

0.1 中国剩余定理

定理 0.1 (中国剩余定理)


设 \mathbb{F} 是一个域, $m_1, m_2, \dots, m_n \in \mathbb{F}[x]$ 且两两互素, 则对任何 $a_1, a_2, \dots, a_n \in \mathbb{F}[x]$, 存在 $f \in \mathbb{F}[x]$ 使得

$$f(x) \equiv a_i(x) \pmod{m_i(x)}, i = 1, 2, \dots, n,$$

即存在 $k_i \in \mathbb{F}[x]$ 使得

$$f(x) = k_i(x)m_i(x) + a_i(x), i = 1, 2, \dots, n.$$



 **笔记** 本定理是抽象代数或者初等数论中的经典定理, 可以无脑直接使用, 和整数版本的证明也完全一致.
注 若

$$f_1(x), f_2(x) \equiv a_i(x) \pmod{m_i(x)}, i = 1, 2, \dots, n,$$

我们有

$$f_1(x) - f_2(x) \equiv 0 \pmod{m_i(x)}, i = 1, 2, \dots, n,$$

这等价于

$$f_1 - f_2 \equiv 0 \pmod{\left(\prod_{i=1}^n m_i\right)}.$$

即全部解为

$$\left\{ f_1(x) + k(x) \cdot \prod_{i=1}^n m_i(x) : k \in \mathbb{F}[x] \right\}.$$

其中 $f_1(x)$ 是任意一个特定解.

证明 设

$$\varphi_i(x) = m_1(x)m_2(x) \cdots m_{i-1}(x)m_{i+1}(x) \cdots m_n(x), i = 1, 2, \dots, n.$$

对每一个 $i \in \{1, 2, \dots, n\}$, 我们有 φ_i 和 m_i 互素, 因此由裴蜀等式知存在 $u_i, v_i \in \mathbb{F}[x]$ 使得

$$\varphi_i(x)u_i(x) + m_i(x)v_i(x) = 1.$$

考虑

$$f(x) = \sum_{j=1}^n a_j(x)\varphi_j(x)u_j(x) \in \mathbb{F}[x],$$

我们有

$$\begin{aligned} f(x) - a_i(x) &= a_i(x) [\varphi_i(x)u_i(x) - 1] + \sum_{\substack{1 \leq j \leq n, \\ j \neq i}} a_j(x)\varphi_j(x)u_j(x) \\ &= -a_i(x)v_i(x)m_i(x) + \sum_{\substack{1 \leq j \leq n, \\ j \neq i}} a_j(x)\varphi_j(x)u_j(x). \end{aligned}$$

现在 m_i 是上式右边每一项的因子, 从而

$$m_i | (f - a_i), i = 1, 2, \dots, n,$$

即

$$f(x) \equiv a_i(x) \pmod{m_i(x)}, i = 1, 2, \dots, n.$$

□

例题 0.1 求次数最小的 f 使得

$$\begin{cases} f(x) \equiv 6 \pmod{x+1} \\ f(x) \equiv 3x \pmod{x^2+x+1} \\ f(x) \equiv (x-1)^2 \pmod{2x^3+1} \end{cases}$$

注 直接用中国剩余定理是难算的. 我们应该具体问题具体分析.

注 由中国剩余定理的注可知, 原方程的全部解为

$$f_1(x) + k(x)(x+1)(x^2+x+1)(2x^3+1),$$

其中 $f_1(x)$ 为任一特解, $k(x) \in \mathbb{C}[x]$. 因为 $\deg[(x+1)(x^2+x+1)(2x^3+1)] = 6$, 所以当 $\deg f_1(x) \geq 6$ 时, 可以取合适的 $k(x)$, 使得 $f_1(x) + k(x)(x+1)(x^2+x+1)(2x^3+1)$ 中高于 6 次项全部消去. 故原方程组的最小次解必定小于等于 5 次.

证明 因为

$$\deg[(x+1)(x^2+x+1)(2x^3+1)] = 6,$$

我们设

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5.$$

不妨在 \mathbb{Q} 上考虑, 因为如果还有一个 $g \in \mathbb{C}[x]$ 使得 $\deg g \leq 5$ 为解, 则 $g - f$ 有一个六次因子, 即只能有 $f = g$.

条件第一个同余式等价于

$$f(-1) = 6 \Leftrightarrow a_0 - a_1 + a_2 - a_3 + a_4 - a_5 = 6.$$

对第二个同余式, 等价于若 $x^2 + x + 1 = 0$ 则 $f(x) - 3x = 0$. 注意到若 $x^2 + x + 1 = 0$ 则

$$x^3 - 1 = (x-1)(x^2+x+1) = 0 \Rightarrow x^3 = 1,$$

我们有

$$\begin{aligned} f(x) - 3x &= a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 - 3x \\ &= a_0 + a_3 + (a_1 + a_4 - 3)x + (a_2 + a_5)x^2 \\ &= a_0 + a_3 + (a_1 + a_4 - 3)x + (a_2 + a_5)(-x - 1) \\ &= a_0 + a_3 - a_2 - a_5 + (a_1 + a_4 - a_2 - a_5 - 3)x, \end{aligned}$$

即容易验证等价于

$$a_0 + a_3 - a_2 - a_5 = 0, \quad a_1 + a_4 - a_2 - a_5 = 3.$$

对第三个同余式, 等价于若 $2x^3 + 1 = 0$ 则 $f(x) - x^2 + 2x - 1 = 0$. 现在若 $2x^3 + 1 = 0$ 则

$$f(x) - x^2 + 2x - 1 = \left(a_2 - \frac{1}{2}a_5 - 1\right)x^2 + \left(a_1 - \frac{1}{2}a_4 + 2\right)x + \left(a_0 - \frac{1}{2}a_3 - 1\right),$$

即容易验证等价于

$$a_2 - \frac{1}{2}a_5 = 1, \quad a_1 - \frac{1}{2}a_4 = -2, \quad a_0 - \frac{1}{2}a_3 = 1.$$

解线性方程组得

$$f(x) = 4x^4 + x^2 + 1,$$

这就完成了计算.

□