# DISCRETE MATHEMATICS 2018

## QUESTION 1

(a) $A \setminus (A \setminus B) = A \cap B$

$\cdot\ x \in A \setminus (A \setminus B) \Rightarrow x \in A$ and $x \notin A \setminus B \Rightarrow x \in A$ and $(x \notin A$ or $x \in B) \Rightarrow$

$\Rightarrow (x \in A$ and $x \notin A)$ or $(x \in A$ and $x \in B) \Rightarrow x \in A \cap B \Rightarrow A \setminus (A \setminus B) \subseteq A \cap B$

$\cdot\ x \in A \cap B \Rightarrow x \in A$ and $x \in B \Rightarrow (x \in A$ and $x \notin A)$ or $(x \in A$ and $x \in B) \Rightarrow$

$\Rightarrow x \in A$ and $(x \notin A$ or $x \in B) \Rightarrow x \in A$ and $x \notin A \setminus B \Rightarrow x \in A \setminus (A \setminus B) \Rightarrow A \cap B \subseteq A \setminus (A \setminus B)$ $\Rightarrow$

$\Rightarrow$ by double-inclusion proof that $A \setminus (A \setminus B) = A \cap B$

(b) (i) $A \cap C = B \cap C \Rightarrow A = B$

False: $A = \emptyset$, $B = \{1\}$, $C = \{2\}$

$A \cap C = B \cap C = \emptyset$, but $A \neq B$

(ii) $A \cup C = B \cup C \Rightarrow A = B$

False: $A = \emptyset$, $B = \{1\}$, $C = \{1\}$

$A \cup C = B \cup C$, but $A \neq B$

(iii) $A \cap C \overset{①}{=} B \cap C$ and $A \cup C \overset{②}{=} B \cup C \Rightarrow A = B$

True: $\cdot\ x \in A \Rightarrow x \in A \cup C \overset{②}{\Rightarrow} x \in B \cup C \Rightarrow x \in B$ or $x \in C$

if $x \in B \Rightarrow$ we are done

if $x \in C \Rightarrow x \in A \cap C \overset{①}{\Rightarrow} x \in B \cap C \Rightarrow x \in B$ $\Big|\ \Rightarrow x \in B \Rightarrow A \subseteq B$

$\cdot\ x \in B \Rightarrow x \in B \cup C \overset{②}{\Rightarrow} x \in A \cup C \Rightarrow x \in A$ or $x \in C$

if $x \in A \Rightarrow$ we are done

if $x \in C \Rightarrow x \in B \cap C \overset{①}{\Rightarrow} x \in A \cap C \Rightarrow x \in A$ $\Big|\ \Rightarrow x \in A \Rightarrow B \subseteq A$

$\Rightarrow A = B$

(iv) $A \setminus C = B \setminus C \Rightarrow A = B$

False: $A = \emptyset$, $B = \{1\}$, $C = \{1, 2\}$

$A \setminus C = B \setminus C = \emptyset$, but $A \neq B$

(c) $R_1, R_2$ relations on $A$, $R_2 \circ R_1$

(i) $R_1$ and $R_2$ reflexive $\Rightarrow R_2 \circ R_1$ reflexive

True: $a R_1 a$ and $a R_2 a$ for every $a \in A$

$a (R_2 \circ R_1) a \iff (\exists)\, x \in A$ s.t. $a R_1 x$ and $x R_2 a$

if $x = a$

$\Rightarrow a (R_2 \circ R_1) a \Rightarrow R_2 \circ R_1$ reflexive

(ii) $R_1$ and $R_2$ transitive $\Rightarrow R_2 \circ R_1$ transitive

False : $R_2 = \{(x,y), (z,t)\}$ , $R_1 = \{(a,x), (y,z)\}$

$R_2 \circ R_1 = \{(a,y), (y,t)\}$ is not transitive since $(a,t) \notin (R_2 \circ R_1)$

