# COMP8760

Handout Note - 1

(on $\mathbb{Z}_N, \mathbb{Z}_N^*, \mathbb{F}_p, \mathbb{F}_p^*, \mathbb{QR}_p, \mathbb{QNR}_p$, Legendre and Jacobi symbols)

Sanjay Bhattacherjee

This handout note should be useful as a quick reference on some of the mathematical notions and notations introduced in this module.

1. The set $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$ has all remainders of $N$.

2. The algebraic structure $(\mathbb{Z}_N, +, \cdot)$ forms a ring with respect to addition and multiplication modulo $N$. This means, $(\mathbb{Z}_N, +)$ is a commutative group. However, $(\mathbb{Z}_N, \cdot)$ follows the properties closure, associativity, identity and commutativity, but not all elements of $\mathbb{Z}_N$ will have inverses.

   *An element $a \in \mathbb{Z}_N$ has a multiplicative inverse if and only if*
   $$\gcd(a, N) = 1.$$
   *All $a \in \mathbb{Z}_N$ such that* $\gcd(a, N) = 1$ *form the set $\mathbb{Z}_N^*$.*

3. If $N$ is *composite*, the set $\mathbb{Z}_N^*$ *will not have* all the non-zero elements from $\mathbb{Z}_N$. It will only have elements $a \in \mathbb{Z}_N$ which have $\gcd(a, N) = 1$. These elements will not have any common divisor with $N$ that is greater than 1.

4. Unlike point 3 above, if $N$ is *prime*, the set $\mathbb{Z}_N^*$ *will have* all the non-zero elements from $\mathbb{Z}_N$.

| | |
|---|---|
| $\mathbb{Z}_5$ | $= \{0, 1, 2, 3, 4\}$ |
| $\mathbb{Z}_5^*$ | $= \{1, 2, 3, 4\}$ |
| $\mathbb{Z}_6$ | $= \{0, 1, 2, 3, 4, 5\}$ |
| $\mathbb{Z}_6^*$ | $= \{1, 5\}$ |
| $\mathbb{Z}_7$ | $= \{0, 1, 2, 3, 4, 5, 6\}$ |
| $\mathbb{Z}_7^*$ | $= \{1, 2, 3, 4, 5, 6\}$ |
| $\mathbb{Z}_8$ | $= \{0, 1, 2, 3, 4, 5, 6, 7\}$ |
| $\mathbb{Z}_8^*$ | $= \{1, 3, 5, 7\}$ |

Table 1: Examples for $N \in \{5, 6, 7, 8\}$ to demonstrate points 3 and 4.

5. In point 2 above, we noticed that $(\mathbb{Z}_N, \cdot)$ is not a multiplicative group because all its elements may not have inverses. In other words, there may not be a solution to the equation
   $$a \cdot x = 1 \pmod N$$
   unless $\gcd(a, N) = 1$. In Table 2, this can be checked for all $a \in \mathbb{Z}_{12}$ that are not mutually prime to 12. However, all elements of $\mathbb{Z}_N^*$ have multiplicative inverses. From point 2 we know that every $a \in \mathbb{Z}_N^*$ has $\gcd(a, N) = 1$. By substituting the value of $\gcd(a, N)$ in the expression for the extended Euclidean algorithm, we get that there exists integers $x, y$ such that
   $$1 = a \cdot x + N \cdot y \pmod N.$$
   Since $N \cdot y = 0 \pmod N$, we can say that there exists an $x \in \mathbb{Z}_N^*$ such that $a \cdot x = 1 \pmod N$. Hence, $\mathbb{Z}_N^*$ is a multiplicative group under multiplication modulo $N$.

| $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b$ | | | | | | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 2 | 0 | 2 | 4 | 6 | 8 | 10 | 0 | 2 | 4 | 6 | 8 | 10 |
| 3 | 0 | 3 | 6 | 9 | 0 | 3 | 6 | 9 | 0 | 3 | 6 | 9 |
| 4 | 0 | 4 | 8 | 0 | 4 | 8 | 0 | 4 | 8 | 0 | 4 | 8 |
| 5 | 0 | 5 | 10 | 3 | 8 | 1 | 6 | 11 | 4 | 9 | 2 | 7 |
| 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 |
| 7 | 0 | 7 | 2 | 9 | 4 | 11 | 6 | 1 | 8 | 3 | 10 | 5 |
| 8 | 0 | 8 | 4 | 0 | 8 | 4 | 0 | 8 | 4 | 0 | 8 | 4 |
| 9 | 0 | 9 | 6 | 3 | 0 | 9 | 6 | 3 | 0 | 9 | 6 | 3 |
| 10 | 0 | 10 | 8 | 6 | 4 | 2 | 0 | 10 | 8 | 6 | 4 | 2 |
| 11 | 0 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Table 2: The multiplication table for elements of $\mathbb{Z}_{12}$. The variables $a$ and $b$ both take values from $\mathbb{Z}_{12}$ and the result of $a \cdot b \pmod{12}$ is mentioned in the corresponding entry in the table. We have the set $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ such that for each $a \in \mathbb{Z}_{12}^*$, $\gcd(a, 12) = 1$. To corroborate with the result of substituting this value of $\gcd(a, 12) = 1$ in the extended Euclidean algorithm, we note that there are solutions to the equation $a \cdot x = 1 \pmod{12}$ if and only if $a \in \mathbb{Z}_{12}^*$.

