MA1100 - Basic Discrete Mathematics Suggested Solutions

(Semester 1 : AY2020/21)

Written by : Chow Yong Lam
Audited by : Yip Jung Hon

Question 1

Consider the Fibonacci numbers F_n (for $n \in \mathbb{Z}_{\geq 0}$) defined recursively by:
$F_0 := 0$, $F_1 := 1$, and $F_n := F_{n-1} + F_{n-2}$ for all $n \geq 2$
Show that for any positive integers $m, n \in \mathbb{Z}_{>0}$, one has

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$$

Solution

When $n = 1$, we have $\forall m \in \mathbb{Z}_{>0}$,

$$\begin{aligned} F_{m+n} &= F_{m+1} \\ &= F_{m-1} + F_m \\ &= F_{m-1}F_n + F_mF_{n+1} \end{aligned}$$

because $F_n = F_1 = 1$ and $F_{n+1} = F_2 = 1$

When $n = 2$, we have $\forall m \in \mathbb{Z}_{>0}$,

$$\begin{aligned} F_{m+n} &= F_{m+2} \\ &= (F_{m-1} + F_m) + F_m \\ &= F_{m-1}F_n + F_mF_{n+1} \end{aligned}$$

because $F_n = F_2 = 1$ and $F_{n+1} = F_3 = 2$

Fix $N \in \mathbb{Z}_{>0}$ with $N \geq 2$ and assume the induction hypothesis such that $\forall m, n \in \mathbb{Z}_{>0}$ with $n \leq N$, one has $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$
Then $\forall m \in \mathbb{Z}_{>0}$, one has

$$\begin{aligned} F_{m+N+1} &= F_{m+N} + F_{m+N-1} \quad \text{(by recursive definition of } F_{m+N+1}) \\ &= F_{m-1}F_N + F_mF_{N+1} + F_{m-1}F_{N-1} + F_mF_N \quad \text{(by induction hypothesis for } n = N \text{ and } n = N-1) \\ &= F_{m-1}F_{N+1} + F_mF_{N+2} \quad \text{(by recursive definition of } F_{N+1} \text{ and } F_{N+2}) \end{aligned}$$

Thus by strong induction, for any positive integers $m, n \in \mathbb{Z}_{>0}$, one has

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$$

Question 2

Keep the notation F_n for the Fibonacci numbers as in the previous question. Show that for any $d, n \in \mathbb{Z}_{>0}$,

$$\text{if} \quad d|n, \ \text{then} \quad F_d|F_n.$$

Solution

Fix $d \in \mathbb{Z}_{>0}$, we claim that $\forall q \in \mathbb{Z}_{>0}$, one has $F_d|F_{qd}$.

When $q = 1$, $F_{qd} = F_d$, and clearly $F_d|F_{qd}$ in this case.

Suppose our claim holds for a fixed $q \in \mathbb{Z}_{>0}$. Then

$$\begin{aligned} F_{(q+1)d} &= F_{qd+d} \\ &= F_{qd-1}F_d + F_{qd}F_{d+1} \ \ \text{(by result in Question 1)} \end{aligned}$$

$F_{qd-1}F_d$ is divisible by F_d and $F_{qd}F_{d+1}$ is divisible by F_d by the induction hypothesis on q.
Hence, $F_d|F_{(q+1)d}$
By induction, our claim holds for all $q \in \mathbb{Z}_{>0}$.
Now given $n \in \mathbb{Z}_{>0}$, if $d|n$, then there exists $q \in \mathbb{Z}_{>0}$, such that $n = qd$.
It follows that $F_d|F_n = F_{qd}$ by our claim.

