2.8 Arithmetic mod n

For any integer $n \geq 2$, we introduce the set

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

For example, $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. The elements of $\mathbb{Z}_n$ can be added, subtracted and multiplied according to the following rule (we say that the arithmetic operations are performed mod n):

> Perform the operation (addition, subtraction or multiplication) in the usual way to get some number M, and then replace M by the unique element of $\mathbb{Z}_n$ that is congruent to M mod n.

The set $\mathbb{Z}_n$ is an example of an algebraic structure called a *ring*.

Example 36. In the ring $\mathbb{Z}_6$, the following is true:

$$\begin{aligned} 2+3 &= 5 \\ 3+4 &= 1 \\ 5+5 &= 4 \\ 3-4 &= 5 \\ 0-4 &= 2 \\ 5-1 &= 4 \\ 4 \cdot 2 &= 2 \\ 2 \cdot 3 &= 0 \\ 3 \cdot 3 &= 3 \\ 5 \cdot 5 &= 1 \end{aligned}$$

Example 37. In the ring $\mathbb{Z}_{13}$, the following is true:

$$\begin{aligned} 8+7 &= 2 \\ 1+12 &= 0 \\ 4-6 &= 11 \\ 1-12 &= 2 \\ 5 \cdot 8 &= 1 \\ 4 \cdot 2 &= 8 \\ 2 \cdot 11 &= 9 \end{aligned}$$

For any integer $n \geq 2$, we also introduce the set

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid k \text{ is coprime to } n\}$$

Examples:

$$\begin{aligned}
\mathbb{Z}_4^* &= \{1,3\} \\
\mathbb{Z}_6^* &= \{1,5\} \\
\mathbb{Z}_{11}^* &= \{1,2,3,4,5,6,7,8,9,10\} \\
\mathbb{Z}_8^* &= \{1,3,5,7\} \\
\mathbb{Z}_9^* &= \{1,2,4,5,7,8\}
\end{aligned}$$

Note that the number of elements in $\mathbb{Z}_n^*$ is equal to $\varphi(n)$. The elements of $\mathbb{Z}_n^*$ can be multiplied, by the same rule as above. However, if you try to add or subtract, it will not work, because you sometimes will get a result that is not in $\mathbb{Z}_n^*$. For example, $2+4$ doesn't make sense in $\mathbb{Z}_9^*$. The set $\mathbb{Z}_n^*$ is an example of a *group*.

Example 38. In the group $\mathbb{Z}_9^*$, the following is true:

$$\begin{aligned}
5 \cdot 2 &= 1 \\
4 \cdot 8 &= 5 \\
2 \cdot 2 &= 4
\end{aligned}$$

Example 39. In the group $\mathbb{Z}_8^*$, the following is true:

$$\begin{aligned}
1 \cdot 5 &= 5 \\
3 \cdot 3 &= 1 \\
5 \cdot 5 &= 1 \\
7 \cdot 7 &= 1 \\
5 \cdot 7 &= 3
\end{aligned}$$

We make the following definition:

Definition 17. Let x be an element of the group $\mathbb{Z}_n^*$. We define the *order* of x to be the smallest positive integer k with the property that $x^k = 1$.

Example 40. We compute the order of 2 in the group $\mathbb{Z}_9^*$.

$$\begin{aligned}
2^2 &= 4 \\
2^3 &= 8 \\
2^4 &= 7 \\
2^5 &= 5 \\
2^6 &= 1
\end{aligned}$$

so the order of 2 is 6.

Example 41. We compute the order of 4 in the group $\mathbb{Z}_5^*$.

$$4^2 = 1$$

so the order of 4 is 2.

Example 42. In any group $\mathbb{Z}_n^*$, the order of 1 is 1.

Example 43. From the calculations in Example 39 above, we see that every element in $\mathbb{Z}_8^*$ (except the element 1) has order 2.

In the ring $\mathbb{Z}_n$ we can solve equations, just as we usually do with ordinary numbers. The general way of solving any such equation is to check *all* possible values of x, to see which ones satisfy the equation.

Example 44. Solve the equation

$$x + 6 = 2$$

in the ring $\mathbb{Z}_8$.
Solution: $x = 4$. This can be seen either by adding 2 to both sides of the equation, or by trying all possible values of x (that is 0, 1, 2, 3, 4, 5, 6, 7) to see that 4 is the only solution.

Example 45. Solve the equation

$$3x + 5 = 1$$

in the ring $\mathbb{Z}_5$.
Solution: Try all possible values of x. You will find that the only solution is $x = 2$.

Example 46. Solve the equation

$$x^2 = 1$$

in the ring $\mathbb{Z}_8$.
Solution: Try all possible values of x. You will find that there are four solutions: $x = 1$, $x = 3$, $x = 5$ and $x = 7$.

Example 47. Solve the equation

$$x^2 = 3$$

in the ring $\mathbb{Z}_7$.
Solution: Try all possible values. You will see that there are no solutions.

2.8.1 Exercises

Compute in the ring $\mathbb{Z}_{12}$
E194 $3 \cdot 7$
E195 $3 \cdot 8$
E196 $2 \cdot 7$
E197 $5 \cdot 5$
E198 $10 \cdot 1$
E199 $3 + 11$
E200 $3 - 11$
E201 $0 - 1$
E202 $6 + 7$
Compute in the ring $\mathbb{Z}_5$
E203 $3 \cdot 2$
E204 $4 - 4$
E205 $1 - 4$
E206 $4 \cdot 4$
Solve the following equations in the ring $\mathbb{Z}_9$
E207 $x - 6 = 7$
E208 $8x - 3 = 2$
E209 $x^2 + 3 = 1$
E210 $x^2 = 0$
Solve the following equations in the ring $\mathbb{Z}_5$
E211 $x^2 = 1$
E212 $x - 3 = 2$
E213 $x^2 = 3$
E214 $x^2 + x = 0$
E215 $x^3 = 2$
E216 Compute the order of 5 in the group $\mathbb{Z}_7$.
E217 Compute the order of 2 in the group $\mathbb{Z}_{11}$.
E218 Compute the order of 14 in the group $\mathbb{Z}_{15}$.

2.8.2 Problems

P20 Consider the function

$$\begin{aligned} f : \mathbb{Z}_5 &\to \mathbb{Z}_5 \\ x &\mapsto 4x \end{aligned}$$

Is f injective? Is f surjective? Is f bijective?
P21 Consider the function

$$\begin{aligned} g : \mathbb{Z}_{10} &\to \mathbb{Z}_{10} \\ x &\mapsto 4x \end{aligned}$$

Is g injective? Is g surjective? Is g bijective?