Homework 1 (due Jan. 22)

MATH 110 | Introduction to Number Theory | Winter 2023

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* principle" 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-varibales analogy of the material covered in lectures.

(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 $g = \gcd(a, \gcd(b, c))$.

(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 $\gcd(\,\cdot\,,\,\cdot\,)$, 2, the *transitivity* $\cdot \mid \cdot$, and 3, the *reflexivity* 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* of the notion of the *greatest common divisor of a, b and c.*

We will use $\gcd(a, b, c)$ to denote the greatest common divisor of a, b and c. Then problem 2.(a) says that $\gcd(a, \gcd(b, c))$ gives an *implementation* of $\gcd(a, b, c)$. Namely, it gives a way to compute the $\gcd(a, b, c)$ from the given integers a, b, c: first compute $\gcd(b, c)$, and then plug it in $\gcd(a, \gcd(b, c))$, the final result would be the answer.

Problem 3 (5 pts)**.** Treat $\gcd(\cdot\,,\,\cdot)$ as a binary operation on $\mathbb{Z}$. Show that it is *associative*:

$$\forall a, b, c \in \mathbb{Z}\colon\ \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c).$$

Remark. By symmetry, the same results as in problems 2 and 3 holds for $\operatorname{lcm}(\cdot\,,\,\cdot)$.

Problem 4. Let $a_1, \cdots, a_n$ be n integers.

(a) (2pts) Mimicking problem 2, give the *defining properties* of the notion of the *greatest common divisor of* $a_1, \cdots, a_n$. (In other words, give a reasonable *definition* of this notion involving two properties mimicking (i) and (ii))
Then give an *implementation* of such a notion in terms of $\gcd(\cdot\,,\,\cdot)$. (In other words, give a way to compute the greatest common divisor of $a_1, \cdots, a_n$ using only the two variable version $\gcd(\cdot\,,\,\cdot)$.)

Remark. We will use the notation $\gcd(a_1, \cdots, a_n)$ or $\gcd\limits_{1\leqslant i\leqslant n} a_i$ to denote this notion.

(b) (2pts) Give the *defining properties* of the notion of the *least common multiple of* $a_1, \cdots, a_n$. Then give an *implementation* of such a notion in terms of $\operatorname{lcm}(\cdot\,,\,\cdot)$.

Remark. We will use the notation $\operatorname{lcm}(a_1, \cdots, a_n)$ or $\operatorname*{lcm}\limits_{1\leqslant i\leqslant n} a_i$ to denote this notion.

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

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

$$\operatorname*{lcm}_{1\leqslant i\leqslant n} \gcd_{1\leqslant j\leqslant m} a_{ij} \mid \gcd_{1\leqslant j\leqslant m} \operatorname*{lcm}_{1\leqslant i\leqslant n} a_{ij}.$$

Hint. What facts are used in the proof?

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

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

Proof. Define $f(i)$ $(1 \leqslant i \leqslant n)$ to be $\min\limits_{1\leqslant j\leqslant m} x_{ij}$. Then we have

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

Therefore, we have

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

In particular, we have

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

as desired. ∎