3.2: Residue Systems and Euler’s $\varphi$-Function

Residue of $(a \mod m)$. As a result, we see that any integer is congruent to one of the integers $(0, 1, 2, ..., m-1)$ modulo $m$.

A complete residue system modulo $(m)$ is a set of integers such that every integer is congruent modulo $(m)$ to exactly one integer of the set.

The easiest complete residue system modulo $(m)$ is the set of integers $(0, 1, 2, ..., m-1)$. Every integer is congruent to one of these integers modulo $(m)$.

The set of integers $(\{0, 1, 2, 3, 4\})$ form a complete residue system modulo $(5)$. Another complete residue system modulo $(5)$ could be $(\{6, 7, 8, 9, 10\})$.

A reduced residue system modulo $(m)$ is a set of integers $(r_i)$ such that $((r_i, m)=1)$ for all $(i)$ and $(r_i \neq r_j \mod m)$ if $(i \neq j)$.

Notice that, a reduced residue system modulo $(m)$ can be obtained by deleting all the elements of the complete residue system set that are not relatively prime to $(m)$.

The set of integers $(\{1, 5\})$ is a reduced residue system modulo $(6)$.

The following lemma will help determine a complete residue system modulo any positive integer $(m)$.

Lemma

A set of $(m)$ incongruent integers modulo $(m)$ forms a complete residue system modulo $(m)$.
We will prove this lemma by contradiction. Suppose that the set of \( \{m\} \) integers does not form a complete residue system modulo \( \{m\} \). Then we can find at least one integer \( \{a\} \) that is not congruent to any element in this set. Hence non of the elements of this set is actually congruent to the remainder when \( \{a\} \) is divided by \( \{m\} \). Thus dividing by \( \{m\} \) yields to at most \( \{m-1\} \) remainders. Therefore by the pigeonhole principle, at least two integers in the set that have the same remainder modulo \( \{m\} \). This is a contradiction since the set of integers is formed of \( \{m\} \) integers that are incongruent modulo \( \{m\} \).

If \( \{a_1, a_2, ..., a_m\} \) is a complete residue system modulo \( \{m\} \), and if \( \{k\} \) is a positive integer with \( \{(k,m)=1\} \), then \( \{ka_1+b, ka_2+b, ..., ka_m+b\} \) is another complete residue system modulo \( \{m\} \) for any integer \( \{b\} \).

Let us prove first that no two elements of the set \( \{\{ka_1+b, ka_2+b, ..., ka_m+b\}\} \) are congruent modulo \( \{m\} \). Suppose there exists \( \{i\} \) and \( \{j\} \) such that \( \{ka_i+b\equiv ka_j+b(mod\ m)\} \). Thus we get that \( \{ka_i\equiv ka_j(mod\ m)\} \). Now since \( \{(k,m)=1\} \), we get \( \{a_i\equiv a_j(mod\ m)\} \). But for \( \{i\neq j\} \), \( \{a_i\} \) is inequivalent to \( \{a_j\} \) modulo \( \{m\} \). Thus \( \{i=j\} \).

Now notice that there are \( \{m\} \) inequivalent integers modulo \( m \) and thus by Lemma 10, the set form a complete residue system modulo \( \{m\} \).

---

**Euler’s \( \phi \)-Function**

We now present a function that counts the number of positive integers less than a given integer that are relatively prime to that given integer. This function is called Euler \( \phi \)-function. We will discuss the properties of Euler \( \phi \)-function in details in chapter 5. It will be sufficient for our purposes in this chapter to the notation.

The Euler \( \phi \)-function of a positive integer \( n \), denoted by \( \phi(n) \) counts the number of positive integers less than \( n \) that are relatively prime to \( n \).

Since 1 and 3 are the only two integers that are relatively prime to 4 and less than 4, then \( \phi(4)=2 \). Also, 1, 2, ..., 6 are the integers that are relatively prime to 7 that are less than 7, thus \( \phi(7)=6 \).

Now we can say that the number of elements in a reduced residue system modulo \( n \) is \( \phi(n) \).

If \( \{a_1, a_2, ..., \{\phi(n)\}\} \) is a reduced residue system modulo \( n \) and \( \{(k,n)=1\} \), then \( \{ka_1, ka_2, ..., ka_{\{\phi(n)\}}\} \) is a reduced residue system modulo \( n \).

The proof proceeds exactly in the same way as that of Theorem 24.

**Exercises**

1. Give a reduced residue system modulo 12.
2. Give a complete residue system modulo 13 consisting only of odd integers.
3. Find \( \phi(8) \) and \( \phi(101) \).
Contributors and Attributions

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.