NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 15

2023 年 11 月 21 日

Problem 1

设 F 是域, $f(x)$ 与 $g(x)$ 是 F 上不全为零的两个多项式, 则存在 F 上的多项式 $s(x)$ 和 $t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = \gcd(f(x), g(x)).$$

解: **类似整数最大公因子的证明:** 假设 $d(x)$ 是首一多项式集合

$$S = \{p(x)f(x) + q(x)g(x) : p(x), q(x) \in F[x]\}$$

中次数最小的多项式, 因此有 $s(x), t(x) \in F[x]$ 满足 $d(x) = s(x)f(x) + t(x)g(x)$. 接下来证明 $d(x) \mid f(x)$: 利用长除法, 有 $f(x) = a(x)d(x) + b(x)$, 其中 $b(x) = 0$ 或者 $\deg(b(x)) < \deg(d(x))$. 则有

$$\begin{aligned} b(x) &= f(x) - a(x)d(x) = f(x) - a(x)\left(s(x)f(x) + t(x)g(x)\right) \\ &= f(x)\left(1 - a(x)s(x)\right) + g(x)\left(-a(x)t(x)\right), \end{aligned}$$

即 $b(x)$ 是 $f(x)$ 和 $g(x)$ 的组合, 因此 $b(x) \in S$. 但 $d(x)$ 是集合 S 中次数最小的多项式, 故 $b(x) = 0$, 也就是说 $d(x) \mid f(x)$. 同理可得 $d(x) \mid g(x)$. 因此 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式.

再设存在 $d'(x) \mid f(x)$ 和 $d'(x) \mid g(x)$, 则有 $d'(x) \mid s(x)f(x) + t(x)g(x)$, 故 $d'(x) \mid d(x)$. 因此 $d(x)$ 的次数在 $f(x)$ 和 $g(x)$ 的公因式集合中是最大的, 也就是说 $d(x) = \gcd(f(x), g(x))$.

Problem 2

构造两个有限域并给出其乘法表 (使用的 $\mathbb{F}_2[x]$ 上的 3 次和 4 次不可约多项式分别是 $x^3 + x + 1$ 和 $x^4 + x + 1$)

解: 仅给出 3 次的情况, 4 次的结果直接列乘法表.

$$\begin{aligned}\frac{\mathbb{F}_2[x]}{\langle x^3+x+1\rangle} &= \left\{\overline{a_0+a_1x+a_2x^2} : a_0,a_1,a_2\in\mathbb{F}_2\right\}\\ &= \left\{\overline{0},\overline{1},\overline{x},\overline{1+x},\overline{x^2},\overline{1+x^2},\overline{x+x^2},\overline{1+x+x^2}\right\}.\end{aligned}$$

PS: 为了方便书写, 忽略元素上方的求模符号.

由于域的加法和乘法具有分配律, 则对仅需计算出标红的 $1, x, x^2$ 这三行的结果, 其余 4 行均为这三行的线性组合; 乘法表中 1 这一行不需要计算, 而 x, x^2 这两行的结果不外乎是下列几个运算的线性组合

$$1*x=x, 1*x^2=x^2, x*x=x^2, x*x^2=x^3=1+x, x^2*x^2=x^3*x=x+x^2,$$

故整个乘法表可以通过上述结果计算得到.

$\times$	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
1	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
x		x^2	$x+x^2$	$1+x$	1	$1+x+x^2$	$1+x^2$
$1+x$			$1+x^2$	$1+x+x^2$	x^2	1	x
x^2				$x+x^2$	x	$1+x^2$	1
$1+x^2$					$1+x+x^2$	$1+x$	$x+x^2$
$x+x^2$						x	x^2
$1+x+x^2$							$1+x$

$\times$	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$	x^3	$1+x^3$	$x+x^3$	$1+x+x^3$	x^2+x^3	$1+x^2+x^3$	$x+x^2+x^3$	$1+x+x^2+x^3$
1	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$	x^3	$1+x^3$	$x+x^3$	$1+x+x^3$	x^2+x^3	$1+x^2+x^3$	$x+x^2+x^3$	$1+x+x^2+x^3$
x		x^2	$x+x^2$	x^3	$x+x^3$	x^2+x^3	$x+x^2+x^3$	$1+x$	1	$1+x+x^2$	$1+x^2$	$1+x+x^3$	$1+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$
$1+x$			$1+x^2$	x^2+x^3	$1+x+x^2+x^3$	$x+x^3$	$1+x^3$	$1+x+x^3$	x^3	$1+x^2+x^3$	$x+x^2+x^3$	$1+x+x^2$	x^2	1	x
x^2				$1+x$	$1+x+x^2$	$1+x+x^3$	$1+x+x^2+x^3$	$x+x^2$	x	$x+x^2+x^3$	$x+x^3$	$1+x^2$	1	$1+x^2+x^3$	$1+x^3$
$1+x^2$					x	$1+x^2+x^3$	x^3	$x+x^2+x^3$	$1+x+x^3$	x^2	1	$1+x^3$	x^2+x^3	$1+x$	$x+x^2$
$x+x^2$						$1+x+x^2$	1	$1+x^2$	$1+x$	$1+x^3$	$1+x+x^2+x^3$	$x+x^2+x^3$	x^3	x	x^2
$1+x+x^2$							$x+x^2$	$1+x^2+x^3$	$x+x^3$	$1+x$	x^2	x	$1+x^2$	x^2+x^3	$1+x+x^3$
x^3								x^2+x^3	x^2	$1+x+x^2+x^3$	$1+x+x^2$	$x+x^3$	x	$1+x^3$	1
$1+x^3$									$1+x^2+x^3$	$1+x^2$	x^2+x^3	$x+x^2$	$1+x+x^2+x^3$	$1+x+x^2$	$x+x^2+x^3$
$x+x^3$										x^3	x	1	$1+x+x^3$	$x+x^2$	x^2+x^3
$1+x+x^3$											$1+x^3$	$1+x^2+x^3$	$x+x^2$	x^3	$1+x$
x^2+x^3												$1+x+x^2+x^3$	$1+x$	x^2	x^3
$1+x^2+x^3$													$x+x^2+x^3$	$x+x^3$	$1+x+x^2$
$x+x^2+x^3$														$1+x+x^3$	$1+x^2$
$1+x+x^2+x^3$															$x+x^3$