COMP8760

Lecture 3

Solutions to Worksheet for Practice

Sanjay Bhattacherjee

1. Consider the set $\mathbb{Z}_{11} = \{0, 1, 2, \ldots, 10\}$. How many elements are there in the set $\mathbb{Z}_{11}$?
Note: The number of elements in $\mathbb{Z}_{11}$ is called its cardinality and is denoted as $|\mathbb{Z}_{11}|$.
Answer:

$$|\mathbb{Z}_{11}| = 11.$$

2. Consider the set $\mathbb{Z}_{11}$ and the operation $+ \pmod{11}$ on its elements. Create a table for all operations $x + y \pmod{11}$ where $x, y \in \mathbb{Z}_{11}$. We will call it the "addition table of $\mathbb{Z}_{11}$".
Answer:

	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

3. From the table in question 2, find the element $\bar{x}$ for each $x \in \mathbb{Z}_{11}$ such that

$$x + \bar{x} = 0 \pmod{11}.$$

Hint: In the row corresponding to the number x, find the column $\bar{x}$ with the entry 0. Such a pair $x, \bar{x}$ are additive inverses of each other with respect to $+ \pmod{11}$.
Answer:

x	0	1	2	3	4	5	6	7	8	9	10
$\bar{x}$	0	10	9	8	7	6	5	4	3	2	1

4. Prove that $(\mathbb{Z}_{11}, + \pmod{11})$ is a group.
Hint: Show that all four properties (closure, associativity, identity and inverse) hold.
Note: This proof is for advanced learning only. You may skip this question.
Answer:

- Let $x, y \in \mathbb{Z}_{11}$ be arbitrary (any two elements from the set $\mathbb{Z}_{11}$) and let $z = x + y$. Then, using the division theorem, we can uniquely write $z = 11q + r$, such that $0 \leq r < 11$. Hence, $z \pmod{11} \in \mathbb{Z}_{11}$. Hence, the closure property holds.
- From the addition table, we see that for arbitrary $x, y, z \in \mathbb{Z}_{11}$, we have $(x+y)+z = x + (y + z) \pmod{11} \in \mathbb{Z}_{11}$. Hence, associativity holds. (A proof for a general $\mathbb{Z}_N$ will be routine, but much longer.)
- Let $x \in \mathbb{Z}_{11}$ be arbitrary. Then, $x+0 = x \pmod{11}$. Hence, 0 is the identity element.
- Let $x \in \mathbb{Z}_{11}$ be arbitrary. Then, $\bar{x} = 11 - x \in \mathbb{Z}_{11}$, and $x + \bar{x} \pmod{11} = 0$. Hence, $\bar{x}$ is the inverse of x.

5. Find all numbers $1 \leq x \leq 20$ that are mutually prime to 20. We will denote this set of numbers as $\mathbb{Z}^{\star}_{20}$.
Answer: The following table shows the values of $\gcd(20, x)$ for all $x \in \{1, 2, \ldots, 19, 20\}$.

x	1	2	3	4	5	6	7	8	9	10
$\gcd(20, x)$	1	2	1	4	5	2	1	4	1	2
x	11	12	13	14	15	16	17	18	19	20
$\gcd(20, x)$	1	4	1	2	5	4	1	2	1	20

Hence, the set of numbers mutually prime to 20 is

$$\mathbb{Z}^{\star}_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

6. Find all numbers $1 \leq x \leq 11$ that are mutually prime to 11. We will denote this set of numbers as $\mathbb{Z}^{\star}_{11}$.
Answer: The following table shows the values of $\gcd(11, x)$ for all $x \in \{1, 2, \ldots, 10, 11\}$.

x	1	2	3	4	5	6	7	8	9	10	11
$\gcd(11, x)$	1	1	1	1	1	1	1	1	1	1	11

Hence, the set of numbers mutually prime to 11 is

$$\mathbb{Z}^{\star}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

7. What is the value of $|\mathbb{Z}^{\star}_{11}|$?
Answer:

$$|\mathbb{Z}^{\star}_{11}| = 10.$$

8. What is the value of $\phi(11)$?
Answer:

$$\phi(11) = 11\left(1 - \frac{1}{11}\right) = 11\left(\frac{11-1}{11}\right) = 10.$$

9. What is the relationship between $\phi(11)$ and $\mathbb{Z}_{11}^\star$?
Answer:
The number of elements in the set $\mathbb{Z}_{11}^\star$ is $\phi(11)$. In other words,

$$\phi(11) = |\mathbb{Z}_{11}^\star| = 10.$$

10. Consider the set $\mathbb{Z}_{11}^\star = \{1, 2, \dots, 10\}$ of all $1 \leq x \leq 11$ that are mutually prime to 11 and the operation $\cdot \pmod{11}$ on its elements. Create a table for all operations $x \cdot y \pmod{11}$ where $x, y \in \mathbb{Z}_{11}^\star$. We will call it the "multiplication table of $\mathbb{Z}_{11}^\star$".
Answer:

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

11. From the table in question 10, find the element $\bar{x}$ for each $x \in \mathbb{Z}_{11}^\star$ such that

$$x \cdot \bar{x} = 1 \pmod{11}.$$

Hint: In the row corresponding to the number x, find the column $\bar{x}$ with the entry 1. Such a pair $x, \bar{x}$ are multiplicative inverses of each other with respect to $\cdot \pmod{11}$.
Answer:

x	1	2	3	4	5	6	7	8	9	10
$\bar{x}$	1	6	4	3	9	2	8	7	5	10

12. Prove that $(\mathbb{Z}_{11}^\star, \cdot \pmod{11})$ is a group.
Hint: Show that all four properties (closure, associativity, identity and inverse) hold.
Note: This proof is for advanced learning only. You may skip this question.
Answer:
Similar to the previous proof.

13. What is the value of 3^{10} where $3 \in \mathbb{Z}_{11}^\star$?
In other words, find the value of $3^{10} = \underbrace{3 \times 3 \times \cdots \times 3}_{\text{10 times}} \pmod{11}$.
Answer:
You may find the value of $3^{10} = \underbrace{3 \times 3 \times \cdots \times 3}_{\text{10 times}} \pmod{11}$ by doing the multiplications.

However, there is a mathematical result that we can use in this situation when the exponent is $\phi(N)$.

By Lagrange's Theorem, when any element of a group is operated with itself as many times as the order of the group (number of elements in the group), we get the identity element. We note that $(\mathbb{Z}_{11}^{\star}, \cdot \pmod{11})$ forms a group of order $|\mathbb{Z}_{11}^{\star}| = 10$. We use Lagrange's Theorem on the element 3 of the group. Since $3 \in \mathbb{Z}_{11}^{\star}$, and $|\mathbb{Z}_{11}^{\star}| = 10$, hence we have

$$3^{10} = 1.$$

14. For any $x \in \mathbb{Z}_{11}^{\star}$, let us define $x^{10} = \underbrace{x \times x \times \cdots \times x}_{\text{10 times}} \pmod{11}$. Find the values of x^{10} for all $x \in \mathbb{Z}_{11}^{\star}$.

Answer:

By Lagrange's Theorem, when any element of a group is operated with itself as many times as the order of the group, we get the identity element. Since $(\mathbb{Z}_{11}^{\star}, \cdot \pmod{11})$ forms a group of order $|\mathbb{Z}_{11}^{\star}| = 10$, then for an arbitrary $x \in \mathbb{Z}_{11}^{\star}$, we have

$$x^{10} = 1.$$