Basic Mathematics（基礎數學）MA1015A Midterm Exam II

National Central University, May. 17 2019

系級：____________________ 學號：____________________ 姓名：____________________

Problem 1. (10%) Show that for each even natural number n,

$$\prod_{k=2}^{n}\Big(1-\frac{(-1)^k}{k}\Big)=\frac{1}{2}\,.$$

Proof. Let $S=\Big\{n\in\mathbb{N}\,\Big|\,\prod\limits_{k=2}^{2n}\Big(1-\frac{(-1)^k}{k}\Big)=\frac{1}{2}\Big\}$.

1. $1\in S$ since
$$\prod_{k=2}^{2}\Big(1-\frac{(-1)^k}{k}\Big)=1-\frac{1}{2}=\frac{1}{2}\,.$$

2. Assume that $n\in S$. Then $\prod\limits_{k=2}^{2n}\Big(1-\frac{(-1)^k}{k}\Big)=\frac{1}{2}$; thus
$$\begin{aligned}\prod_{k=2}^{2(n+1)}\Big(1-\frac{(-1)^k}{k}\Big)&=\prod_{k=2}^{2n}\Big(1-\frac{(-1)^k}{k}\Big)\cdot\Big(1-\frac{(-1)^{2n+1}}{2n+1}\Big)\cdot\Big(1-\frac{(-1)^{2n+2}}{2n+2}\Big)\\&=\frac{1}{2}\cdot\Big(1-\frac{-1}{2n+1}\Big)\cdot\Big(1-\frac{1}{2n+2}\Big)=\frac{1}{2}\cdot\frac{2n+2}{2n+1}\cdot\frac{2n+1}{2n+2}=\frac{1}{2}\,.\end{aligned}$$
Therefore, $n+1\in S$.

By **PMI**, we conclude that $S=\mathbb{N}$. □

Problem 2. (10%) Let $a_1=a_2=1$, and for each natural number $n\geqslant 2$, let

$$a_{n+1}=\frac{1}{2}\Big(a_n+\frac{2}{a_{n-1}}\Big)\,.$$

Show that for each natural number n, $1\leqslant a_n\leqslant 2$.

Proof. Let $S=\big\{n\in\mathbb{N}\,\big|\,1\leqslant a_n\leqslant 2 \text{ and } 1\leqslant a_{n+1}\leqslant 2\big\}$.

1. Then by assumption, $1\in S$.

2. Suppose that $\{1,2,\cdots,n-1\}\subseteq S$. Then $1\leqslant a_{n-1},a_n\leqslant 2$; thus
$$a_{n+1}=\frac{1}{2}\Big(a_n+\frac{2}{a_{n-1}}\Big)\geqslant\frac{1}{2}\Big(1+\frac{2}{2}\Big)=\frac{1}{2}\cdot 2=1$$
and
$$a_{n+1}=\frac{1}{2}\Big(a_n+\frac{2}{a_{n-1}}\Big)\leqslant\frac{1}{2}\Big(2+\frac{2}{1}\Big)=\frac{1}{2}\cdot 4=2\,.$$
Therefore, $1\leqslant a_{n+1}\leqslant 2$. Combining with $1\leqslant a_n\leqslant 2$, we find that $n\in S$.

By **PCI**, we conclude that $S = \mathbb{N}$. $\square$

Problem 3. (10%) Let A be a set, and R be a relation on A. Show that R is transitive if and only if $R \circ R \subseteq R$.

Proof. "$\Rightarrow$" Assume that R is transitive and $(a, c) \in R \circ R$ be given. By the definition of the composition of relations, there exists b in A such that $(a, b) \in R$ and $(b, c) \in R$. Since R is transitive, $(a, c) \in R$ which shows that $R \circ R \subseteq R$.

"$\Leftarrow$" Assume that $R \circ R \subseteq R$ and $(a, b), (b, c) \in R$. By the definition of the composition of relations, $(a, b) \in R \circ R$; thus by the assumption that $R \circ R \subseteq R$, we conclude that $(a, b) \in R$. Therefore, R is transitive. $\square$

Problem 4. (10%) Let X be a non-empty set and A be a non-empty proper subset of X. Set $R = X \times X - (A \times A)$. Is R reflexive on X? Symmetric? Transitive? Prove your answers.

Proof. 1. **R is not reflexive on X** since if $a \in A$, then $a \in X$ but the fact that $(a, a) \in A \times A$ implies that $(a, a) \notin R = X \times X - A \times A$.

