信息安全数学基础8—有限域

杨礼珍

同济大学计算机科学与技术系, 2017

Outline

1 Finite Fields

有限域
作业

- 阅读：《密码学原理与实践》6.4节（P197-200）
- 练习：《密码学原理与实践》P219习题6.11

有限域

有限域的应用：

- 构造Elgamal公钥体制
- AES
- 数字签名、认证等密码协议应用
- 纠错码。。。

我们学习过的域(Field)：

- 无限域（元素个数无限）：
  1. 实数域$(R, +, \cdot)$
  2. 有理数域$(Q, +, \cdot)$
  3. 复数域$(C, +, \cdot)$
- 有限域（元素个数有限个）：
  1. 模素数p剩余系：$(\mathbb{Z}_p, +, \cdot)$

有限域

域$(\mathbb{F},+,\cdot)$的定义：

- $\mathbb{F}$为元素集合，如果数量有限则称为有限域。
- 有两个F上的二元运算：$+,\cdot$
- 关于运算$+$构成交换群，即$(\mathbb{F},+)$是交换群，其中单位元记为0。
- 记$\mathbb{F}^*=\mathbb{F}/\{0\}$，那么$(\mathbb{F}^*,\cdot)$是交换群，其中单位元记为1。
- 满足分配律：对任意$x,y,z\in\mathbb{F}$有：$(x+y)z=xz+yz$

有限域

有限域的基本性质：

- 性质1：有限域的元素个数为p^n，其中p为素数。
- 性质2：元素个数相同的有限域同构，即实质上元素个数为p^n的有限域是唯一的，仅是符号表示不同。
    - 因此把元素个数为p^n的有限域记为$\mathbb{F}_{p^n}$，或者$GF(p^n)$。
- 性质2：$\mathbb{F}^*_{p^n} = F_{p^n} \setminus \{0\}$是关于乘法运算是循环群。

有限域$\mathbb{F}_{p^n}$的构造：

1. $\mathbb{Z}_p$上的多项式集合记为$\mathbb{Z}_p[x]$，即
$$\mathbb{Z}_p[x] = \{a_n x^n + \ldots + a_0, a_i \in \mathbb{Z}_p, i = 0, \ldots, n, n = 0, 1, \ldots\}$$
2. 找到$\mathbb{Z}_p$上一个次数为n的不可约多项式f(x)：“不可约多项式”类似于整数中的“素数”，即不存在次数不为0的多项式$f_1(x), f_2(x) \in \mathbb{Z}_p[x]$，满足
$$f(x) = f_1(x) f_2(x)$$
3. $\mathbb{F}_{p^n} = \{a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, a_i \in \mathbb{Z}_p, i = 0, \ldots, n-1\}$
4. “加法”运算+定义为：对元素$\alpha = g_1(x), \beta = g_2(x)$，定义
$$\alpha + \beta = (g_1(x) + g_2(x)) \bmod f(x)$$
5. “乘法”运算·定义为：对元素$\alpha = g_1(x), \beta = g_2(x)$，定义
$$\alpha \cdot \beta = (g_1(x) g_2(x)) \bmod f(x)$$

有限域$\mathbb{F}_{p^n}$的构造的补充说明：

- 多项式$f(x)$的最高次数记为$\deg(f(x))$
- $g(x) \bmod f(x)$定义：如果

$$g(x) = q(x)f(x) + r(x), q(x), r(x) \in \mathbb{Z}_p[x] \tag{1}$$

且$\deg(r(x)) < \deg(f(x))$，那么定义

$$g(x) \bmod f(x) = r(x)$$

可以证明(1)的表示是唯一的。

- 幂乘运算（指数运算）：$g(x)^k \pmod{f(x)}$使用平方-乘算法提高效率，注意：对应的运算改成$\mathbb{F}_{p^n}$上的运算。

有限域$\mathbb{F}_{p^n}$的构造的补充说明：
设$g(x) = g_{n-1}x^{n-1} + \ldots + g_1 x + g_0$

- $g(x)$关于加法$+$运算的逆元为：$-g(x)$，即

  $$-g(x) = (-g_{n-1} \bmod p)x^{n-1} + \ldots + (-g_1 \bmod p)x + (-g_0 \bmod p)$$

  如果$p = 2$，$-g(x) = g(x)$。
- 计算$g(x)$关于乘法运算的逆元：即求$g^{-1}(x)$满足$g^{-1}g(x) \equiv 1 \bmod f(x)$，和$\mathbb{Z}_p^*$一样，$g(x)$使用扩展Euclidean算法求逆元，注意：对应的运算改成$\mathbb{F}_{p^n}$上的运算。

Example

例6.8：构造$\mathbb{F}_{2^3}$

1. 找到$\mathbb{Z}_2$上一个次数为3的不可约多项式$f(x) = x^3 + x + 1$
2. $\mathbb{F}_{2^3}$的$2^3 = 8$个元素定义为8个次数小于3的多项式：

