Homework 03

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 3

1. When we analyzed the Josephus problem in Chap 1, we represented an arbitrary positive integer n in the form $n = 2^m + l$, where $0 \le l < 2^m$. Give explicit formulas for l and m as functions of n, using floor and/or ceiling brackets.

   Solution. The explicit formulas for l and m as functions of n are as follows (Equation (1)).

   $$m = \lfloor \log_2 n \rfloor, \quad l = n - 2^m = n - 2^{\lfloor \log_2 n \rfloor} \tag{1}$$

   □

2. What is a formula for the nearest integer to a given real number x? In case of ties, when x is exactly halfway between two integers, give an expression that rounds **(a)** up - that is, to $\lceil x \rceil$; **(b)** down - that is, to $\lfloor x \rfloor$.

   Solution. **(a)** If we use round-up when x is halfway between two integers, then $\lfloor x + 0.5 \rfloor$ is the nearest integer to a given real number x; **(b)** If we use round-down when x is halfway between two integers, then $\lceil x - 0.5 \rceil$ is the nearest integer to a given real number x. □

3. Evaluate $\lfloor \lfloor m\alpha \rfloor n/\alpha \rfloor$, when m and n are positive integers and α is an irrational number greater than n.

   Solution. The formula can be derived as follows (Equation (2)), noticing that $0 \le \{\cdot\} < 1$ and $0 < n/\alpha < 1$.

   $$\begin{aligned} \lfloor \lfloor m\alpha \rfloor n/\alpha \rfloor &= \lfloor (m\alpha - \{m\alpha\}) n/\alpha \rfloor \\ &= \lfloor mn - \{m\alpha\} \cdot (n/\alpha) \rfloor \\ &= mn + \lfloor -\{m\alpha\} \cdot (n/\alpha) \rfloor \\ &= mn - 1 \end{aligned} \tag{2}$$

   □

4. The text describes the problems at levels 1 through 5. What is a level 0 problem? (This, by the way, is not a level 0 problem.)

   Solution. In my opinion, a level 0 problem is the problem which only requires us to guess the conclusions - even without proving them! □

5. Find a necessary and sufficient condition that $\lfloor nx \rfloor = n\lfloor x \rfloor$, when n is a positive integer. (Your condition should involve $\{x\}$.)

   Solution. The condition and the derivation process are as follows (Equation (3)).

   $$\begin{aligned} \lfloor nx \rfloor = n\lfloor x \rfloor &\iff \lfloor nx \rfloor = nx - n\{x\} \\ &\iff nx - n\{x\} \le nx < nx - n\{x\} + 1 \\ &\iff \{x\} < \frac{1}{n} \end{aligned} \tag{3}$$

   □

6. Can something interesting be said about $\lfloor f(x) \rfloor$ when $f(x)$ is a continuous monotonically decreasing function that takes integer values only when x is an integer?

Conclusion. $\lfloor f(x) \rfloor = \lfloor f(\lceil x \rceil) \rfloor$.

Proof. Notice that $x \le \lceil x \rceil$. If $x = \lceil x \rceil$, then the conclusion is obviously true. Consider about the condition that $x < \lceil x \rceil$. $f(x)$ is a continuous monotonically decreasing function and $\lfloor \cdot \rfloor$ is a monotonically non-decreasing function, so $\lfloor f(x) \rfloor$ is a monotonically non-increasing function, which means that $\lfloor f(x) \rfloor \ge \lfloor f(\lceil x \rceil) \rfloor$.

- If $\lfloor f(x) \rfloor = \lfloor f(\lceil x \rceil) \rfloor$, then we derive the conclusion successfully!
- If $\lfloor f(x) \rfloor > \lfloor f(\lceil x \rceil) \rfloor$, then combining with $f(x) \ge \lfloor f(x) \rfloor$, we get the following formula.

$$\lfloor f(\lceil x \rceil) \rfloor < \lfloor f(x) \rfloor \le f(x)$$

  Since $\lfloor f(x) \rfloor$ is an integer, we can transform the left part of the formula above as follows.

$$f(\lceil x \rceil) < \lfloor f(x) \rfloor \le f(x)$$

  According to the formula above and the property that $f(x)$ is continuous, there exists a y satisfying that $x \le y < \lceil x \rceil$ and $f(y) = \lfloor f(x) \rfloor$. Then we can come to a conclusion that y is an integer because of the special property of $f(x)$ and the fact that $f(y) = \lfloor f(x) \rfloor$ is an integer. However, there is no integer in range $[x, \lceil x \rceil)$ according to the definition of $\lceil \dot{\rceil}$, which leads to a contradiction. Thus, this case cannot happen.

