MA1100(T) - Basic Discrete Mathematics (T) Suggested Solutions

Written by: Poon Chun Wai Victor
Audited by: Daryl Chew

(Semester 1 : AY2023/24)

1. (4 points) Suppose a, b and n are positive integers. Suppose $\gcd(a,b)$ is a prime, say q, and that $ab = n^2$. Prove that there exists **integers** c and d such that

$$\frac{a}{q} = c^2 \quad \text{and} \quad \frac{b}{q} = d^2.$$

Solution:

We can construct c and d by

$$e_c(p) = \begin{cases} \frac{1}{2}e_a(p), & p \neq q, \\ \frac{1}{2}(e_a(p) - 1), & p = q, \end{cases} \quad \text{and} \quad e_d(p) = \begin{cases} \frac{1}{2}e_b(p), & p \neq q, \\ \frac{1}{2}(e_b(p) - 1), & p = q, \end{cases}$$

First, since q is a prime, $e_q(p) = 0$ for all primes $p \neq q$, and $e_q(q) = 1$.

Hence, $e_{c^2q} = 2e_c + e_q = e_a$ and $e_{d^2q} = 2e_c + e_q = e_a$, so $\frac{a}{q} = c^2$ and $\frac{b}{q} = d^2$.

It remains to show that e_c and e_d are well defined.

Since $ab = n^2$, we have $e_a(p) + e_b(p) = 2e_n(p)$ for all primes p. We consider two cases:

Case 1: $p = q$.

Since $\gcd(a,b) = q$, either $1 = e_a(q) \leq e_b(q)$ or $1 = e_b(q) \leq e_a(q)$.

In either case, since $e_a(p) + e_b(p) = 2e_n(p)$, both $e_a(q)$ and $e_b(q)$ are positive odd integers.

Hence, $e_c(q) = \frac{1}{2}(e_a(q) - 1)$ and $e_d(q) = \frac{1}{2}(e_a(q) - 1)$ are in $\mathbb{N}$.

Case 2: $p \neq q$.

Since $\gcd(a,b) = q$, at least one of $e_a(p)$ and $e_b(p)$ is 0.

if $e_a(p) = 0$, we have $e_b(p) = 2e_n(p)$, so $e_c(p) = 0$ and $e_d(p) = e_n(p)$.

If $e_b(p) = 0$, we have $e_a(p) = 2e_n(p)$, so $e_c(p) = e_n(p)$ and $e_c(p) = 0$.

Hence, for all primes p, $e_c(p) \in \mathbb{N}$ and $e_d(p)$ are in $\mathbb{N}$.

Furthermore, $e_c(p) \leq e_a(p)$ and $e_d(p) \leq e_a(p)$. Since e_a, e_b have finite support, so do e_c and e_d.

Hence, e_c and e_d are well defined. $\square$

2. (3 points) Suppose $a, b \in \mathbb{N}^+$. Prove that $\gcd(a, b) = 1$ if and only if $\gcd(ab, a + b) = 1$.

Solution:

Lemma: Suppose x, $y \in \mathbb{N}^+$. If there exists m, $n \in \mathbb{Z}$ such that $mx + ny = 1$, then $\gcd(x, y) = 1$.

Proof of Lemma:

Let $\gcd(x, y) = d$. Then, $d \mid x$ and $d \mid y$, so $d \mid mx + ny = 1$.

Hence, $d \leq 1$. Since $d \geq 1$ by definition, $d = 1$. □

Proof of question:

($\Rightarrow$) Suppose $\gcd(a, b) = 1$.

Then, by Bezout's Identity, there exists $h, k \in \mathbb{Z}$ such that $ha + kb = 1$.

Then, we have the following equalities:

$$\begin{aligned} 1 &= ha + kb \\ &= (ha + kb)^2 \\ &= h^2a^2 + 2hkab + k^2b^2 \\ &= h^2a^2 + h^2ab + k^2ab + k^2b^2 + 2hkab - h^2ab - k^2ab \\ &= (h^2a + k^2b)(a + b) + (2hk - h^2 - k^2)ab \end{aligned}$$

Hence, by the Lemma, $\gcd(ab, a + b) = 1$.

($\Leftarrow$) Suppose $\gcd(ab, a + b) = 1$.

Then, by Bezout's Identity, there exists $p, q \in \mathbb{Z}$ such that $pab + q(a + b) = 1$.

