NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Associate Professor Victor Tan

solutions prepared by Joseph Andreas

MA1100 Fundamental Concepts of Mathematics
AY 2010/2011 Sem 1

Question 1

(a) ($\Rightarrow$) Suppose $(u, v) \in (A \times C) - (B \times C)$, then we can deduce that $(u, v) \in (A \times C)$ but $(u, v) \notin (B \times C)$. From the first statement, we deduce that $u \in A$ and $v \in C$. Now, if $u \in B$, the fact $v \in C$ implies $(u, v) \in (B \times C)$, a contradiction. Hence, $u \notin B$, and together with $u \in A$, we deduce that $u \in (A - B)$. Finally, since $v \in C$, we conclude $(u, v) \in (A - B) \times C$.
($\Leftarrow$) Suppose $(u, v) \in (A - B) \times C$. Then we have $v \in C$ and $u \in (A - B)$, which implies $u \in A$ and $u \notin B$. From there, we get $(u, v) \in (A \times C)$ and $(u, v) \notin (B \times C)$. Thus, we conclude $(u, v) \in (A \times C) - (B \times C)$.

(b) The answer is no. Take $A = \{1, 2, 3\}$ and $B = \{1, 4\}$. We get $A - B = \{2, 3\}$. Now, take a set $S = \{1, 2\}$. Notice that $S \in \mathcal{P}(A)$ and $S \notin \mathcal{P}(B)$, so we conclude $S \in (\mathcal{P}(A) - \mathcal{P}(B))$. However, clearly, $S \notin \mathcal{P}(A - B)$.

Question 2

(a) Let $P(n)$ be the statement that $f_2 + f_4 + \ldots + f_{2n} = f_{2n+1} - 1$.

- Base step :
  Since $f_2 = 1$ and $f_3 = f_2 + f_1 = 2$, we see that $f_2 = f_3 - 1$, so $P(1)$ is true.
- Inductive step :
  Suppose $P(k)$ is true for some positive integer k. Then we have $f_2 + f_4 + \ldots f_{2k} = f_{2k+1} - 1$ which implies $f_2 + f_4 + \ldots f_{2k} + f_{2k+2} = f_{2k+1} + f_{2k+2} - 1 = f_{2k+3} - 1$. Hence, $P(k + 1)$ is true.

By the principle of mathematical induction, we conclude $P(n)$ is true for all positive integer n.

(b) Answer : $U = \{4k - 1 | k \in \mathbb{N}\}$. Suppose there is a positive integer that is congruent to 3 in modulo 4 and that is not in U. By Well Ordering Principle, we can pick such smallest integer $n = 4l - 1$. Note that $l > 1$ since $3 \in U$ by the definition of our problem. Therefore, $4l - 5 > 0$, so we conclude $4l - 5 \in U$. However, we get $4l - 5 + 4 \in U$, a contradiction. Thus, such positive integer does not exist, so every positive integer that is congruent to 3 in modulo 4 is in U. Therefore, we have proven that U is the universal set we have proven $(\forall n \in U)P(n)$.

(c) Answer : $5, 6, 7, 8, 9, 10$. Firstly, since the inductive step only covered when $k \leq 7$, it follows that $k = 5, 6$ must be solved separately. Since the inductive step grows preserving parity, i.e if we put an even number k, and know that $P(k), P(k+2)$ are both true, then $k+4$ is still even. The case is similar for odd numbers. Furthermore, for even numbers, since every inductive step requires two previous steps to be true, then we need at least two even base cases outside 5 and 6. The same case happens for odd numbers. Hence, we need at least 4 base cases outside 5 and 6. Clearly, since the inductive step grows increasingly, i.e we need smaller numbers to prove larger ones, we conclude that base cases should be smallest possible. Thus, the numbers $5, 6, 7, 8, 9, 10$ are chosen. It is obvious that with such base cases, $P(n)$ is true for all $n \in \mathbb{N}$.

Question 3

(a) Assume that there are two congruence classes $[x]_7$ and $[y]_7$ in $\mathbb{Z}_7$ such that $[5]_7 \cdot [x]_7 = [5]_7 \cdot [y]_7 = [3]_7$. Then we have $5x \equiv 3 \pmod 7$ and $5y \equiv 3 \pmod 7$. Hence, $5x \equiv 5y \pmod 7$ which implies $7|5(x-y)$. Since $\gcd(7,5) = 1$, by Euclid Lemma we have $7|x-y$. Therefore, $x \equiv y \pmod 7$ which implies $[x]_7 = [y]_7$. Thus, there are only one possible congruence class satisfying our problem. Now since $5 \cdot 2 \equiv 3 \pmod 7$, we conclude that $[2]_7$ is all congruence class satisying $[5]_7 \cdot [x]_7 = [5]_7$.

