密码学理论与技术
– 计算机密码学理论与应用

田园

$$ed = 1 \bmod \varphi(N)$$
$$Y = M^e \bmod N$$
$$M = Y^d \bmod N$$

有限域的基本性质与应用

- (1) 素域F_p的性质。
- (2) 素域F_p上的多项式的性质，素多项式，多项式的运算。
- (3) 有限域的扩张，任意次数的有限域。
- (4) 有限域上的难解性问题：
- 离散对数问题（DLP: *Discrete Logarithm Problem*）；
- *Diffie-Hellman*问题.

- 参阅Stallings教程4.4~4.7。

有限域的基本性质与应用(1)

- p是素数，素域 F_p 的算术性质
- F_p={0,1,2,…,p-1}上的两种**算术运算**：
- (1) 运算$(a + b) \bmod p$，简记为a+b：
- \+ 运算的中性元素为0，a的逆元为 $p - a$，简记为 **- *a***。
-
- (2)运算 $ab \bmod p$，简记为ab，中性元素为 1；
- 乘法运算的中性元素为1，对任何a≠0，a的逆元是$ax = 1 \bmod p$的解，
- 简记为$a^{-1} \bmod p$ 或 a^{-1} 。
- 常用的记号：a+…+a 记为 na，a…a 记为a^n。
- (3)乘法运算和加法运算之间满足分配律，且
- $(m+n)a = ma + na, (a^m)^n = a^{mn}$
-

有限域的基本性质与应用(2)

- p是素数，素域 F_p 的算术性质（续）
- (4) 对素域的任何元素，恒有$a^p = a$, $(a + b)^p = a^p + b^p = a + b$,
- 更一般地，对任何正整数m恒成立：
- $$(a+b)^{p^m} = a^{p^m} + b^{p^m}$$
- 【习题】由二项式公式验证上式，注意对素域中的任何元素a有$pa = 0$。
- (5) 素域的乘法群F_p^*是一个循环群，生成子是p的原根g：
- $$F_p^* = \{ 1, g, g^2, \ldots, g^{p-2} \}$$
- 关于素域的另一种等价的观点：
- F_p^* 是方程 $x^p = x \bmod p$的解的集合。

有限域的基本性质与应用(3)

- 素域 F_p 上的多项式
- (1) F_p 上的多项式 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ，系数a_j属于素域 F_p。
- (2) F_p 上的全体多项式的集合记为$\mathbf{F_p[x]}$
-
- (3) 多项式上存在加法运算：
- $$f(x) + g(x) = \sum_{i=0}^{n}(a_i + b_i)\, x^i$$
- 多项式的加法运算是交换、可逆的，$f(x)$的逆元素是 - $f(x)$，
- 且以0为中性元素。
-
- (4) 多项式上存在乘法运算：
- $$f(x)g(x) = \sum_{i=0}^{n}(a_ib_0 + a_{i-1}b_1 + \dots + a_0b_i)\, x^i$$
- 多项式的加法运算是交换的， 且以1为中性元素。

有限域的基本性质与应用(3^+)

- 多项式 运算的例： $f(x) = 1 + x + x^2 + x^6$, $g(x) = x + x^2 + x^3$

- (1) $f(x) + g(x) = 1 + x + x^2 + x^6 + x + x^2 + x^3 =$ (合并同类项后) $1 + x^3 + x^6$;
- (2) $f(x)g(x) = (1 + x + x^2 + x^6)(x + x^2 + x^3)$
- $= x + x^2 + x^3 + x^7 +$
- $+ x^2 + x^3 + x^4 + x^8 +$
- $+ x^3 + x^4 + x^5 + x^9$
- $= x + \quad x^3 + \quad x^5 + x^7 + x^8 + x^9$;

(3) $f(x) \div g(x) = (1 + x + x^2 + x^6) \div (x + x^2 + x^3)$ 长除法：

- $f(x) = x^6 + x^2 + x + 1 = x^3(x^3 + x^2 + x) \underline{+ x^5 + x^4} + x^2 + x + 1$
- $= x^3(x^3 + x^2 + x) + x^2(x^3 + x^2 + x) + \underline{x^4 + x^3} + x^4 + x^2 + x + 1$
- $= x^3(x^3 + x^2 + x) + x^2(x^3 + x^2 + x) + x^3 + x^2 + x + 1$
- $= (x^3+x^2+1)(x^3 + x^2 + x) + 1$ 绿色：商式；红色：余式

