NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Associate Professor Victor Tan

solutions prepared by Wu Jiawei, Terry Lau

MA1100 Fundamental Concepts of Mathematics
AY 2008/2009 Sem 1

Question 1

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

(b) Let $P(n)$ be the proposition that $S_1, S_2, \cdots, S_n$ are divisible by 4.
By the conditions given, $P(1)$ and $P(2)$ are true.
Assume $P(k)$ is true, Consider S_{k+1}.
$S_{k+1} = 5S_k + S_{k-1}^2 \equiv 5 \times 0 + 0^2 \equiv 0 (\text{mod } 4)$
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) Since $7 - 2 = 5$ and $3 \nmid 5$, $7 \nsim 2$.
Since $2 - 5 = -3$ and $3 \mid -3$, $2 \sim 5$.
Since $8 - 8 = 0$ and $3 \mid 0$, $8 \sim 8$.

(b) $x \sim y \iff \{(x, y) \in Z \times Z | x \equiv y \text{ mod } 3\}$

(c) Since $x - x = 0$ and $3 \mid 0$, $\sim$ is reflexive.
Since $x \sim y \Leftrightarrow 3 \mid x - y \Leftrightarrow 3 \mid y - x \Leftrightarrow y \sim x$, $\sim$ is symmetric.
Since $x \sim y$ and $y \sim z \Leftrightarrow 3 \mid x - y$ and $3 \mid y - z$
$\Rightarrow 3 \mid (x - y) - (y - z) \Leftrightarrow 3 \mid x - z \Leftrightarrow x \sim z$, $\sim$ is transitive.

(d)

$$[2]_3 = \{2, 5, 8\}$$

$$[3]_3 = \{3, 6\}$$

$$[4]_3 = \{4, 7\}$$

Question 3

(a) f is injective since $f(x) = f(y) \Leftrightarrow 16x - 5 = 16y - 5 \Leftrightarrow x = y$.
f is surjective since for any real number y, $\exists x = \frac{y+5}{16}$ such that $f(x) = y$.

(b) Let $y = f(x) = 16x - 5$. Then $x = f^{-1}(y) = \frac{y+5}{16}$.

(c) g is an injection since $g(x) = g(y) \Leftrightarrow 16x - 5 = 16y - 5 \Leftrightarrow x = y$.

(d) g is not a surjection since 0 is not mapped to by any x in the domain of g.

Question 4

(a) By Euclidean algorithm,

$$\begin{aligned} 284 &= 168 + 116 \\ &= 52 + 2 \times 116 \\ &= 5 \times 52 + 2 \times 12 \\ &= 5 \times 4 + 22 \times 12 \\ &= 71 \times 4 + 0 \end{aligned}$$

$$\begin{aligned} \gcd(284, 168) &= \gcd(116, 168) \\ &= \gcd(116, 52) \\ &= \gcd(12, 52) \\ &= \gcd(12, 4) \\ &= \gcd(0, 4) = 4 \end{aligned}$$

(b) $\{n \mid n \equiv 0 (\bmod 4)\}$

(c) $4 = 52 \times 1 - 12 \times 4 = 52 \times 1 - (116 - 52 \times 2) \times 4$
$= 52 \times 9 - 116 \times 4 = (168 - 116) \times 9 - 116 \times 4 = 168 \times 9 - 116 \times 13$
$= 168 \times 9 - (284 - 168) \times 13 = 168 \times 22 - 284 \times 13$.

Therefore the general solution to $284x + 168y = 4$ is: $x = -13 + 42a, y = 22 - 71a, a \in \mathbb{Z}$.
The smallest integer x is 29.

Question 5

(a) $0^2 \equiv 0 (\bmod 7)$, $1^2 \equiv 1 (\bmod 7)$, $2^2 \equiv 4 (\bmod 7)$, $3^2 \equiv 2 (\bmod 7)$,
$4^2 \equiv 2 (\bmod 7)$, $5^2 \equiv 4 (\bmod 7)$, $6^2 \equiv 1 (\bmod 7)$.
Therefore the congruence classes are $[0]_7, [1]_7, [2]_7, [4]_7$.

