Homework 04

CS499-Mathematical Foundations of Computer Science, Jie Li, Spring 2020.

Name: 方泓杰(Hongjie Fang) Student ID: 518030910150 Email: galaxies@sjtu.edu.cn

1 Exercises of Chapter 4

7. Ten people numbered 1 to 10 are lined up in a circle as in the Josephus problem, and every m-th person is executed (The value of m may be much larger than 10.) Prove that the first three people to go cannot be 10, k and $(k+1)$ (in this order), for any k.

   Proof. Suppose there exists a k that the first three people to go are 10, k and $(k+1)$ (in this order). Then we can derive the following formulas based on the premises.

   - The first people to go is 10, then we have
   $$m \equiv 0 \pmod{10} \tag{1}$$
   - The second people to go is k, then we have
   $$m \equiv k - 0 = k \pmod 9 \tag{2}$$
   - The third people to go is $(k+1)$, then we have
   $$m \equiv (k+1) - k = 1 \pmod 8 \tag{3}$$

   Equation (1) suggests that m is an even number, which contradicts with the conclusion derived by Equation (3) that m is an odd number.

   Therefore, the first three people to go cannot be 10, k and $(k+1)$ (in this order). $\square$

8. The residue number system $(x \mod 3,\ x \mod 5)$ considered in the text has the curious property that 13 corresponds to $(1, 3)$, which looks almost the same. Explain how to find all instances of such a coincidence, without calculating all fifteen pairs of residues. In other words, find all solutions to the congruences
$$10u + v \equiv u \pmod 3, \quad 10u + v \equiv v \pmod 5.$$
   Hint: Use the facts that $10u + 6v \equiv u \pmod 3$ and $10u + 6v \equiv v \pmod 5$.

   Solution. We can make the following derivations according to the premises.
$$\begin{aligned} 10u + v \equiv u \pmod 3 &\implies v \equiv 9u \pmod 3 \\ &\implies v \equiv 0 \pmod 3 \end{aligned}$$
   We also have the restrictions that $0 \le u < 3$ and $0 \le v < 5$. Therefore, we have $u = 0, 1, 2$ and $v = 0, 3$. Thus, all the possible solutions are $0, 3, 10, 13, 20, 23$. $\square$

9. Show that $(3^{77}-1)/2$ is odd and composite. Hint: What is 3^{77} mod 4?

Proof. It's easy to derive the following conclusions by induction of k.

$$3^{2k} \equiv 1 \pmod 4, \quad 3^{2k+1} \equiv 3 \pmod 4.$$

Let k be 38 then we can make the following derivations.

$$\begin{aligned} 3^{77} \equiv 3 \pmod 4 \quad &\Longrightarrow \quad 3^{77}-1 \equiv 2 \pmod 4 \\ &\Longrightarrow \quad 3^{77}-1 = 4p+2 \quad (p \in \mathbb{Z}) \\ &\Longrightarrow \quad \frac{3^{77}-1}{2} = 2p+1 \quad (p \in \mathbb{Z}) \\ &\Longrightarrow \quad \frac{3^{77}-1}{2} \equiv 1 \pmod 2 \end{aligned}$$

Therefore, $(3^{77}-1)/2$ is odd.

According to the summation formula of geometric sequence, we have the following equation (Equation (4)).

$$\frac{3^{77}-1}{2} = 3^0 + 3^1 + \cdots + 3^{76} = \sum_{i=0}^{76} 3^i \tag{4}$$

Therefore, $(3^{77}-1)/2$ is divisible by $\sum_{i=0}^{6} 3^i$ (also known as $(3^7-1)/2$) because of the following equation (Equation (5)).

$$\frac{\sum_{i=0}^{76} 3^i}{\sum_{i=0}^{6} 3^i} = 3^0 + 3^7 + 3^{14} + \cdots + 3^{70} = \sum_{i=0}^{10} 3^{7i} \in \mathbb{Z} \tag{5}$$

Therefore, $(3^{77}-1)/2$ is composite. In conclusion, $(3^{77}-1)/2$ is odd and composite. □

10. Compute $\varphi(999)$.

Solution. Since $999 = 3 \times 11 \times 37$, the result can be derived as follows (Equation (6)).

$$\varphi(999) = \varphi(3) \cdot \varphi(11) \cdot \varphi(37) = 2 \times 10 \times 36 = 720 \tag{6}$$

□

11. Find a function $\sigma(n)$ with the property that

$$g(n) = \sum_{0 \le k \le n} f(k) \quad \Longleftrightarrow \quad f(n) = \sum_{0 \le k \le n} \sigma(k) g(n-k)$$

(This is analogous to the *Möbius Function*; see (4.56) in textbook.)

