Discrete Mathematics HW4

20180617 You SeungWoo

October 9, 2023

Problem 1

(a) *Proof.* Suppose some two of them are the same in $\mathbb{Z}_p$. i.e. assume $ma \equiv na \mod p$ for some $1 \leq m, n < p, m \neq n$.

$$\begin{aligned} & ma \equiv na \mod p \\ \Rightarrow\ & ma = kp + na \text{ for some integer } k \\ \Rightarrow\ & (m-n)a = kp \end{aligned}$$

Since $p \nmid a$, $p \mid (m-n)$. This gives $m \equiv n \mod p$. But since $1 \leq m, n < p$, $m = n$. Contradiction. Therefore, no two of them are the same in $\mathbb{Z}_p$.

□

(b) *Proof.* By the *modulo multiplication*,

$$1a \cdot 2a \cdot \cdots \cdot (p-1)a \mod p = [(1a \mod p) \cdot (2a \mod p) \cdot \cdots \cdot ((p-1)a \mod p)] \mod p. \tag{1}$$

By (a), a total of $p-1$ elements of the form ma have different elements in $\mathbb{Z}_p$. i.e. if $m_1 a \equiv n_1 \mod p, m_2 a \equiv n_2 \mod p$ for $1 \leq m_1, m_2, n_1, n_2 < p$, then $n_1 \neq n_2$ if $m_1 \neq m_2$. Since $|\mathbb{Z}_p| = p-1$, all elements in $\mathbb{Z}_p$ appears in RHS of (1). Therefore,

$$\begin{aligned} & 1a \cdot 2a \cdot \cdots \cdot (p-1)a \mod p = 1 \cdot 2 \cdot \cdots \cdot (p-1) \mod p \\ \Rightarrow\ & a^{p-1}(p-1)! \mod p = (p-1)! \mod p \end{aligned}$$

□

(c) *Proof.* Note that $p \nmid k$ for $1 \leq k < p$ because p is a prime. This gives $p \nmid (p-1)!$. Then from (b),

$$\begin{aligned} & a^{p-1}(p-1)! \mod p = (p-1)! \mod p \\ \Rightarrow\ & a^{p-1}(p-1)! = kp + (p-1)! \text{ for some integer } k \\ \Rightarrow\ & \left(a^{p-1} - 1\right)(p-1)! = kp \\ \Rightarrow\ & p \mid a^{p-1} \\ \Rightarrow\ & \left(a^{p-1} - 1\right) \equiv 0 \mod p \\ \Rightarrow\ & a^{p-1} \equiv 1 \mod p \end{aligned}$$

□

Problem 2

Solution. Use the given encoding rule: A $\to$ 00, B $\to$ 01, $\cdots$, Z $\to$ 25. Then UPLOAD $\to$ 20 15 10 14 00 03. Since $n = 3233$ which have 4 digits, divide the code into 4 digits. Then UPLOAD $\to$ 2015 1014 0003. Let $m_1 = 2015, m_2 = 1014, m_3 = 0003$. Encrypt each block by the *RSA method*: $[c_i = m_i^e \mod n]$. Then we get $c_1 = m_1^{17} \mod 3233 = 2545$, $c_2 = m_2^{17} \mod 3233 = 37$, $c_3 = m_3^{17} \mod 3233 = 1211$. Therefore, the result is 2545 0037 1211. Note that you have to write each c_i in 4-digit like 0037 instead 37.

$\square$

Problem 3

Solution. First, find the inverse of $e \mod (p-1)(q-1)$ where $n = pq$, p and q are primes. i.e. find d such that $d \cdot e \equiv 1 \mod (p-1)(q-1)$. Here, $e = 13$, $p = 43$, $q = 59$, $(p-1)(q-1) = 2436$, $n = 2537$. We can use *Euclid algorithm* because of the following:

$$\begin{aligned} & 13d \equiv 1 \mod 2436 \\ \Rightarrow\ & 13d = 2436k + 1 \text{ for some integer } k \\ \Rightarrow\ & 13d + 2436y = 1 = \gcd(13, 2436) \text{ for some integer } y \end{aligned}$$

Since RSA method always gives $gcd(e, (p-1)(q-1)) = 1$, you don't have to show this step. Just run Euclid algorihm directly. Here, we get $d = 937$.
After finding d, decrypt c_i similarly to the previous problem: $[m_i = c_i^d \mod n]$. Then $m_1 = c_1^{937} \mod 2537 = 1808$, $m_2 = c_2^{937} \mod 2537 = 1121$, $m_3 = c_3^{937} \mod 2537 = 417$. Since n have 4 digits, match each m_i to a 4-digit number and cut it by 2. Then 0667 1947 0671 $\rightarrow$ 1808 1121 0417 $\rightarrow$ 18 08 11 21 04 17. Therefore, the result is SILVER.

