密码理论与技术

–计算机密码学理论与应用

田园

$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Y^d \bmod N$$

二次剩余的基本理论

- (1) 二次方程 $x^2 = a \bmod p$可解性的判定条件：第一基本定理。
- (2) 素数p的原根及其重要性质：第二基本定理。
- (3) Euler-Gauss二次互反律。
- (4) 互反律的应用：Legender符号与Jaccobi符号的计算。
- (5) 互反律的应用：素性检验的现代随机算法
- (6) 二次方程 $x^2 = a \bmod p$的解及其计算复杂性。

二次剩余理论(1)

- 从Euler公式的一个有用的推论开始....

- p是奇素数, a是不以p素因子的任何整数，则
- $$a^{(p-1)/2} = \pm 1 \bmod p$$

- 证明：根据Euler公式有$a^{p-1} = 1 \bmod p$，即
- $$p \mid (a^{p-1} - 1) = (a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1)$$
- p素，因此$p \mid (a^{(p-1)/2} + 1)$ 或 $p \mid (a^{(p-1)/2} - 1)$，等价地：
- $a^{(p-1)/2} = 1 \bmod p$ 或者 $a^{(p-1)/2} = -1 \bmod p$。

二次剩余理论(2)

- P是奇素数, a是不以p素因子的任何整数，二次方程
- $$x^2 = a \bmod \mathrm{p} \qquad \text{(i)}$$
- 在$F_p^*=\{1,2,\ldots,p-1\}$中是否有解的判定准则：
- (1) 以上方程有解，若 $a^{(p-1)/2} = 1 \bmod p$。
- (2) 以上方程无解，若 $a^{(p-1)/2} = -1 \bmod p$。
- (3) 引进Legend记号
- $\left(\frac{a}{p}\right) = +1$，若方程(i)有解； $\left(\frac{a}{p}\right) = -1$，若方程(i)无解；
- $\left(\frac{a}{p}\right) = 0$，若$p|a$ ；
- 第一基本定理： $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod \mathrm{p}$

二次剩余理论(2)

- P是奇素数, a是不以p为素因子的任何整数，二次方程
- $$x^2 = a \bmod p \qquad (i)$$
- 在$F_p^*=\{1,2,\dots,p-1\}$中是否有解的判定准则:
- (1) 以上方程有解，若 $a^{(p-1)/2} = 1 \bmod p$。
- (2) 以上方程无解，若 $a^{(p-1)/2} = -1 \bmod p$。
- (3) 引进Legend记号
- $\left(\frac{a}{p}\right) = +1$，若方程(i)有解; $\left(\frac{a}{p}\right) = -1$，若方程(i)无解;
- $\left(\frac{a}{p}\right) = 0$，若$p|a$;
- 第一基本定理: $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$

二次剩余理论(3)

存在原根真是个神奇的现象！

- 第一基本定理的证明(必要性部分)：

- 若方程 $x^2 = a \bmod p$有解x(属于$F_p{}^*$), 则由Euler公式
- 有 $1 = x^{p-1} = x^{2(p-1)/2} = a^{(p-1)/2} \; mod \; p$.

- 为证明第一基本定理的充分性部分，需借助以下命题。
- 第二基本定理：
- 对任何素数p，恒存在g属于$F^*{}_p$使
- $F^*{}_p = \{g^i \; mod \; p: i=0,1,2,\ldots,p-2\}$

- 注：g称为素数p的**原根**(primative-root)或$F_p{}^*$的生成子；原根及离散对数问题参阅8.5节。

二次剩余理论(4)

注：第二定理的初等证明篇幅较长，可参阅N.Koblitz著A Course in Number Theory and Cryptography, 1987, 第二章。

原根的基本性质：

(1) $g^{(p-1)/2} = -1 \bmod p$

(2) 对$a = g^t \bmod p$，t是偶数当且仅当 $a^{(p-1)/2} = 1 \bmod p$；

t是奇数当且仅当 $a^{(p-1)/2} = -1 \bmod p$；

【注】指数t称为a在F_p^*上以g为底的离散对数；

以上性质表明，$a^{(p-1)/2} \bmod p$完全由a的离散对数的奇偶决定。

(3) $a = g^t \bmod p$也是p的原根，当且仅当$(t,p-1)$互素。

(4) p的原根恰有$\varphi(p-1)$个，φ是Euler函数。

【习题】证明以上性质。

二次剩余理论(5)

- 第一基本定理的证明(充分性部分)：
- 令g是p的一个原根，因此存在i使$a = g^{t} \bmod p$。
- 若$a^{(p-1)/2} = 1 \bmod p$，则 t 必是偶数，故一次同余式方程
- $$2y = t \bmod (p-1)$$
- 必存在解y，进而 $x = g^{y} \bmod p$ 就是二次方程的一个解，这是因为
- $$x^2 = g^{2y} = g^{t \bmod (p-1)} = a \bmod p$$
- 证毕。

【习题】将以上证明中的计算性细节补全。

二次剩余理论(6)

- $g^x \bmod p$ 的快速算法A(g,x,p), g是任何与p互素的整数：

记 x 的 2-进制表达式为 $x(0)+2x(1)+2^2x(2)+\ldots+2^{n-1}x(n-1)$，其中$x(i)$=0 或 1，再记

$$y(i) = g^{2^{n-1-i}x(n-1)+2^{n-2-i}x(n-2)+\ldots+2x(i+1)+x(i)},\ i=0,1,\cdots,n-1$$

注意以下关系：

$$y(0)=y;\quad y(n-1)=g^{x(n-1)}=\begin{cases}1 : x(n-1)=0\\ g : x(n-1)=1\end{cases}$$

$$y(i)=g^{x(i)}y(i+1)^2=\begin{cases}y(i+1)^2 : x(i)=0\\ gy(i+1)^2 : x(i)=1\end{cases},\ i=0,1,\cdots,n-2$$

由此可以导出计算$g^x \bmod p$ 的一个递归算法，每次递归仅需一次模p的平方运算，至多递归n次，n是指数x的二进制位数。

【习题】以伪C语言完整给出算法A(g,x,p)，并分析你算法的复杂度。

二次剩余理论(7)

- 基本结论：
- 二次方程
- $$x^2 = a \bmod p$$
- 解的存在性问题，完全归结为计算余数 $a^{(p-1)/2} \bmod p$ ，
- 且后者存在高效算法。

- 另一种等价的计算方法：基于互反律的Legende符号的快速算法。