Question 3

Let $a, b, c, d \in \mathbb{Z}_{>0}$ be positive integers such that $ad - bc = 1$. Show that

$$a + b \ \text{ and } \ c + d \ \text{ are relatively prime.}$$

Solution

We have

$$d(a + b) - b(c + d) = ad - bc = 1$$

or

$$a(c + d) - c(a + b) = ad - bc = 1$$

By Bezout's theorem, since there exists integeers d, b (or $a, -c$) such that the two equations above are fulfilled, either of the equations shows that $a + b$ and $c + d$ are relatively prime.
Explicitly, suppose $g := \gcd(a + b, c + d) \in \mathbb{Z}_{>0}$,
Then $g = 1$ in $\mathbb{Z}_{>0}$.

Question 4

Let S be a set with the following property:

$$(*) \text{ For any set } X \text{, there exists a unique function } f : X \to S.$$

Show that $\text{card}(S) = 1$.

Solution
Apply the property (*) with $X = \{0\}$ (the singleton set with only one element called 0).
Thus, $f(0) \in S$, so $S \neq \varnothing$, which means $\text{card}(S) \geq 1$.

Suppose $\text{card}(S) > 1$. Then, $\exists s_1,\ s_2 \in S$ with $s_1 \neq s_2$.
Let $g : \{0\} \to S$ be the function $g(0) := s_1$,
and $h : \{0\} \to S$ be the function $h(0) := s_2$,
Then g and h are distinct functions from $\{0\}$ to S, which contradicts the uniqueness in (*).
Hence, we must have $\text{card}(S) = 1$.

Questions 5 to 8: True or False

Question 5

(a) For any sets A, B, C, one has $A \backslash (B \cup C) = (A \backslash B) \cup (A \backslash C)$.
False. A counterexample will be when $A = \{1, 2\}, B = \{1\}, C = \{2\}$. Then, $LHS = \varnothing,\ RHS = A$
(b) For any sets A, B, C, one has $A \backslash (B \cap C) = (A \backslash B) \cap (A \backslash C)$. Then, $LHS = A,\ RHS = \varnothing$
False. A counterexample will be when $A = \{1, 2\}, B = \{1\}, C = \{2\}$.
(c) For any sets A, B, C, one has $(A \cup B) \backslash C = (A \backslash C) \cup (B \backslash C)$.
True. Let x be an arbitrary element in $(A \cup B) \backslash C$

$$\begin{aligned}
x \in (A \cup B) \backslash C &\iff x \in (A \cup B) \wedge x \notin C \\
&\iff (x \in A \vee x \in B) \wedge x \notin C \\
&\iff (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C) \\
&\iff (x \in A \backslash C) \vee (x \in B \backslash C) \\
&\iff x \in (A \backslash C) \cup (B \backslash C)
\end{aligned}$$

(d) For any sets A, B, C, one has $(A \cap B) \backslash C = (A \backslash C) \cap (B \backslash C)$.
True. Let x be an arbitrary element in $(A \cap B) \backslash C$

$$\begin{aligned}
x \in (A \cap B) \backslash C &\iff x \in (A \cap B) \wedge x \notin C \\
&\iff (x \in A \wedge x \in B) \wedge x \notin C \\
&\iff (x \in A \wedge x \notin C) \wedge (x \in B \wedge x \notin C) \\
&\iff (x \in A \backslash C) \wedge (x \in B \backslash C) \\
&\iff x \in (A \backslash C) \cap (B \backslash C)
\end{aligned}$$

(e) For any sets A, B, C, one has $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
True. Let (x, y) be an arbitrary element in $A \times (B \cup C)$

$$\begin{aligned}
(x, y) \in A \times (B \cup C) &\iff (x \in A) \wedge (y \in (B \cup C)) \\
&\iff (x \in A) \wedge ((y \in B) \vee (y \in C)) \\
&\iff (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\
&\iff ((x, y) \in (A \times B)) \vee ((x, y) \in (A \times C)) \\
&\iff (x, y) \in (A \times B) \cup (A \times C)
\end{aligned}$$