用下面将要定义的同余等价关系，该结果表达为 $f(x) = 1 \bmod g(x)$。

【习题】$f(x) = x + x^8 + x^{15}$, $g(x) = 1 + x^2 + x^5 + x^7$, 计算$f(x) \div g(x)$的商式和余式。

有限域的基本性质与应用(4)

- 素域上的多项式（续）：多项式和整数的相似性、Euclid定理

(1) 证明：按照多项式通常的加法运算和乘法运算，F_p都构成群，注意这是无限群的例子。

(2) n阶多项式$f(x)\in F_p[x]$称为可约的，如果$f(x)$能分解为$F_p[x]$中阶数全部严格小于n的两个多项式的乘积。不可约的多项式称为素多项式，任何$f(x)\in F_p[x]$在$F_p[x]$中都有唯一的素因子分解[10]，因此对任何两个多项式$g(x)$、$h(x)\in F_p[x]$都可以明确定义最高公因子，用记号$(g(x),h(x))$表示。证明对多项式也有相应的Euclid定理及等价形式：

任给$g(x)$、$h(x)\in F_p[x]$，必存在唯一的$q(x)$、$r(x)\in F_p[x]$满足$f(x)=g(x)q(x)+r(x)$及$0\le deg(r(x))<deg(g(x))$，deg表示多项式的阶。

任给$g(x)$、$h(x)\in F_p[x]$，总存在$u(x)$和$v(x)\in F_p[x]$(但不唯一)满足$g(x)u(x)x+h(x)v(x)=(g(x),h(x))$。

任给$f(x)$、$g(x)$、$h(x)\in F_p[x]$，则存在$u(x)\in F_p[x]$满足线性同余式$g(x)u(x)=h(x) \mod f(x)$当且仅当$(g(x),f(x))|h(x)$，且这时u唯一。特别地，若g、f互素则$g(x)u(x)=1 \mod f(x)$必存在解$u\in F_p[x]$。

有限域的基本性质与应用(5)

- 素域上的多项式（续）

- 根据多项式的Euclid定理，给定素域上的多项式P(*x*)，可定义模*P*(*x*)的
- 多项式运算:
- (6) 模P(*x*)的多项式加法运算：
- $f(x) + g(x) = [\sum_{i=0}^{n}(a_i + b_i)\, x^i]\ mod\ \mathrm{P}(x)$
- 多项式的加法运算是交换、可逆的，$f(x)$的逆元素是 $-f(x)$，
- 且以0为中性元素。
-
- (7) 模P(*x*)的多项式乘法运算：
- $f(x)g(x) = [\sum_{i=0}^{n}(a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i)\, x^i]\ mod\ \mathrm{P}(x)$

- 【注】前一页的例子 $f(x) = (x^3+x^2+1)(x^3 + x^2 + x) + 1$ 可表示为
- $(x^3+x^2+1)(x^3 + x^2 + x) = 1\ mod\ f(x)$，也可表示为$f(x) = 1\ mod\ (x^3 + x^2 + x)$.

有限域的基本性质与应用(6)

- 素域上的多项式（续）
- (8) 根据多项式的第三Euclid定理，若$P(x)$是不可约多项式，即$P(x)$不存在
- 任何非平凡的因子，则对任何次数低于$P(x)$的多项式$f(x)$，恒存在$g(x)$
- 满足
- $$f(x)g(x) = 1 \bmod P(x)$$
- 且$g(x)$唯一，记做 $f(x)^{-1} \bmod P(x)$。
- 以不可约多项式$P(x)$为模的乘法运算是可逆的。
- (9) 给定素域F_p上的某个不可约多项式$P(x)$, 记d = P(x)的次数，F_p[x]上的
- 模P(x)的加法运算和乘法运算构成一个有p^d个元素的有限域，称为
- F_p的d次扩域，记为F_{p^d}。
- 【注】不可约(*irreducible*)多项式也称为素(*primitive*)多项式，文献常混用两种称呼。

有限域的基本性质与应用(7)

- 扩域F_{p^d}的性质

- 两种等价的观点：
- (1) <u>构造性观点</u> F_{p^d}是系数属于F_p 的多项式的有限集合，按照 mod P(x)
- 定义加法和乘法运算，P(x)是系数属于F_p 的某个d次不可约多项式。
- (2) <u>抽象的观点</u>F_{p^d}是通过添加系数属于F_p 的某个d次不可约多项式
- P(x)的全部根$\beta_1,\ldots,\beta_d$以及这些根的加减乘除运算表达式构成的集合。

