CS 173: Discrete Mathematical Structures, Spring 2009
Honors Homework 1

Due by 4pm on Wednesday, March 18th. Please give to Margaret or push it under the door of her office (3214 Siebel).

1 The integers mod k

Given a positive integer k,[1] we can define the set of integers mod k to be $\mathbb{Z}_k = \{0, 1, \ldots, k-1\}$. [2] For example, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

If x and y are elements of $\mathbb{Z}_k$, we define their sum and product in $\mathbb{Z}_k$ to be

$$x +_k y = (x + y) \bmod k$$
$$x \times_k y = (x \times y) \bmod k$$

That is, to add or multiply numbers in $\mathbb{Z}_k$, you combine them using normal addition or multiplication, then remove all factors of k from the result. For example, here's the addition and multiplication tables for $\mathbb{Z}_4$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	3

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2 More properties of operations

Suppose we have a binary operation $\star$ on a set A. An element $e \in A$ is an *identity for* $\star$ if

$$\forall x \in A, x \star e = x \text{ and } e \star x = x$$

[1] Though in practice k is always at least 2 because you get something pretty limited if $k = 1$.

[2] There's a classier way to define $\mathbb{Z}_k$ using equivalence classes, which you might run into if you look things up on wikipedia. However, we don't yet have enough background to do things that way right now.

Looking at the tables above should convince you that 0 is an identity for addition and 1 is an identity for multiplication in $\mathbb{Z}_k$ (for any choice of k) just as they are for addition and multiplication in the normal integers.

Suppose that our operation $\star$ on A has identity $\mathbf{e}$. Suppose that t is an element of A. Then an element d in A is a *(two-sided) inverse* for t if

$$d \star t = t \star d = \mathbf{e}$$

Not every element has an inverse. For example, in the normal integers, 0 has no inverse under the multiplication operation.

3 Problems

The first two problems are not too hard. The third problem is a bit tricky. It may help to work on it for a bit, put it aside to rest, and have another go later.

1. For any k, show that all elements of $\mathbb{Z}_k$ have inverses for the addition operation.
2. Under multiplication, elements of $\mathbb{Z}_k$ don't always have inverses.
   (a) Write out the multiplication table for $\mathbb{Z}_7$. Zero obviously doesn't have an inverse. Find the inverses for all the other elements of $\mathbb{Z}_7$.
   (b) Find a non-zero element of $\mathbb{Z}_4$ that doesn't have a multiplicative inverse.
3. Given k, there's a simple way to tell whether all non-zero elements of $\mathbb{Z}_k$ have multiplicative inverses.
   (a) What property does k need to have, in order for all non-zero elements of $\mathbb{Z}_k$ to have multiplicative inverses? Explain informally why your answer is right.
   To figure this out, it may help to write out multiplication tables for some sample values of k. I recommend starting with 5 and 6.
   (b) Prove that your answer is correct, using the following theorem (a special case of theorem 1 on p. 232 of Rosen).
   Theorem: If a and b are positive integers with $\text{GCD}(a, b) = 1$, then there are integers s and t such that $1 = sa + tb$.