$\square$

Problem 4

Solution. There is no optimal algorithm to find the secret key! This is known as *Diffie-Hellman problem*. An efficient way for solving this problem is not yet known(intuitively, if such algorithm exists, then it is not a part of cryptology). Therefore, you should try all $k_1, k_2 \in \mathbb{N}$(This is called *Brute-force algorithm*). If we start from 1 and calculate directly, then $k_1 = 10$ and $k_2 = 21$, so $s = 3^{210} \mod 31 = 1$.

□

Problem 5

Proof. Proof by (strong) induction. Let the given statement be $P(j = m)$. Consider $P(j = 1)$. Then $(x_1)^n = \sum_{n_1=n} \frac{n!}{n_1!} x_1^{n_1}$ is true, because $\sum_{n_1=n} \Leftrightarrow n_1 = n$(There is only one case).
Suppose $P(j)$ is true for $j \le m$. Consider $P(j = m+1)$. Note that the notation of x does not matter.

$$\begin{aligned}
& (x_1 + x_2 + \cdots + x_{m-1} + x_{k_1} + x_{k_2})^n \\
= \ & (x_1 + x_2 + \cdots + x_{m-1} + (x_{k_1} + x_{k_2}))^n \\
= \ & (x_1 + x_2 + \cdots + x_{m-1} + x_k)^n \qquad \text{where } x_k = x_{k_1} + x_{k_2} \\
= \ & \sum_{n_1+n_2+\cdots+n_{m-1}+n_k=n} \frac{n!}{n_1!n_2!\cdots n_{m-1}!n_k!} x_1^{n_1} x_2^{n_2} \cdots x_{m-1}^{n_{m-1}} x_k^{n_k}
\end{aligned}$$

Denote $\mu = n_1 + n_2 + \cdots + n_{m-1} + n_k$ and $C = \frac{n!}{n_1!n_2!\cdots n_{m-1}!n_k!} x_1^{n_1} x_2^{n_2} \cdots x_{m-1}^{n_{m-1}}$.

$$\begin{aligned}
\Rightarrow & \sum_{\mu=n} C(x_k)^{n_k} \\
= & \sum_{\mu=n} C(x_{k_1} + x_{k_2})^{n_k} \\
= & \sum_{\mu=n} C \left[\sum_{n_{k_1}+n_{k_2}=n_k} \frac{n_k!}{n_{k_1}!n_{k_2}!} x_{k_1}^{n_{k_1}} x_{k_2}^{n_{k_2}} \right]
\end{aligned}$$

Since C is independent to k_1 and k_2, it is constant related to inner $\sum$. Put C into inner $\sum$.

$$\begin{aligned}
\Rightarrow & \sum_{\mu=n} \left[\sum_{n_{k_1}+n_{k_2}=n_k} C \frac{n_k!}{n_{k_1}!n_{k_2}!} x_{k_1}^{n_{k_1}} x_{k_2}^{n_{k_2}} \right] \\
= & \sum_{\mu=n} \left[\sum_{n_{k_1}+n_{k_2}=n_k} \frac{n!}{n_1!n_2!\cdots n_{m-1}! \cancel{n_k}!} x_1^{n_1} x_2^{n_2} \cdots x_{m-1}^{n_{m-1}} \frac{\cancel{n_k}!}{n_{k_1}!n_{k_2}!} x_{k_1}^{n_{k_1}} x_{k_2}^{n_{k_2}} \right] \\
= & \sum_{\mu=n} \left[\sum_{n_{k_1}+n_{k_2}=n_k} \frac{n!}{n_1!n_2!\cdots n_{m-1}!n_{k_1}!n_{k_2}!} x_1^{n_1} x_2^{n_2} \cdots x_{m-1}^{n_{m-1}} x_{k_1}^{n_{k_1}} x_{k_2}^{n_{k_2}} \right] \\
= & \sum_{n_1+n_2+\cdots+n_{m-1}+n_k=n} \left[\sum_{n_{k_1}+n_{k_2}=n_k} \frac{n!}{n_1!n_2!\cdots n_{m-1}!n_{k_1}!n_{k_2}!} x_1^{n_1} x_2^{n_2} \cdots x_{m-1}^{n_{m-1}} x_{k_1}^{n_{k_1}} x_{k_2}^{n_{k_2}} \right]
\end{aligned}$$

