NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Lee Yung Hei, Joseph Nah

MA1100 Fundamental Concepts of Mathematics
AY 2007/2008 Sem 1

Question 1

Let $P(n)$ be the proposition that $1+2+\cdots+(3n-2)=\frac{n(3n-1)}{2}$.
Consider $P(1)$:
LHS: $(3n-2)=(3-2)=1$.
RHS: $\frac{n(3n-1)}{2}=\frac{1(3-1)}{2}=1$.
So, P(1) is true.
Assume $P(k)$ is true, consider $P(k+1)$.
LHS: $1+2+\cdots+(3k-2)+(3(k+1)-2)=\frac{k(3k-1)}{2}+(3(k+1)-2)=\frac{3k^2-k}{2}+3k+1=\frac{3k^2+5k+2}{2}$.
RHS: $\frac{(k+1)(3(k+1)-1)}{2}=\frac{(k+1)(3k+2)}{2}=\frac{3k^2+5k+2}{2}$.
Therefore, $P(k+1)$ is true whenever $P(k)$ is true.
By Mathematical Induction, $P(n)$ is true for all $n\in\mathbb{Z}^+$.

Question 2

(a) $\mathbb{Z}_4$ has 4 equivalence classes [0], [1], [2] and [3].
Considering by cases:
$[0]^2=[0]$,
$[1]^2=[1]$,
$[2]^2=[4]=[0]$,
$[3]^2=[9]=[1]$.
Therefore, given $[x]^2=[0]$, we have $[x]=[0]$ or $[x]=[2]$.

(b) $([2]\otimes[x])\oplus[3]=[1]$ in $\mathbb{Z}_6$ gives us $[2]\otimes[x]=[1]\oplus[-3]=[-2]=[4]$.
Considering by cases:
$[2]\otimes[0]=[0]$,
$[2]\otimes[1]=[2]$,
$[2]\otimes[2]=[4]$,
$[2]\otimes[3]=[6]=[0]$,
$[2]\otimes[4]=[8]=[2]$,
$[2]\otimes[5]=[10]=[4]$.
Therefore, given $([2]\otimes[x])\oplus[3]=[1]$, we have $[x]=[2]$ or $[x]=[5]$.

(c) $[4]\otimes[x]=[3]$ in $\mathbb{Z}_8$.
Considering by cases:
$[4]\otimes[0]=[0]$,
$[4]\otimes[1]=[4]$,
$[4]\otimes[2]=[8]=[0]$,
$[4]\otimes[3]=[12]=[4]$,
$[4]\otimes[4]=[16]=[0]$,
$[4]\otimes[5]=[20]=[4]$,
$[4]\otimes[6]=[24]=[0]$,

$[4] \otimes [7] = [28] = [4]$.
Therefore, given $[4] \otimes [x] = [3]$, there is not solution.

Question 3

(a) Let $\gcd(a, a+9) = k$, then $k|a$ and $k|a+9$.
So there exists $m, n \in \mathbb{Z}$ such that $km = a$ and $kn = a+9$.
It thus follows that $kn = km + 9$ and $k(n-m) = 9$.
So $k|9$ and so k can only be 1, 3 or 9.
By checking $a = 1$, $\gcd(a, a+9) = 1$; $a = 3$, $\gcd(a, a+9) = 3$; $a = 9$, $\gcd(a, a+9) = 9$.

(b) Let $a \in \{3k \mid k \in \mathbb{Z}\}$. Then $3 \mid a$. Together with $3 \mid 9$, we have $3 \mid a+9$.
Thus $3 \mid \gcd(a, a+9)$. Therefore we have $\gcd(a, a+9) \neq 1$.

Let $a \in \mathbb{Z} - \{3k \mid k \in \mathbb{Z}\}$ instead. Then $3 \nmid a$, which implies that $3 \nmid \gcd(a, a+9)$.
Therefore together with result from (3a.), we have $\gcd(a, a+9) = 1$.

So $\mathbb{Z} - \{3k \mid k \in \mathbb{Z}\}$ contains all the possible values of a such that a and $a+9$ are relatively prime.