Then, we have the following equalities:

$$\begin{aligned} 1 &= pab + q(a + b) \\ &= (pb + q)a + qb \end{aligned}$$

Hence, by the Lemma, $\gcd(a, b) = 1$. □

3. Define a relation $\sim$ on $\mathbb{R}$ such that $x \sim y$ if $x - y \in \mathbb{Q}$.

(a) (3 points) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.

Solution:

Reflexivity:

For all $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Q}$. Hence, $x \sim x$ for all $x \in \mathbb{R}$, and $\sim$ is reflexive.

Symmetric:

Suppose $x, y \in \mathbb{R}$ are such that $x \sim y$.

Then, $x - y \in \mathbb{Q}$, so $y - x = -(x - y) \in \mathbb{Q}$, so $y \sim x$. Hence, $\sim$ is symmetric.

Transitivity:

Suppose $x, y, z \in \mathbb{R}$ are such that $x \sim y$ and $y \sim z$.

Then, $x - y$ and $y - z$ are in $\mathbb{Q}$.

Hence, $x - z = (x - y) + (y - z) \in \mathbb{Q}$, so $x \sim z$. Hence, $\sim$ is transitive. $\square$

(b) (2 points) Prove that the quotient set $\mathbb{R}/\sim$ is infinite.

Solution:

Consider the set $S = \{[\sqrt{2}k]_\sim : k \in \mathbb{Z}\}$.

Note that the mapping $f : \mathbb{Z} \to S$ by $k \mapsto [\sqrt{2}k]_\sim$ is injective:

If $[\sqrt{2}k]_\sim = [\sqrt{2}k']_\sim$, we have $\sqrt{2}k \sim \sqrt{2}k'$.

Hence, $\sqrt{2}k - \sqrt{2}k' = (k - k')\sqrt{2} \in \mathbb{Q}$.

Since $k - k'$ is an integer and $\sqrt{2}$ is irrational, for $(k - k')\sqrt{2} \in \mathbb{Q}$ to hold, $k - k' = 0$.

Hence, $k = k'$.

Since f injects from $\mathbb{Z}$ to S, and $\mathbb{Z}$ is infinite, S is also infinite.

Then, $S \subseteq \mathbb{R}/\sim$, so $\mathbb{R}/\sim$ is infinite. $\square$

4. (4 points) Suppose J is a nonempty indexing set. Let $(A_j)_{j\in J}$ be a family of sets, and define their *disjoint union* as

$$\bigsqcup_{j\in J} A_j = \{(j,a) : j \in J, a \in A_j\}.$$

For each $j \in J$, define the function $i_j : A_j \to \bigsqcup_{j\in J} A_j$ by $a \mapsto (j,a)$. Define also the family of functions $(f_j : A_j \to X)_{j\in J}$ (consisting of one such f_j for each $j \in J$). Prove that there exists a unique function $f : \bigsqcup_{j\in J} A_j \to X$ such that $f_j = f \circ i_j$ for each $j \in J$.

Solution:

Define f by $(j,a) \mapsto f_j(a)$. We first prove f is well-defined.

$f(j,a)$ always exists, because the family of functions has one f_j for every $j \in J$.

Then, Suppose $(j_1,a_1) = (j_2,a_2)$. Then, $j_1 = j_2$, so $f_{j_1} = f_{j_2}$, and $a_1 = a_2$.

Since all the f_j's are well defined functions, and $a_1 = a_2$, we have

$$f(j_1,a_1) = f_{j_1}(a_1) = f_{j_1}(a_2) = f_{j_2}(a_2) = f(j_2,a_2)$$

so f is well-defined.

Then, for each $j \in J$, we have that

$$f \circ i_j(a) = f(i_j(a)) = f(j,a) = f_j(a)$$

for all $a \in A_j$, so $f_j = f \circ i_j$.

To show f is unique, suppose $g : \bigsqcup_{j\in J} A_j \to X$ is a function such that $f_j = g \circ i_j$ for each $j \in J$.

Note that i_j is onto, as for each $(j,a) \in \bigsqcup_{j\in J} A_j$, $i_j(a) = (j,a)$.

