MATH453 Elementary Number Theory

Lecture 8: Congruence Classes and Residue System

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

8.1 Congruence Classes

Recall that from last lecture, we defined

Definition 8.1 (Congruence Classes). The congruence class of a modulo m, denoted $[a]_m$, is the set of all integers that are congruent to a modulo m

$$\{z \in \mathbb{Z} \mid m \mid (a - z)\}$$

And we have the proposition

Proposition 8.1. Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then

$$a + c \equiv b + d \mod m \tag{8.1}$$

$$ac \equiv bd \mod m \tag{8.2}$$

From these two properties, we can define the **addition** and **multiplication** operations on congruence classes $(+, \times)$.

$$[a]_m + [c]_m = [a + c]_m$$

and

$$[a]_m \times [c]_m = [ac]_m$$

Also, recall from last lecture that we cannot just cancel common factors in a congruence relation. We established that in the general case, this will not work. For example, $6 \equiv 3 \mod 3$ but $2 \not\equiv 1 \mod 3$. However, there are cases where we can cancel factors in a congruence.

Proposition 8.2.

$$ca \equiv cb \mod m \iff a \equiv b \mod \frac{m}{\gcd(c, m)}$$

For example, say we have $6 \equiv 3 \mod 3$. By Proposition 8.2, we have $2 \equiv 1 \mod \frac{3}{\gcd(3,3)}$ so $2 \equiv 1 \mod 1$. Now, we prove this proposition.

Proof.

($\implies$): Assume that $ca \equiv cb \mod m$, which by definition, implies that $m \mid (ca - cb)$ and $m \mid c(a - b)$. By definition of divisibility, there exists some d such that $c(a - b) = md$. Then, we can divide both sides by the greatest common divisor of c and m, giving us

$$\frac{c}{\gcd(c, m)}(a - b) = \frac{m}{\gcd(c, m)}d$$

Further, since $\gcd(c, m)$ is the greatest common divisor, $\gcd\left(\frac{c}{\gcd(c,m)}, \frac{m}{\gcd(c,m)}\right) = 1$. This implies

$$\frac{m}{\gcd(c,m)} \mid (a-b)$$

which by definition means $a \equiv b \mod \frac{m}{\gcd(c,m)}$.

($\Longleftarrow$): Assume that $a \equiv b \mod \frac{m}{\gcd(c,m)}$. By definition, $\frac{m}{\gcd(c,m)} \mid (a-b)$. So there exists some d such that

$$a - b = \frac{m}{\gcd(c,m)} d \implies ca - cb = \frac{cm}{\gcd(c,m)} d = \frac{cd}{\gcd(c,m)} m$$

This implies $m \mid (ca - cb)$ since $\frac{cd}{\gcd(c,m)}$ is an integer. Then by definition of congruence, $ca \equiv cb \mod m$. ■

8.2 Reduced Residue System

Also recall that from last lecture, we defined a ***complete residue system***.

> **Definition 8.2** (Complete Residue System). A **complete residue system** modulo m is a set S of integers such that every $n \in \mathbb{Z}$ is congruent to one and only one member of S.

> **Definition 8.3** (Reduced Residue System). A **reduced residue system** modulo m is a set of integers $r_1, \ldots, r_n$ such that if $\gcd(a, m) = 1$, then $a \equiv r_j \mod m$ for one and only one value of j.

Stated slightly differently, a reduced residue system modulo m is a set of integers r_i such that $\gcd(r_i, m) = 1$ for all i, and $r_i \not\equiv r_j \mod m$ for all $j \neq i$. That is, each element in a reduced residue system is relatively prime to m and no two elements of the set are congruent modulo m.

Note that the definition of a reduced residue system immediately implies that $n < m$. To see why, suppose $n = m$ and we have a complete residue system. Then, $m \equiv m \mod m$. WLOG, suppose $m = r_j$ for some j (otherwise, we can choose r_j to be some multiple of m). By definition, there's some a such that $a \equiv m \mod m$ but this is impossible since a and m are relatively prime by definition of a reduced residue system. This implies that m or any multiple of m must not be an element in a reduced residue system.

Another way of looking at a reduced residue system is that we can take a complete residue system, remove certain numbers, and get back a reduced residue system. In particular, if we have a complete residue system modulo m, and we remove all r_j such that $\gcd(r_j, m) = 1$, the resulting system is a reduced residue system. This should be clear from the definition of a reduced system.

Additionally, if $\gcd(a, m) = 1$ and $a \equiv r_j \mod m$ for some a, then $\gcd(r_j, m) = 1$. This essentially shows that our alternative definition is the same as the original definition.

Proof. Suppose not. That is, there exists a such that $\gcd(a, m) = 1$ and $m \mid (a - r_j)$ but $\gcd(r_j, m) \neq 1$. This implies there exists some p such that $p \mid r_j$ and $p \mid m$. But we also have $a - r_j = md$ for some d since $m \mid (a - r_j)$. This implies $p \mid a$. But by our assumption, a and m should be relatively prime, so this is a contradiction. ■

8.3 Euler's Phi Function

The number of elements in a reduced residue system modulo m for some fixed m is **constant**. We call this number ***Euler's phi function*** or ***Euler's totient function***. The Euler's phi function for m is denoted by

$$\varphi(m)$$

Theorem 8.1. Let $r_1, \dots, r_n$ be a complete/reduced residue system modulo m. Let $\gcd(a, m) = 1$. Then,

$$\{ar_1, \dots, ar_n\}$$

is still a complete/reduced residue system modulo m.

Proof. Suppose for contradiction that $\{ar_1, \dots, ar_n\}$ is not a complete/reduced residue system modulo m for some m. Then, there must exitsts some i and j such that $ar_i \equiv ar_j \mod m$ (if no such i, j exists, then $\{ar_1, \dots, ar_n\}$ would indeed be complete/reduced). But since $\gcd(a, m) = 1$, $ar_i \equiv ar_j \mod m \iff r_i \equiv r_j \mod m$. This is a contradiction to the assumption that $\{r_1, \dots, r_n\}$ is a complete/reduced residue system. ■