

3. 求 (x^7+x^6+1) 关于模 $m(x)=x^8+x^4+x^3+x+1$ 的乘法逆元。◀

条件：是在 $F_2[X]$ 中, $a_n \equiv a'_n \pmod{2}$

$f(x) = x^7 + x^6 + 1, m(x) = x^8 + x^4 + x^3 + x + 1$, 欲求 $f(x)$ 逆元 $f^{-1}(x)$

即 $f(x)f^{-1}(x) = 1 + k(x)m(x)$, 即寻找 $f^{-1}(x)f(x) + k(x)m(x) = 1$

多项式欧几里得除法, $m(x)$ 是不可约多项式

$$m(x) = x^8 + x^4 + x^3 + x + 1 = (x+1)(f(x) = x^7 + x^6 + 1) + (x^6 + x^4 + x^3)$$

$$x^7 + x^6 + 1 = (x+1)(x^6 + x^4 + x^3) + (x^5 + x^3 + 1) \quad \text{以上经过模 2 处理}$$

$$x^6 + x^4 + x^3 = x(x^5 + x^3 + 1) + (x^3 + x)$$

$$x^5 + x^3 + 1 = x^2(x^3 + x) + 1$$

反向计算得：

$$1 = (x^5 + x^3 + 1) - x^2(x^3 + x)$$

$$= (x^5 + x^3 + 1) - x^2((x^6 + x^4 + x^3) - x(x^5 + x^3 + 1))$$

$$= (1 + x^3)(x^5 + x^3 + 1) - x^2(x^6 + x^4 + x^3)$$

$$= (1 + x^3)((x^7 + x^6 + 1) - (x+1)(x^6 + x^4 + x^3)) - x^2(x^6 + x^4 + x^3)$$

$$= (1 + x^3)(x^7 + x^6 + 1) - ((1 + x^3)(x+1) + x^2)(x^6 + x^4 + x^3)$$

$$= (1 + x^3)(x^7 + x^6 + 1) - (x^4 + x^3 + x + 1)(x^6 + x^4 + x^3)$$

$$= (1 + x^3)(x^7 + x^6 + 1) - (x^4 + x^3 + x + 1)[(x^8 + x^4 + x^3 + x + 1) - (x+1)(x^7 + x^6 + 1)]$$

$$= [1 + x^3 + (x^4 + x^3 + x + 1)(x+1)](x^7 + x^6 + 1) - (x^4 + x^3 + x + 1)(x^8 + x^4 + x^3 + x + 1)$$

因此, $f(x)$ 乘法逆元 $f^{-1}(x) = 1 + x^3 + (x^4 + x^3 + x + 1)(x+1) = 1 + x^3 + x^5 + 1 = x^3 + x^5$