(f) For any sets A, B, C, one has $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
True. Let (x, y) be an arbitrary element in $A \times (B \cap C)$

$$\begin{aligned}
(x, y) \in A \times (B \cap C) &\iff (x \in A) \wedge (y \in (B \cap C)) \\
&\iff (x \in A) \wedge ((y \in B) \wedge (y \in C)) \\
&\iff (x \in A \wedge y \in B) \wedge (x \in A \wedge y \in C) \\
&\iff ((x, y) \in (A \times B)) \wedge ((x, y) \in (A \times C)) \\
&\iff (x, y) \in (A \times B) \cap (A \times C)
\end{aligned}$$

(g) For any sets A, B, one has $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.
False. A counterexample will be when $A = \{1\}, B = \{2\}$. Then, $LHS = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$, $RHS = \{\varnothing, \{1\}, \{2\}\}$.
(h) For any sets A, B, one has $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
True. Let $x \in \mathcal{P}(A \cap B)$ be arbitrary.

$$\begin{aligned}
x \in \mathcal{P}(A \cap B) &\iff x \subseteq (A \cap B) \\
&\iff x \subseteq A \wedge x \subseteq B \\
&\iff x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B) \\
&\iff x \in \mathcal{P}(A) \cap \mathcal{P}(B)
\end{aligned}$$

(i) For any sets A, B, one has $\mathcal{P}(A \backslash B) = \mathcal{P}(A) \backslash \mathcal{P}(B)$.
False. A counterexample will be when $A = \{1, 2\}, B = \{2\}$.Then, $LHS = \{\varnothing, \{1\}\}$, $RHS = \{\{1\}, \{1, 2\}\}$
(j) For any sets A, B, one has $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$.
False. A counterexample will be when $A = \{1\}, B = \{2\}$.
Then, $LHS = \{\varnothing, \{(1, 2)\}\}$, $RHS = \{(\varnothing, \varnothing), (\varnothing, \{2\}), (\{1\}, \varnothing), (\{1\}, \{2\})\}$.

Question 6

(a) For any sets X, Y and for any injective function $f : X \to Y$, there exists a function $g : Y \to X$ which is injective.
False. Take X to be the empty set $\varnothing$. Then, f will be injective. However, there does not exist any function with $\varnothing$ as the codomiain.
(b) For any sets X, Y and for any injective function $f : X \to Y$, there exists a function $g : Y \to X$ which is surjective.
False. Take X to be the empty set $\varnothing$. Then, f will be injective. However, there does not exist any function with $\varnothing$ as the codomiain.
(c) For any sets X, Y and for any surjective function $f : X \to Y$, there exists a function $g : Y \to X$ which is injective.
True. f being surjective means that for any y in Y, there exist at least one element x in X such that $f(x) = y$. We can define a choice function by the Axiom of Choice, $\phi : \{f^{-1}[\{y\}] \mid y \in Y\} \to X$ such that we can choose one element from all elements in X that is being mapped to y by f, for every y in Y. Also, define $\alpha : Y \to \{f^{-1}[\{y\}] \mid y \in Y\}$ such that α maps every element y in Y to its corresponding inverse image set $f^{-1}[\{y\}]$. (Note that by the surjectivity of f, $f^{-1}[\{y\}]$ is never empty, since every element in Y has at least one element from X being mapped onto it). Both functions defined above are injective. (Note that α is injective, or else it would mean that x can be mapped by f to two distinct values of y in Y. Hence when we define $g = \phi \circ \alpha$, $g : Y \to X$ is injective.
(d) For any sets X, Y and for any surjective function $f : X \to Y$, there exists a function $g : Y \to X$ which is surjective.
False. Take $X = \{1, 2\}$ and $Y = \{0\}$. Define f such that $f(1) = 0, f(2) = 0$. Then, f is surjective. However, for any well-defined function g from Y to X, we can define either $g(0) = 1$ or $g(0) = 2$, i.e. not all elements in X can be mapped from Y via the function g
(e) For any sets X, Y and for any function $f : X \to Y$ and for any subsets A, B of X, one has $f[A \cap B] \subseteq f[A] \cap f[B]$.
True. Let $y \in Y$ be an arbitrary element such that $y \in f[A \cap B]$. Then, $\exists x \in A \cap B$ s.t. $f(x) = y \implies$ for both sets A and B, $\exists x$ in each set s.t. $f(x) = y$. Then, $y \in f[A] \wedge y \in f[B]$. It follows that $y \in f[A] \cap f[B]$. Thus the claim holds.

