11.5 The Integers Modulo n

Benjamin Basseri

January 10, 2025

Problem 1

Write the addition and multiplication tables for $\mathbb{Z}_2$.

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}, \quad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Problem 2

Write the addition and multiplication tables for $\mathbb{Z}_3$.

$$\begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}, \quad \begin{array}{c|ccc} \times & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$$

Problem 3

Write the addition and multiplication tables for $\mathbb{Z}_4$.

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}, \quad \begin{array}{c|cccc} \times & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}$$

Problem 4

Write the addition and multiplication tables for $\mathbb{Z}_6$.

$$\begin{array}{c|cccccc} + & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 5 & 0 & 1 & 2 & 3 & 4 \end{array}, \quad \begin{array}{c|cccccc} \times & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 2 & 4 & 0 & 2 & 4 \\ 3 & 0 & 3 & 0 & 3 & 0 & 3 \\ 4 & 0 & 4 & 2 & 0 & 4 & 2 \\ 5 & 0 & 5 & 4 & 3 & 2 & 1 \end{array}$$

Problem 5

Suppose $[a], [b] \in \mathbb{Z}_5$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?

Yes because we can see from its multiplication chart that the only products becoming [0] come from factors of [0]. More generally any member of $[5] = 5x$ for some integer x. In the prime factorization of $5x$, the prime 5 has at least a power of 1. And if $5x = a \cdot b$ for some integers a and b, it would require that either a or b have a factor of 5 which would require $[a] = 0$ or $[b] = 0$.

Problem 6

Suppose $[a], [b] \in \mathbb{Z}_6$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$? What if $[a], [b] \in \mathbb{Z}_7$?

No, we saw from its multiplication table that nonzero classes could multiply to [0] such as $[2] \cdot [3] = [0]$. More generally, the prime factorization of any element in [0] looks like $2 \cdot 3 \cdot x$ for some integer x. This means if $2 \cdot 3 \cdot x = a \cdot b$ for some integers a and b, it could be that a provides the factor of 2 and b provides the factor of 3. For example, $a = 2, b = 3, x = 1$.

If we're in $\mathbb{Z}_7$ we might observe that we're in a field which would require that $[a] = [0]$ or $[b] = [0]$. If we don't make that observation again we could argue using prime decomposition. The prime factorization of any number in $[0] = 7n$ for some integer n. If $7n = a \cdot b$ for integers a and b, then either a or b must have a factor of 7, since 7 is prime and cannot be the product of smaller factors. And if a or b has a factor of 7 then it is a multiple of 7 and belongs to [0].

Problem 7

Do the following calculations in $\mathbb{Z}_9$, in each case expressing your answer as $[a]$ with $0 \le a \le 8$.

1. $[8] + [8]$
2. $[24] + [11]$
3. $[21] \cdot [15]$
4. $[8] \cdot [8]$

1. $[8] + [8] = [16] = [7]$
2. $[24] + [11] = [35] = [8]$
3. $[21] \cdot [15] = [3] \cdot [6] = [18] = [0]$
4. $[8] \cdot [8] = [64] = [1]$

Problem 8

Suppose $[a], [b] \in \mathbb{Z}_n$ and $[a] = [a']$ and $[b] = [b']$. Alice adds $[a]$ and $[b]$ as $[a] + [b] = [a + b]$. Bob adds them as $[a'] + [b'] = [a' + b']$. Show that their answers $[a + b]$ and $[a' + b']$ are the same.

Since $a \in [a]$ we can write it as $a = xn + c$ where c is the remainder. Likewise $a' \in [a]$ so $a' = x'n + c$. Also write $b = yn + d, b' = y'n + d$.

Now $a + b = (x + y)n + (c + d)$ so it is in the equivalence class $[c + d]$. Likewise $a' + b' = (x' + y')n + (c + d)$ so it is in the equivalence class $[c + d]$. Therefore Alice and Bob's answers are the same.