(b) Suppose we have $a + b \equiv ab \pmod 4$. It follows that $ab - a - b + 1 \equiv 1 \pmod 4$, so we get $(a-1)(b-1) \equiv 1 \pmod 4$. Thus, $(a-1)(b-1)$ is an odd number which in turn leads that both $a-1$ and $b-1$ are odd numbers. We check all possible cases of $a-1$ and $b-1$.

- If $a - 1 \equiv 1 \pmod 4$, then $1.(b-1) \equiv 1 \pmod 4$ which implies $b - 1 \equiv 1 \pmod 4$. In this case, $a \equiv b \equiv 2 \pmod 4$.
- If $a - 1 \equiv 3 \pmod 4$, then $3.(b-1) \equiv 1 \pmod 4$ which implies $b - 1 \equiv 3 \pmod 4$. In this case, $a \equiv b \equiv 0 \pmod 4$.

We conclude that if $a + b \equiv ab \pmod 4$ then either $a \equiv b \equiv 2 \pmod 4$ or $a \equiv b \equiv 0 \pmod 4$. Alternatively, one can work directly using addition and multiplication table of a and b in $\mathbb{Z}_4$ as described in the hint.

Question 4

(a) $R = \{(1,1), (1,3), (3,1), (3,3), (2,2), (2,4), (4,2), (4,4)\}$.

(b) (i) Let us check three properties of equivalence relation.

Reflexive Take any positive integer x, we get x^2 is a perfect square. Thus, $x \sim x$. We conclude, S is reflexive.

Symmetric Take any two positive integers a, b. If $a \sim b$ then $ab = k^2$ for some positive integer k. Then $ba = k^2$ so $b \sim a$. Thus, S is symmetric.

Transitivity Take any three positive integers a, b, c. Suppose $a \sim b$ and $b \sim c$. Then we have $ab = k^2$ abd $bc = l^2$ for some positive integers k and l. We get $ab^2c = k^2l^2$ which implies $ac = \left(\frac{kl}{b}\right)^2$. However, we still need to prove that $\frac{kl}{b}$ is indeed a positive integer or in other words, $b|kl$.
Claim : $b|kl$.
Proof : Let $b = p_1^{a_1} \cdot p_2^{a_2} \cdots p_m^{a_m}$ be the prime representation of b. Since for any $i \neq j$, $\gcd(p_i, p_j) = 1$, we conclude that $b|kl$ if and only if $p_i^{a_i}|kl$ for all $i = 1, 2, \dots, m$. Now take any $i \in \{1, 2, \dots, m\}$. For simplicity of writing, let $p = p_i$ and $t = a_i$. We shall show that $p^t|kl$. Notice that $p^t|b$. Together with $ab = k^2$ and $bc = l^2$, we have $p^t|k^2$ and $p^t|l^2$. Thus $(p^t)^2|(kl)^2$ which implies the prime factorization of $(kl)^2$ must contain at least $2t$ number of times of p. Hence the prime factorization of kl must contain at least t number of times of p. Thus, $p^t|kl$. Therefore, the claim is proved.
Thus, S is transitive.

Since S satisfies all three properties of equivalence relation, we conclude that S is an equivalence relation.

(ii) We define a positive integer n to be *squarefree* if it is not divisible by any other perfect square except 1. Some example of squarefree positive integers are $1, 2, 3, 5, 6, 7, 10$. In other words,

if n is squarefree, either $n = 1$ or its prime factorization is $n = p_1p_2 \dots p_k$. Let U be the set of all squarefree positive integers.
Let $T = \{[x]_S | x \in U\}$. (we list some elements of T to give the reader some example about our set T. $T = \{[1]_S, [2]_S, [3]_S, [5]_S, [6]_S, [7]_S, [10]_S, \dots\}$)
Claim : T is the set of all equivalence classes of S.
Proof of claim : We shall prove that T is a partition of $\mathbb{N}$.

