THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5510 Foundation of Advanced Mathematics 2017-2018
Suggested Solution to Final Exmaination

1. Find an integer x such that

$$\begin{aligned} x &\equiv 14 (\bmod 18) \\ x &\equiv 5 (\bmod 25) \end{aligned}$$

Ans:

By extended Euclidean Algorithm, we have

$$18 \times 7 + 25 \times (-5) = 1$$

By Chinese Remainder Theorem, $x \equiv 14 \times [25 \times (-5)] + 5 \times (18 \times 7) \equiv -1120 \equiv 230 (\bmod 450)$.

2. (a) Let n be a positive integer.
   Show that if $a \equiv a' (\bmod n)$ and $b \equiv b' (\bmod n)$, then $ab \equiv a'b' (\bmod n)$.
   (b) Find $\varphi(18)$, where φ is the Euler's phi function.
   Hence, or otherwise, find the remainder if 11^{200} is divided by 18.
   (c) Find an integer x such that $0 \leq x < 79$ and $23x \equiv 3 (\bmod 79)$.

Ans:

(a) By assumption, we have $a = a' + nk$ and $b = b' + np$ for some integers k and p. Then,

$$\begin{aligned} ab &= (a' + nk)(b' + np) \\ &= a'b' + n(kb' + pa' + npk) \end{aligned}$$

where $kb' + pa' + npk$ is an integer. Therefore, $ab \equiv a'b' (\bmod n)$.

(b) The positive integers that is less than 18 and relatively prime to 18 are 1, 6, 7, 11, 13 and 17, so $\varphi(18) = 6$.
Then, $11^{200} \equiv (11^6)^{33} \times 11^2 \equiv 1 \times 121 \equiv 13 (\bmod 18)$.

(c) By extended Euclidean Algorithm, we have

$$7 \times 79 - 24 \times 23 = 1$$

Then,

$$\begin{aligned} 21 \times 79 - 72 \times 23 &= 3 \\ 23 \times (-72) &\equiv 3 (\bmod 79) \\ 23 \times 7 &\equiv 3 (\bmod 79) \end{aligned}$$

Therefore, $x = 7$.

3. Let A, B and C be sets. Suppose that $f : B \to C$ and $g : A \to B$ are two bijective functions.
   Show that $f \circ g : A \to C$ is a bijective function.
   Let $x_1, x_2 \in A$ such that $(f \circ g)(x_1) = (f \circ g)(x_2)$, i.e. $f(g(x_1)) = f(g(x_2))$.

Since f is injective, $g(x_1) = g(x_2)$. Then, since g is injective, $x_1 = x_2$.

Therefore $f \circ g$ is injective.

Let $y \in C$. Since f is surjective, there exists $w \in B$ such that $f(w) = y$.

Also, since g is surjective, there exists $x \in A$ such that $g(x) = w$.

Then, we have $(f \circ g)(x) = f(g(x)) = f(w) = y$ and so $f \circ g$ is surjective.

4. (a) By constructing an explicit bijective function $f : [0, 1) \to (0, 1)$, show that both sets $[0, 1)$ and $(0, 1)$ have the same cardinality.
   (b) Show that both sets $(-1, 0) \cup (0, 1)$ and $(-1, 1)$ have the same cardinality.
   (c) Let $a, b, c \in \mathbb{R}$ such that $a < b < c$. Show that the sets $(a, b) \cup (b, c)$ and (a, c) have the same cardinality.

Ans:

(a) Let $a_n = 1 - \dfrac{1}{2^n}$ where $n = 0, 1, 2, \ldots$. Define a function $f : [0, 1) \to (0, 1)$ by

$$f(x) = \begin{cases} a_{n+1} & \text{if } x = a_n; \\ x & \text{otherwise.} \end{cases}$$

Then, f is a bijective function and so $[0, 1)$ and $(0, 1)$ have the same cardinality.

(b) Let $g : (-1, 1) \to (-1, 0) \cup (0, 1)$ be a function defined by

$$g(x) = \begin{cases} f(x) & \text{if } \quad 0 \le x < 1; \\ x & \text{if } \quad -1 < x < 0. \end{cases}$$

By the construction of the function and the fact that f is a bijective function, g is also a bijective function. Therefore, both sets $(-1, 0) \cup (0, 1)$ and $(-1, 1)$ have the same cardinality.

