CLASS HOUR - 15/9

1 The function $< \cdot >_n$

Consider the additive group $(\mathbb{Z}/n\mathbb{Z}, +, 0)$[1] and consider an element a.
Define the function $< \cdot >: \mathbb{Z}/n\mathbb{Z} \to \wp(\mathbb{Z}/n\mathbb{Z})$, where $\wp(\mathbb{X})$ is the power set of $\mathbb{X}$.

Algorithm 1 $< a >_n$

Require: $a \in \mathbb{Z}/n\mathbb{Z}$. If not, this is not a valid input.
  $S \leftarrow \{a\}$
  $x \leftarrow (a + a \pmod n)$
  while $x \notin S$ **do**
    $S \leftarrow S \cup \{x\}$
    $x \leftarrow (x + a \pmod n)$
  end while
  return S

It is clear that $< 1 >_n$ regenerates the set $\mathbb{Z}/n\mathbb{Z}$ for all $n \geq 2$.

Exercise:
Given a number $2 \leq n \leq 10$, how many $a \in \mathbb{Z}/n\mathbb{Z}$ satisfy the property
$(< a >_n, +, 0) = (\mathbb{Z}/n\mathbb{Z}, +, 0)$?
Can you find the answer for any $n \geq 2$?

[1] There is an abuse of notation here, the operation $+$ is $a + b \pmod n$ if the associated set is $\mathbb{Z}/n\mathbb{Z}$

2 Assignment

This is not evaluative.

Consider the two additive groups $(\mathbb{Z}/2\mathbb{Z}, +, 0)$ and $(\mathbb{Z}/4\mathbb{Z}, +, 0)$.
Observe $< 1 >_2$ and $< 2 >_4$ are both sets of cardinality 2.
Given the groups $(\mathbb{Z}/8\mathbb{Z}, +, 0)$ and $(\mathbb{Z}/16\mathbb{Z}, +, 0)$. Verify:
$< 1 >_2$, $< 2 >_4$, $< 4 >_8$, and $< 8 >_{16}$ all have the same cardinality - that of 2.

In fact, given any $k > 1$, the set $< 2^{k-1} >_{2^k}$ in $\mathbb{Z}/2^k\mathbb{Z}$ has the cardinality of 2.

This sort of identification establishes that $\mathbb{Z}/2\mathbb{Z}$ can be identified as a subset[2] of $\mathbb{Z}/2^k\mathbb{Z}$ for all $k > 1$[3].
The `descent.gif` animation explores this identification pictorially.

Exercise:
Can you show that $\mathbb{Z}/4\mathbb{Z}$ can be identified in $\mathbb{Z}/2^k\mathbb{Z}$ for all $k > 2$?
You can use the code in `descent.txt` on SAGE's online platform to visualize this pictorially.

Do all the subgroups of $\mathbb{Z}/2^n\mathbb{Z}$ look like $\mathbb{Z}/2^k\mathbb{Z}$ for some $0 \leq k \leq n$?
Or are there subgroups that have been missed out?

[2] In fact it's a subgroup!
[3] Henceforth $\mathbb{Z}/2^n\mathbb{Z}$ will be used for the tuple $(\mathbb{Z}/2^n\mathbb{Z}, +, 0)$