MATH 410 Problem Set # 1

Qilin Ye

January 30, 2021

Ex.1.2.3 Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

> *Proof.*
> $$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \text{ and } x \in B \cup C \\ &\iff x \in A \text{ and } (x \in B \text{ or } x \in C) \\ &\iff (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$ □

Ex.1.3.4 (*Cancellation Laws*). Show that if $a, b, c \in \mathbb{Z}$ then we have the following laws.

(a) If $a + b = a + c$ then $b = c$.

> *Proof.* By R4 there exists some additive inverse a, one (in fact, the only) of which we denote as $(-a)$. Then,
> $$\begin{aligned} a + b = a + c &\implies -a + (a + b) = -a + (a + c) \\ &\implies (-a + a) + b = (-a + a) + c && \text{(R2)} \\ &\implies 0 + b = 0 + c && \text{(R4)} \\ &\implies b = c. && \text{(R3)} \end{aligned}$$ □

(b) If $a \neq 0$ and $ab = ac$ then $b = c$.

> *Proof.* By Ex.1.3.3 the additive inverse of x is denoted as $-x := (-1)x$ and by the previous part such $-x$ is unique once x is fixed. Hence, since $ab = ac$,
> $$\begin{aligned} ab + (-1)ab = ab + (-1)ac = 0 &\implies ab + a(-c) = 0 && \text{(R2 \& Ex.1.3.3)} \\ &\implies a(b + (-c)) = 0 && \text{(R5)} \\ &\implies a \cdot (b + (-c)) = 0 && \text{(R3 \& Ex.1.3.3)} \\ &\implies b + (-c) = 0. && \text{(R6)} \end{aligned}$$
> Now if we simply apply part (a) to $b + (-c) = c + (-c) = 0$ we get $b = c$, as desired. □

Ex.1.4.1 Use induction to show that $\sum_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Proof. Let $\varphi(n)$ be the statement that the above equation holds true for n. Base case is clearly true as $1^2 = 1 = (1 \cdot 2 \cdot 3)/6$. Now for the inductive step we assume $\varphi(n)$ holds. Then,

$$\begin{aligned}\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2 \overset{\varphi(n)}{=\!=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ = \frac{n+1}{6}[n(2n+1) + 6(n+1)] \\ = \frac{(n+1)(n+2)(2n+3)}{6},\end{aligned}$$

from which we see $\varphi(n) \implies \varphi(n+1)$. Thus $\varphi(n)$ holds for all $n \in \mathbb{N}$ and we are done. $\square$

Ex.1.4.9 Prove for $n \geqslant 1$, $\displaystyle\sum_{k=1}^{2^n} \frac{1}{k} \geqslant 1 + \frac{n}{2}$.

Proof. Let $\varphi(n)$ be the statement that the above equation holds true for n. Clearly $\varphi(1)$ the base case is true as $1 + 1/2 \geqslant 1 + 1/2$. For the inductive step, assuming $\varphi(n)$ is true. Then,

$$\begin{aligned}\sum_{k=1}^{2^{n+1}} \frac{1}{k} &= \sum_{k=1}^{2^n} \frac{1}{k} + \sum_{k=2^n+1}^{2^{n+1}} \frac{1}{k} \\ &\geqslant 1 + \frac{n}{2} + \sum_{k=2^n+1}^{2^{n+1}} \frac{1}{k} && (\varphi(n)) \\ &\geqslant 1 + \frac{n}{2} + \frac{2^n}{2^n + 1} && \text{(bound by largest term)} \\ &\geqslant 1 + \frac{n}{2} + \frac{1}{2} = 1 + \frac{n+1}{2}.\end{aligned}$$

Therefore $\varphi(n) \implies \varphi(n+1)$ and $\varphi(n)$ holds for all $n \in \mathbb{N}$. Done. $\square$

Ex.1.5.4 Show that there are infinitely many primes.

Proof. Suppose not, then we may enumerate all the primes $\mathcal{P} := \{p_i\}_{i=1}^n$. Now consider $M := 1 + \displaystyle\prod_{i=1}^n p_i$. It follows that $M - \displaystyle\prod_{i=1}^n p_i = 1$. If M is composite then it has some prime factor p_k. Since $\{p_i\}_{i=1}^n$ is an enumeration of *all* primes, $p_k \in \mathcal{P}$. Hence $p \mid M \wedge p \mid \displaystyle\prod_{i=1}^n p_i$ implies p divides the LHS, and so it also divides the RHS, i.e., $p_k \mid 1$, which is absurd. Hence this contradiction tells us there are infinitely many primes. $\square$

Ex.1.6.3 Prove that $a \equiv b \pmod{m}$ if and only if a and b have the same remainder upon division by m.