Question 4

We have $4 \nmid 1+1$, i.e. $1 \not\sim 1$. So $\sim$ is not reflexive.
Since $4 \mid a+b$ implies $4 \mid b+a$, $a \sim b$ implies $b \sim a$, i.e. $\sim$ is symmetric.
We have $4 \mid 1+3$ and $4 \mid 3+1$, i.e. $1 \sim 3$ and $3 \sim 1$.
However $1 \not\sim 1$ as shown, which give us $\sim$ to not be transitive.

Question 5

(a) Let $x_1, x_2 \in \left[\frac{1}{2}, \infty\right)$ be such that $f(x_1) = f(x_2)$. This give us,

$$\begin{aligned}
(2x_1 - 1)^2 &= (2x_2 - 1)^2 \\
(2x_1 - 1)^2 - (2x_2 - 1)^2 &= 0 \\
(2x_1 - 1 + 2x_2 - 1)(2x_1 - 1 - 2x_2 + 1) &= 0 \\
(2x_1 + 2x_2 - 2)(2x_1 - 2x_2) &= 0.
\end{aligned}$$

So, $2x_1 + 2x_2 - 2 = 0$ or $x_1 - x_2 = 0$.
If $2x_1 - 2x_2 = 0$, then $x_1 = x_2$.
If $2x_1 + 2x_2 - 2 = 0$, then $x_1 + x_2 = 1$.
Since $x_1 \geq \frac{1}{2}$ and $x_2 \geq \frac{1}{2}$, these give us $x_1 = \frac{1}{2} = x_2$.
So, f is injective.

(b) f is not a surjection.
We have -1 is inside the co-domain.
However $\forall x \in \left[\frac{1}{2}, \infty\right)$, we have $f(x) \geq 0 > -1$, and so $f(x) \neq -1$.

Question 6

(a) Assume on the contrary that $(A - B) \cap (A - C) \neq \emptyset$.
Then, there exists $x \in (A - B) \cap (A - C)$.
So, $x \in (A - B)$ and $x \in (A - C)$.

This give us $x \in A$, $x \notin B$ and $x \notin C$.
However, since $x \in A$ and $A \subseteq B \cup C$, we have $x \in B \cup C$.
This implies that $x \in B$ or $x \in C$, a contradiction with $x \notin B$ and $x \notin C$.

(b) Consider $A = \{1\}$ and $B = C = \emptyset$, then $(A - B) \cap (A - C) = \{1\} \cap \{1\} = \{1\} \neq \emptyset$.
So, the conclusion does not hold.

Question 7

(i) $(P \wedge Q) \wedge \neg R$ can only be false.

Assume on the contrary that $(P \wedge Q) \wedge \neg R$ is true. Then $P \wedge Q$ is true, i.e. P and Q are true.
Since $P \to (Q \to R)$ is given to be true, and P is true, we have $Q \to R$ to be true.
Together with Q to be true, we have R to be true.
However $(P \wedge Q) \wedge \neg R$ is true implies R is false, a contradiction.

Note: You could also deduce that the statement is false by observing that $(P \cap Q)$ and $\neg R$ is the negation of $P \to (Q \to R)$.

(ii) $(P \to Q) \to R$ can be true or false.

Let P, Q and R be true.
This case give us $P \to (Q \to R)$ to be true, while $(P \to Q) \to R$ is true.

Let P and R be false, but Q is true.
Since P is false, we have $P \to (Q \to R)$ to be true.
Since P is false and Q is true, we have $P \to Q$ is true.
Together with R is false, we have $(P \to Q) \to R$ to be false.

Question 8

(a) $657 = 2(306) + 45$, $306 = 6(45) + 36$, $45 = 36 + 9$, $36 = 4(9)$.
$\gcd(657, 306) = 9$.

$9 = 45 - 36 = 45 - (306 - 6(45)) = 7(45) - 306 = 7(657 - 2(306)) - 306 = 7(657) - 15(306)$.
$657(7 + \frac{306}{9}k) + 306(-15 - \frac{657}{9}k) = 9$
$657(7 + 34k) + 306(-15 - 73k) = 9$
Therefore, all integers solutions of the linear equation is $y = 7 + 34k$ and $x = -15 - 73k$, $k \in \mathbb{Z}$.