(c) Let $h_1 : (-1, 0) \cup (0, 1) \to (a, b) \cup (b, c)$ be a function defined by

$$h_1(x) = \begin{cases} b + (c - b)x & \text{if } \quad 0 < x < 1; \\ b + (b - a)x & \text{if } \quad -1 < x < 0. \end{cases}$$

Also, let $h_2 : (-1, 1) \to (a, c)$ be a function defined by $h_2(x) = c + \dfrac{(c - a)(x - 1)}{2}$. Note that both h_1 and h_2 are bijective functions. Then, $h_1 \circ g \circ h_2^{-1}$ is a bijective function from (a, c) to $(a, b) \cup (b, c)$ which shows that the sets $(a, b) \cup (b, c)$ and (a, c) have the same cardinality.

5. (a) Let A be a subset of $\mathbb{R}$. State the definition of a cluster point of A.
   (b) Let A be a subset of $\mathbb{R}$, c be a cluster point of A, and $f : A \to \mathbb{R}$ be a function.
   State the definition of $\lim_{x \to c} f(x) = L$, where L is a real number.
   (c) By using the definition stated in (b), show that
      i. $\lim_{x \to 3} 2x + 1 = 7$.
      ii. $\lim_{x \to c} x^2 + x = c^2 + c$, where c is a real number.

Ans:

(a) Let A be a subset of $\mathbb{R}$. c is a cluster point of A if for all $\delta > 0$, there exists $x \in A \backslash \{c\}$ such that $|x - c| < \delta$.

(b) $\lim_{x \to c} f(x) = L$ if for all $\epsilon > 0$, there exists $\delta > 0$ such that for all $x \in A$ with $0 < |x - c| < \delta$, we have $|f(x) - L| < \epsilon$.

(c) i. Let $\epsilon > 0$, take $\delta = \frac{\epsilon}{2} > 0$.
Then, for all $0 < |x - 3| < \delta = \frac{\epsilon}{2}$, we have

$$-\frac{\epsilon}{2} < x - 3 < \frac{\epsilon}{2}$$
$$-\epsilon < 2x - 6 < \epsilon$$
$$-\epsilon < (2x + 1) - 7 < \epsilon$$
$$|(2x + 1) - 7| < \epsilon$$

Therefore, $\lim_{x \to 3} 2x + 1 = 7$.

ii. Let $\epsilon > 0$, take $\delta = \min\{1, \frac{\epsilon}{2|c| + 2}\} > 0$.
Then, for all $0 < |x - c| < \frac{\epsilon}{2|c| + 2}$, we have

$$|x - c| < \delta \leq \frac{\epsilon}{2|c| + 2}$$

and

$$|x - c| < \delta \leq 1$$
$$-1 < x - c < 1$$
$$-2|c| - 2 \leq 2c - 1 < x + c + 1 < 2c + 2 \leq 2|c| + 2$$
$$|x + c + 1| < 2|c| + 2$$

Thus,

$$\begin{aligned} |(x^2 + x) - (c^2 + c)| &= |x - c||x + c + 1| \\ &< \frac{\epsilon}{2|c| + 2} \cdot (2|c| + 2) \\ &= \epsilon \end{aligned}$$

Therefore, $\lim_{x \to c} x^2 + x = c^2 + c$.

6. (a) Let A be a subset of $\mathbb{R}$ and c is a cluster point of A.
Suppose that $f, g : A \to \mathbb{R}$ are functions such that f is bounded on A, i.e. there exists $M > 0$ such that $|f(x)| \leq M$ for all $x \in A$, and $\lim_{x \to c} g(x) = 0$.
Show that $\lim_{x \to c} f(x)g(x) = 0$.

(b) By using the result in (a), evaluate $\lim_{x \to 0} x^2 \cos(\frac{1}{x})$.