- Firstly, for every $[x]_S \in T$, we see that $x \in [x]_S$. Hence, all elements of T are non-empty sets.
- Secondly, for every positive integer n, we can factorize $n = p_1^{a_1}p_2^{a_2} \dots p_k^{a_k}$. For each $i = 1, 2, \dots, k$ define $b_i = 1$ if a_i is odd, and $b_i = 0$ if a_i is even. Let $m = p_1^{b_1}p_2^{b_2} \dots p_k^{b_k}$. Since $b_i \leq 1$ for each i, we conclude that m is squarefree. Thus, $[m]_S \in T$. Furthermore, $mn = p_1^{a_1+b_1}p_2^{a_2+b_2} \dots p_k^{a_k+b_k}$ and since $a_i + b_i$ is even for each $i = 1, 2, \dots, k$, we get mn is a square. Hence, $n \in [m]_S$. We conclude that every positive integer is in some element of T. Therefore, the union of all elements of T is $\mathbb{N}$.
- Thirdly, suppose $x \neq y$ are two squarefree positive integers. Assume that $u \in [x]_S$ and $u \in [y]_S$. Then, we get ux and uy are both square of some positive integers. We may write $ux = a^2$ and $uy = b^2$ for some positive integers a, b. On the other hand, since $x \neq y$ and x, y are squarefree, then there must be a prime p such that $p \mid x$ but $p \nmid y$ or $p \mid y$ but $p \nmid y$, as otherwise the prime factorization of x and y would be exactly the same, a contradiction to $x \neq y$. WLOG, there is a prime p such that $p \mid x$ but $p \nmid y$. Since $ux = a^2$, then u must have odd number of p factors in its prime factorization. However since $p \nmid y$, we have uy have also odd number of p factors in its prime factorization. Therefore uy cannot be a square. But $uy = b^2$ for some b, contradiction. Therefore, our assumption is false, thus any two different elements of T are disjoint.

It follows that our set T satisfies three properties of being a partition of $\mathbb{N}$. Therefore, T is a set of all equivalence classes of S. Claim proved.
Finally, we have all equivalence classes of S are all elements of T, namely all $[x]_S$ with x being a squarefree integer.

Question 5

(a) Since $\sqrt{2}$ is irrational, it follows that $n + \sqrt{2}$ is irrational for each positive integer n. Thus, all elements of the infinite set $S_1 = \{n + \sqrt{2} \mid n \in \mathbb{N}\}$ are irrational. Furthermore, the function $f : \mathbb{N} \to S_1$ with $f(n) = n + \sqrt{2}$ for each positive integer n is clearly bijective. Hence, S_1 is denumerable.
For any positive integer n, $0 < \frac{1}{n+1} < 1$. Thus, all elements of the infinite set $S_2 = \{\frac{1}{n+1} \mid n \in \mathbb{N}\}$ are within the open interval $(0, 1)$. Furthermore, the function $g : \mathbb{N} \to S_2$ with $g(n) = \frac{1}{n+1}$ for each positive integer n is clearly bijective. Hence, S_2 is denumerable.

(b) False. Let $\mathbb{I}^+$ be the set of positive irrational numbers and $\mathbb{I}^-$ be the set of negative real numbers. Note that both $\mathbb{I}^+$ and $\mathbb{I}^-$ are uncountable. Define $A = \mathbb{Q} \cup \mathbb{I}^+$ and $B = \mathbb{Q} \cup \mathbb{I}^-$. Note that A and B are uncountable. Furthermore, $A \cap B = \mathbb{Q}$ is infinite. But, $\mathbb{Q}$ is countable, contradiction.

Question 6

(a) **Injectivity** Note that $f(a, b) = f(c, d)$ implies $(2a + 1, 2b - 1) = (2c + 1, 2d - 1)$ which implies $2a + 1 = 2c + 1$ and $2b - 1 = 2d - 1$. Thus, $a = c, b = d$ or in other words $(a, b) = (c, d)$. Thus, f is injective.

Surjectivity Let (a, b) be an element in codomain. Then we have $f(\frac{a-1}{2}, \frac{b+1}{2}) = (a, b)$. Hence, f is surjective.

We conclude that f is bijective.

(b) (i) $h(h(x)) = h(\frac{2x}{x-2}) = \frac{2\frac{2x}{x-2}}{\frac{2x}{x-2}-2} = \frac{\frac{4x}{x-2}}{\frac{4}{x-2}} = x$. Since $h(h(x)) = x$, it's obvious that h is surjective. Furthermore, $h(a) = h(b)$ implies $h(h(a)) = h(h(b))$ that implies $a = b$. Thus, h is injective. Therefore, h is bijective. Since $h(h(x)) = x$ and $h(h^{-1}(x)) = x$, by injectivity we have $h^{-1}(x) = h(x) = \frac{2x}{x-2}$ for each $x \in \mathbb{R} - \{2\}$.

(ii) Let T be the range of function h. Notice that $h(x) = 2$ leads no solution. Furthermore, $h(x)$ is rational if x is rational, hence $T \subseteq \mathbb{Q} - \{2\}$. Suppose $x \in \mathbb{Q} - \{2\}$. Then we get $\frac{2x}{x-2}$ is rational and not equal to 2. Furthermore, we have $h(\frac{2x}{x-2}) = \frac{2\frac{2x}{x-2}}{\frac{2x}{x-2}-2} = \frac{\frac{4x}{x-2}}{\frac{4}{x-2}} = x$. Thus, $\mathbb{Q} - \{2\} \subseteq T$. Thus T, the range of h is equal to $\mathbb{Q} - \{2\}$.

