Number Theory 1: Unique Factorization

Erzhuo Wang
July 20,2024
Youth STEM Academy

Definition (整除)

The integer n is a divisor of the integer m if there is an integer k such that $m = kn$. In this case we say that m is divisible by n and write $n \mid m$.

Definition (素数)

An integer $n > 1$ is a prime number(素数) if its only positive divisors are 1 and n. Otherwise, n is called composite(合数).

Definition (最大公约数)

Two nonzero integers m and n have a greatest common divisor, denoted $\gcd(m, n)$, that is the greatest integer that is a divisor of both m and n. If $\gcd(m, n) = 1$, we say m and n are coprime.

Definition (最小公倍数)

Two nonzero integers m and n have a leastest common multiple, denoted $\mathrm{lcm}(m, n)$, that is the leastest integer d such that $m|d$, $n|d$.

Prime Factorization

Theorem (Unique Factorization Theorem(唯一因子分解定理))

Every positive integer n can be factored into a product of prime numbers in a unique way, apart from the order of factors. That is

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

where each p_i is prime, each k_i is a positive integer, and $p_1 < p_2 < \cdots < p_m$.
每个正整数 n 可以被唯一分解为不同素数幂的乘积, 这里的唯一指的是素数的幂次和种类均唯一.

Example

$$2640 = 2^2 \times 5 \times 11 \times 12, 2016 = 2^5 \times 3^2 \times 7$$

$\sqrt{2}$ is irrational

Example

$\sqrt{2}$ is an irrational number.
$\sqrt{2}$ 是一个无理数.

Proof: If $\sqrt{2} = \frac{p}{q}, p, q$ are integers, we have $2q^2 = p^2$. On the left side, the power(幂次) of 2 is odd, however, on the right side, the power of 2 is even, which contradicts to the Unique Factorization Theorem.

Perfect Square and Perfect Cube

Definition

A positive integer n is a Perfect Square(**完全平方数**) if $n = k^2$ for some $k \geq 1$.

Definition

A positive integer n is a Perfect Square(**完全平方数**) if $n = k^2$ for some $k \geq 1$.

GCD and LCM(最大公约数, 最小公倍数)

Theorem

Suppose n and m have the following prime factorizations

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}, \quad \text{and} \quad m = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

Then,

$$\gcd(n, m) = p_1^{\min(k_1, e_1)} p_2^{\min(k_2, e_2)} \ldots p_m^{\min(k_m, e_m)}$$

and

$$\operatorname{lcm}(n, m) = p_1^{\max(k_1, e_1)} p_2^{\max(k_2, e_2)} \ldots p_m^{\max(k_m, e_m)}$$

Question

When three positive integers a, b, and c are multiplied together, their product is 100 . Suppose $a < b < c$. In how many ways can the numbers be chosen?
当三个正整数 a, b 和 c 相乘时, 它们的乘积是 100. 假设 $a < b < c$. 数组 (a, b, c) 有多少种选择数字的方法?

Question (更困难的版本)

When three positive integers a, b, and c are multiplied together, their product is 3000. In how many ways can the numbers be chosen?
当三个正整数 a, b 和 c 相乘时, 它们的乘积是 3000. 数组 (a, b, c) 有多少种选择数字的方法? (提示: 使用组合课程中 $x_1 + \cdots + x_k = n, x_i \geq 0$ 的解数公式)

Exercise

Question (AMC 8,2016-20)

The least common multiple of a and b is 12 , and the least common multiple of b and c is 15 . What is the least possible value of the least common multiple of a and c ?
(A) 20 (B) 30 (C) 60 (D) 120 (E) 180

Chinese remainder Theorem(中国剩余定理)

Definition

m 是一个正整数, 如果 $m|a-b$, 我们称 $a \equiv b \pmod m$.

Theorem

$m_1, \ldots, m_k$ 为 k 个两两互素的整数, 则方程

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

在 1 到 $m_1 \ldots m_k$ 内有唯一解 x_0, 且所有解为 $x_0 + km_1 \ldots m_k, k \in \mathbb{Z}$

Exercise

Example

How many positive three-digit integers have a remainder of 2 when divided by 6 , a remainder of 5 when divided by 9 , and a remainder of 7 when divided by 11?
(A) 1 (B) 2 (C) 3 (D) 4 (E) 5

Example (AMC 8, 2017-24, 比较难的一道题)

Mrs. Sanders has three grandchildren, who call her regularly. One calls her every three days, one calls her every four days, and one calls her every five days. All three called her on December 31, 2016. On how many days during the next year did she not receive a phone call from any of her grandchildren?
(A) 78 (B) 80 (C) 144 (D) 146 (E) 152

Homework

Question (AMC 8, 2020-12)

整数 N 满足如下方程, 求 N 的值.

$$5! \cdot 9! = 12 \cdot N!$$

Question (AMC 8, 2016-15)

What is the largest power of 2 that is a divisor of $13^4 - 11^4$.

$13^4 - 11^4$ 质因数分解中 2 的幂次是多少?

Question

How mant ordered pairs (x, y, z) satisfy

$\operatorname{lcm}(x, y) = 72, \operatorname{lcm}(x, z) = 600, \operatorname{lcm}(y, z) = 900.$