(m-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n-1)m & (n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+(m-1). \end{array}$$

The last entry is $nm - 1$ and so this is a complete residue system, modulo mn. Therefore $\varphi(mn)$ is the number of elements of the array comprime to mn.

Pick a column and suppose the first entry is a. The other entries in that column are $m + a$, $2m + a$, $\dots$, $(n - 1)m + a$ and so every entry in that column is congruent to a modulo m. So if a is not coprime to m then no entry in that column is coprime to m, let alone mn. Thus we can focus on those columns whose first entry a is coprime to a.

The first row is a complete residue system modulo m, so that $\varphi(m)$ elements of the first row are coprime to m. Thus there are only $\varphi(m)$ columns we need to focus on. On the other hand, the entries in this column are the numbers $m \cdot 1 + a$, $m \cdot 2 + a$, $m \cdot 3 + a$, and so they are a complete residue system modulo n, by (8.3). Thus $\varphi(n)$ elements of this column are coprime to n.

Thus $\varphi(m)\varphi(n)$ elements of the array are coprime to both m and n. But as m and n are coprime, it follows that an integer l is coprime to mn if and only if it is coprime to m and n. Thus $\varphi(m)\varphi(n)$ elements of the array are coprime to mn. $\square$

Multiplicative functions are relatively easy to compute; if

$$n = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

is the prime factorisation of n and f is multiplicative then

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_n^{e_n}).$$

Therefore it suffices to compute

$$f(p^e),$$

where p is a prime.

Lemma 8.13. *If p is a prime then*
$$\varphi(p^e) = p^e - p^{e-1}.$$

Proof. Consider the numbers from to 1 to p^e. These are a complete residue system. Now a is coprime to p^e if and only if it is coprime to p. In other words, a is not coprime to p^e if and only if it is a multiple of p. Of the numbers from 1 to p^e, exactly
$$\frac{p^e}{p} = p^{e-1}.$$
are multiples of p. Therefore the remaining
$$p^e - p^{e-1}$$
numbers are coprime to p^e. □

Theorem 8.14. *If*
$$n = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$
is the prime factorisation of n then
$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_n^{e_n} - p_n^{e_n-1}).$$

Question 8.15. *How many units are there in the ring $\mathbb{Z}_{1656}$?*

In other words, what is the cardinality of U_{1656}? This is the same as $\varphi(1656)$. We first factor 1656.
$$\begin{aligned} 1656 &= 2 \cdot 828 \\ &= 2^2 \cdot 414 \\ &= 2^3 \cdot 207 \\ &= 2^3 \cdot 3 \cdot 69 \\ &= 2^3 \cdot 3^2 \cdot 23. \end{aligned}$$

We have
$$\begin{aligned} \varphi(1656) &= \varphi(2^3 \cdot 3^2 \cdot 23) \\ &= \varphi(2^3)\varphi(3^2)\varphi(23) \\ &= (2^3 - 2^2)(3^2 - 3)(23 - 1) \\ &= 4 \cdot 6 \cdot 22 \\ &= 2^4 \cdot 3 \cdot 11 \\ &= 528. \end{aligned}$$