

同余

Congruence

性质

- 自反, 传递, 对称
- 加法、减法、乘法、幂次
- 除法: 若 $ac \equiv bc \pmod{m}$, 则:

$$a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$$

证: 设 $ac = km + bc$, 则 $a = b + \frac{km}{c}$ 。由于 $a - b = \frac{km}{c} = \frac{k \frac{m}{\gcd(c, m)}}{\frac{c}{\gcd(c, m)}} \in \mathbb{Z}$, 故 $\frac{c}{\gcd(c, m)} \mid k$ 。可设 $k = k' \cdot \frac{c}{\gcd(c, m)}$, 于是 $a = b + k' \frac{m}{\gcd(c, m)}$, 故

$$a \equiv b \pmod{\frac{m}{\gcd(c, m)}}. \text{ 证毕。}$$

- 若 $a \equiv b \pmod{m}$, $n \mid m$, 则 $a \equiv b \pmod{n}$ 。

证: 设 $a = km + b$, $m = rn$, 则 $a = krn + b = k'n + b$, 故 $a \equiv b \pmod{n}$ 。证毕。

九余数定理

一个十进制数的所有数位相加与它本身模 9 同余。即: 设 $n = \overline{b_m b_{m-1} b_1 b_0}$, 则 $n \equiv \sum_{i=0}^m b_i \pmod{9}$ 。

证:

$$\begin{aligned} n &\equiv 10^m b_m + \cdots + 10 b_1 + b_0 \\ &\equiv 1^m b_m + \cdots + 1^1 b_1 + 1^0 b_0 \\ &= \sum_{i=0}^m b_i \pmod{9} \end{aligned}$$

证毕。

进一步, 一个 p 进制数 $n = (b_m b_{m-1} \cdots b_1 b_0)_p$ 所有数位相加与它本身模 b 同余的充要条件是: $p \equiv 1 \pmod{b}$, 或写作 $(p-1) \mid b$ 。

证:

充分性:

$$\begin{aligned} n &\equiv b_m p^m + b_{m-1} p^{m-1} + \cdots + b_1 p + b_0 \\ &= b_m 1^m + b_{m-1} 1^{m-1} + \cdots + b_1 + b_0 \\ &\equiv \sum_{i=0}^m b_i \pmod{b} \end{aligned}$$

必要性: 假设 $p \equiv c \pmod{b}$, 则

$$\begin{aligned} n &\equiv b_m p^m + b_{m-1} p^{m-1} + \cdots + b_1 p + b_0 \\ &\equiv b_m c^m + b_{m-1} c^{m-1} + \cdots + b_1 c + b_0 \\ &\equiv b_m + b_{m-1} + \cdots + b_1 + b_0 \pmod{b} \end{aligned}$$

于是有:

$$b \mid b_m(c^m - 1) + b_{m-1}(c^{m-1} - 1) + \cdots + b_1(c - 1)$$

如果 $c \neq 1$, 显然上式不能对所有的 n 成立, 故 $c = 1$ 。证毕。

概念

- 剩余类 Residue class:

$$\bar{r}_n = \{m \in \mathbb{Z} \mid m \equiv r \pmod{n}\}$$

即所有模 n 余 r 的数的集合。

- 完全剩余系 Complete residue system: n 个模 n 不同余的整数构成一个模 n 的完全剩余系。
- 缩剩余系 Ruduced residue system: 完全剩余系中取出所有与 n 互质的数 (共有 $\varphi(n)$ 个)。

威尔逊定理 Wilson's theorem

p 为质数的充要条件是:

$$(p-1)! \equiv -1 \pmod{p}$$

Proof:

充分性: $(p-1)! \equiv -1 \pmod{p} \iff p \mid (p-1)! + 1$ 。设 $a \mid p$ ($a < p$), 则 $a \mid (p-1)! + 1$; 又 $a \mid (p-1)!$, 而 $\gcd((p-1)!, (p-1)! + 1) = 1$, 故只能是 $a = 1$, 所以 p 是质数;

必要性: 只需证: $(p-2)! \equiv 1 \pmod{p}$ 。当 $p = 2$ 时, 成立; 当 $p > 2$ 时, p 是奇数, 现在证明: $2, 3, \dots, p-2$ 这偶数个数字可以两两配对, 使得每一对都互为模 p 意义下的逆元。首先, 对于 $x < p$, 一定能找到 $y < p$ 使得 x, y 互为逆元; 其次, 对于 $2 \leq x \leq p-2$, x 不可能是自己的逆元; 再次, 假设 x, y 互为逆元, 则必不会有第三者 $z < p$ 与 x 或 y 为逆元, 综上易知, $2, 3, \dots, p-2$ 可以两两配对形成逆元对。于是, $(p-2)! \equiv 1 \pmod{p}$ 成立。证毕。