6. Euler's totient function $\phi(n)$ is defined to take as input an integer $n$ and gives as output the number of positive integers $a$ smaller than $n$ for which $\gcd(a, n) = 1$. Let the prime factorisation of $n$ be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then, the value of $\phi(n)$ is given by the formula:

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Note here that the notation $\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$ denotes the product of terms $\left(1 - \frac{1}{p_i}\right)$ where $i$ varies from 1 to $k$.

7. When the integer $N$ is prime, we use the notation $p$ instead.
From point 4, we know that the set $\mathbb{Z}_p^*$ will have all non-zero elements of $\mathbb{Z}_p$. So,

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}.$$

By counting the number of elements in $\mathbb{Z}_p^*$, we get the cardinality of the set

$$|\mathbb{Z}_p^*| = p - 1.$$

From point 6 on the Euler's totient function, we get that for a prime $p$,

$$\phi(p) = p\left(1 - \frac{1}{p}\right) = p - 1.$$

In summary, $|\mathbb{Z}_p^*| = \phi(p) = p - 1$.

8. From point 5, we know that the non-zero elements of $\mathbb{Z}_p$ form a multiplicative group, where every element has an inverse. The following properties hold:

- $(\mathbb{Z}_p, +)$ is an additive abelian group with identity 0.
- $(\mathbb{Z}_p^*, \cdot)$ is a multiplicative abelian group with identity 1.
- The distributive law holds in $(\mathbb{Z}_p, +, \cdot)$.

Based on these three properties, we say that $(\mathbb{Z}_p, +, \cdot)$ is a *field*.
(Note from point 2 that in general, $(\mathbb{Z}_N, +, \cdot)$ is a *ring* and not a *field* because of the absence of inverses for elements that are not mutually prime with $N$.)

> *We use the notation $\mathbb{F}_p$ to denote the field of integers module a prime $p$.*

Henceforth, whenever we are concerned with a prime $p$, we will use the notation $\mathbb{F}_p$ in place of $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ to denote all the remainders modulo the prime $p$ and the notation $\mathbb{F}_p^*$ to denote $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

9. We define the set of *quadratic residues modulo $p$* as $\mathbb{QR}_p$ that contains all $a^2$ such that $a \in \mathbb{F}_p^*$. Using formal mathematical notation, we write

$$\mathbb{QR}_p = \{a^2 : a \in \mathbb{F}_p^*\}.$$

The set of *quadratic non-residues modulo $p$* is denoted as $\mathbb{QNR}_p$. It contains all $a \in \mathbb{F}_p^*$ that are not in $\mathbb{QR}_p$. More formally,

$$\mathbb{QNR}_p = \{a : a \in \mathbb{F}_p^*, a \notin \mathbb{QR}_p\}.$$

This set is also denoted using the *set minus notation* as $\mathbb{F}_p^* \setminus \mathbb{QR}_p$ (read as $\mathbb{F}_p^*$ setminus $\mathbb{QR}_p$).

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^2$ | 1 | 4 | 9 | 3 | 12 | 10 | 10 | 12 | 3 | 9 | 4 | 1 |

Table 3: The values of $a^2$ for all $a \in \mathbb{F}_{13}^*$. From this computation we get that, the set of quadratic residues $\mathbb{QR}_{13} = \{1, 3, 4, 9, 10, 12\}$ and the set of quadratic non-residues $\mathbb{QNR}_{13} = \mathbb{F}_{13}^* \setminus \mathbb{QR}_{13} = \{2, 5, 6, 7, 8, 11\}$.

10. For $a \in \mathbb{F}_p$, the Legendre symbol is denoted by $\left(\frac{a}{p}\right)$. It is defined to take one of three values.

$$\left(\frac{a}{p}\right) = \begin{cases} -1 = p - 1 \pmod p, & \text{if } a \in \mathbb{QNR}_p, \\ 0, & \text{if } p \text{ divides } a, \textit{and} \\ 1, & \text{if } a \in \mathbb{QR}_p. \end{cases}$$

The Legendre symbol can be computed using the formula:

$$\left(\frac{a}{p}\right) = a^{\frac{(p-1)}{2}} \pmod p.$$

11. Let $n \geq 3$ be odd and its prime factorisation be

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

The Jacobi symbol is defined in terms of the Legendre symbol as:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$