Here, the caculation order is [outer $\sum \rightarrow$ inner $\sum$]. This means n_k is selected at outer $\sum$ at first and then n_{k_1} and n_{k_2} is selected at inner $\sum$. In this process, the inner formula does not effected, just related to selection of all n_i. Therefore, we can merge two $\sum$ by putting $n_k = n_{k_1} + n_{k_2}$.

$$\Rightarrow \sum_{n_1+n_2+\cdots+n_{m-1}+[n_{k_1}+n_{k_2}]=n} \frac{n!}{n_1!n_2!\cdots n_{m-1}!n_{k_1}!n_{k_2}!} x_1^{n_1} x_2^{n_2} \cdots x_{m-1}^{n_{m-1}} x_{k_1}^{n_{k_1}} x_{k_2}^{n_{k_2}}$$

Replace $k_1 = m$ and $k_2 = m+1$, then we get the desired equation.

□

Problem 6

Proof. Proof by (strong) induction. Let the given statement be $P(j = n)$. Consider $P(j = 1)$. Then $|X_1| = \sum_{1\le i\le 1} |X_i|$ is true, because $\sum_{1\le i\le 1} \Leftrightarrow i = 1$(There is only one case).
Suppose $P(j)$ is true for $j \le n$. Consider $P(j = n + 1)$.

$$\begin{aligned} & |X_1 \cup X_2 \cup \cdots \cup X_n \cup X_{n+1}| \\ = \; & |(X_1 \cup X_2 \cup \cdots \cup X_n) \cup X_{n+1}| \end{aligned}$$

Denote $X_\mu = X_1 \cup X_2 \cup \cdots \cup X_n$.

$$\begin{aligned} \Rightarrow \; & |X_\mu \cup X_{n+1}| \\ = \; & \sum_{i=\mu,n+1} |X_i| - \sum_{(i,j)=(\mu,n+1)} |X_i \cap X_j| \\ = \; & |X_\mu| + |X_{n+1}| - |X_\mu \cap X_{n+1}| \\ = \; & |X_1 \cup X_2 \cup \cdots \cup X_n| + |X_{n+1}| - |(X_1 \cup X_2 \cup \cdots \cup X_n) \cap X_{n+1}| \end{aligned}$$

Note that *Distributive law of sets*: [for all sets $A, B,$ and $C, A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$]. Apply this to the second term.

$$\begin{aligned} \Rightarrow \; & |X_1 \cup X_2 \cup \cdots \cup X_n| + |X_{n+1}| - |(X_1 \cap X_{n+1}) \cup (X_2 \cap X_{n+1}) \cup \cdots \cup (X_n \cap X_{n+1})| \\ = \; & \sum_{1\le i\le n} |X_i| - \sum_{1\le i<j\le n} |X_i \cap X_j| + \sum_{1\le i<j<k\le n} |X_i \cap X_j \cap X_k| - \cdots (-1)^{n+1} |X_1 \cap X_2 \cap \cdots \cap X_n| \\ & + |X_{n+1}| \\ & - \left[\sum_{1\le i\le n} |X_i \cap X_{n+1}| - \sum_{1\le i<j\le n} |X_i \cap X_j \cap X_{n+1}| \right. \\ & \left. + \sum_{1\le i<j<k\le n} |X_i \cap X_j \cap X_k \cap X_{n+1}| - \cdots (-1)^{n+1} |X_1 \cap X_2 \cap \cdots \cap X_n \cap X_{n+1}| \right] \\ = \; & \sum_{1\le i\le n} |X_i| - \sum_{1\le i<j\le n} |X_i \cap X_j| + \sum_{1\le i<j<k\le n} |X_i \cap X_j \cap X_k| - \cdots (-1)^{n+1} |X_1 \cap X_2 \cap \cdots \cap X_n| \\ & + |X_{n+1}| \\ & - \sum_{1\le i\le n} |X_i \cap X_{n+1}| + \sum_{1\le i<j\le n} |X_i \cap X_j \cap X_{n+1}| \\ & - \sum_{1\le i<j<k\le n} |X_i \cap X_j \cap X_k \cap X_{n+1}| + \cdots (-1)^{n+2} |X_1 \cap X_2 \cap \cdots \cap X_n \cap X_{n+1}| \end{aligned}$$