Ans:

(a) Let $\epsilon > 0$. Given that $\lim_{x \to c} g(x) = 0$, so there exists $\delta > 0$ such that for all $x \in A$ with $0 < |x - c| < \delta$, we have $|g(x) - 0| < \frac{\epsilon}{M}$. Then,

$$|f(x)g(x) - 0| \leq M|g(x)| < M \cdot \frac{\epsilon}{M} = \epsilon$$

Therefore, $\lim_{x \to c} f(x)g(x) = 0$.

(b) By considering $c = 0$, $f(x) = \cos(\frac{1}{x})$ and $g(x) = x^2$. Then, both f and g are functions defined on $\mathbb{R}\backslash\{0\}$.
Note that 0 is a cluster point of $\mathbb{R}\backslash\{0\}$, $|f(x)| \leq 1$ for all $x \in \mathbb{R}\backslash\{0\}$ and $\lim_{x \to 0} g(x) = 0$.
Therefore, by the result in (a), we have $\lim_{x \to 0} x^2 \cos(\frac{1}{x}) = 0$.

7. (a) Let $m, n \in \mathbb{N}$. State the definition of $m \leq n$.

   (b) Let $m, n \in \mathbb{N}$. Prove that if $m \leq n$, then $m^+ \leq n^+$, where $m^+ = m \cup \{m\}$ and $n^+ = n \cup \{n\}$ are successor sets of m and n respectively.

   (c) Let $m, n, p \in \mathbb{N}$. Prove that if $m \leq n$, then $m + p \leq n + p$.
   (Hint: Using mathematical induction on p.)

Ans:

(a) $m \leq n$ if m is a subset of n.

(b) Suppose that $m \leq n$, i.e. $m \subseteq n$.
Let $x \in m^+ = m \cup \{m\}$. Then, there are two cases:
- Case 1: $x \in m$, then $x \in m \subseteq n$ and so $x \in n^+$.
- Case 2: $x \in \{m\}$, i.e. $x = m$, then $x \subseteq n \subsetneq n^+$. Therefore, $x \in n^+$.

We have $m^+ \subseteq n^+$ and so $m^+ \leq n^+$.

(c) When $p = 0$, it is obvious that $m + 0 = m \leq n = n + 0$.
Assume that for a natural number p, if m and n are natural numbers such that $m \leq n$, then we have $m + p \leq n + p$. Then, by (b) and the definition of addition,

$$m + p^+ = (m + p)^+ \leq (n + p)^+ = n + p^+.$$

By mathematical induction, let m, n and p be natural numbers, if $m \leq n$, then we have $m + p \leq n + p$.

8. Suppose that $+$ and $\cdot$ are usual addition and multiplication on $\mathbb{N}$ respectively.
Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ such that $(m, n) \sim (p, q)$ if and only if $m + q = p + n$.
An addition $\boxplus$ on $\mathbb{N} \times \mathbb{N}$ is defined by

$$(m, n) \boxplus (p, q) = (m + p, n + q)$$

and a multiplication $\boxdot$ on $\mathbb{N} \times \mathbb{N}$ is defined by

$$(m, n) \boxdot (p, q) = (m \cdot p + n \cdot q, n \cdot p + m \cdot q).$$

   (a) Show that $\sim$ defines an equivalence relation.

   (b) The set of all integers $\mathbb{Z}$ is defined as $(\mathbb{N} \times \mathbb{N})/\sim$.

      i. Show that the addition $\boxplus$ and the multiplication $\boxdot$ on $\mathbb{N} \times \mathbb{N}$ induces an addition $\oplus$ and an multiplication $\odot$ on $\mathbb{Z}$ respectively.

      ii. The integers -1, 0 and 1 are defined as $[(0, 1)]$, $[(0, 0)]$ and $[(1, 0)]$ respectively.
      Show that $(-1) \oplus 1 = 0$, $(-1) \odot (-1) = 1$ and $0 \odot x = 0$ for all integers x.

      iii. Let $f : \mathbb{N} \to \mathbb{Z}$ be a function defined by $f(a) = [(a, 0)]$.
      Show that f is an injective function and $f(a \cdot b) = [(a, 0)] \odot [(b, 0)]$.

Ans:

(a)
- Since $m + n = m + n$, we have $(m, n) \sim (m, n)$.
- If $(m, n) \sim (p, q)$, then $m + q = p + n$ and so $p + n = m + q$ which implies $(p, q) \sim (m, n)$.

