Algebra 411.2

Homework 2

Due Thursday September 29, in class.

All answers should be justified!

♡

[Division of integers.] Let n be a positive integer. By *dividing an integer* N *by* n we man finding two integers q and r such that

- qn is the largest multiple of n which is still $\leq N$;
- $r = \ N - qn$ is the difference between N and this closest multiple of n which is not $> N$.

Then q is called the *quotient* for the of the division of N by n. Also, r is called the *reminder of* N *modulo* n, so we denote the reminder r by $R_n(N)$.

For instance if we are dividing $N = 17$ by $n = 7$ then $q = 2$ and $r = 3$ since we have $2{\cdot}7 \leq 17 < 3{\cdot}7$ and also $17 - 2{\cdot}7 = 3$. So, $R_7(17) = 3$.

1. [**Euclidean division.**] (a) Explain why for the division of N by n one has

(1) $N = qn + r$.
(2) $0 \leq r < n$.

(b) Find q and r when

(1) $N = 351$ and $n = 11$,
(2) $N = -21$ and $n = 11$,
(3) $N = -351$ and $n = 11$,

♡

[Addition and multiplication modulo n.] For a positive integer n, denote by $\mathbb{Z}_n$ the set of integers $\{0, 1, 2, 3, ..., n-1\}$. We will define on $\mathbb{Z}_n$ the operation $+_n$ of *addition modulo* n and the operation $\cdot_n$ of *multiplication modulo* n by

- For $a, b \in \mathbb{Z}_n$ let $a +_n b \stackrel{\text{def}}{=}$ the remainder of dividing $a + b$ with n.
- For $a, b \in \mathbb{Z}_n$ let $a \underset{n}{\cdot} b \stackrel{\text{def}}{=}$ the remainder of dividing $a{\cdot}b$ with n.

[Group $\mathbb{Z}_n$.] We will show in class that $(\mathbb{Z}_n, +_n)$ is a group with neutral element 0. When we say "group $\mathbb{Z}_n$" we mean the group $(\mathbb{Z}_n, +_n)$.

2. (a) Write the tables for operations $+_5$ and $\cdot 5$ on $\mathbb{Z}_5$.

(b) Write the tables for operations $+_9$ and $\cdot_9$ on $\mathbb{Z}_9$.

♡

[Powers ef elements of a group.] For an element g of a group $(G, \circ)$ we define the non-negative powers of g by: zero$^{\text{th}}$ power of g is e, the 1^{st} power of g is g and for $n > 1$ the n^{th} power of g is $g \circ g \circ \cdots \circ g$ (the product of n copies of g).

3. In the group S_5 find all nonnegative powers of the permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{smallmatrix}\right)$.

4. (a) Assume that $(\mathbb{Z}_n, +_n)$ is a group with neutral element 0. Find inverses of

(1) 3 in $(\mathbb{Z}_{11}, +_{11})$,
(2) 12 in $(\mathbb{Z}_{25}, +_{25})$,
(3) 16 in $(\mathbb{Z}_{32}, +_{32})$,

(b) Find all nonnegative powers of

(1) element 3 in $(\mathbb{Z}_{15}, +_{15})$.
(2) element 4 in $(\mathbb{Z}_{15}, +_{15})$.
(3) element 5 in $(\mathbb{Z}_{15}, +_{15})$.

5. We will show in class that the subset $\mathbb{Z}_{15}^* \stackrel{\text{def}}{=} \{1, 2, 4, 7, 8, 11, 13, 14\}$ of $\mathbb{Z}_{15}$ is a group for the operation $\cdot_{15}$ and the neutral element (unit) is 1. Find inverses of all elements.

♡

0. Read sections 4 and 5 in the book.