(b) Since $\gcd(c, b) \mid c$, we have $\gcd(c, b) \mid ac$. Together with $\gcd(c, b) \mid b$, we have $\gcd(c, b) \mid \gcd(ac, b)$.

Since $\gcd(a, b) = 1$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
Also, there exists $x', y' \in \mathbb{Z}$ such that $cx' + by' = \gcd(c, b)$.
This give us $\gcd(c, b) = cx' + by' = cx'(ax + by) + by' = ac(xx') + b(cx'y + y')$.
This give us $\gcd(c, b)$ to be a linear combination of ac and b over $\mathbb{Z}$, and so $\gcd(ac, b) \mid \gcd(c, b)$.

Therefore $\gcd(ac, b) = \gcd(c, b)$.

Question 9

(a) False.
We have $\sqrt{2}, \sqrt{2}, -2 \cdot \sqrt{2} \in \mathbb{R} - \mathbb{Q}$ but $\sqrt{2} + \sqrt{2} - 2 \cdot \sqrt{2} = 0 \in \mathbb{Q}$.

(b) False.
Let $x = 5$, $6(5) + 15y = 3$. So, $15y = 3 - 30 = -27$ and $y = \frac{-27}{15} = -\frac{9}{5} \notin \mathbb{Z}$.

(c) True.
Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$.
This give us $(f \circ f)(x_1) = (f \circ f)(x_2)$, and since $f \circ f$ is injective, we have $x_1 = x_2$.
Let $a \in A$. Since $f \circ f$ is surjective, there exists $x \in A$, such that $(f \circ f)(x) = a$.
This give us $f(x)$ to be a pre-image of a.
Therefore f is bijective.

(d) True.
For $n = 1$, $n^3 - 1 = 0$. For $n = 2$, $n^3 - 1 = 7$ which is prime.
For $n \geq 3$, $n^3 - 1 = (n-1)(n^2 + n + 1)$.
Since $n - 1 \geq 2$ and $n^2 + n + 1 \geq 2$, for $n \geq 3$, $n^3 - 1$ is not prime.
Therefore, $n^3 - 1$ is prime only when $n = 2$, giving us the prime number 7.

(e) False.
Counterexample: Let $A = \mathbb{Z}^+ \cup \{0\}$ and $B = \mathbb{Z}^+ \cup \{-1\}$.
Then, both A and B are countably infinite.
Also, $0 \in A$ and $0 \notin B$, so $A \not\subseteq B$.
Also, $-1 \in B$ and $-1 \notin A$, so $B \not\subseteq A$.
$A \cap B = \mathbb{Z}^+$ which is countably infinite.
However, $A - B = \{0\}$ which is finite.

Question 10

(a) Assume on the contrary that f is not injective.
Then there exists $t \in T$ such that there is $s_1, s_2 \in S$ with $s_1 \neq s_2$ but $f(s_1) = t = f(s_2)$.
Then we have $\{s_1\} = f^{-1}[f[\{s_1\}]] = f^{-1}[\{t\}] = \{s_1, s_2\}$, a contradiction.
Therefore f is injective.

(b) Let $Q = \{g^{-1}[C] \mid C \in P\}$. Since P is a partition of T, C is non-empty.
So, there exists $a \in P \subseteq T$, it follows that since g is surjective, there exists $b \in S$ such that $g(b) = a$.
So, $b \in Q$ and Q is not empty.

Assume on the contrary that elements in Q are not mutually exclusive.
Then there exists $s \in S$, $C_1, C_2 \in P$ such that $s \in g^{-1}[C_1]$ and $s \in g^{-1}[C_2]$.
This implies that $g(s) \in C_1$ and $g(s) \in C_2$.
So, $C_1 \cap C_2 \neq \emptyset$, a contradiction to P being a partition of T.

Let $s' \in S$. Then we have $g(s') \in T$.
Since P is a partition of T, there exists $C \in P$ such that $g(s') \in C$.
This give us $s' \in g^{-1}[C]$, i.e. every element of S lies in an element of Q.

Therefore Q is a partition of S.