NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Teo Wei Hao, Lee Yung Hei

MA1100 Basics of Mathematics
AY 2006/2007 Sem 1

Question 1

(a) True.

p	q	$p \wedge q$	$(\neg p) \wedge (\neg q)$	$(p \wedge q) \vee ((\neg p) \wedge (\neg q))$	$p \leftrightarrow q$
T	T	T	F	T	T
T	F	F	F	F	F
F	T	F	F	F	F
F	F	F	T	T	T

From the above truth table, we see that $p \leftrightarrow q$ and $(p \wedge q) \vee ((\neg p) \wedge (\neg q))$ are equivalent.

(b) False.
Let $P(x)$ and $Q(x)$ be the predicate "$x = 0$" and "$x = 1$" respectively. Since $P(0) \to Q(0)$ is false, $(\forall\, x \in \mathbb{R})[P(x) \to Q(x)]$ is false. Also as $P(x)$ is false for all $x \neq 0$, $(\forall\, x \in \mathbb{R})[P(x)]$ is false, and thus $(\forall\, x \in \mathbb{R})[P(x)] \to (\forall\, x \in \mathbb{R})[Q(x)]$ is true. Therefore $(\forall\, x \in \mathbb{R})[P(x) \to Q(x)]$ and $(\forall\, x \in \mathbb{R})[P(x)] \to (\forall\, x \in \mathbb{R})[Q(x)]$ are not equivalent.

(c) False.
Let $X = \emptyset$, we see that $\{\emptyset\} \nsubseteq X$.

(d) True.
For any set X, we have $\emptyset \subseteq X$. Thus $\emptyset \in \mathcal{P}(X)$, which give us $\{\emptyset\} \subseteq \mathcal{P}(X)$.

(e) True.
Assume on the contrary that $\alpha + \beta \in \mathbb{Q}$. Together with $\alpha \in \mathbb{Q}$, we have $\beta = (\alpha + \beta) + (-\alpha) \in \mathbb{Q}$, a contradiction. Thus $\alpha + \beta$ is irrational.

(f) False.
Let $\alpha = \sqrt{2}$, $\beta = -\sqrt{2}$. This give us α and β are irrational but $\alpha + \beta = 0$ is rational.

(g) False.
Let $a = 4$, $b = 2$, $c = 2$. This give us $a \mid bc$ but $a \nmid b$ and $a \nmid c$.

(h) False.
Let $a = 2$, $b = 2$, $c = 2$. This give us $a \mid c$ and $b \mid c$ but $ab \nmid c$.

(i) False.
Let $A = \{1\}$, $B = \{1, 2\}$ and $C = \{1\}$. We notice that $f : A \to B$ such that $f(1) = 1$, and $g : B \to C$ such that $g(b) = 1$ for $b = 1, 2$ are well-defined functions. This give us $g \circ f : A \to C$ which is surjective but f is not surjective.

(j) True.
For all $c \in C$, since $g \circ f$ is surjective, there exists $a \in A$ such that $(g \circ f)(a) = c$. Thus $g[f(a)] = c$, i.e. $f(a) \in B$ is a pre-image of $c \in C$ under g. Thus g is surjective.

Question 2

(a) Using Euclidean algorithm, we have

$$\begin{aligned} 2006 &= (194)(10) + 66 \\ 194 &= (66)(2) + 62 \\ 66 &= (62)(1) + 4 \\ 62 &= (4)(15) + 2 \\ 4 &= (2)(2). \end{aligned}$$

Thus $\gcd(2006, 194) = 2$.

(b) Using the equations generated in (2a.), we have,

$$\begin{aligned} 2 &= 62 - (4)(15) = 62 - [66 - (62)(1)](15) \\ &= (66)(-15) + (62)(16) = (66)(-15) + [194 - (66)(2)](16) \\ &= (194)(16) + (66)(-47) = (194)(16) + [2006 - (194)(10)](-47) \\ &= (2006)(-47) + (194)(486). \end{aligned}$$

And thus $10 = 5(2) = 5[(2006)(-47) + (194)(486)] = (2006)(-235) + (194)(2430)$. Therefore we have $(x, y) = (-235, 2430)$ to be one pair of integers that satisfy the condition.

(c) No.
Since $\gcd(2006, 194) = 2$, we have $2006s + 194t \equiv 0 \mod 2$, $\forall\ s, t \in \mathbb{Z}$. However, $17 \equiv 1 \mod 2$, and thus there does not exists $s, t \in \mathbb{Z}$ such that $2006s + 194t = 17$.

