Homework 4 Solutions

Problem 1. Which pairs $(a, b) \in \mathbb{Z}_+ \times \mathbb{Z}_+$ have $\gcd(a, b) = 18$ and $\operatorname{lcm}(a, b) = 540$?

Solution 1. We have the prime power decompositions $540 = 2^2 \cdot 3^3 \cdot 5^1$ and $18 = 2^1 \cdot 3^2 \cdot 5^0$. Clearly a and b are of the form $a = 2^i 3^j 5^k$ and $b = 2^I 3^J 5^K$, for some integers $i, j, k, I, J, K \geq 0$. Then $\max\{i, I\} = 2$ and $\min\{i, I\} = 1$, so $i \in \{1, 2\}$, and similarly $j \in \{2, 3\}$ and $k \in \{0, 1\}$. This gives 8 possible triples (i, j, k) corresponding to the values

$$a \in \{18, 36, 54, 90, 108, 180, 270, 540\},$$

with $b = \frac{540 \cdot 18}{a}$ in every case.

Problem 2. Show that there are no integer solutions to $x^2 + y^2 = 1000003$.

Solution 2. Assume that $(x, y) \in \mathbb{Z}^2$ is a solution. Since

$$x^2 \bmod 4, y^2 \bmod 4 \in \{[0]^2, [1]^2, [2]^2, [3]^2\} = \{[0], [1], [0], [1]\} = \{[0], [1]\}$$

we have

$$x^2 + y^2 \bmod 4 \in \{[0], [1], [2]\}.$$

But $1000003 \bmod 4 = [3]$, a contradiction. So there are no solutions.

Problem 3. Find all integer solutions (x, y, z) to the equation

$$2x + 3y + 4z = 5.$$

Which ones have $x, y, z \geq 0$?

Solution 3. We view one of the variables, say z, as a parameter, and solve for x and y. Since $(2, 3) = 1$ the equation

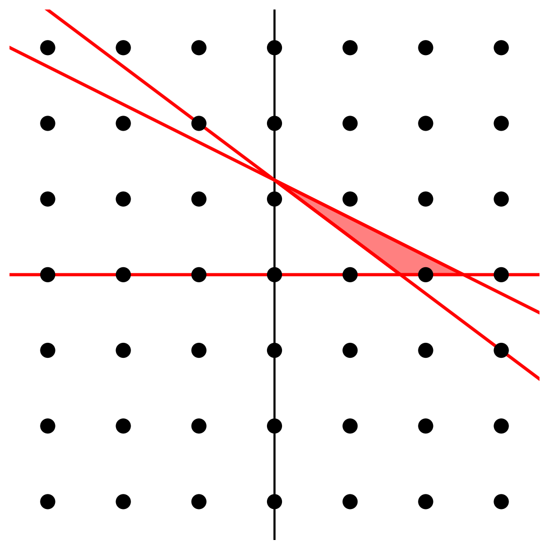
$$2x + 3y = 5 - 4z$$

has solutions (x, y) for every $z \in \mathbb{Z}$. To find one of them, we use that $3 - 2 = 1$, so $3(5 - 4z) + 2(4z - 5) = 5 - 4z$. Hence $(x, y) = (4z - 5, 5 - 4z)$ is a solution. All other solutions are of them form $(x, y) = (4z - 5 + 3k, 5 - 4z - 2k)$.

So the solutions (x, y, z) of the original equation are exactly the triples $(4n-5+3k, 5-4n-2k, n)$, for all integers $n, k \in \mathbb{Z}$. The nonnegative solutions are those with

$$n \geq 0, \quad 4n-5+3k \geq 0, \quad 5-4n-2k \geq 0.$$

We can show with elementary algebra that the only integer solution to this system of inequalities is $(k, n) = (2, 0)$, which corresponds to the solution $(x, y, z) = (1, 1, 0)$. We can also see this graphically: in the figure below, the x–axis represents k and the y–axis represents n. The black dots are the points where k, n are integers, and the three lines are defined by $n = 0$, $4n-5+3k = 0$ and $5-4n-2k = 0$. The red triangle (including its boundary) indicates all solutions of the system of inequalities. It contains a single integral point $(2, 0)$.



Problem 4. To understand the multiplication operation on $\mathbb{Z}/m\mathbb{Z}$ better, it can be helpful to compile a multiplication table, that is to list the product $x \cdot y$ for all pairs $x, y \in \mathbb{Z}/m\mathbb{Z}$. To do this, we should fix a single representative for every congruence class, for example by using the least non–negative representatives. For example, the multiplication table for $\mathbb{Z}/3\mathbb{Z}$ would look like this (for example $[2]_3 \cdot [2]_3 = [4]_3 = [1]_3$):

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Create a multiplication table for $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$. Do you see interesting patterns?

Solution 4.

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The tables are symmetric, reflecting the commutativity of multiplication. In $\mathbb{Z}/5\mathbb{Z}$ there are no 0 entries except in the first row and column, indicating that $\mathbb{Z}/5\mathbb{Z}$ is an integral domain, while $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ are not. Every non-zero row or column of the $\mathbb{Z}/5\mathbb{Z}$ contains all numbers (since $\mathbb{Z}/5\mathbb{Z}$ is a field). These are just some examples, there are lots of other patterns.

Problem 5. Let $m \in \mathbb{Z}_+$ be composite. Show that $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain.

Solution 5. Let $m = nk$ with $1 < n, k < m$, and set $x = [n]_m$ and $y = [k]_m$. Then $x, y \neq [0]_m$, but

$$x \cdot y = [n]_m \cdot [k]_m = [nk]_m = [m]_m = [0]_m.$$

Problem 6. Compute the following expressions. Give the answer as a least non–negative residue. You can (and should!) do this without a calculator, and write down intermediate steps.

a) $2^6 \bmod 11$

b) $2^{12} \bmod 11$

c) $5^{1030} \bmod 3$

d) $78^3 \bmod 3$

e) $(1! + 2! + \cdots + 10!) \mod 5$

f) $(1! + 2! + \cdots + 100!) \mod 15$

Solution 6.

a) $[2^6]_{11} = [64]_{11} = [9]_{11}$,

b) $[2^{12}]_{11} = [2^6]_{11}^2 = [9]_{11}^2 = [81]_{11} = [4]_{11}$,

c) $[5^2]_3 = [25]_3 = [1]_3$, so $[5^{1030}]_3 = [5^2]_3^{515} = [1]_3^{515} = [1]_3$,

d) $[78]_3 = [0]_3$, so $[78^3]_3 = [0]_3^3 = [0]_3$,

e) if $k \geq 5$ then $5 \mid k!$, so $[k!]_5 = [0]_5$, hence $[1!+\cdots+10!]_5 = [1+2+6+24]_5 = [33]_5 = [3]_5$,

f) if $k \geq 5$ then $5 \mid k!$ and $3 \mid k!$, so $15 \mid k!$, hence $[1! + \cdots + 10!]_{15} = [1 + 2 + 6 + 24]_{15} = [33]_{15} = [3]_{15}$.