Solution. It's obvious that $g(n) - g(n-1) = f(n)$ for any $n > 0$. Therefore, we set $\sigma(n)$ as follows (Equation (7)).

$$\sigma(n) = \begin{cases} 1 & (n = 0) \\ -1 & (n = 1) \\ 0 & (otherwise) \end{cases} \tag{7}$$

It's easy to verify that $\sigma(n)$ satisfies the conditions because of the property we stated above. □

12. Simplify the formula $\sum_{d|m}\sum_{k|d}\mu(k)g(d/k)$.

Solution. The result is $g(m)$ according to Equation (8).

$$
\begin{aligned}
\sum_{d|m}\sum_{k|d}\mu(k)g\left(\frac{d}{k}\right) &= \sum_{i|m}\sum_{j|(m/i)}\mu(j)g(i) \\
&= \sum_{i|m} g(i)\cdot\left(\sum_{j|(m/i)}\mu(j)\right) \\
&= \sum_{i|m} g(i)\cdot[m/i == 1] \\
&= g(m)
\end{aligned}
\tag{8}
$$

□

13. A positive integer n is called square-free if it is not divisible by m^2 for any $m > 1$. Find a necessary and sufficient condition that n is square-free,

a in terms of the prime-exponent representation ((4.11) in textbook) of n;

b in terms of $\mu(n)$.

Solution. The conditions are as follows.

a $n_p \le 1$ for all p.

Proof. We are going to prove that n is square-free $\Longleftrightarrow$ $n_p \le 1$ for all p.
($\Longleftarrow$) If n satisfies the condition that $n_p \le 1$ for all p, then no prime divisors appears twice in n, that is, there exists no prime p such that $p^2 \mid n$. Therefore, there exists no integer m ($m > 1$) such that $m^2 \mid n$, which indicates that n is square-free.
($\Longrightarrow$) If n is square-free, then there exists no prime number p such that $p^2 \mid n$. Therefore, we must have $n_p \le 1$ for all p. □

b $\mu(n) \ne 0$.

Proof. We are going to prove that $n_p \le 1$ for all $p \Longleftrightarrow \mu(n) \ne 0$ first.
Since $\mu(\cdot)$ is a multiplicative function, $\mu(n) = \prod_p \mu(p^{n_p})$.
($\Longleftarrow$) If $\mu(n) \ne 0$, then we must have $\mu(p^{n_p}) \ne 0$ for all prime p, that is, $n_p \le 1$ for all p.
($\Longrightarrow$) If we have $n_p \le 1$ for all p, then $\mu(p^{n_p}) \ne 0$. Therefore, $\mu(n) = \prod_p \mu(p^{n_p}) \ne 0$.
Combine the conclusion with the previous conclusion that n is square-free $\Longleftrightarrow$ $n_p \le 1$ for all p, we can derive that n is square-free $\Longleftrightarrow$ $\mu(n) \ne 0$. □

□

2 Exercises of Chapter 5

1. What is 11^4? Why is this number easy to compute for a person who knows binomial coefficients?

   Solution. Actually, $11^4 = 14641$, which is exactly the binomial coefficients arranged in order. This is because of the following equation (Equation (9)).

$$11^n = (10+1)^n = \sum_{k=0}^{n} \binom{n}{k} 10^k \tag{9}$$

   where, $\binom{n}{k}$ is the binomial coefficients. Therefore, we can compute 11^n easily by combining the binomial coefficients together in order.

   What's more, we have $(11)_r^4 = (14641)_r$, where r is the radix number satisfying $r \geq 7$, which is a more general conclusion. □

2. For which value(s) of k is $\binom{n}{k}$ a maximum, when n is a given positive integer? Prove your answer.

   Conclusion. *The maximum occurs when $k = \lfloor n/2 \rfloor$ and $k = \lceil n/2 \rceil$.*

   Proof. Considering two consecutive binomial coefficients $\binom{n}{k}$ and $\binom{n}{k+1}$, we have Equation (10).

$$\frac{\binom{n}{k+1}}{\binom{n}{k}} = \frac{n-k}{k+1} \tag{10}$$

   Therefore,

   - When $k < \lceil \frac{n}{2} \rceil$, we have $\frac{n-k}{k+1} \geq 1$, which means $\binom{n}{k+1} \geq \binom{n}{k}$.
   - When $k \geq \lfloor \frac{n}{2} \rfloor$, we have $\frac{n-k}{k+1} \leq 1$, which means $\binom{n}{k+1} \leq \binom{n}{k}$.