(b) From part (a), we know that $\forall k \in \mathbb{Z}$,

$$n^2, m^2 \in [0]_7 \text{ or } [1]_7 \text{ or } [2]_7 \text{ or } [4]_7$$

We list out all the possibilities of $n^2 + m^2$, we have

$$\begin{aligned} 0+0 &\equiv 0 \bmod 7, & 0+1 &\equiv 1 \bmod 7 \\ 0+2 &\equiv 2 \bmod 7, & 0+4 &\equiv 4 \bmod 7 \\ 1+1 &\equiv 2 \bmod 7, & 1+2 &\equiv 3 \bmod 7 \\ 1+4 &\equiv 5 \bmod 7, & 2+2 &\equiv 1 \bmod 7 \\ 2+4 &\equiv 6 \bmod 7, & 4+4 &\equiv 1 \bmod 7 \end{aligned}$$

Since only $n^2 \in [0]_7$ and $m^2 \in [0]_7$ gives a sum of 0, from part (a), $n \equiv 0 \bmod 7$ and $m \equiv 0 \bmod 7$, implies that m and n are both divisible by 7.

(c) No. For $a = 1, b = 2, c = 3$, $a^2 + b^2 + c^2 \equiv 1 + 4 + 2 \equiv 0 (\text{mod } 7)$.

Question 6

(a) Since a function that maps to itself is one to one and onto, $f : A \to A$ is a bijection
$\Rightarrow A \sim A$, $\sim$ is reflexive.
If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.
Therefore, $A \sim B \Leftrightarrow B \sim A$. $\sim$ is symmetric.
If $f : A \to B$ and $g : B \to C$ are both bijections, Let $h = g \circ f$. We want to show that $h : A \to C$ is also a bijection.

(Injectivity) Let $a_1, a_2 \in A$, we want to show that if $h(a_1) = h(a_2)$, then $a_1 = a_2$.

$$\begin{aligned} h(a_1) = h(a_2) \quad &\Rightarrow g \circ f(a_1) = g \circ f(a_2) \\ &\Rightarrow f(a_1) = f(a_2) \quad (\text{since } g \text{ is injective}) \\ &\Rightarrow a_1 = a_2 \quad (\text{since } f \text{ is injective}) \end{aligned}$$

Therefore h is an injective function from A to C.

(Surjectivity) Let $c \in C$, since g is surjective function, there exists $b \in B$ such that $g(b) = c$. Since f is surjective function, there exists $a \in A$ such that $f(a) = b$. Therefore $\forall c \in C$, there exists $a \in A$ such that

$$h(a) = g \circ f(a) = g(b) = c$$

Therefore h is an surjective function from A to C.

Therefore $\sim$ is an equivalence relation.

(b) First of all, we try to list the elements of $S(U)$.

$$S(U) = \{\{[0]_3\}, \{[1]_3\}, \{[2]_3\}, \{[0]_3, [1]_3\}, \{[0]_3, [2]_3\}, \{[1]_3, [2]_3\}, \{[0]_3, [1]_3, [2]_3\}\}$$

If there exists a bijection, $f : A \to B$, then the cardinality of A and B must be the same. Hence there are in total 3 different equivalence class on $S(U)$. They are

