数学

临沂一中 Menci

数学

- 数论
  - 模运算
  - 乘法逆元、费马小定理
  - 最大公约数、唯一分解定理、最小公倍数
  - 线性同余方程、扩展欧几里得算法
  - 素数判定、筛法、质因数分解
  - 欧拉函数
- 组合数学
  - 计数原理
  - 排列与组合

数 论

研究整数的性质的数学分支。

模运算

- a 除以 b 的余数，称为 a 模 b，记作 $a \bmod b$。
- a 和 b 模 p 的值相同，称为 a 在模 p 意义下同余于 b，记作 $a \equiv b \pmod p$。

- 对于非负整数 a 和 b（如无特殊说明，下文均为非负整数），有：
- $a + b \equiv (a \bmod p) + (b \bmod p) \pmod p$
- $a - b \equiv (a \bmod p) - (b \bmod p) \pmod p$
- $a \times b \equiv (a \bmod p) \times (b \bmod p) \pmod p$

- 我们将这种性质称为「模运算对加法、减法和乘法封闭」。
- 需要注意的是，除法不满足上述性质。

乘法逆元

- 对于**互质**的非负整数 a 与 p，存在

$$ax \bmod p = 1$$

- 称 x 是 a 在模 p 意义下的乘法逆元，记作 a^{-1}。
- 乘法逆元可用于计算模意义下的除法。

费马小定理

- 对于正整数 a 与**质数** p（其中 a 不是 p 的倍数），有

$$a^{p-1} \bmod p = 1$$

- 可用于求解乘法逆元：

$$a^{-1} \equiv a^{p-2} \pmod p$$

- 仅适用于 p 为质数的情况。

最大公约数

- 能同时整除 a 与 b 的最大的数，称为 a 与 b 的最大公约数，记作 $\gcd(a,b)$，简写为 (a,b)。
- 当 $a>b$ 时，有

$$\gcd(\mathrm{a},\mathrm{b})=\gcd(a,a-b)=\gcd(b,a-b)$$

欧几里得算法

- 考虑 a 远大于 b 时

$$\begin{aligned}
&\gcd(a,b)\\
=&\gcd(b,a-b)\\
=&\gcd(b,a-b-b)\\
=&\cdots\\
=&\gcd(b,a \bmod b)
\end{aligned}$$

- 实现如下:

```
int gcd(int a, int b) {
    return !b ? a : gcd(b, a % b);
}
```

唯一分解定理

- 任何一个非负整数 x，都能被写成如下形式

$$p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots$$

- 其中 p_i 是从小到大的所有质数，k_i 可为零。

最小公倍数

- 将 a 和 b 写成唯一分解定理的形式

$$a = p_1^{A_1} \cdot p_2^{A_2} \cdot p_3^{A_3} \cdots$$
$$b = p_1^{B_1} \cdot p_2^{B_2} \cdot p_3^{B_3} \cdots$$

- 则其最大公约数与最小公倍数为

$$\gcd(a, b) = p_1^{\min(A_1,B_1)} \cdot p_2^{\min(A_2,B_2)} \cdot p_3^{\min(A_3,B_3)} \cdots$$
$$\operatorname{lcm}(a, b) = p_1^{\max(A_1,B_1)} \cdot p_2^{\max(A_2,B_2)} \cdot p_3^{\max(A_3,B_3)} \cdots$$

- 所以

$$\gcd(a, b) \times \operatorname{lcm}(a, b) = ab$$

```
int lcm(int a, int b) {
    return a / gcd(a, b) * b;
}
```