(iii) $R_1$ and $R_2$ symmetric $\Rightarrow$ $R_2 \circ R_1$ symmetric

False : $R_2 = \{(x,y), (y,x)\}$ , $R_1 = \{(x,z), (z,x)\}$

$R_2 \circ R_1 = \{(z,y)\}$ is not symmetric since $(y,z) \notin (R_2 \circ R_1)$

(d) · 10 identical bananas

· 4 distinguishable boxes

· min 1 , max 5

Case 1 : 5, 3, 1, 1 in boxes

$\frac{4!}{2! \cdot 1! \cdot 1!} = 12$ ways

Case 2 : 5, 2, 2, 1 in boxes

$\frac{4!}{2!} = 12$ ways

Case 3 : 4, 4, 1, 1 in boxes

$\frac{4!}{2! \cdot 2!} = 6$ ways

Case 4 : 4, 3, 2, 1 in boxes

$4! = 24$ ways

Case 5 : 3, 3, 3, 1 in boxes

$\frac{4!}{3!} = 4$ ways

Case 6 : 3, 3, 2, 2 in boxes

$\frac{4!}{2! \cdot 2!} = 6$ ways

$12 + 12 + 6 + 24 + 4 + 6 = 64$ ways

QUESTION 2

(a) $27^{17} \pmod 7 = (-1)^{17} \bmod 7 = (-1) \bmod 7 = 6$

(b) $m, n \in \mathbb{N}^+$

$x, y \in \mathbb{Z}$ s.t. $g = mx + ny$, $g = \gcd(m,n)$

$p$ prime

$a^{-1} \pmod p$ exists for any $a \in \mathbb{Z}_p$, $a \not\equiv 0 \pmod p$

We know that $g = \gcd(a,p) = 1$, since $p$ is prime and $a \not\equiv 0 \pmod p \Rightarrow$

$(\exists)\, x, y \in \mathbb{Z}$ s.t. $1 = xp + ya \Rightarrow 1 \equiv ya \pmod u \Rightarrow a^{-1} \equiv y \pmod p$.

(c) $p$ = prime

$a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod p$, then

$$a^{p-1} \equiv 1 \pmod p$$

We will prove by induction that $a^{p-1} \equiv 1 \pmod p$ for $a \in \mathbb{N}$

$P(0)$ cannot be used as $0 \equiv 0 \pmod p$

$P(1)$: $1^p = 1 \equiv 1 \pmod p$ ✓

$P(a) \Rightarrow P(a+1)$ $\qquad\qquad \binom{p}{i}$ divisible by $p$

$$(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^i \overset{\downarrow}{\equiv} a \pmod p$$

So, $a^p \equiv a \pmod p$ and from b we know that $(\exists)\, a^{-1} \Rightarrow a^{p-1} \equiv 1 \pmod p$

For $a < 0$, we have $a^{p-1} = (-b)^{p-1} = (-1)^{p-1} b^{p-1}$

for $p = 2$ it's trivial as $a$ is odd $\Rightarrow a \equiv 1 \pmod 2$ $\Bigg|$ $\Rightarrow$

for $p > 2$ $p$ is odd $\Rightarrow (-1)^{p-1} = 1$

$$\Rightarrow a^{p-1} = b^{p-1} \overset{b>0}{\equiv} 1 \pmod p$$

(d) $(a_n)$, $n \in \mathbb{N}_+$, $a_n = O(n)$

$K \geq 2$, $({}^K b_n)$, $n \in \mathbb{N}_+$

$${}^K b_1 = {}^{K-1} b_1$$

$${}^K b_2 = \frac{1}{2}\left({}^{K-1} b_1 + {}^{K-1} b_2\right)$$

$$\vdots$$

$${}^K b_n = \frac{1}{n}\left({}^{K-1} b_1 + {}^{K-1} b_2 + \dots + {}^{K-1} b_n\right)$$

${}^1 b_n = a_n$

We'll prove by induction on $k \geq 1$ that ${}^{k}b_n = o(n)$

$P(1)$: ${}^{1}b_n = a_n = o(n)$

$P(k) \Rightarrow P(k+1)$

We know that ${}^{k}b_n = o(n)$ and we have

$${}^{k+1}b_n = \frac{1}{n}\left({}^{k}b_1 + {}^{k}b_2 + \dots + {}^{k}b_n\right)$$