$$[\{[0]_3\}] = \{\{[0]_3\}, \{[1]_3\}, \{[2]_3\}\}$$

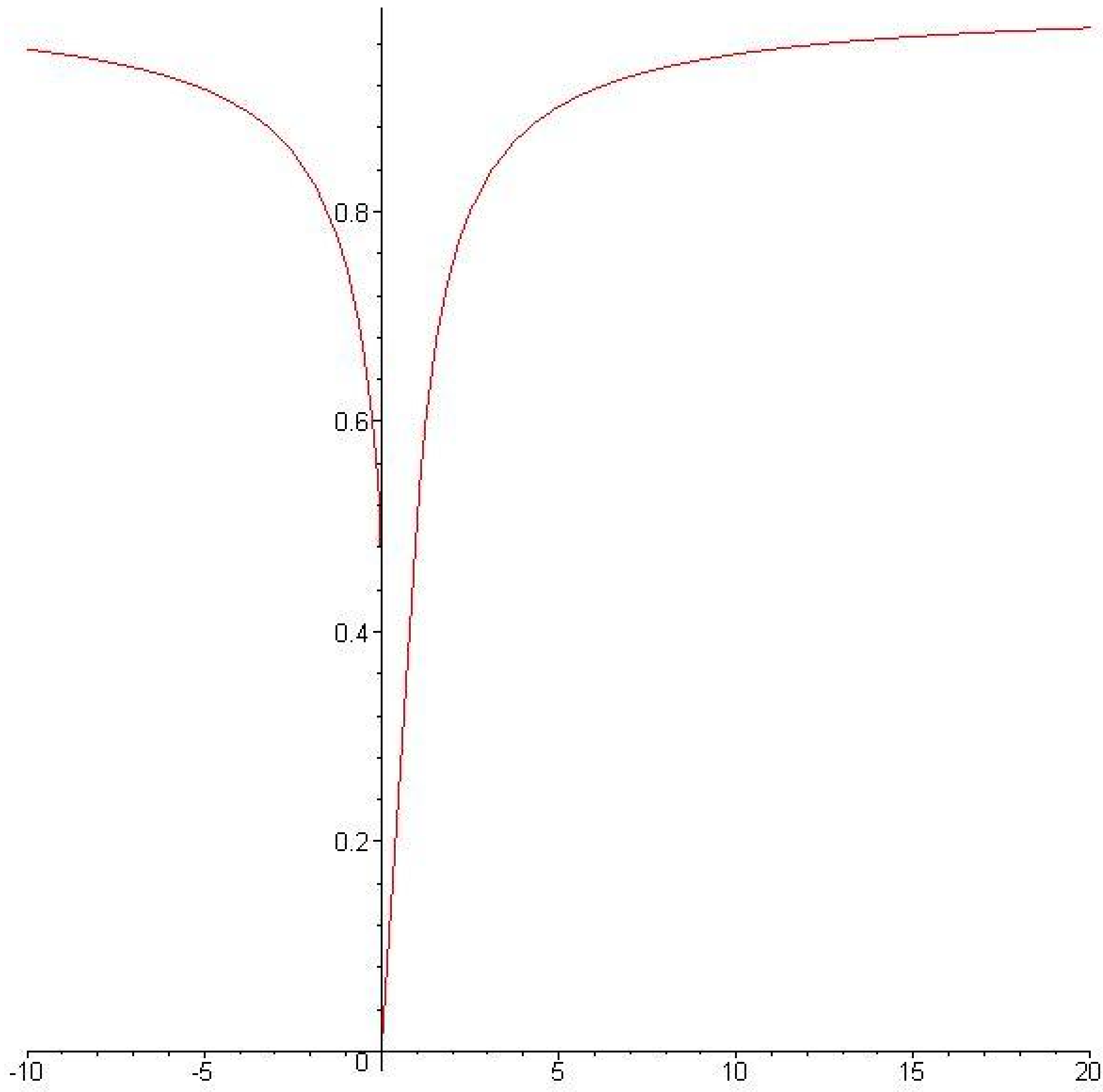
$$[\{[0]_3, [1]_3\}] = \{\{[0]_3, [1]_3\}, \{[0]_3, [2]_3\}, \{[1]_3, [2]_3\}\}$$
$$[\{[0]_3, [1]_3, [2]_3\}] = \{\{[0]_3, [1]_3, [2]_3\}\}$$

Question 7

(a) Yes. For all $x \in h(A \cup B)$, either $x \in h(A)$ or $x \in h(B)$, and in the first case $h(x) = f(x)$ covers the entire range of A, since f is surjective, and in the second case $h(x) = g(x)$ covers the entire range of B, since g is surjective, the range of h covers the union of A and B, h is a surjection.

