

# Homework 1 (due Oct. 2)

MATH 110 | Introduction to Number Theory | Fall 2022

Whenever you use a result or claim a statement, provide a **justification** or a **proof**, unless it has been covered in the class. In the later case, provide a **citation** (such as “by the *2-out-of-3* property of *division*” or “by Coro. 0.31 in the textbook”).

You are encouraged to *discuss* the problems with your peers. However, you must write the homework **by yourself** using your words and **acknowledge your collaborators**.

**Problem 1.** This problem is a 3-variables analogy of the material covered in class.

- (a) (5pts) Prove that there exists no integer solution  $(x, y, z)$  to the equation

$$18x - 27y + 39z = 4.$$

- (b) (5pts) Find **an** integer solution  $(x, y, z)$  to the equation  $18x - 27y + 39z = 6$ .  
(\*c). (optional, with extra credit up to 5pts) Find **all** the integer solutions  $(x, y, z)$  to the equation  $18x - 27y + 39z = 6$ . Your answer should give explicit formulae for  $x, y, z$  in terms of two free independent integer parameters  $m$  and  $n$ .

*Remark.* Can you work out a general algorithm?

**Problem 2.** Let  $a, b, c$  be three integers, and let  $g = \text{GCD}(a, \text{GCD}(b, c))$ .

- (a) (8pts) Prove that  $g$  satisfies the following properties:  
(i)  $g$  is a common divisor of  $a, b$  and  $c$ , in other words, we have  $g \mid a, g \mid b$  and  $g \mid c$ .  
(ii) If  $d$  is any common divisor of  $a, b$  and  $c$ , then  $d \mid g$ .  
(b) (2pts) Prove that  $g$  is the unique natural number satisfying both (i) and (ii).

*Optional* (with extra credit up to 2pts). During your proof, try to only use the following facts: 1, the *definition* of  $\text{GCD}(\cdot, \cdot)$ , 2, the *transitive* property of  $\cdot \mid \cdot$ , and 3, the *reflexive* property of  $\cdot \mid \cdot$ .

*Hint.* Compare this problem with the fact that  $\max\{a, b, c\} = \max\{a, \max\{b, c\}\}$ .

The properties (i) and (ii) together are called the *defining property* or the *universal property* of the notion of the *greatest common divisor* of  $a, b$  and  $c$ . Notation:  $\text{GCD}(a, b, c)$ .

Then [problem 2.\(a\)](#) says that  $\text{GCD}(a, \text{GCD}(b, c))$  gives an implementation of  $\text{GCD}(a, b, c)$ .

**Problem 3.** Let  $a_1, \dots, a_n$  be  $n$  integers.

- (a) (2pts) Mimicking [problem 2](#), give the *defining properties* of the notion of the *greatest common divisor* of  $a_1, \dots, a_n$ . Then give an implementation of such a notion in terms of  $\text{GCD}(\cdot, \cdot)$ .

We will use the notation  $\text{GCD}(a_1, \dots, a_n)$  or  $\text{GCD}_{1 \leq i \leq n} a_i$  to denote this notion.

- (b) (2pts) Give the *defining properties* of the notion of the *least common multiple* of  $a_1, \dots, a_n$ . Then give an implementation of such a notion in terms of  $\text{LCM}(\cdot, \cdot)$ . We will use the notation  $\text{LCM}(a_1, \dots, a_n)$  or  $\text{LCM}_{1 \leq i \leq n} a_i$  to denote this notion.

- (c) (6pts) Mimicking the proof of the attached proposition, show that:

For any matrix  $(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$  of integers, we have

$$\text{GCD}_{1 \leq i \leq n} \text{LCM}_{1 \leq j \leq m} a_{ij} \mid \text{LCM}_{1 \leq j \leq m} \text{GCD}_{1 \leq i \leq n} a_{ij}.$$

*Hint.* What facts are used in the proof?

**Proposition.** Let  $(x_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$  be a matrix of real numbers, then we have

$$\max_{1 \leq i \leq n} \min_{1 \leq j \leq m} x_{ij} \leq \min_{1 \leq j \leq m} \max_{1 \leq i \leq n} x_{ij}.$$

*Proof.* Define  $f(i)$  ( $1 \leq i \leq n$ ) to be  $\min_{1 \leq j \leq m} x_{ij}$ . Then we have

$$f(i) \leq x_{ij} \quad \text{for all } 1 \leq i \leq n, 1 \leq j \leq m.$$

Therefore, we have

$$\max_{1 \leq i \leq n} f(i) \leq \max_{1 \leq i \leq n} x_{ij} \quad \text{for all } 1 \leq j \leq m.$$

In particular, we have

$$\max_{1 \leq i \leq n} f(i) \leq \min_{1 \leq j \leq m} \max_{1 \leq i \leq n} x_{ij}$$

as desired. □