Proof. There exists $a_1, b_1, a_r, b_r \in \mathbb{Z}$ with $0 \leqslant a_r, b_r < m$ such that $a = ma_1 + a_r$ and $b = mb_1 + b_r$.
$\implies$: if $a \equiv b$ then $m \mid a - b = m(a_1 - b_1) + (a_r - b_r)$. It follows that $m \mid a_r - b_r$. By construction $-m < a_r - b_r < m$ so the only possibility is if $a_r = b_r$, i.e., a and b have the same remainder.
$\impliedby$: if $a_r = b_r$ then $m \mid m(a_1 - b_1) - 0 = m(a_1 - b_1) + (a_r - b_r) = a - b$, i.e., $a \equiv b \pmod{m}$. $\square$

Ex.1.6.4 Create addition and multiplication tables of $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$.

Solution

See below. $\mathbb{Z}/7\mathbb{Z}$ on the right and $\mathbb{Z}/8\mathbb{Z}$ on the left.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Ex.1.6.8 (a) Compute $d := \gcd(83, 38)$ using the Euclidean algorithm.

Solution

$$\begin{aligned} 83 &= 2\cdot 38 + 7 \\ 38 &= 5\cdot 7 + 3 \\ 7 &= 2\cdot 3 + 1 \\ 3 &= 3\cdot 1 \implies \gcd(83,38) = 1. \end{aligned}$$

(b) Use the result of (a) to write $d = 83m + 38n$ for integers m, n.

Solution

$$\begin{aligned} 83 = 2\cdot 38 + 7 &\implies 7 = 83 + (-2)(38) \\ 38 = 5\cdot 7 + 3 &\implies 3 = 38 + (-5)(7) = (-5)(83) + (11)(38) \\ 7 = 2\cdot 3 + 1 &\implies 1 = 7 + (-2)(3) = (11)(83) + (-24)(38). \end{aligned}$$

Hence $m = 11$ and $n = -24$.

(c) Use (b) to solve $38x \equiv 1 \pmod{83}$.

Solution

This is immediate from (b): $38 \cdot (-24) = 11 \cdot (-83) + 1$. Since $\gcd(38, 83) = 1$, the general solution is $83k - 24$, where $k \in \mathbb{Z}$.

Ex.1.7.5 Define a relation on $a, b \in \mathbb{R}$ by $a \sim b \iff a - b \in \mathbb{Z}$. Show that this is an equivalence relation on $\mathbb{R}$. Find a nice set of representatives for the equivalence classes.

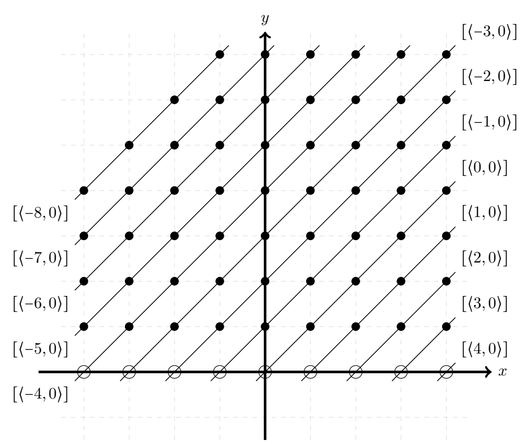
Solution

First we show $\sim$ is indeed an equivalence relation:

(1) Reflexivity: $\forall a \in \mathbb{R}, a - a = 0 \in \mathbb{Z}$ so $a \sim a$.

(2) Symmetry: if $a \sim b$ then $a - b \in \mathbb{Z}$. Clearly $b - a \in \mathbb{Z}$ too. Thus $b \sim a$.

(3) Transitivity: if $a \sim b \wedge b \sim c$ then $a - b, b - c \in \mathbb{Z}$. Hence $a - c = (a - b) + (b - c) \in \mathbb{Z}$ and so $a \sim c$.



A *nice representation* of the collection of equivalence classes: $\{[\langle x_0, 0\rangle] : x_0 \in \mathbb{Z}\}$. A *nice representative* for these equivalence classes? I'd go with the set of lattice points on the x-axis.

Geometric interpretation of these equivalence classes: each line (more formally put, a collection of points on $\mathbb{R}^2$) is the equivalence class $[\langle x_0, 0\rangle]$ where x_0 is the x-intercept. Their slopes are all 1. The x-intercepts are all lattice points, i.e., with integer coordinates.