(d) From (2b.), we have $4 = 2(2) = 2[(2006)(-47) + (194)(486)] \equiv 2006(-94) \mod 194$.
Thus, $2006x \equiv 2006(-94) \mod 194$.
This give us $y \in \mathbb{Z}$ such that $2006x = 2006(-94) + 194y$, i.e. $y = \dfrac{1003}{97}(x - (-94))$.
Since $\gcd(97, 1003) = 1$, we have $97 \mid (x - (-94))$, i.e. $x \equiv -94 \mod 97$. Thus the only 2 possible $x \in \mathbb{Z}$ that satisfy $0 \leq x < 194$ are $x = -94 + (97) = 3$ and $x = -94 + 2(97) = 100$.

Question 3

(a) Let P_n be the statement $(a, b^n) = 1$, $n \in \mathbb{Z}^+$.
Since we are given that $(a, b) = 1$, we have P_1 to be true.

Assume P_k is true for some $k \in \mathbb{Z}^+$, i.e. $(a, b^k) = 1$. Then $\exists\ x_k, y_k \in \mathbb{Z}$ such that $x_k a + y_k b^k = 1$. Also since $(a, b) = 1$, there exists $x, y \in \mathbb{Z}$ such that $xa + yb = 1$. Thus,

$$\begin{aligned} 1 &= (x_k a + y_k b^k)(xa + yb) \\ &= (x_k xa + y_k x b^k + x_k yb)a + (y_k y)b^{k+1}. \end{aligned}$$

If we let $x_{k+1} = x_k xa + y_k x b^k + x_k yb$ and $y_{k+1} = y_k y$, we get $x_{k+1}a + y_{k+1}b^{k+1} = 1$. Together with the fact that $x_{k+1}, y_{k+1} \in \mathbb{Z}$, we have $(a, b^{k+1}) = 1$, i.e. p_{k+1} is true.

Therefore by Mathematical Induction, P_n is true for all $n \in \mathbb{Z}^+$.

(b) Using the result of (3a.), we see that for any $x, y \in \mathbb{Z}^+$, if $(x, y) = 1$, then $\forall\ n \in \mathbb{Z}^+$, we have $(x, y^n) = 1$. Since we have established that $(a, b^n) = 1$, we can let $x = b^n$, $y = a$, and this give us $\forall\ n \in \mathbb{Z}^+$, we have $(a^n, b^n) = 1$.

Question 4

(a) Let $f : X \to \mathbb{Z}_{\geq 0}$ be such that $f(A) = |A|$. $\forall\ n \in \mathbb{Z}_{\geq 0}$, consider $A_n = \{k \in \mathbb{Z}_{\geq 0} \mid k < n\}$.
This give us $f(A_n) = |A_n| = n$ for all $n \in \mathbb{Z}_{\geq 0}$.
Thus $A_n \in X$ is a pre-image of $n \in \mathbb{Z}_{\geq 0}$ under f, i.e. f is surjective.

Note: For this question, $\mathbb{N}$ is intended to include 0 by Prof Yang Yue, the lecturer of this module in 2006/2007. If it is not explicitly stated in some maths module in NUS, chances is that $\mathbb{N}$ always includes 0. Nevertheless, confirm with your Prof in doubts.

Tip: There are possibly infinitely many ways to define our f, even though it is hard to come out with a good one. Some examples are $f(A) =$ min/max element of A, $f(A) =$ sum of elements of A, etc. Even though these examples look abit wordy / not so mathematical, they do serve their purpose and should be employed if a good expression cannot be found in time during exam conditions.

(b) Yes.
To map [0,1] to (0,1), we realise that there are 2 extra points in [0,1] and we'll need to find a way to squeeze them into (0,1). So, the intuitive way to map $[0, 1]$ to $(0, 1)$ is to map $0 \to \frac{1}{2}$, $1 \to \frac{1}{3}$, $\frac{1}{2} \to \frac{1}{4}$, $\ldots$, $\frac{1}{k} \to \frac{1}{k+2}$, etc, and everything else remains the same.
This intuition lead us to come out with $f : [0, 1] \to (0, 1)$ such that

$$f(x) \quad = \quad \begin{cases} \frac{1}{2}, & x = 0; \\ \frac{1}{2+\frac{1}{x}}, & x = \dfrac{1}{k},\ k \in \mathbb{Z}^+; \\ x, & \text{otherwise.} \end{cases}$$

It direct to check that f is bijective. Therefore $[0, 1]$ and $(0, 1)$ have the same cardinality.