Combine term-by-term. For example, $|X_{n+1}|$ is the same as $|X_i|$ for $i = n + 1$, so we can put in $\sum_{1\le i\le n} |X_i|$. Then we get $\sum_{1\le i\le n+1} |X_i|$. For next term, since $\sum_{1\le i\le n} |X_i \cap X_{n+1}| = \sum_{1\le i<j=n+1} |X_i \cap X_j|$, we can put it into $\sum_{1\le i<j\le n} |X_i \cap X_j|$. Then we get $\sum_{1\le i<j\le n+1} |X_i \cap X_j|$. The equation after combining is the same as desired. Note that the number of terms of the result is $n+1$(When a complete formula cannot be written, it is better to write down the number of terms but not necessary).

□

Problem 7

Proof. First, note that ${}_n\mathrm{C}_k = C(n,k) = \binom{n}{k}$. I use the notation ${}_n\mathrm{C}_k$.
The string has k 0's and $n-k$ 1's. List the 1's in a row.

$$\underbrace{1 \quad 1 \quad 1 \quad \cdots \quad 1}_{\text{total } n-k \text{ 1's}}$$

There are a total of $n-k+1$ places where you can place 0's(red spots in below).

$$\underbrace{\bullet \quad 1 \quad \bullet \quad 1 \quad \bullet \quad \cdots \quad \bullet \quad 1 \quad \bullet}_{\text{total } n-k \text{ 1's and } n-k+1 \ \bullet\text{'s}}$$

Choose k $\bullet$'s among $(n-k+1)$ $\bullet$'s and put 0. This is the total number of cases, ${}_{n-k+1}\mathrm{C}_k$.

$\square$

Problem 8

Proof. The biggest digits of a number is 7, but it is only one case: 1,000,000. This number does not satisfy the desired statement. Therefore, just consider 1 to 999,999. The biggest digits of a number is 6. Let each digits be $a_1, a_2, \cdots, a_6$. i.e. $12345 = 012345 \to a_1 = 0, a_2 = 1, a_3 = 2, a_4 = 3, a_5 = 4, a_6 = 5$. Initialize them to 0. We want to make them satisfy the formula below.

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = 15$$

Use the following algorithm:

1) Choose one of a_i, and $a_i = a_i + 1$

2) Repeat 1) 15 times.

If we list them after this process, the number satisfies the given statement if all $0 \leq a_i \leq 9$. This cases are total ${}_6\mathrm{H}_{15} = {}_{6+15-1}\mathrm{C}_{6-1} = {}_{20}\mathrm{C}_5$. But it contains some $a_i \geq 10$. We need to discard this.
Suppose one $a_j \geq 10$. Then since $\sum\limits_{i \text{ in others}} a_i = 15 - a_j < 10$, others cannot be greater than 10. Therefore, just choose one of them and consider it as greater than or equal to 10. For that element, we have total 6 impossible numbers: $10, 11, 12, 13, 14, 15$. Calculate them case-by-case. For example, WLOG, suppose $a_6 = 10$. Then $a_1 + a_2 + \cdots + a_5 = 15 - a_6 = 5$. This cases are ${}_5\mathrm{H}_5$. If $a_6 = 11$, then $a_1 + a_2 + \cdots + a_5 = 15 - a_6 = 4$, so ${}_5\mathrm{H}_4$. Continue this, then we get $\sum\limits_{k=10}^{15} {}_5\mathrm{H}_{15-k}$ if $a_6 = 10, 11, 12, \cdots, 15$. There are a total of ${}_6\mathrm{C}_1 = 6$ choices for the way to choose a_6 position: $a_1, a_2, \cdots, a_6$. Therefore, total impossible cases are $6 \sum\limits_{k=10}^{15} {}_5\mathrm{H}_{15-k}$.

