University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Problem Set n°2

Jean-Baptiste Campesato

Due on February 26$^{\text{th}}$, 2021

Except otherwise stated, you can only use the material covered in Chapters 1, 2 & 3.
You can also use the results proved in the exercise sheets 1, 2, 3 & 4.

Write your solutions concisely but without skipping important steps.
Make sure that your submission is readable on Crowdmark.

Exercise 1.
Find all $n \in \mathbb{Z}$ such that $n - 4 | 3n - 17$.

Exercise 2.
Find the integer solutions of $x^2 + 6x = y^2 + 12$.

Exercise 3.

1. Prove that
$$\forall a, x_1, x_2 \in \mathbb{Z} \setminus \{0\},\ \left(\gcd(a, x_1) = \gcd(a, x_2) = 1\right) \implies \gcd(a, x_1 x_2) = 1$$
2. Let $n \geq 2$ be an integer. Prove that
$$\forall a, x_1, \dots, x_n \in \mathbb{Z} \setminus \{0\},\ \left(\gcd(a, x_1) = \gcd(a, x_2) = \cdots = \gcd(a, x_n) = 1\right) \implies \gcd\left(a, x_1 x_2 \cdots x_n\right) = 1$$

Exercise 4.
Prove that the equation $x^3 - x^2 + x + 1 = 0$ has no rational solution.

For this question, you can assume that $\mathbb{Q} = \left\{ \frac{p}{q} \ : \ p \in \mathbb{Z},\ q \in \mathbb{N} \setminus \{0\},\ \gcd(p, q) = 1 \right\}$ *with the usual operations.*

Sample solution to Exercise 1.
Let $n \in \mathbb{Z}$ such that $n-4|3n-17$.
Since $n-4|n-4$ and $n-4|3n-17$ then $n-4|(3n-17)-3(n-4)=-5$.
Hence the only possible solutions are $n-4=-5,-1,1,5$, i.e. $n=-1,3,5,9$.
Conversely, we need to check which are solutions:

- $n=-1$: then $n-4=-5$ and $3n-17=-20$. So it is a solution since $-5|-20$
- $n=3$: then $n-4=-1$. So it is a solution since -1 divides any integer.
- $n=5$: then $n-4=1$. So it is a solution since 1 divides any integer.
- $n=9$: then $n-4=5$ and $3n-17=10$. So it is a solution since $5|10$.

Sample solution to Exercise 2.
Let $x, y \in \mathbb{Z}$, then

$$x^2+6x=y^2+12 \Leftrightarrow (x+3)^2=y^2+21 \Leftrightarrow (x+3)^2-y^2=21 \Leftrightarrow (x+y+3)(x-y+3)=21$$

Since the divisors of 21 are ±1, ±3, ±7 and ±21, we get the following cases:

1. $\begin{cases} x+y+3=21 \\ x-y+3=1 \end{cases} \Leftrightarrow (x,y)=(8,10)$
2. $\begin{cases} x+y+3=-21 \\ x-y+3=-1 \end{cases} \Leftrightarrow (x,y)=(-14,-10)$
3. $\begin{cases} x+y+3=7 \\ x-y+3=3 \end{cases} \Leftrightarrow (x,y)=(2,2)$
4. $\begin{cases} x+y+3=-7 \\ x-y+3=-3 \end{cases} \Leftrightarrow (x,y)=(-8,-2)$
5. $\begin{cases} x+y+3=3 \\ x-y+3=7 \end{cases} \Leftrightarrow (x,y)=(2,-2)$
6. $\begin{cases} x+y+3=-3 \\ x-y+3=-7 \end{cases} \Leftrightarrow (x,y)=(-8,2)$
7. $\begin{cases} x+y+3=1 \\ x-y+3=21 \end{cases} \Leftrightarrow (x,y)=(8,-10)$
8. $\begin{cases} x+y+3=-1 \\ x-y+3=-21 \end{cases} \Leftrightarrow (x,y)=(-14,10)$

Hence the integer solutions are $(8,\pm10),(-14,\pm10),(2,\pm2),(-8,\pm2)$.

Sample solution to Exercise 3.