Question 7

(a) By Euclidean Algorithm, $54 = 33 + 21$. Next, $33 = 21 + 12$. Next, $21 = 12 + 9$. Next, $12 = 9 + 3$. Next, $9 = 3 \times 3 + 0$. Hence, $\gcd(54, 33) = 3$.
Next, $\gcd(54, 33) = 12 - 9 = 12 - (21 - 12) = 2 \times 12 - 21 = 2 \times (33 - 21) - 21 = 2 \times 33 - 3 \times 21 = 2 \times 33 - 3 \times (54 - 33) = 5 \times 33 - 3 \times 54$. Hence, $x = 5, y = -3$.

(b) Let $d = \gcd(p^2 + 1, (p + 1)^2)$. We have $\gcd(p^2 + 1, (p + 1)^2) = \gcd(p^2 + 1, p^2 + 2p + 1) = \gcd(p^2 + 1, p^2 + 2p + 1 - (p^2 + 1)) = \gcd(p^2 + 1, 2p)$. All factors of $2p$ are $1, 2, p, 2p$. Hence, d is one of $1, 2, p, 2p$. Since $p > 1$ it follows that $p \nmid p^2 + 1$. Hence, $d = 1$ or $d = 2$. Since both $p^2 + 1$ and $2p$ are even, we have $d = 2$ as desired.

(c) Let $p, p + 2, p + 4$ be three consecutive odd numbers that are primes. Since $p, p + 2, p + 4$ form a complete residue modulo 3 (i.e, congruent to 0, 1, 2 in some order), it follows that one of $p, p+2, p+4$ are divisible by 3. However, a prime that is divisible by 3 must be the 3 itself. Thus, either $p = 3$ or $p + 2 = 3$ or $p + 4 = 3$. The last equation is absurd, while $p + 2 = 3$ leads to $p = 1$, not a prime. Hence, $p = 3$. We conclude that we can't find another three consecutive odd numbers that are all primes except $3, 5, 7$.

Question 8

(a) Since $\bigcup_{i=1}^{\infty} A_i = \mathbb{Q}^+$, it follows that for each i, $A_i \subseteq \mathbb{Q}^+$. Thus, A_i is countable. Furthermore, $\bigcap_{i=1}^{\infty} A_i = \mathbb{N}$, it follows that, A_i has infinitely many elements. Thus, A_i is denumerable. Therefore, for each i, there exists a function $f : A_i \to \mathbb{N}$ that is a bijection.

(b) Let $B_i = \left\{\frac{a}{i+1} \mid \gcd(a, i + 1) = 1, a \in \mathbb{N}\right\}$. We shall prove that for each $i = 1, 2, \ldots$, if we define $A_i = \mathbb{N} \cup B_i$ then $\mathcal{C} = \{A_i \mid i \in \mathbb{N}\}$ satisfying all desired properties.

- Note that for each positive rational number $\frac{a}{b}$, first we may assume $\frac{a}{b}$ is in the lowest term. If $b = 1$, then $\frac{a}{b}$ is clearly an element on all A_i. If $b > 1$, then since $\gcd(a, b) = 1$, we get $\frac{a}{b} \in B_{b-1}$. Hence, $\frac{a}{b} \in A_{b-1}$. Hence, any positive rational number is an element of A_i for some i. Thus, $\bigcup_{i=1}^{\infty} A_i = \mathbb{Q}^+$.
- Suppose $x \in A_1$ and $x \in A_2$. If x is not a positive integer, then $x = \frac{p}{2}$ for some odd positive integer p. However, $\frac{p}{2}$ is itself not in A_2, contradiction. Thus, $A_1 \cap A_2 = \mathbb{N}$. Hence, $\bigcap_{i=1}^{\infty} A_i \subseteq \mathbb{N}$. On the other hand, every natural number is an element of A_i for each $i = 1, 2, \ldots$. Thus, every natural number is an element of $\bigcap_{i=1}^{\infty} A_i$. Thus, $\bigcap_{i=1}^{\infty} A_i = \mathbb{N}$

- Finally, we check that for every pair of different positive integers i and j, we have $A_i \nsubseteq A_j$. However, that is obvious since $\frac{1}{i+1}$ is clearly not an element of A_j as A_j contains only natural numbers and all fractions in the form of $\frac{a}{j+1}$.

Therefore $\mathcal{C} = \{A_i \mid i \in \mathbb{N}\}$ satisfying all desired properties.