APPENDIX: it is allowed to write up to this, but it is better to calculate $\sum\limits_{k=10}^{15} {}_5\mathrm{H}_{15-k}$.

$$\begin{aligned}
&\sum_{k=10}^{15} {}_5\mathrm{H}_{15-k} \\
&= {}_5\mathrm{H}_5 + {}_5\mathrm{H}_4 + \cdots + {}_5\mathrm{H}_0 \\
&= {}_{5+5-1}\mathrm{C}_{5-1} + {}_{5+4-1}\mathrm{C}_{5-1} + \cdots + {}_{5+0-1}\mathrm{C}_{5-1} \\
&= {}_9\mathrm{C}_4 + {}_8\mathrm{C}_4 + \cdots + {}_4\mathrm{C}_4 \\
&= {}_9\mathrm{C}_4 + {}_8\mathrm{C}_4 + \cdots + {}_5\mathrm{C}_4 + {}_5\mathrm{C}_5
\end{aligned}$$

By the *Pascal's rule*: $[{}_n\mathrm{C}_r + {}_n\mathrm{C}_{r+1} = {}_{n+1}\mathrm{C}_{r+1}]$, that expression can be compressed.

$$\begin{aligned}
&\Rightarrow {}_9\mathrm{C}_4 + {}_8\mathrm{C}_4 + \cdots + {}_5\mathrm{C}_4 + {}_5\mathrm{C}_5 \\
&= {}_9\mathrm{C}_4 + {}_8\mathrm{C}_4 + {}_7\mathrm{C}_4 + {}_6\mathrm{C}_4 + {}_6\mathrm{C}_5 \\
&= {}_9\mathrm{C}_4 + {}_8\mathrm{C}_4 + {}_7\mathrm{C}_4 + {}_7\mathrm{C}_5 \\
&= \cdots = {}_9\mathrm{C}_4 + {}_9\mathrm{C}_5 \\
&= {}_{10}\mathrm{C}_5
\end{aligned}$$

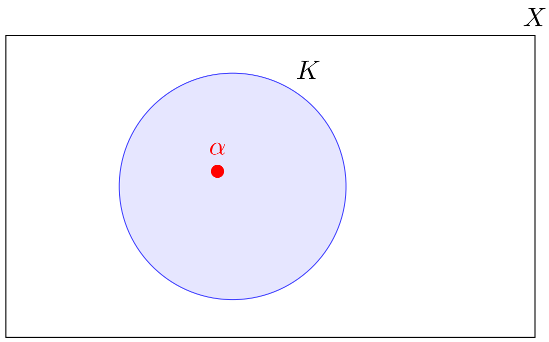
Therefore, the result is ${}_{20}\mathrm{C}_5 - 6 \cdot {}_{10}\mathrm{C}_5 = 13992$.

$\square$

Problem 9

(a) *Proof.* Consider the below situation:

Let X be a set with $|X| = n$. Make a new subset of X with k elements, let the subset be K. Choose one element in K, let it be α.



There are 2 ways to make this:

- Make K and choose α from K
- Choose α from X and make K including α

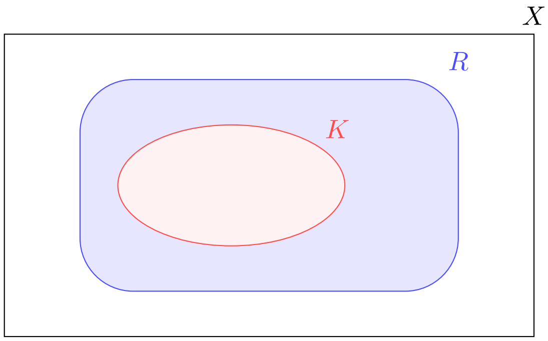
The first way is ${}_n\mathrm{C}_k \cdot {}_k\mathrm{C}_1 = k \cdot {}_n\mathrm{C}_k$ (make K be ${}_n\mathrm{C}_k$, choose α be ${}_k\mathrm{C}_1$).
The second way is ${}_n\mathrm{C}_1 \cdot {}_{n-1}\mathrm{C}_{k-1} = n \cdot {}_{n-1}\mathrm{C}_{k-1}$ (choose α be ${}_n\mathrm{C}_1$, make K be ${}_{n-1}\mathrm{C}_{k-1}$).
Therefore, $k \cdot {}_n\mathrm{C}_k = n \cdot {}_{n-1}\mathrm{C}_{k-1}$.
WARNING: This method is called *combinatorial argument*. You **MUST** tell the story in **sentences**, not in figures. Figures are not necessary, just for supporting purposes only. Drawing is not a logical explanation. If you only draw figures and do not write specific sentences, then you may get close to 0 points.
APPENDIX: The *algebraic argument* is just calculate directly like following:

$$\begin{aligned}
&k \cdot {}_n\mathrm{C}_k \\
&= k \cdot \frac{n!}{k!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k)!} \\
&= n \cdot \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= n \cdot \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= n \cdot \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} \\
&= n \cdot {}_{n-1}\mathrm{C}_{k-1}
\end{aligned}$$

□

(b) *Proof.* Consider the below situation:

Let X be a set with $|X| = n$. Make a new subset of X with r elements, let the subset be R. Make a new subset of R with k elements, let it be K.