- If $(m,n) \sim (p,q)$ and $(p,q) \sim (r,s)$, then $m+q = p+n$ and $p+s = r+q$. We have

$$\begin{aligned}(m+q)+(p+s) &= (p+n)+(r+q)\\ (m+s)+(p+q) &= (r+n)+(p+q)\\ m+s &= r+n\end{aligned}$$

  Therefore, $(m,n) \sim (r,s)$.

By the above, $\sim$ is an equivalence relation.

(b) i. - Claim: If $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$, then $(m,n) \boxplus (p,q) \sim (m',n') \boxplus (p',q')$. We have $m+n' = m'+n$ and $p+q' = p'+q$. Then,

$$\begin{aligned}(m+n')+(p+q') &= (m'+n)+(p'+q)\\ (m+p)+(n'+q') &= (m'+p')+(n+q)\end{aligned}$$

  Therefore, $(m,n) \boxplus (p,q) \sim (m',n') \boxplus (p',q')$ and the addition $\boxplus$ on $\mathbb{N}\times\mathbb{N}$ induces an addition $\oplus$ on $\mathbb{Z}$.

- Claim: If $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$, then $(m,n) \boxdot (p,q) \sim (m',n') \boxdot (p',q')$. We have $m+n' = m'+n$ and $p+q' = p'+q$. Then,

$$\begin{aligned}m\cdot p+n\cdot q+n'\cdot p'+m'\cdot q'+m\cdot q' &= m\cdot p'+n\cdot q+n'\cdot p'+m'\cdot q'+m\cdot q\\ &= m'\cdot p'+n\cdot q+n\cdot p'+m'\cdot q'+m\cdot q\\ &= m'\cdot p'+n\cdot q'+n\cdot p+m'\cdot q'+m\cdot q\\ &= m'\cdot p'+n'\cdot q'+n\cdot p+m\cdot q'+m\cdot q\\ &= m'\cdot p'+n'\cdot q'+n\cdot p+m\cdot q+m\cdot q'\\ m\cdot p+n\cdot q+n'\cdot p'+m'\cdot q' &= m'\cdot p'+n'\cdot q'+n\cdot p+m\cdot q\end{aligned}$$

  Therefore, $(m,n) \boxdot (p,q) \sim (m',n') \boxdot (p',q')$ and the multiplication $\boxdot$ on $\mathbb{N}\times\mathbb{N}$ induces a multiplication $\odot$ on $\mathbb{Z}$.

ii. -

$$\begin{aligned}(-1)\oplus 1 &= [(0,1)] \oplus [(1,0)]\\ &= [(0,1) \boxplus (1,0)]\\ &= [(0+1, 1+0)]\\ &= [(1,1)]\\ &= [(0,0)]\\ &= 0\end{aligned}$$

-

$$\begin{aligned}(-1)\odot(-1) &= [(0,1)] \odot [(0,1)]\\ &= [(0,1) \boxdot (0,1)]\\ &= [(0\cdot 0+1\cdot 1, 1\cdot 0+0\cdot 1)]\\ &= [(1,0)]\\ &= 1\end{aligned}$$

- Let $x = [(a,b)] \in \mathbb{Z}$, where $a, b \in \mathbb{N}$.

$$\begin{aligned} 0 \odot x &= [(0,0)] \odot [(a,b)] \\ &= [(0,0) \boxdot (a,b)] \\ &= [(0 \cdot a + 0 \cdot b, 0 \cdot b + 0 \cdot a)] \\ &= [(0,0)] \\ &= 0 \end{aligned}$$

iii. Suppose that $f(a) = f(b)$, then $[(a,0)] = [(b,0)]$ which means $(a,0) \sim (b,0)$. It implies that $a + 0 = b + 0$, i.e. $a = b$. Therefore, f is an injective function.
Also, $f(a \cdot b) = [(a \cdot b, 0)] = [(a \cdot b + 0 \cdot 0, b \cdot 0 + a \cdot 0)] = [(a,0) \boxdot (b,0)] = [(a,0)] \odot [(b,0)]$.