In summary, we prove that $\lfloor f(x) \rfloor = \lfloor f(\lceil x \rceil) \rfloor$ is correct for all $x \in \mathbb{R}$. □

7. Solve the recurrence

$$X_n = \begin{cases} n & (0 \le n < m) \\ X_{n-m} + 1 & (n \ge m) \end{cases}$$

Conclusion. $X_n = \lfloor n/m \rfloor + (n \mod m)$

Proof. We will prove the conclusion by induction.

- The conclusion is obviously true for $0 \le n < m$.
- Suppose the conclusion is true for $km \le n < (k+1)m$ $(k \ge 0)$, we will prove it is still true for $(k+1)m \le n < (k+2)m$. According to the recurrence function, we can derive the following formula (Equation (4)) for all n in range $[(k+1)m, (k+2)m)$.

$$\begin{aligned} X_n &= X_{n-m} + 1 \\ &= \left\lfloor \frac{n-m}{m} \right\rfloor + ((n-m) \mod m) + 1 && \text{(According to the induction hypothesis)} \\ &= \left\lfloor \frac{n}{m} - 1 \right\rfloor + (n \mod m) + 1 && \text{(According to the property of mod)} \\ &= \left\lfloor \frac{n}{m} \right\rfloor - 1 + (n \mod m) + 1 && \text{(According to the property of } \lfloor \cdot \rfloor) \\ &= \left\lfloor \frac{n}{m} \right\rfloor + (n \mod m) \end{aligned} \tag{4}$$

  Hence, we complete the proof process of induction step.

Therefore, the conclusion is correct. □

8. Prove the Dirichlet box principle: If n objects are put into m boxes, some box must contain $\geq \lceil n/m \rceil$ objects, and some box must contain $\leq \lfloor n/m \rfloor$.

   Proof. We divide the principle into two parts and prove them respectively.

   - **Part 1** (some box must contain $\geq \lceil n/m \rceil$ objects): If every box contain strictly less than $\lceil n/m \rceil$ objects, the number of objects is at most $m(\lceil n/m \rceil - 1)$. But we can derive $m(\lceil n/m \rceil - 1) < m \cdot (n/m) = n$, which contradicts the premise that there are n objects. Thus, some box must contain no less than $\lceil n/m \rceil$ objects.
   - **Part 2** (some box must contain $\leq \lfloor n/m \rfloor$ objects): If every box contain strictly more than $\lfloor n/m \rfloor$ objects, the number of objects is at least $m(\lfloor n/m \rfloor + 1)$. But we can derive $m(\lfloor n/m \rfloor + 1) > m \cdot (n/m) = n$, which contradicts the premise that there are n objects. Thus, some box must contain no more than $\lfloor n/m \rfloor$ objects.

   Therefore, we complete the proof of the Dirichlet box principle. □

9. Egyptian mathematicians in 1800 B.C. represented rational numbers between 0 and 1 as sums of unit fractions $1/x_1 + \cdots + 1/x_k$, where the x's were distinct positive integers. For example, they wrote $\frac{1}{3} + \frac{1}{15}$ instead of $\frac{2}{5}$. Prove that it is always possible to do this in a systematic way: if $0 \leq m/n \leq 1$, then

$$\frac{m}{n} = \frac{1}{q} + \left\{ \text{representation of } \left(\frac{m}{n} - \frac{1}{q} \right) \right\}, \qquad q = \left\lceil \frac{n}{m} \right\rceil$$

   (This is Fibonacci's algorithm, due to Leonardo Fibonacci, A.D. 1202.)

   Proof. The process is obviously correct, what we have to prove is that the process will terminates in finite steps. Notice that

$$\frac{m}{n} - \frac{1}{q} = \frac{mq - n}{nq} = \frac{m \cdot \lceil \frac{n}{m} \rceil - n}{n \lceil \frac{n}{m} \rceil} = \frac{n \text{ mumble } m}{n \lceil \frac{n}{m} \rceil}$$

   where, n mumble m is a simplified notation of $(m \cdot \lceil \frac{n}{m} \rceil - n)$, which appears in the textbook.

   Consider about the numerator of the result, we know that $0 \leq n \text{ mumble } m < m$. So the numerator of the rest number will strictly decrease after each step. At first the numerator of the $\frac{m}{n}$ is m, so the process will take at most m steps since the strictly-decreasing property of the numerator. Thus, the process will end in finite steps. So it is always possible to do the process in the systematic way above. □

2 Exercises of Chapter 4

1. What is the smallest positive integer that has exactly k divisors, for $1 \leq k \leq 6$?

   Solution. We can get the following answer after a few calculations.

   - 1 is the smallest positive integer that has exactly 1 divisors (1 itself).
   - 2 is the smallest positive integer that has exactly 2 divisors $(1, 2)$.
   - 4 is the smallest positive integer that has exactly 3 divisors $(1, 2, 4)$.
   - 6 is the smallest positive integer that has exactly 4 divisors $(1, 2, 3, 6)$.
   - 16 is the smallest positive integer that has exactly 5 divisors $(1, 2, 4, 8, 16)$.