2. **R is symmetric on X**: Let $(b, c) \in X \times X$. Then

$$(b, c) \in R \Leftrightarrow (b, c) \notin A \times A \Leftrightarrow (b \notin A) \vee (c \notin A) \Leftrightarrow (c \notin A) \vee (b \notin A) \Leftrightarrow (c, b) \notin A \times A$$
$$\Leftrightarrow (c, b) \in R\,.$$

3. **R is not transitive** on X: Let $a, b \in X$ but $a \in A$ and $b \notin A$. Then (by the argument above) $(a, b) \in R$ and $(b, a) \in R$. If R is transitive on X, we must have $(a, a) \in R$, a contradiction. $\square$

Problem 5. (10%) Let p be a prime number, and $a \in \mathbb{N}$. Show that $a^2 = 1 \pmod{p}$ if and only if $a = 1 \pmod{p}$ or $a = -1 \pmod{p}$.

Proof. "$\Rightarrow$" Suppose that $a^2 = 1 \pmod{p}$. Then $p \mid (a^2 - 1)$. Since $a^2 - 1 = (a-1)(a+1)$ and p is a prime number, $p \mid (a-1)$ or $p \mid (a+1)$. Therefore, $a = 1 \pmod{p}$ or $a = -1 \pmod{p}$.

"$\Leftarrow$" If $a = 1 \pmod{p}$, then $a = kp + 1$ for some $k \in \mathbb{Z}$; thus $a^2 - 1 = k^2p^2 + 2kp$ which implies that $p \mid a^2 - 1$. Therefore, $a = 1 \pmod{p}$ implies that $a^2 = 1 \pmod{p}$. On the other hand, if $a = -1 \pmod{p}$, then $a = kp - 1$ for some $k \in \mathbb{Z}$; thus $a^2 - 1 = k^2p^2 - 2kp$ which implies that $p \mid a^2 - 1$. Therefore, $a = -1 \pmod{p}$ implies that $a^2 = 1 \pmod{p}$; thus $a = 1 \pmod{p}$ or $a = -1 \pmod{p}$ implies that $a^2 = 1 \pmod{p}$. $\square$

Problem 6. Prove the Fermat's Little Theorem

$$\boxed{\text{Let } p \text{ be a prime, and let } a \in \mathbb{N} \text{ such that } p \nmid a. \text{ Then } a^{p-1} = 1 \pmod{p}}$$

by the following steps.

(i) (5%) Show that none of the $p - 1$ integers a, $2a$, $3a$, $\cdots$, $(p-1)a$ is divisible by p.

(ii) (5%) Show that no two of the integers a, $2a$, $3a$, $\cdots$, $(p-1)a$ are congruent modulu p.

(iii) (5%) Show that $\prod_{j=1}^{p-1}(ja) = (p-1)! \pmod{p}$.

(iv) (5%) Conclude from (iii) that $a^{p-1} = 1 \pmod{p}$.

Proof. (i) Assume the contrary that there exists an integer $1 \leqslant j \leqslant p-1$ such that $p \mid ja$. Then $p \mid j$ or $p \mid a$. By assumption, $p \nmid a$; thus $p \mid j$ which implies that p divides an integer between 1 and $p-1$, a contradiction. Therefore, none of the $p-1$ integers a, $2a$, $3a$, $\cdots$, $(p-1)a$ is divisible by p.

(ii) Assume the contrary that there exist $1 \leqslant j, k \leqslant p-1$ such that $ja = ka \pmod{p}$. Then $p \mid (j-k)a$ which implies that $p \mid j-k$ or $p \mid a$. By assumption, $p \nmid a$; thus $p \mid j-k$, a contradiction. Therefore, no two of the integers a, $2a$, $3a$, $\cdots$, $(p-1)a$ are congruent modulu p.

(iii) Let $0 \leqslant r_j < p$ be the remainder satisfying $ja = r_j \pmod{p}$. By (i), $r_j \neq 0$ for all $1 \leqslant j \leqslant p-1$. By (ii), $r_j \neq r_k$ if $j \neq k$ and $1 \leqslant j, k \leqslant p-1$. Therefore, $\{r_1, r_2, \cdots, r_{p-1}\}$ is a permutation of $\{1, 2, \cdots, n\}$ which implies that

$$\prod_{j=1}^{p-1} r_j = (p-1)!\,. \tag{$\star$}$$

Since $ja = r_j \pmod{p}$, we conclude that

$$\prod_{j=1}^{p-1}(ja) = \prod_{j=1}^{p-1} r_j \pmod{p}\,,$$

and the conclusion in (iii) follows from $(\star)$.