There are 2 ways to make this:

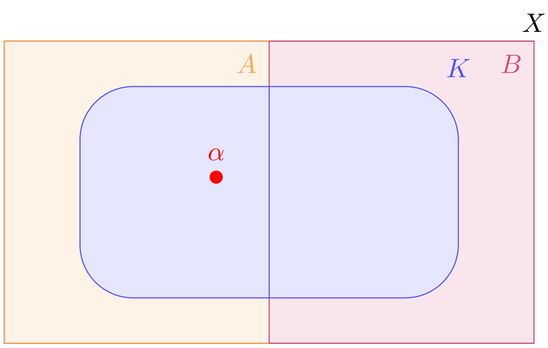
- Make R from X and make K from R
- Make K from X and make R including K

The first way is ${}_n\mathrm{C}_r \cdot {}_r\mathrm{C}_k$ (make R be ${}_n\mathrm{C}_r$, make K be ${}_r\mathrm{C}_k$).
The second way is ${}_n\mathrm{C}_k \cdot {}_{n-k}\mathrm{C}_{r-k}$ (make K be ${}_n\mathrm{C}_k$, make R be ${}_{n-k}\mathrm{C}_{r-k}$).
Therefore, ${}_n\mathrm{C}_r \cdot {}_r\mathrm{C}_k = {}_n\mathrm{C}_k \cdot {}_{n-k}\mathrm{C}_{r-k}$.

□

(c) *Proof.* Consider the below situation:

Let X be a set with $|X| = 2n$. There are 2 subsets of X: A and B. They satisfy $|A| = n, |B| = n, A \cap B = \emptyset$. Make a new subset of X with n elements, let the subset be K. Choose one element in $A \cap K$, let it be α.



There are 2 ways to make this:

- Make K from X(Choose from A and B each) and choose α from $A \cap K$
- Choose α from A and make K from X including α

Consider the first way. if you choose k elements from A, then you can choose $n-k$ elements in B. This gives ${}_n\mathrm{C}_k \cdot {}_n\mathrm{C}_{n-k} = ({}_n\mathrm{C}_k)^2$. This is true for $1 \leq k \leq n$. Note that $k = 0$ is impossible because we need to choose α in A. Choose α gives ${}_k\mathrm{C}_1 = k$. From here, we get $\sum\limits_{k=1}^{n} k\left({}_n\mathrm{C}_k\right)^2$.
The second way is ${}_n\mathrm{C}_1 \cdot {}_{2n-1}\mathrm{C}_{n-1} = n \cdot {}_{2n-1}\mathrm{C}_{n-1}$ (choose α be ${}_n\mathrm{C}_1$, make K be ${}_{2n-1}\mathrm{C}_{n-1}$).
Therefore, $\sum\limits_{k=1}^{n} k\left({}_n\mathrm{C}_k\right)^2 = n \cdot {}_{2n-1}\mathrm{C}_{n-1}$.

□

Problem 10

Proof. Proof by induction. Let the given statement be $P(j=r)$. Consider $P(j=1)$. Then

$$\begin{aligned}\sum_{k=0}^{1} {}_{n+k}\mathrm{C}_k &= {}_n\mathrm{C}_0 + {}_{n+1}\mathrm{C}_1 \\ &= {}_{n+1}\mathrm{C}_0 + {}_{n+1}\mathrm{C}_1 \\ &= {}_{n+2}\mathrm{C}_1\end{aligned}$$

by the *Pascal's rule*: $[{}_n\mathrm{C}_r + {}_n\mathrm{C}_{r+1} = {}_{n+1}\mathrm{C}_{r+1}]$. Therefore, $P(j=1)$ is true.
Suppose $P(j=r)$ is true, consider $P(j=r+1)$.

$$\begin{aligned}\sum_{k=0}^{r+1} {}_{n+k}\mathrm{C}_k &= \sum_{k=0}^{r} {}_{n+k}\mathrm{C}_k + {}_{n+r+1}\mathrm{C}_{r+1} \\ &= {}_{n+r+1}\mathrm{C}_r + {}_{n+r+1}\mathrm{C}_{r+1} \\ &= {}_{n+r+2}\mathrm{C}_{r+1}\end{aligned}$$

Therefore, $P(j=r+1)$ is true.

□