数论初步

同余

- 同余方程：
  - 方程

$$ax \equiv c \mod m \tag{1}$$

    有解的充分必要条件是

$$\gcd(a,m)|c$$

  - 方程

$$ax \equiv 1 \mod m$$

    有解的充分必要条件是 a,m 互素。
  - 一般来说，方程 (1) 的解不唯一，首先注意到每个解所在的模 m 同余类都是解；其次一般的，有 $\gcd(a,m)$ 个同余类是解。
- 欧拉数ϕ_n： $\{1,2,\dots,n\}$ 中与 n 互素的数的个数。
  设 $n=p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$ ，则：

$$\phi_n=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$$

- 欧拉定理：设 a， n 互素，则：

$$a^{\phi_n} \equiv 1 \mod n$$

- 费马小定理：设 p 为素数，a,p 互素，则：

$$a^{p-1} \equiv 1 \mod p$$

  另一种表述为：设 p 为素数，$\forall a \in \mathbb{Z}$ 有：

$$a^{p} \equiv a \mod p$$