1. **Method 1 (with Bézout's theorem):**
   Let $a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}$ be such that $\gcd(a, x_1) = \gcd(a, x_2) = 1$.
   By Bézout's identity, there exist $u, v, u', v' \in \mathbb{Z}$ such that $au + x_1 v = 1$ and $au' + x_2 v' = 1$.
   Then $1 = (au + x_1 v)(au' + x_2 v') = a(auu' + ux_2 v' + x_1 vu') + x_1 x_2 (vv')$.
   Therefore $\gcd(a, x_1 x_2) = 1$.

   Method 2 (with Euclid's lemma):
   Let $a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}$ be such that $\gcd(a, x_1) = \gcd(a, x_2) = 1$.
   Assume by contradiction that $d = \gcd(a, x_1 x_2) > 1$, then there exists a prime number p such that $p|d$.
   Since $p|d$ and $d|a$, we have that $p|a$.
   Since $p|d$ and $d|x_1 x_2$, we have that $p|x_1 x_2$.
   By Euclid's lemma, either $p|x_1$ or $p|x_2$. WLOG, we may assume that $p|x_1$.
   Then $p|x_1$ and $p|a$, therefore $p|\gcd(a, x_1) = 1$. Which is a contradiction.

   Method 3 (with prime factorization):
   Let $a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}$ be such that $\gcd(a, x_1) = \gcd(a, x_2) = 1$.
   Write the prime decompositions $a = \prod_p p^{\alpha_p}$, $x_1 = \prod_p p^{\beta_{1p}}$ and $x_2 = \prod_p p^{\beta_{2p}}$.
   Since $\gcd(a, x_i) = 1$, we know that, for p prime, we have $\min(\alpha_p, \beta_{ip}) = 0$.
   Therefore, for p prime, we have $\min(\alpha_p, \beta_{1p} + \beta_{2p}) \leq \min(\alpha_p, \beta_{1p}) + \min(\alpha_p, \beta_{2p}) = 0$.
   Note that $x_1 x_2 = \prod_p p^{\beta_{1p} + \beta_{2p}}$.
   Thus $\gcd(a, x_1 x_2) = \prod_p p^{\min(\alpha_p, \beta_{1p} + \beta_{2p})} = 1$.

2. Let's prove by induction on $n \geq 2$ that

$$\forall a, x_1, \dots, x_n \in \mathbb{Z} \setminus \{0\}, \left(\gcd(a, x_1) = \gcd(a, x_2) = \cdots = \gcd(a, x_n) = 1 \right) \implies \gcd\left(a, x_1 x_2 \cdots x_n\right) = 1$$

   - **Base case at $n = 2$:** it is exactly the previous question.
   - **Induction step.** Assume that the statement holds for some $n \geq 2$.
     Let $a, x_1, \dots, x_n, x_{n+1} \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, x_1) = \gcd(a, x_2) = \cdots = \gcd(a, x_{n+1}) = 1$.
     By the induction hypothesis, $\gcd\left(a, x_1 x_2 \cdots x_n\right) = 1$.
     Since
     $$\gcd\left(a, x_1 x_2 \cdots x_n\right) = \gcd(a, x_{n+1}) = 1$$
     by the previous question, we get that
     $$\gcd(a, x_1 x_2 \dots x_{n+1}) = 1$$
     Which proves the induction step.

Sample solution to Exercise 4.
Assume by contradiction that there exists $x \in \mathbb{Q}$ such that $x^3 - x^2 + x + 1 = 0$.
Then $x = \frac{p}{q}$ where $p \in \mathbb{Z}$, $q \in \mathbb{N} \setminus \{0\}$ and $\gcd(p, q) = 1$.
Therefore $x^3 - x^2 + x + 1 = 0$ implies $(p/q)^3 - (p/q)^2 + p/q + 1 = 0$ from which we derive that $p^3 - p^2 q + pq^2 + q^3 = 0$.
Hence $p|q^3 = -p^3 + p^2 q - pq^2$.
Since $\gcd(p, q) = 1$, by Gauss' lemma, $p|q^2$ and similarly $p|q$.
Hence $\gcd(p, q) = |p|$. So either $p = -1$ or $p = 1$.
Similarly $q|p^3 = p^2 q - pq^2 - q^3$ so $q = 1$.
Thence the only possible rational solutions are -1 and 1.
But they don't satisfy the equation.