Math 330 Section 4 - Fall 2021 - Homework 09

Published: Thursday, October 7, 2021 *Running total:* 39 *points*
Last submission: Friday, October 22, 2021

Status - previously assigned reading Assignments:

B/G (Beck/Geoghegan) Textbook:
ch.1-7 (until Theorem 7.17)

MF lecture notes:
ch.2-3, ch.4 (skim), ch.5-6

B/K lecture notes:
ch.1.1 (Introduction to sets) (optional)
ch.1.2 (Introduction to Functions) but skip ch.1.2.4: Floor and Ceiling Functions (optional)

New reading assignments:

Reading assignment 1 - due: Monday, October 4:

- Read carefully MF ch.7.1–7.3. Chapter 7.1 is particularly important!

Reading assignment 2 - due: Wednesday, October 6:

a. Read carefully the remainder of MF ch.7.
b. Read carefully MF ch.8.1. Be sure you understand the connection between arbitrary intersections and the $\forall$ quantifier and the connection between arbitrary unions and the $\exists$ quantifier.

Reading assignment 3 - due Friday, October 8:

a. Read carefully MF ch.8.3
b. Read carefully MF ch.8.4 until before Proposition 8.11 and skim the remainder of this chapter.

Written assignments are on the next page.

Written assignments:

Written assignment 1: Prove Lemma 6.5: Let p be prime and let $n \in \mathbb{N}$. Then

(a) Either $\gcd(p, n) = 1$ or $\gcd(p, n) = p$.
(b) If $p \nmid n$ (p does not divide n) then $\gcd(p, n) = 1$.

One point each for (a) and (b).

#2 and #3 are about proving MF thm.6.8 (Division Algorithm for Integers – same as B/G thm.6.13): Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. There exists a unique combination of two integers q ("quotient") and r ("remainder") such that

$$m = n \cdot q + r \quad \text{and } 0 \leq r < n.$$

Do not use induction for assignments 2 and 3. It would only make your task more difficult!

Written assignment 2:

Prove uniqueness of the "decomposition" $m = qn + r$ such tbat $0 \leq r < n$: If you have a second such decomposition $m = \tilde{q}n + \tilde{r}$ then show that this implies $q = \tilde{q}$ and $r = \tilde{r}$. Start by assuming that $r \neq \tilde{r}$ which means that one of them is smaller than the other and take it from there.

Written assignment 3:

Much harder than #2: Prove the existence of q and r.

Hints for #3: Review the Extended Well–Ordering principle MF thm.6.7. Its use will give the easiest way to prove this assignment: Show that $A \neq \emptyset$. That probably is the hardest part of the proof! Now you can apply thm.6.7 to the set

$$A := A(m, n) := \{r' \in [0, \infty[_{\mathbb{Z}} : r' = m - q'n \text{ for some } q' \in \mathbb{Z}\}.$$

What can you do with $\min(A)$?

Hint for both #2 and #3: MF prop. 3.61 and cor.3.5 at the end of ch.3.5 will come in handy in connection with using or proving $0 \leqq r < n$. They assert for the ordered integral domain $(\mathbb{Z}, +, \cdot, \mathbb{N})$ the following.

If $a, b \in [0, n[_{\mathbb{Z}}$ then

$$|a - b| \leqq \max(a, b), \text{ i.e.,} \tag{3.45}$$
$$-\max(a, b) \leqq a - b \leqq \max(a, b), \tag{3.46}$$
$$-n < a - b < n. \tag{3.47}$$