Note: The fact that "if A is a infinite set and B is a finite set, then $|A \cup B| = |A|$" is not proven in MA1100, but just a stated fact. Thus it will be the rationale to lead people saying "Yes" to this question (since we can have $A = (0, 1)$ and $B = \{0, 1\}$, which give us $A \cup B = [0, 1]$).

Reasonably, the construction of the function above is not required in the exam (which is not obvious and too hard for some of us), as stated in the question. However it is included by us just to convince the reader that our solution is valid. Nevertheless it is good to understand how the proof works, which give us some insight into the beauty of cardinality.

Question 5

(a) $\forall\ x \in A$, since E_1 and E_2 are reflexive, $(x, x) \in E_1$ and $(x, x) \in E_2$. This give us $(x, x) \in E_1 \cap E_2$, and so $E_1 \cap E_2$ is reflexive.

$\forall\ x, y \in A$ such that $(x, y) \in E_1 \cap E_2$, we have $(x, y) \in E_1$ and $(x, y) \in E_2$. Since E_1 and E_2 are symmetric, $(y, x) \in E_1$ and $(y, x) \in E_2$. Thus $(y, x) \in E_1 \cap E_2$, and so $E_1 \cap E_2$ is symmetric.

$\forall\ x, y, z \in A$ such that $\{(x, y), (y, z)\} \subseteq E_1 \cap E_2$, we have $\{(x, y), (y, z)\} \subseteq E_1$ and $\{(x, y), (y, z)\} \subseteq E_2$. Since E_1 and E_2 are transitive, $(x, z) \in E_1$ and $(x, z) \in E_2$. Thus $(x, z) \in E_1 \cap E_2$, and so $E_1 \cap E_2$ is transitive.

Therefore $E_1 \cap E_2$ is an equivalent relation on A.

(b) Let $i_n = \dfrac{n(n+1)}{2}$ be the n-th triangle number, $n \in \mathbb{Z}^+$, and also let $i_0 = 0$.

Let us define $A_n = \{x \in \mathbb{Z}_{\geq 0} \mid i_{n-1} \leq x < i_n\}$. We have $|A_n| = \dfrac{n(n+1)}{2} - \dfrac{(n-1)n}{2} = n$.
Effectively, this give us $A_1 = \{0\}$, $A_2 = \{1, 2\}$, $A_3 = \{3, 4, 5\}$, $A_4 = \{6, 7, 8, 9\}$, etc.
Therefore $Q = \{A_n \mid n \in \mathbb{Z}^+\}$ is a partition of $\mathbb{Z}_{\geq 0}$.

This partition Q will induce an equivalence relation E as follows:-
$(x, y) \in E$ iff there exists $A \in Q$, such that $x \in A$ and $y \in A$.

Thus for any $k \in \mathbb{Z}^+$, we have $[i_k]_E = A_k$, which has k elements.
Thus E is an equivalent relation that satisfy the properties.

Question 6

(a) Assume on the contrary that there are only a total of $n \in \mathbb{Z}^+$ prime numbers, $p_1, p_2, \ldots, p_n$, with $p_i \equiv 2 \mod 3$, $i = 1, 2, \ldots, n$. Let $k = 3p_1p_2 \cdots p_n$.
Notice that $\gcd(k, k-1) = 1$. Since $p_i \mid k$ for all $i = 1, 2, \ldots, n$, we have $p_i \nmid k - 1$. Similarly, $3 \nmid k - 1$. Thus $k - 1$ has no factors of 0 and 2 $\mod 3$, and so $k - 1 = q_1q_2 \cdots q_m$, $m \in \mathbb{Z}^+$, where q_i are prime numbers such that $q_i \equiv 1 \mod 3$, $i = 1, 2, \ldots, m$. However $k - 1 \equiv 2 \mod 3$, but $q_1q_2 \cdots q_m \equiv (1)^m = 1 \mod 3$, a contradiction. Therefore there are infinitely many prime number p with $p \equiv 2 \mod 3$.

(b) Assume on the contrary that such a prime number does not exists for $n \geq 3$. Consider $n! - 1$. Again notice that $\gcd(n!, n! - 1) = 1$. Let q be a prime number such that $q \mid (n! - 1)$, which give us $q \leq n! - 1$. Since there is no prime number such that $n < q \leq n! - 1$, we have $q \leq n$. However this will implies that $q \mid n!$, which give us $q \nmid (n! - 1)$, a contradiction.

Therefore for $n \geq 3$, there exists a prime number p such that $n < p < n!$.