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

3. 加法运算：元素$\alpha = a_2x^2 + a_1x + a_0$，$\beta = b_2x^2 + b_1x + b_0$，因为$\alpha, \beta$的次数小于$f(x)$，那么

$$\alpha + \beta = (a_2 \oplus b_2)x^2 + (a_1 \oplus b_1)x + (a_0 \oplus b_0)$$

注意：mod2加法运算其实是异或$\oplus$运算。例子：

$$\begin{aligned}(x^2+x+1) + (x+1) \bmod f(x) &= x^2\\(x^2+x+1) + (x^2+1) \bmod f(x) &= x\end{aligned}$$

Example

例6.8：构造$\mathbb{F}_{2^3}$（续）

1. 乘法运算：首先在$\mathbb{Z}_2[x]$中计算乘积，如$\alpha = x^2+1, \beta = x^2+x+1$，那么

$$(x^2+1)(x^2+x+1) = x^4+x^3+2\cdot x^2+x+1 = x^4+x^3+x+1$$

然后乘积结果mod$(f(x) = x^3+x+1)$：

$$x^4+x^3+x+1 = (x+1)(x^3+x+1)+(x^2+x)$$

$$\begin{pmatrix} g(x) & x^4 & +x^3 & & +x & +1 \\ xf(x) & x^4 & & +x^2 & +x & \\ g(x)-xf(x) & & x^3 & +x^2 & & +1 \\ f(x) & & x^3 & & +x & 1 \\ g(x)-xf(x)-f(x) & & & x^2 & +x & \end{pmatrix}$$

因此$(x^2+1)(x^2+x+1) = x^2+x$

Example

例6.8：构造$\mathbb{F}_{2^3}$（续）

1. 如果把多项式$a_2x^2+a_1x+a_0$表示成三元组$a_2a_1a_0$，那么课本中的例6.6的表格给出了所有元素的乘法运算结果。
2. 关于乘法运算的逆元计算：应用扩展Euclidean算法计算。
   如求x^2的逆：

i	r_j	q_j	s_j	t_j
0	x^3+x+1		1	0
1	x^2	x	0	1
2	$x+1$	x	1	x
3	x	1	x	x^2+1
4	1	x	$x+1$	x^2+x+1

因此$(x+1)(x^3+x+1)+(x^2+x+1)(x^2)=1$，
则x^2的逆元为x^2+x+1

Example

例6.8：构造$\mathbb{F}_{2^3}$（续）

$$\begin{aligned}
x & \\
x^2 & \\
x^3 &= x+1 \\
x^4 &= (x+1)x = x^2+x \\
x^5 &= (x^2+x)x = x^3+x^2 = x^2+x+1 \\
x^6 &= (x^2+x+1)x = x^3+x^2+x = x^2+1 \\
x^7 &= (x^2+1)x = x^3+x = 1
\end{aligned}$$

可见$\mathbb{F}_{2^8}^* = \langle x \rangle$

有限域

我们前面构造的$(F_{p^n},+,\cdot)$是有限域：

- 满足分配律。
- $(F_{p^n},+)$是Abel群：对加法满足封闭性、结合律、单位元为0、$f(x)$的加法逆元是$-f(x)$、任何元素可交换。
- $(F^*_{p^n},\cdot)$是Abel群：
  1. 对乘法满足封闭性；
  2. 满足结合律；
  3. 单位元是1；
  4. 满足交换律；
  5. 任何非0元素的乘法逆元存在（可用证明$\gcd(a,b)=sa+tb$的非构造性方法证明）。

定理： 以上所构造的$F_{p^n}^*$的乘法逆元存在。

引理： 若任给两不全为0的$a, b \in \mathbb{Z}_p[x]$，则存在$m, n \in \mathbb{Z}_p[x]$使得$\gcd(a, b) = ma + nb$。

引理证明（和整数情形的证明不同之处用红字表示出来）： 设$I = \{sa + tb | s, t \in \mathbb{Z}_p[x]\}$。则$I \neq \{0\}$，令$d$为$I$中次数最小的非0多项式，作为$I$的成员，有$m, n \in \mathbb{Z}_p[x]$使得$d = ma + nb$。
以下证明对任意$c = sa + tb$有$d | c$。由带余除法，$c = qd + r$，其中$\deg(r) < \deg(d)$。如果$r \neq 0$，则$r = c - qd \in I$，与d是次数最小的非0多项式相矛盾。因此$d | c$。
特别地$d | a, d | b$，则$d | (a, b)$。
另一方面$(a, b) | b, (a, b) | a$，因此$(a, b) | ma + nb = d$。
综上所述，$(a, b) = d$。

定理证明： 因为$f(x)$为$\mathbb{Z}_p$上的不可约多项式，因此对任何$\alpha \in F_{p^n}^*$有$\gcd(\alpha, f(x)) = 1$。由引理得到，$\exists m, n \in \mathbb{Z}_p[x]$有$1 = m\alpha + nf(x)$，因此

$$m\alpha \equiv 1 \pmod{f(x)}$$

即使$m \bmod f(x) \in F_{p^n}^*$是$\alpha$的逆元。

有限域

数论中有以下结论

- 对任意正整数n，存在$\mathbb{Z}_p$上的不可约多项式；因此存在有限域F_{p^n}。
- 不存在有效的通用算法判定$\mathbb{Z}_p$上的多项式是否为不可约多项式，但对某些情形的多项式有一些判定准则，可参考《数论讲义》下册第七章。