(iv) Note that $\prod_{j=1}^{p-1}(ja) = \Big(\prod_{j=1}^{p-1} j\Big)a^{p-1} = (p-1)!a^{p-1}$; thus (iii) implies that

$$(p-1)!a^{p-1} = (p-1)! \pmod{p}\,.$$

Since $p \nmid (p-1)!$, by the cancellation law for $\mathbb{Z}_p$, we conclude that $a^{p-1} = 1 \pmod{p}$. $\square$

Problem 7. Let $f : X \to Y$ be a function, and $E \subseteq Y$. Show that

1. (10%) $E = f(f^{-1}(E))$ if and only if $E \subseteq \text{Rng}(f)$.
2. (10%) $f(f^{-1}(E)) = E \cap \text{Rng}(f)$.

Proof. 1. Since we have shown that $f(f^{-1}(E)) \subseteq E$ for all $E \subseteq Y$ in class, it suffices to show that $E \subseteq f(f^{-1}(E))$ if and only if $E \subseteq \text{Rng}(f)$.

"$\Rightarrow$" Assume that $E \subseteq f(f^{-1}(E))$ and $y \in E$. Then there exists $x \in f^{-1}(E)$ such that $y = f(x)$. Therefore, $y \in \text{Rng}(f)$ which shows $E \subseteq \text{Rng}(f)$.

"$\Leftarrow$" Assume that $E \subseteq \text{Rng}(f)$ and $y \in E$. Then there exists $x \in \text{Dom}(f)$ such that $y = f(x)$. Since $y \in E$, $x \in f^{-1}(E)$; thus $y \in f(f^{-1}(E))$. Therefore, $E \subseteq f(f^{-1}(E))$.

2. Let $A = E \cap \text{Rng}(f)$. Then $A \subseteq \text{Rng}(f)$; thus we conclude from 1 that

$$A = f(f^{-1}(A)) .$$

Moreover, $A \subseteq E$; thus $f^{-1}(A) \subseteq f^{-1}(E)$ which implies that $f(f^{-1})(A)) \subseteq f(f^{-1}(E))$. Therefore, $E \cap \text{Rng}(f) \subseteq f(f^{-1}(E))$.

On the other hand, suppose that $y \in f(f^{-1}(E))$. Then $y \in \text{Rng}(f)$ and there exists $x \in f^{-1}(E)$ such that $y = f(x)$. Since $x \in f^{-1}(E)$ if and only if $f(x) \in E$, we find that $y \in E$. Therefore, $y \in E \cap \text{Rng}(f)$ which shows that $f(f^{-1}(E)) \subseteq E \cap \text{Rng}(f)$. □

Problem 8. (10%) Let $f : X \to Y$ be a function. Prove that f is a one-to-one function if and only if

$$f(A) \cap f(B) = f(A \cap B) \qquad \forall\, A, B \subseteq X$$

Proof. Since have shown that $f(A \cap B) \subseteq f(A) \cap f(B)$ in class, it suffices to show that f is one-to-one if and only if $f(A) \cap f(B) \subseteq f(A \cap B)$ for all $A, B \subseteq X$.

"$\Rightarrow$" Suppose that f is one-to-one and $A, B \subseteq X$. Let $y \in f(A) \cap f(B)$. Then there exists $x_1 \in A$ and $x_2 \in B$ such that $y = f(x_1) = f(x_2)$. Since f is one-to-one, we must have $x_1 = x_2$; thus $x_1 \in A \cap B$ which implies that $y \in f(A \cap B)$. Therefore, $f(A) \cap f(B) \subseteq f(A \cap B)$.

"$\Leftarrow$" Suppose that $f(A) \cap f(B) \subseteq f(A \cap B)$ for all $A, B \subseteq X$, and $f(x_1) = f(x_2)$. Let $A = \{x_1\}$ and $B = \{x_2\}$. Then $f(A) = f(B) = f(A) \cap f(B)$ which implies that $f(A \cap B) \neq \varnothing$. Therefore, $A \cap B \neq \varnothing$; thus $x_1 = x_2$. Therefore, f is one-to-one. □