【注】素域和扩域统称为有限域，用于当代通信编码、数字信号处理、安全方案和网络安全协议的设计等领域。

有限域的基本性质与应用(8)

- 有限域上的离散对数问题
- 基本定理
- 任何有限域F均存在生成子g，使F的每个非零元素a都能唯一表示为
- $a = g^t$
- t 是不超过$|F|$-1的某个整数。
- (1) 对任何有限域F，均存在高效算法**A**(g, a, x)计算 $a = g^t$，**A**的复杂度
- 不超过 x 的位数。
- 【注】参考上一讲“二次剩余理论”中的递归算法。
- (2) 离散对数问题**DLP**
- 在给定的有限域F上，已知y和生成子g，求整数x使$y = g^x$。
- 【注】为符号简洁，以下仅描述素域F_p上的DLP。

有限域的基本性质与应用(9)

- 素域F_p上的**DLP** (*Discrete Logarithm Problem*)：

- 给定素数p、原根g和y，求整数x使$y = g^x \bmod p$。

- <u>基本事实</u>(V.Shoup, 1997)　DLP问题的复杂度有下界O($p^{1/2}$)。

【例】对当代密码方案，常取素数$p \approx 2^{1000}$数量级，因此求解DLP问题至少需要
- 2^{500}次1000位乘法运算。

【思考】如果每秒执行1000亿次1000位乘法运算，完成2^{500}次这种运算需要多少年？
基本数值：　1000亿$= 10^{11} \approx 2^{35}$，一天≈8万秒 $\approx 2^{17}$秒，3年$\approx 2^{27}$秒；
宇宙年龄≈100亿年。

【注】关于DLP复杂度的基本事实，可参阅Stinson教程第六章。

有限域的基本性质与应用(10)

- 用于安全方案/协议设计的两类同DLP密切相关的问题：

- (1) 计算性Diffie-Hellam问题(**CDHP**)
- 给定素数p、原根g、$u = g^x \bmod p$和$v = g^y \bmod p$ (但x和y未知)，
- 求 $g^{xy} \bmod p = ?$
- (2) 判定性Diffie-Hellam问题(**DDHP**)
- 给定素数p、原根g、$u = g^x \bmod p$、$v = g^y \bmod p$ 和 w (但x和y未知)，
- 判定是否成立 $w = g^{xy} \bmod p$?

- (3) 如果DLP存在多项式复杂度算法，则CDHP和DDHP均存在多项式复杂度算法。

- (4) 基本事实：
- 对CDHP和DDHP，均不存在平均时间为多项式复杂度的随机算法。
-

有限域的基本性质与应用(11)

- 求解素域F_p上的DLP问题 $y = g^x \bmod p$和求解方程$z^2 = a \bmod p$ 的关系

- (1) 设已知F_p的一个生成子g.
- (2) 设$B(a,p)$是求解方程$z^2 = a \bmod p$ 的某个算法。
- (3) 对DLP问题，设x的二进制表示为$x=x_0 + 2x_1 + 2^2x_2 +\ldots+ 2^n x^n$,
- $x_i = 0, 1$, 求解x归结为求每个比特x_i。
- 分 析：
- (i) x的奇偶性等价于x_0=1或0，(根据上一讲的二次剩余理论)x的奇偶性等价于$y^{(p-1)/2} \bmod p = -1$还是+1，因此通过计算$y^{(p-1)/2} \bmod p$能完全确定x的最低位x_0.
- (ii) 确定x_0后，注意到$y = g^x \bmod p = g^{x_0} (g^{x_1+2x_2+\cdots+2^{n-1}x_n})^2 \bmod p$，
- 因此$(g^{x_1+2x_2+\cdots+2^{n-1}x_n})^2 \bmod p = yg^{-x_0} \bmod p$, 再通过调用算法
- $B(yg^{-x_0} \bmod p, p)$解出出$y_1 = g^{x_1+2x_2+\cdots+2^{n-1}x_n} \bmod p$。
- (iii) 应用(i)同样的方法，确定出次低位$x_1 = 1$还是0。
- 如此反复下去，确定出x的全部比特x_i.

- 【习题一】根据以上分析，建立基于算法B求解DLP问题的算法A。
- 【习题二】建立一个基于求解DLP问题的算法A来求解二次同余式方程的算法B。
- 结　论：**素域上的DLP问题和求解二次同余式方程的计算复杂度等价。**
-