(f) For any sets X, Y and for any function $f : X \to Y$ and for any subsets A, B of X, one has $f[A] \cap f[B] \subseteq f[A \cap B]$.
False. Take $X = \{1, 2\}, A = \{1\}, B = \{2\}, Y = \{0\}$. Define $f : X \to Y$ such that $f(1) = 0, f(2) = 0$. We can see that $f[A] = f[B] = Y$ so $f[A] \cap f[B] = Y$. However, since $A \cap B = \varnothing$, $f[A \cap B] = \varnothing$. It is impossible that a non-empty set Y is a subset of $\varnothing$, thus we have provided a counterexample.
(g) For any sets X, Y and for any function $f : X \to Y$ and for any subsets A, B of X, one has $f[A \cup B] \subseteq f[A] \cup f[B]$.
True. Denote A as A_1 and B as A_2 Let $y \in Y$ be arbitrary such that $y \in f[A_1 \cup A_2]$.

$$\begin{aligned} y \in f[A_1 \cup A_2] &\iff \exists x \in A_1 \cup A_2 \text{ s.t. } y = f(x) \\ &\iff y \in f[A_1] \cup f[A_2]. \end{aligned}$$

(h) For any sets X, Y and for any function $f : X \to Y$ and for any subsets A, B of X, one has $f[A] \cup f[B] \subseteq f[A \cup B]$.
True. Refer to the explanation in (g). The converse is also true since the relation above is an 'if and only if' relation.
(i) For any sets X, Y and for any function $f : X \to Y$ and for any subsets A of X, one has $f[X \backslash A] \subseteq Y \backslash f[A]$.
False. Consider $X = \{1, 2\}, A = \{1\}, Y = \{0\}$ and define the function $f : X \to Y$ such that $f(1) = f(2) = 0$. Note that $f(1) = 0 \implies f[A] = \{0\} = Y$. $f[X \backslash A] = f[\{2\}] = \{0\} = Y$, while $Y \backslash f[A] = \varnothing$. It is impossible for a non-empty set Y to be a subset of $\varnothing$, thus we have provided a counterexample.
(j) For any sets X, Y and for any function $f : X \to Y$ and for any subsets A of X, one has $Y \backslash f[A] \subseteq f[X \backslash A]$.
False. Consider $X = \{1, 2\}, A = \{1\}, Y = \{a, b\}$ and define the function $f : X \to Y$ such that $f(1) = f(2) = a$. Note that $f(1) = a \implies f[A] = \{a\}$. $f[X \backslash A] = f[\{2\}] = \{a\}$, while $Y \backslash f[A] = \{b\}$.Since $b \notin f[X \backslash A]$, $Y \backslash f[A] \not\subseteq f[X \backslash A]$. Thus we have provided a counterexample.

