Algebra 411.1

Homework 3

Due Thursday October 6, in class.

All answers should be justified!

♡

[Congruence modulo N.] Let N be an integer. We say that N divides n (symbolically $N|n$) if there is an integer q such that $n = Nq$. We say that integers m, n are *congruent modulo* N (symbolically $m\overset{N}{\equiv}n$) if N divides the difference $n - m$.

1. (a) Show that the congruence modulo N is an equivalence relation, i.e.,

(1) [*Relation is reflexive.*] For each $n \in \mathbb{N}$ we have $n\overset{N}{\equiv}n$.
(2) [*Relation is symmetric.*] If $m\overset{N}{\equiv}n$. then $n\overset{N}{\equiv}m$.
(3) [*Relation is transitive.*] If $m\overset{N}{\equiv}n$ and $n\overset{N}{\equiv}p$. then $m\overset{N}{\equiv}p$.

From now on assume that $N > 0$.

(b) Show that any integer n is congruent modulo N to its remainder modulo $N : n\overset{N}{\equiv}R_N(n)$.

(c) Prove that $m\overset{N}{\equiv}n$ iff $R_N(m) = R_N(n)$.

(d) Show that for each $n \in \mathbb{Z}$ the remainder $R_N(n)$ is the unique number r in the set $\mathbb{Z}_N = \{0, 1, ..., N-1\}$ such that $r\overset{N}{\equiv}n$.

♡

2. Let N be a positive integer. (a) Show that for $a, b \in \mathbb{Z}_N$

(1) $a +_N b$ is the unique integer that both: (i) lies in $\mathbb{Z}_N$ and i(ii) is congruent modulo N to $a + b$.
(2) $a \cdot_N b$ is the unique integer that both: (i) lies in $\mathbb{Z}_N$ and (ii) is congruent modulo N to ab.

(b) Show that congruences modulo N can be added and multiplied. In other words if $m\overset{N}{\equiv}m'$ and $n\overset{N}{\equiv}n'$ then $m + n\overset{N}{\equiv}m' + n'$ and $mn\overset{N}{\equiv}m'n'$

(c) For $a, b \in \mathbb{Z}_N$, $a\overset{N}{\equiv}b$ is equivalent to $a = b$.

3. Show that for any positive integer N :

(a) $(\mathbb{Z}_N, +_N)$ and $(\mathbb{Z}_N, \cdot_N)$ are both monoids and both operations are commutative.

(b) Show that $(\mathbb{Z}_N, +_N)$ is a group.

(c) Show that $(\mathbb{Z}_N^*, \cdot_N)$ is a group (here, $\mathbb{Z}_N^*$ denotes the invertible elements in the monoid $(\mathbb{Z}_N, \cdot_N)$).

[*Hint.*] The definition $a +_N b \stackrel{\text{def}}{=} R_N(a+b)$ is good for calculating examples. However, from this point if you calculate what the associativity of addition claim $(a +_N b) +_N c = a +_N (b +_N c)$ means, you will get the equation $R_N(R_N(a+b)+c) = R_N(a + R_N(b+c))$.

This is true but may be confusing to check directly. You should rather use the description of $a +_N b$ from problem 2. By problem 2c, you need to explain why: (i) both $(a +_N b) +_N c$ and $a +_N (b +_N c)$ are in $\mathbb{Z}_N$ and that (ii) $(a +_N b) +_N c$ and $a +_N (b +_N c)$ are congruent modulo N. [*Hint.*[2]] It is not difficult to check (using problems 1 and 2) that both of these numbers are congruent modulo N to $a+b+c$!

[*Notation.*] Group $(\mathbb{Z}_N^*, \cdot)$ is sometimes denoted $U(N)$.

4. (a) Find the orders of groups $U(3)$, $U(9)$, $U(27)$.

(b) Guess the order of $U(3^n)$ for any n.

(c) Can you guess which elements r of $\mathbb{Z}_N$ are in $\mathbb{Z}_N^*$?

♡

5. In S_{10} consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 4 & 7 & 6 & 5 & 2 & 8 & 10 & 1 & 3 \end{pmatrix}.$$

(a) Calculate σ in the cycle notation.

(b) Calculate the powers of σ and its order using the cycle notation.

(c) Make a guess of how the order of any permutation is related to the lengths of cycles in this permutation.

♡

0. Reread sections 4 and 5 in the book.