(b) No. First of all, note that the statement is true when A and B are both finite sets. Thus, we want to find some sets A and B such that they are infinite sets, so that we can arrive to a function h which is not injective.
Consider $A = [0, \infty)$ and $B = (-\infty, 1]$. We define f and g as follows

$$f(x) = \begin{cases} \frac{1}{2}x & \text{if } x \in [0,1], \\ 1 - \frac{1}{2x} & \text{if } x \in (1, \infty). \end{cases} \quad \& \quad g(x) = \begin{cases} \frac{1}{2}x & \text{if } x \in [0,1], \\ 1 + \frac{1}{2(x-1)} & \text{if } x \in (-\infty, 0). \end{cases}$$



Note that f and g are both injective functions. However, h is not injective.

$$h(x) = \begin{cases} 1 + \frac{1}{2(x-1)} & \text{if } x \in (-\infty, 0) \\ \frac{1}{2}x & \text{if } x \in [0,1], \\ 1 - \frac{1}{2x} & \text{if } x \in (1, \infty). \end{cases}$$

For instance, $x_1 = 2 \neq -1 = x_2$ but $h(x_1) = \frac{3}{4} = h(x_2)$.

Question 8

(a) Since p is a prime greater than 3, $p \equiv 1 \bmod 3$ or $p \equiv 2 \bmod 3$. When $p \equiv 1 \bmod 3$, there exists $k \in \mathbb{Z}$ such that $p - 1 = 3k$,

$$2p - 2 = 6k \Rightarrow 2p + 1 = 2p - 2 + 3 = 6k + 3 = 3(2k + 1)$$

$2p+1$ is divisible by 3, thus it is not a prime number. When $p \equiv 2 \bmod 3$, there exists $m \in \mathbb{Z}$ such that $p - 2 = 3m$,

$$4p - 8 = 12m \Rightarrow 4p + 1 = 4p - 8 + 9 = 12m + 9 = 3(4m + 1)$$

$4p + 1$ is divisible by 3, thus it is not a prime number.
Therefore they cannot be prime at the same time.

(b) Consider an integer $n \in \mathbb{Z}^+$. We split the cases of n into two.

(Case 1) n is not a perfect square.
Since n is not a perfect square, i.e $\sqrt{n} \notin \mathbb{Z}^+$, by considering the property of divisors, if a is a divisor of n, then there exists $b \in \mathbb{Z}$ such that $a \times b = n$. WLOG, we assume that $a < b$. In other words, b is the other divisor of n that pairs up with a. Now, we might want to study how many pairs of such divisors are there for n. Since we know that there is a b divisors corresponding to a, then we just need to consider those divisors that are less than $\sqrt{n}$. By the following claim:

Claim: There is no 2 paired-distinct divisors of n such that both of them larger than $\sqrt{n}$.
Assume to the contrary that there are 2 divisors, a and b of n such that both of them larger than $\sqrt{n}$, ie.

$$a > \sqrt{n} \quad \& \quad b > \sqrt{n}, \quad \Rightarrow \quad a \times b > \sqrt{n} \times \sqrt{n} = n$$

We obtain a contradiction. Therefore one of the paired divisors must be less than $\sqrt{n}$ and the other divisor must be greater than $\sqrt{n}$.
Now consider the set of divisors that are less than $\sqrt{n}$, there are at most $\sqrt{n}$ of divisors of n. By the 'pairing' that we have discussed earlier, there are in total at most $2\sqrt{n}$ divisors of n.

(Case 2) n is a perfect square.
Since n is a perfect square, there exists $k \in \mathbb{Z}^+$ such that $\sqrt{n} = k$. As similar in argument in Case 1, we now need to count divisors of n that are not equal to k. By similar argument as above, there are at most $k - 1$ divisors of n that are less than k. Therefore, considering the paired up divisors of n, there are in total at most $2(k - 1) + 1$ divisors of n. The counting of the '1' is the counting of k as a divisor of n. Therefore the number of divisors of n is at most

$$2k - 2 + 1 = 2k - 1 \leq 2k = 2\sqrt{n}$$