   Thus,

   - If n is an odd number, then the maximum occurs when $k = \lfloor n/2 \rfloor$ and $k = \lceil n/2 \rceil$;
   - If n is an even number, then the maximum occurs when $k = \lfloor n/2 \rfloor = \lceil n/2 \rceil = n/2$.

   In conclusion, the maximum occurs when $k = \lfloor n/2 \rfloor$ and $k = \lceil n/2 \rceil$. □

3. Prove the hexagon property.

$$\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} = \binom{n-1}{k}\binom{n+1}{k+1}\binom{n}{k-1}$$

   Proof. We can prove the property by simply unfold the notations of binomial coefficients, as Equation (11) shown.

$$\begin{aligned}
\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} \cdot \frac{n!}{(k+1)!(n-k-1)!} \cdot \frac{(n+1)!}{k!(n-k+1)!} \\
&= \frac{(n-1)!}{k!(n-k-1)!} \cdot \frac{(n+1)!}{(k+1)!(n-k)!} \cdot \frac{n!}{(k-1)!(n-k+1)!} \\
&= \binom{n-1}{k}\binom{n+1}{k+1}\binom{n}{k-1}
\end{aligned} \tag{11}$$

   □

4. Evaluate $\binom{-1}{k}$ by negating (actually un-negating) its upper index.

Solution. With formula (5.14) in textbook, we can derive Equation (12).

$$\binom{-1}{k} = (-1)^k \binom{k-(-1)-1}{k} = (-1)^k \binom{k}{k} = (-1)^k \tag{12}$$

$\square$

5. Let p be prime. Show that $\binom{p}{k} \bmod p = 0$ for $0 < k < p$. What does this imply about the binomial coefficients $\binom{p-1}{k}$?

Solution. We can derive that $p \mid \binom{p}{k}$ as follows.

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = p \cdot \frac{(p-1)!}{(p-k)!k!} \quad \Longrightarrow \quad p \mid \binom{p}{k}$$

The result indicates that $\binom{p}{k} \bmod p = 0$ for $0 < k < p$.

Suppose $\binom{p-1}{k} \equiv f(k) \pmod p$. Because of the facts that $\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$ and $\binom{p}{k} \bmod p = 0$, we can derive the following equation (Equation (13)).

$$f(k) + f(k-1) \equiv 0 \pmod p \tag{13}$$

Therefore, we have $f(k) \equiv f(k-2) \pmod p$ for $k \geq 2$.

Then we are going to determine the values of $f(0)$ and $f(1)$. With the facts that $\binom{p-1}{0} = 1$ and $\binom{p-1}{1} = p-1$, we can set $f(0) = 1$ and $f(1) = -1$ since $-1 \equiv p-1 \pmod p$. Therefore, we can derive the general formula $f(k) = (-1)^k$. The property of binomial coefficients $\binom{p-1}{k}$ is as follows (Equation (14)).

$$\binom{p-1}{k} \equiv (-1)^k \pmod p \tag{14}$$

$\square$

6. Fix up the text's derivation in Problem 6, Section 5.2, by correctly applying symmetry.

Solution. We must add a restriction $k \geq 0$ when we use symmetry. Then we fix a part of the derivation as follows (Equation (15)).

$$\begin{aligned}
\frac{1}{n+1} \sum_k \binom{n+k}{k} \binom{n+1}{k+1} (-1)^k &= \frac{1}{n+1} \sum_{k \geq 0} \binom{n+k}{(n+k)-k} \binom{n+1}{k+1} (-1)^k \\
&= \frac{1}{n+1} \sum_{k \geq 0} \binom{n+k}{n} \binom{n+1}{k+1} (-1)^k \\
&= \frac{1}{n+1} \left(-\binom{n-1}{n} \binom{n+1}{0} (-1)^{-1} + \sum_k \binom{n+k}{n} \binom{n+1}{k+1} (-1)^k \right) \\
&= [n=0] + \frac{1}{n+1} (-1)^n \binom{n-1}{-1} \\
&= [n=0]
\end{aligned} \tag{15}$$

Then the answer $[n = 0]$ is the correct answer according to textbook. $\square$