Modular

同余关系

- 定义：m能整除a-b，则a和b对m同余

$$a \equiv b \pmod{m}$$

- 上式与下面的式子等价

$$a = b + km \\ a \bmod m = b \bmod m$$

- 计算方法

$$(a+b) \pmod{m} = ((a \pmod{m}) + (b \pmod{m})) mod\ m \\ (ab) \pmod{m} = ((a \pmod{m})(b \pmod{m})) mod\ m$$

素数与最大公约数

素数

- 定理
  - 大于1的整数是素数或者素数的乘积
  - 有无穷多个素数（反证法）
    假设素数有限，有n个，分别为p_1、p_2……p_n，又令$q=p_1p_2…p_n+1$，则q无法被任意一个小于q的数整除，则q是第n+1个素数，矛盾，因此素数有无穷多个
  - 素数定理：不超过x的数中，素数的个数不超过$\frac{x}{lnx}$个

最大公约数（gcd）

- 若两数最大公约数为1，则两数互素
- 质因子分解求最大公约数

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n},\ b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}, \\ then, gcd(a,b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \dots p_n^{min(a_n,b_n)}$$

- 最大公倍数（条件同上）

$$lcm(a,b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \dots p_n^{max(a_n,b_n)}$$
$$ab = gcd(a,b) \cdot lcm(a,b)$$

- 欧几里得算法（辗转相除法）

```
procedure gcd(a,b:positive integers)
x:=a
y:=b
while y != 0:
        r:=x mod y
        x:=y
        y:=r
return x
```

- 贝祖定理（s是a的贝祖系数，t是b的贝祖系数）

$$gcd(a,b) = sa + tb$$

线性同余方程（组）

线性同余方程

$$ax \equiv b\,(\,mod\ m\,)$$

- 当b等于1，x为a模m的逆
- 求a模m的逆（要求a和m互素）
  - 利用辗转相除法，推导出贝祖定理的形式，其中a的贝祖系数即为a模m的逆

线性同余方程组

$$\begin{gathered} x \equiv a_1(\,mod\ m_1\,) \\ x \equiv a_2(\,mod\ m_2\,) \\ . \\ . \\ . \\ x \equiv a_n(\,mod\ m_n\,) \end{gathered}$$

- 中国剩余定理
  - 要求m_k互素

$$M = m_1 m_2 \dots m_n$$

$$M_k = \frac{M}{m_k}$$
$$M_k\, y_k \equiv 1\,(\,mod\ m_k\,)$$
$$x = (a_1\, M_1\, y_1 + a_2\, M_2\, y_2 + \cdots + a_n\, M_n\, y_n)\ mod\ M$$