Question 7

(a) For any $a \in \mathbb{Z}$ with $a > 1$, there exists a prime number p such that $p | a$.
True. By the Fundamental Theorem of Arithmetic, every positive integer $a > 1$ can be expressed as a product of primes. Every prime appeared in the expression can divide a.
(b) For any $a \in \mathbb{Z}$ with $a > 1$, there exists a prime number p such that $a | p$.
False. A counterexample is $a = 4$.
(c) For any $a \in \mathbb{Z}$ with $a > 1$, there are infinitely many prime numbers p such that $p | a$.
False. A counterexample is $a = 2$, and the only prime number that divided 2 is 2 itself, hence 2 has only finitely many prime factors.
(d) For any prime number p, there are infinitely many $a \in \mathbb{Z}$ with $a > 1$ such that $p | a$.
True. Let p be a prime number, thus $p > 1$. Since for any positive integer $k \in Z_{>0}$, $p | kp$, from the fact that there are infinitely many positive integers, there exists infinitely many integers $a = kp$ such that $p | a$.
(e) For any $a \in \mathbb{Z}$ with $a > 1$, there are infinitely many prime numbers p such that $a | p$.
False. This is an extension from 7(b). Counterexample: $a = 4$.
(f) For any prime number p, there are infinitely many $a \in \mathbb{Z}$ with $a > 1$ such that $a | p$.
False. A counterexample will be when $p = 2$. The only possible value of a will be $a = 2$. Hence, when $p = 2$, there are finitely many (in fact only one) integers $a > 1$ such that $a | p$.
(g) For any $a \in \mathbb{Z}_{>0}$, if there exists a prime number p such that $2^a = p + 1$, then a is prime.
True. If a is not prime, when $a = 1$, $p = 1$ which is not prime. When $a > 1$, then $\exists x, y \in \mathbb{Z}_{>0}$ s.t. $(x, y \neq 1) \wedge (x, y \neq a) \wedge (a = xy)$. Then,

$$\begin{aligned} p &= 2^a - 1 \\ &= 2^{xy} - 1 \\ &= (2^y)^x - 1 \\ &= (2^y - 1)(\sum_{i=0}^{x-1} 2^{iy}) \end{aligned}$$

$2^y - 1 \in \mathbb{Z}$ because only multiplication, addition and subtraction between integers are involved in computations.
For the same reason, $\sum_{i=0}^{x-1} 2^{iy} \in \mathbb{Z}$.
Since $y > 1$, $2^y > 2^1 \implies (2^y - 1) > 1$. Also, since $y < a, 2^y - 1 < 2^a - 1$. Thus, $1 < (2^y - 1) < p$.
By the inequality above $1 < (\sum_{i=0}^{x-1} 2^{iy}) < p$ as well.
Hence, $\exists h, k \in \mathbb{Z}_{>0}$ s.t. $(h, k \neq 1) \wedge (h, k \neq p) \wedge (p = hk)$. p is thus not prime.
We have proven the contrapositive of the statement in (g), which means that the statement in (g) itself is true.

(h) For any $a \in \mathbb{Z}_{>0}$, if a is prime, then there exists a prime number p such that $2^a = p + 1$.
False. Consider $a = 11$ being a prime number. $2^a = 2^{11} = 2018$. However, $p = 2^a - 1 = 2047 = 23 \times 89$ and thus p is not prime. We have provided a counterexample.
(i) The unique prime factorisation of 2019 is 3×673.
True.
(j) The unique prime factorisation of 2020 is $2 \times 2 \times 2 \times 5 \times 101$.
False. It should be $2 \times 2 \times 5 \times 101$.

Question 8

(a) For any infinite set X, there exists an injective function $\psi : \mathbb{Z} \to X$.
True. Idea: X will have cardinality greater or equal to $\mathbb{N}$, so there is obviously going to be an injective function from $\mathbb{N}$ (smaller cardinality) to X (bigger cardinality). The following is a more rigorous proof.

First, note that $\mathbb{N}$ is equinumerous to $\mathbb{Z}$. There exists a bijective function $g : \mathbb{Z} \to \mathbb{N}$.
Next, we define $f : \mathbb{N} \to X$ recursively. Since X is infinite, it is non-empty. Pick $f(1) = x_1 \in X$. For the recursion, let $n \in \mathbb{N}$ be arbitrary such that we assume:

- $f(1)$ to $f(n)$ has been defined.
- $\forall i, j$ s.t. $1 \leq i, j \leq n, i \neq j \implies f(i) \neq f(j)$.