Then we have the following equalities that hold for all $(j,a) \in \bigsqcup_{j\in J} A_j$:

$$\begin{aligned} g(j,a) &= g(i_j(a)) \quad \text{[because } i_j \text{ is onto]} \\ &= f_j(a) \\ &= f(i_j(a)) \\ &= f(j,a) \end{aligned}$$

so $g = f$ as desired. $\square$

5. (3 points) Suppose $m, n \in \mathbb{N}^+$. We attempt to define a function $f : [mn] \to [m] \times [n]$ by

$$f(R_{mn}(a)) = (R_m(a), R_n(a)).$$

Prove that f is well-defined.

Solution:

Suppose $c \in [mn]$. Since the R_b function is onto for all $b \in \mathbb{N}^+$, there exists some integer a such that $c = R_{mn}(a)$. Hence, $R_m(a)$ and $R_n(a)$ exist, so $f(c)$ exists.

Suppose now that $R_{mn}(a_1) = c = R_{mn}(a_2)$.

Then, $a_1 = q_1(mn) + c$ and $a_2 = q_2(mn) + c$, for some $q_1, q_2 \in \mathbb{Z}$.

Then, $a_1 - a_2 = (q_1 - q_2)mn$, so $m \mid a_1 - a_2$. Hence, $R_m(a_1) = R_m(a_2)$.

Likewise, $n \mid a_1 - a_2$, so $R_n(a_1) = R_n(a_2)$.

Hence, $(R_m(a_1), R_n(a_1)) = (R_m(a_2), R_n(a_2))$, and $f(c)$ has a unique value. $\square$

6. Let C be the set of functions from $\mathbb{N}$ to $\{0, 1\}$ that are *eventually constant*, that is, for each $f \in C$, there exists $n \in \mathbb{N}$ such that for all $m > n$, $f(m) = f(n)$. For each $f \in C$, define the set S_f by

$$S_f = \{n \in \mathbb{N} : (\forall m > n)(f(m) = f(n))\}.$$

Define the function $F : C \to \{0, 1\}^{<\mathbb{N}}$ by

$$F(f) = (f(0), f(1), \ldots, f(\min(S_f))).$$

(a) (3 points) Prove that F is one-to-one.

Solution:

Suppose $F(f_1) = F(f_2)$. Then, by the definition of F, we have

$$(f_1(0), f_1(1), \ldots, f_1(\min(S_{f_1}))) = (f_2(0), f_2(1), \ldots, f_2(\min(S_{f_2}))).$$

For the two sequences to be equal, they must have equal length. Hence, $\min(S_{f_1}) = \min(S_{f_2})$.

Let $\min(S_{f_1}) = \min(S_{f_2}) = k$. For the two sequences to be equal, they are also termwise equal. Hence, for all $m \leq k$, $f_1(m) = f_2(m)$.

By the definition of S_f, for all $m > k$, $f(m) = f(k)$. Hence, $f_1(m) = f_1(k) = f_2(k) = f_2(m)$.

Hence $f_1(m) = f_2(m)$ for all $m \in \mathbb{N}$, so $f_1 = f_2$, as desired. $\square$

(b) (1 point) Prove that C is countable.

Solution:

Since $\{0, 1\}$ is finite, $\{0, 1\}^{<\mathbb{N}}$ is countably infinite.

Hence, there exists a bijection g from $\{0, 1\}^{<\mathbb{N}}$ to $\mathbb{N}$.

Then, $g \circ F$ is an injection from C to $\mathbb{N}$, so C is countable. $\square$

7. (3 points) Prove that for every pair of real numbers $q < r$, there exists an irrational number that is strictly between them.

Solution:

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there is a rational number x strictly between q and r.

Then, by the same argument, there is a rational number y strictly between x and r.

Then we know there is an irrational number strictly between two rational numbers, so we are done, as there is an irrational z such that $q < x < z < y < r$. $\square$

Solution:

(Alternative)

Let $x < y$ be a pair of real numbers such that $q = \sqrt{2}x$ and $r = \sqrt{2}y$.

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists some rational z that is strictly between x and y.

Furthermore, we can take z to be non-zero. If z was 0, we can take some rational z' that is strictly between z and y, since $\mathbb{Q}$ is dense in $\mathbb{R}$. Since $z < z'$, z' would be non-zero.

Hence, we have:

$$x < z < y \implies \sqrt{2}x < \sqrt{2}z < \sqrt{2}y \implies q < \sqrt{2}z < r$$

where $\sqrt{2}z$ is a product of an irrational and a non-zero rational, and is hence irrational. $\square$