Mathematical Foundations of Computer Science

Project 9

Zilong Li

Student ID: 518070910095

May 4, 2021

Warmups

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

Solution.

k	1	2	3	4	5	6
n	1	2	4	6	16	12

$\square$

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

Proof.

$$
\begin{aligned}
&\gcd(m,n) \cdot \operatorname{lcm}(m,n)\\
&\quad = p_1^{\min(m_1,n_1)} p_2^{\min(m_2,n_2)} \cdots p_k^{\min(m_k,n_k)} \cdot && \text{(By (4.14))}\\
&\quad\ \ p_1^{\max(m_1,n_1)} p_2^{\max(m_2,n_2)} \cdots p_k^{\max(m_k,n_k)} && \text{(By (4.15))}\\
&\quad = p_1^{\min(m_1,n_1)+\max(m_1,n_1)} p_2^{\min(m_2,n_2)+\max(m_2,n_2)} \cdots p_k^{\min(m_k,n_k)+\max(m_k,n_k)}\\
&\quad = p_1^{m_1+n_1} p_2^{m_2+n_2} \cdots p_k^{m_k+n_k}\\
&\quad = m \cdot n && \text{(By (4.12))}
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{lcm}(m,n) &= \frac{m \cdot n}{\gcd(m,n)}\\
&= \frac{m \cdot n}{\gcd(n \bmod m, m)}\\
&= \frac{m \cdot n}{\frac{m(n \bmod m)}{\operatorname{lcm}(n \bmod m, m)}}\\
&= \frac{m \cdot n}{n \bmod m} \cdot \operatorname{lcm}(n \bmod m, m) && (n \bmod m \ne 0)
\end{aligned}
$$

$\square$

3 Let $\pi(x)$ be the number of primes not exceeding x. Prove or disprove: $\pi(x) - \pi(x-1) = [x \text{ is prime}]$.

Proof. It only holds for x is an integer. x could be a real number. In fact,

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

You can only count primes up to $\lfloor x \rfloor$. And if $\lfloor x \rfloor$ is a prime, $x-1$ will ignore this prime, thus the gap 1. Otherwise, no prime is ignored. $\square$

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

Solution. All fractions m/n with $m|n$ are constructed.

$\left(\frac{0}{-1}, \frac{-1}{0}\right)$ will give the negative part fractions. Initial Stage always give:

$$\begin{aligned}
1 \times 1 - 0 \times 0 &= 1 \\
0 \times 0 - 1 \times (-1) &= 1 \\
(-1) \times (-1) - 0 \times 0 &= 1 \\
0 \times 0 - (-1) \times 1 &= 1
\end{aligned}$$

which satisfies the requirement of

$$m'n - mn' = 1$$

and the chain reaction will continue. $\square$

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

Solution.

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

Prove by mathematical induction.

Basic steps.

$$L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Induction. Assumming that

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

Then,

$$\begin{aligned}
L^k = L^{k-1}L &= \begin{pmatrix} 1 & k-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \\
R^k = R^{k-1}R &= \begin{pmatrix} 1 & 0 \\ k-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}
\end{aligned}$$

As a result, it holds for all $n \in \mathbb{N}_+$.

$\square$

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

Solution. Based on (4.36):

$$a \equiv b \pmod 0 \Leftrightarrow a - b \text{ is a multiple of } 0$$

Thus,

$$a = b$$

□

7 Ten people numbered 1 to 10 are lined up in a circle as in the Josephus problem, and every mth 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. Prove by contradiction. If the first three people to go is 10, k, and $k+1$.

1	2	3	4	5	6	7	8	9	~~10~~
1	2	3	~~4~~	5	6	7	8	9	~~10~~
1	2	3	~~4~~	~~5~~	6	7	8	9	~~10~~

The first step implies that

$$m \bmod 10 = 0$$

The second step implies that

$$m \bmod 9 = k$$

The third step implies that

$$m \bmod 8 = 1$$

A contradiction comes to m can not be both even and odd from the first step and the third step. □

Basics

14 Prove or disprove:

a. $\gcd(km, kn) = k\gcd(m, n)$

Proof. When k is a positive integer, the statement is true. Let

$$\begin{aligned} m &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ n &= p_1^{\beta_1} \cdots p_k^{\beta_k} \\ \gcd(m, n) &= p_1^{\gamma_1} \cdots p_k^{\gamma_k} \end{aligned}$$

where $\gamma_i = \min(\alpha_i, \beta_i)$. If

$$k = p_1^{\theta_1} \cdots p_k^{\theta_k}$$

Then,

$$\begin{aligned} \gcd(km, kn) &= p_1^{\min(\alpha_1+\theta_1, \beta_1+\theta_1)} \cdots p_k^{\min(\alpha_k+\theta_k, \beta_k+\theta_k)} \\ &= p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)} p_1^{\theta_1} \cdots p_k^{\theta_k} \\ &= k \gcd(m, n) \end{aligned}$$

□

b. $\mathrm{lcm}(km, kn) = k\mathrm{lcm}(m, n)$

Proof. When k is a positive integer, the statement is true. Let

$$\begin{aligned} m &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ n &= p_1^{\beta_1} \cdots p_k^{\beta_k} \\ \mathrm{lcm}(m, n) &= p_1^{\gamma_1} \cdots p_k^{\gamma_k} \end{aligned}$$

where $\gamma_i = \max(\alpha_i, \beta_i)$. If

$$k = p_1^{\theta_1} \cdots p_k^{\theta_k}$$

Then,

$$\begin{aligned} \mathrm{lcm}(km, kn) &= p_1^{\max(\alpha_1+\theta_1, \beta_1+\theta_1)} \cdots p_k^{\max(\alpha_k+\theta_k, \beta_k+\theta_k)} \\ &= p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} p_1^{\theta_1} \cdots p_k^{\theta_k} \\ &= k\mathrm{lcm}(m, n) \end{aligned}$$

□

15 Does every prime occur as a factor of some Euclid number e_n?

Solution. No. For example,

$$\begin{aligned} e_1 \bmod 5 &= 2 \\ e_2 \bmod 5 &= 3 \\ e_3 \bmod 5 &= 2 \\ e_4 \bmod 5 &= 3 \\ &\cdots \end{aligned}$$

In fact, because $e_n \neq 5$, if $e_n \bmod 5 = 0$, then e_n is not a prime, which contradicts the property of e_n as a prime. □