We have ${}^{k}b_1 = O(1) \Rightarrow {}^{k}b_1 < c_1$

${}^{k}b_2 = o(2) \Rightarrow {}^{k}b_2 < 2c_2$

$\vdots$

${}^{k}b_n = o(n) \Rightarrow {}^{k}b_n < nc_n$

$\Rightarrow {}^{k}b_i < iC$ from some value $N$

$C = \max(c_1, \dots, c_n)$

Then, ${}^{k+1}b_n < \frac{1}{\cancel{n}} \cdot \frac{\cancel{n}(n+1)}{2} C$

${}^{k+1}b_n < \frac{n+1}{2} C \Rightarrow {}^{k+1}b_n = o(n+1)$ ✓

## QUESTION 3

(a) $f(n) = o(g(n))$ if $\exists\, c \in \mathbb{R}, N \in \mathbb{N}$ s.t. $(\forall)\, n \geq N$ we have

$$|f(n)| \leq c\,|g(n)|$$

(b) (i) $3n^2 + 5n^{\frac{3}{2}} + 6 = o(n^2)$

True: $3n^2 + 5n^{\frac{3}{2}} + 6 < 4n^2 + 5n^{\frac{3}{2}}$ for $n \geq 3$

$4n^2 + 5n^{\frac{3}{2}} < 9n^2$ for $n \geq 3 \Rightarrow$ we take $C = 9$ and $N = 3$

(ii) $n! = o(2^n)$

False: $\frac{n!}{2^n} = \frac{1 \cdot 2 \cdot \dots \cdot n}{2 \cdot 2 \cdot \dots \cdot 2} \to \infty$ as $n \to \infty \Rightarrow n! > 2^n$ for $n \geq 4$

(iii) $\sum_{k=1}^{n} k^2 = o(n^3)$

True: $\frac{n(n+1)(2n+1)}{6} = o(n^3)$

$\frac{n^3 + 2n^2 + n}{6} = o(n^3)$

$\frac{n^3 + 2n^2 + n}{6} < n^3$ for $n \geq 1 \Rightarrow$ we take $C = 1$, $N = 1$

$$\sum_{k=1}^{n} k^2 = o(n^2)$$

False: $\frac{n^3+2n^2+n}{6} < cn^2$

$n^3+2n^2+n < 6cn^2 = dn^2$

Since $n^3 > dn^2$ $(\forall) d \in \mathbb{R}$ for $n$ sufficiently big

(c) $\leq$ partial order on $A$, subset $S \subseteq A$

(i) least upper bound $m \in A$ for $S$ if

- $m$ is an upper bound for $S$: $x \leq m$ $(\forall)$ $x \in S$ and
- if $m'$ is any other upper bound for $S$, then $m \leq m'$

(ii) maximum:

$m$ is the maximum of $S$ if it is an upper bound and $m \in S$

(d) • vectors in plane $(x, y) \in \mathbb{R} \times \mathbb{R}$

• $\leq$ on $\mathbb{R}$

• $\leq_L$ lexicographic order; $\leq_P$ product order

• $S$ = set of vectors in the interior of the unit disc i.e.

$$S = \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid x^2+y^2<1\}$$

• $\leq_L$: $(x,y) \leq_L (z,t)$ if $x<z$ or $(x=z$ and $y \leq t)$

There is no least upper bound for $\leq_L$ since any vector $(1,a)$ is an upper bound as $x^2+y^2<1$ implies that $x \in (-1,1) \Rightarrow (\forall)\ (x,y) \in S \cdot (x,y) \leq_L (1,a)$

and the least upper bound is $(1,a)$, when $a \to -\infty$, so it can't be defined

• $\leq_P$: $(x,y) \leq_P (z,t)$ if $x \leq z$ and $y \leq t$

The least upper bound is $(1,1)$ since $x \leq 1$, $y \leq 1$ for all $(x,y) \in S$ and it cannot be smaller since $x, y \in (-1,1)$.