- 12 is the smallest positive integer that has exactly 6 divisors $(1, 2, 3, 4, 6, 12)$.

$\square$

2. Prove that $\gcd(m, n) \cdot \mathrm{lcm}(m, n) = m \cdot n$, and use this identity to express $\mathrm{lcm}(m, n)$ in terms of $\mathrm{lcm}(n \mod m, m)$, when $n \mod m \neq 0$. Hint: Use (4.12), (4.14) and (4.15).

   Proof. According to the Equation (4.14) and Equation (4.15) in textbook, we have the following properties.

$$\begin{aligned} k_1 = \gcd(m, n) &\iff \forall p, k_{1,p} = \min(m_p, n_p) \\ k_2 = \mathrm{lcm}(m, n) &\iff \forall p, k_{2,p} = \max(m_p, n_p) \end{aligned}$$

   Suppose $k_1 = \gcd(m, n)$, $k_2 = \mathrm{lcm}(m, n)$, then can get the array $k_{1,p}$ and $k_{2,p}$ using properties above. Therefore, define k as $k_1 \cdot k_2 = \gcd(m, n) \cdot \mathrm{lcm}(m, n)$. According to Equation (5) and Equation (4.12) in textbook, we can derive the following result (Equation (5)).

$$k_p = \min(m_p, n_p) + \max(m_p, n_p) = m_p + n_p \qquad (\forall p) \tag{5}$$

   Using Equation (4.12) in the textbook again, we can derive that $k = mn$, that is, $\gcd(m, n) \cdot \mathrm{lcm}(m, n) = m \cdot n$. $\square$

   Solution. Now we can use this identity to express $\mathrm{lcm}(m, n)$ as follows (Equation (6)).

$$\begin{aligned} \mathrm{lcm}(m, n) &= \frac{mn}{\gcd(m, n})) \\ &= \frac{mn}{\gcd(n \mod m, m)} \\ &= \frac{mn}{\frac{m \cdot (n \mod m)}{\mathrm{lcm}(n \mod m, m)}} \\ &= \mathrm{lcm}(n \mod m, m) \cdot \frac{n}{n \mod m} \end{aligned} \tag{6}$$

$\square$

3. Let $\pi(x)$ be the number of primes not exceeding x. Prove or disprove:

$$\pi(x) - \pi(x - 1) = [x \text{ is prime}]$$

   Solution. If $x \in \mathbb{Z}$, the formula is obviously true. If $x \notin \mathbb{Z}$, then whether x is a prime or not is undefined because prime is defined on the set $\mathbb{Z}$. Thus, we must change the formula as follows (Equation (7)).

$$\pi(x) - \pi(x - 1) = [\lfloor x \rfloor \text{ is prime}] \tag{7}$$

   It is easy to verify that Equation (7) is correct. $\square$

4. What would happen if the Stern-Brocot construction started with the five fractions $(\frac{0}{1}, \frac{1}{0}, \frac{0}{-1}, \frac{-1}{0}, \frac{0}{1})$ instead of with $(\frac{0}{1}, \frac{1}{0})$?

   Solution. In brief, we can get 4 different Stern-Brocot tree between each consecutive pair of the five fractions $(\frac{0}{1}, \frac{1}{0}, \frac{0}{-1}, \frac{-1}{0}, \frac{0}{1})$. From left to right we can get the normal Stern-Brocot tree, the Stern-Brocot tree with denominators negated, the Stern-Brocot tree with both denominators and numerators negated and the Stern-Brocot tree with numerators negated. What's more, the properties of Stern-Brocot tree, such as every fraction $\frac{m}{n}$ satisfying $\gcd(n, m) = 1$ and every consecutive fractions in the same stage $\frac{m}{n}, \frac{m'}{n'}$ satisfying $m'n - mn' = 1$, still hold. $\square$

5. Find simple formulas for L^k and R^k, when L and R are 2×2 matrices of (4.33) in textbook.

Conclusion. *The simple formulas for L^k and R^k are as follows (Equation (8)).*

$$L^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad R^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \tag{8}$$

Proof. We will prove the formula of L^k, and the proof process of the formula of R^k is similar to the proof process of the formula of L^k. We prove the formula of L^k by induction to k.

- When $k = 0$, $L^0 = I$, where I is the identity matrix. The conclusion is obviously correct.
- Suppose the conclusion is correct for k ($k \geq 0$), and we are going to prove that it is still correct for $(k+1)$. We can derive the following equation (Equation (9)

$$L^{k+1} = L^k \cdot L = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix} \tag{9}$$

  Equation (9) shows that the conclusion is correct for $(k+1)$, which completes the induction step.

In summary, the conclusion is correct. □

6. What does $a \equiv b \pmod 0$ mean?

Solution. It means $a = b$, since we have defined $a \bmod 0 = a$ before. □