Worksheet 9

Problems marked with a ($*$) are "key results".

1. Write down addition and multiplication tables for $\mathbb{Z}/n\mathbb{Z}$ for various values of n, like $n = 4, 5, 6, 7, 8$. What observations do you notice? Are there similarities between these tables? Differences? See what you can come up with!

2. Go through the list of axioms for $\mathbb{Z}$ and decide which ones still make sense in $\mathbb{Z}/n\mathbb{Z}$.

3. The point of this problem is to get a feeling for how the structure of $\mathbb{Z}/n\mathbb{Z}$ is very different than from that of $\mathbb{Z}$.

   (a) Find a value of n and $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $ab = 0$ but $a \neq 0$ and $b \neq 0$.

   (b) Find a value of n such that the equation $x^2 = 1$ has more than two solutions in $\mathbb{Z}/n\mathbb{Z}$.

   (c) Find a value of n and an example of $a \in \mathbb{Z}/n\mathbb{Z}$ such that a has two different factorizations into prime integers in $\mathbb{Z}/n\mathbb{Z}$ of different lengths.

   (d) Do you see any way of fixing the problems that arose in your previous examples?

4. We say that $a \in \mathbb{Z}/n\mathbb{Z}$ is **invertible** if there is $b \in \mathbb{Z}/n\mathbb{Z}$ such that $ab = 1$ in $\mathbb{Z}/n\mathbb{Z}$, or equivalently, that $ab \equiv 1 \bmod n$. When b exists, we write $b = a^{-1}$ in $\mathbb{Z}/n\mathbb{Z}$, or if you prefer congruences, $b \equiv a^{-1} \bmod n$.

   (a) Is 2 invertible in $\mathbb{Z}/7\mathbb{Z}$? Is 3 invertible in $\mathbb{Z}/6\mathbb{Z}$? If so, find the inverse. If not, explain what goes wrong.

   (b) Formulate a conjecture on when $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible – it should read something along the lines of "$a \in \mathbb{Z}/n\mathbb{Z}$ is invertible if and only if ______"