We then obtain a finite set. $X_n = \{f(1), f(2), \ldots f(n)\}$.
But since X is infinite, therefore $X \backslash X_n$ is infinite (and thus non-empty).
Now we define a choice function. Take $\mathcal{C} = \{B \in \mathcal{P}(X) | (\exists F \subseteq X)(\text{F is finite} \land B = X \backslash F\}$
Then, we can define a choice function $\alpha : \mathcal{C} \to \cup_{B \in \mathcal{C}} B = X$ such that $\alpha(B) \in (B)$, i.e. $\alpha(B)$ is an element in $B = X \backslash F$ for some finite set F.
By the choice function, for all positive integers $n \in \mathbb{Z}_{>0}$, define $B_n = X \backslash X_n$ and define $f(n+1) = \alpha(B_n) \in B_n$.
Then, $f(n-1) \notin X_n = \{f(1), f(2), \ldots f(n)\}$, i.e. $\forall i \leq n, f(n+1) \neq f(i)$.
By the recursion theorem and mathematical induction, we have defined an injective function f from $\mathbb{N}$ to X.
Since f, g are injective, the function $f \circ g : \mathbb{Z} \to X$ is injective.
(b) For any infinite set X, there exists an injective function $\psi : X \to \mathbb{Z}$.
False. A counterexample will be when X is an uncountable set like $\mathbb{R}$.
(c) For any infinite set X, there exists a surjective function $\psi : \mathbb{Z} \to X$.
False. A counterexample will be when X is an uncountable set like $\mathbb{R}$.
(d) For any infinite set X, there exists a surjective function $\psi : X \to \mathbb{Z}$.
True. This follows from the result in (a). Note that both X and $\mathbb{Z}$ are non-empty.
(e) For any infinite set X and for any finite set S, there exists an injective function $\psi : S \to X$.
True. S is finite, so $\exists n \in \mathbb{N}$ such that there exists a bijective function $f : S \to \mathbb{N}_n$. There also exists an injective function $i_n : \mathbb{N}_n \to \mathbb{N}$. From the result in (a), there exists an injective function $g : \mathbb{N} \to X$. Hence, the composite function $g \circ i_n \circ f : S \to X$ is injective.
(f) For any infinite set X and for any finite set S, there exists a surjective function $\psi : X \to S$.
False. A counterexample will be when $S = \varnothing$, because there does not exist any function with $\varnothing$ as codomain.
(g) For any countable set X, the set $X \times X$ is countable.
True. If $X = \varnothing$, then $X \times X = \varnothing$ is countable.
If X is non-empty and countable, there exists a surjective function $f : N \to X$.
Then, define $g : \mathbb{N} \times \mathbb{N} \to X \times X$ such that $\forall i, j \in \mathbb{N}$, $g(i, j) := (f(i), f(j)) \in A \times B$.
Given $(a, b) \in A \times B$, $\exists i \in \mathbb{N}$ such that $f(i) = a$ and $\exists j \in \mathbb{N}$ such that $f(j) = b$.
Thus, $\exists (i, j) \in \mathbb{N} \times \mathbb{N}$ such that $g(i, j) = (a, b) \in A \times B$. Thus, g is surjective.
Note that $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$, then there exists a bijective function. $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.
Then, the function $g \circ h : \mathbb{N} \to X \times X$ is surjective, implying that $X \times X$ is countable.
(h) For any countable set X, the set $\mathcal{P}(X)$ is uncountable.
False. When $X = \varnothing$, X is countable. $\mathcal{P}(X) = \{\varnothing\}$ has one element, so the power set is finite and countable.
(i) For any countable set X and any uncountable set Y, the set $X \cup Y$ is uncountable.
True. Note that $Y \subseteq (X \cup Y)$. Since Y is uncountable, by the subset relation, the union of the two sets is also uncountable.

(j) For any countable set X and any uncountable set Y, the set $X \times Y$ is uncountable.
False. When $X = \varnothing$, $X \times Y = \varnothing$ is finite and thus countable.