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
- $$x^2 = a \bmod p \qquad (i)$$
- 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：$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$

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 $a^{(p-1)/2} \bmod p$，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。

二次剩余理论(8)

- p素 $x^2 = a \bmod p$ (i)
- (1) Legend记号的定义
- $\left(\frac{a}{p}\right) = +1$，若方程$(i)$有解；$\left(\frac{a}{p}\right) = -1$，若方程$(i)$无解；
- (2) Legend记号的性质
- $(a/p) = (r/p)$, 若$a = r \bmod p$

  $(ab/p)=(a/p)(b/p)$

  $(2/p) = (-1)^{(p^2-1)/8}$、a奇则$(a/p)=a^{(p-1)/2} \bmod p$

  $(p/q)(q/p)=(-1)^{(p-1)(q-1)/4}$ (*Gauss-Euler-Legend*互反律)

- 【习题】根据定义及$a^{(p-1)/2} = \left(\frac{a}{p}\right) \bmod p$，证明前两项性质。

二次剩余理论(9)

- 应用互反律计算Legende符号$\left(\frac{a}{p}\right)$的例题
- $\left(\frac{70}{29}\right) = \left(\frac{12}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{2}{29}\right)\left(\frac{3}{29}\right)$
- $= (-1)(-1)\left(\frac{3}{29}\right) = \left(\frac{3}{29}\right) = \left(\frac{29}{3}\right)(-1)^{(3-1)(29-1)/4}$
- $= \left(\frac{29}{3}\right)$
- $= \left(\frac{2}{3}\right) = (-1)^{(9-1)/8} = -1$
- 即 $x^2 = 70 \bmod 29$ 无解。
- 【习题】通过用互反律计算Legender符号，判定以下方程是否有解:
- $x^2 = 10 \bmod 17$;　$x^2 = -3 \bmod 11$;　$x^2 = -5 \bmod 7$
- 【提示】对负数的处理.例如$\left(\frac{-3}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right)$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \bmod p$.

二次剩余理论(10)

- Legende符号的推广：Jaccobi符号
- (1) 对任何两个互素的整数m和n，Jacco符号($\frac{m}{n}$)取值±1，
- 定义如下：
- 若$m=p_1^{e_1}\ldots p_s^{e_s}$和$n=q_1^{f_1}\ldots q_t^{f_t}$是$m$和$n$的素因子分解，则
- $$\left(\frac{m}{n}\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{p_i}{q_j}\right)^{e_i f_j}$$
- 因此若已知m和n素因子分解，则Jaccobi符号的计算归结为素数的Legende符号的计算。
- (2) Jaccobi 符号($\frac{m}{n}$)在形式上有着与Legende符号($\frac{p}{q}$) 完全相同的运算性质。
- 【习题】根据($\frac{m}{n}$) 的定义，证明($\frac{m}{n}$) 的运算性质。

二次剩余理论(10)

- Legende符号的推广：Jaccobi符号
- (1) 对任何两个互素的整数m和n，Jaccobi符号($\frac{m}{n}$)取值± 1,
- 定义如下：
- 若$m=p_1^{e_1}\ldots p_s^{e_s}$和$n=q_1^{f_1}\ldots q_t^{f_t}$是$m$和$n$的素因子分解，则
- $$\left(\frac{m}{n}\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{p_i}{q_j}\right)^{e_i f_j}$$
- 因此若已知m和n素因子分解，则Jaccobi符号的计算归结为素数的Legende符号的计算。
- (2) Jaccobi 符号($\frac{m}{n}$)在形式上有着与Legende符号($\frac{p}{q}$)完全相同的运算性质。
- 【习题】根据($\frac{m}{n}$)的定义，证明($\frac{m}{n}$)的运算性质。

二次剩余理论(11)

- 计算*Jaccobi*符号$\left(\frac{m}{n}\right)$的例子

- (i) $\left(\frac{78}{35}\right)=\left(\frac{8}{35}\right)=\left(\frac{2}{35}\right)\left(\frac{2}{35}\right)\left(\frac{2}{35}\right)=-1$
- (ii) $\left(\frac{79}{35}\right)=\left(\frac{9}{35}\right)=\left(\frac{35}{9}\right)(-1)^{(35-1)(9-1)/4}$
- $=\left(\frac{35}{9}\right)$
- $=\left(\frac{8}{9}\right)=\left(\frac{2}{9}\right)\left(\frac{2}{9}\right)\left(\frac{2}{9}\right)=1$

【注】若n非素数，则$\left(\frac{m}{n}\right)=\pm1$同 $x^2=m \bmod n$ 是否有解不再有对应关系。

【习题】计算$\left(\frac{6}{8}\right)$, $\left(\frac{12}{18}\right)$, $\left(\frac{18}{25}\right)$.

二次剩余理论(12)

- *Jaccobi*符号的应用
- 大素数的快速生成/素性检验算法

Solovay-Strassen(1973)随机算法

```
Q: 随机生成t位的数n;
i=0;
do {    随机生成a: (a,n)=1;
        计算u = a^((n-1)/2) mod n;
        计算Jaccobi符号v = (a/n);
        if u≠v  then goto Q else i++;
} while(i<N);
output(n);
```

"我不喜欢随机算法，因为它不是必然得到一个正确的解...这怎么能称为是算法？！"

"我喜欢随机算法，因为她算得快呀...虽然可能出错，但毕竟差错的几率可控呀"。

- *Solovay-Strassen*算法在循环*N*次后输出素数的概率$P \geq 1 - 2^{-N}$.
- 证明参阅本单元最后的综合的例题，或Stinson教程第五章或*Koblitz*教程第五章。

二次剩余理论(13)

- 其他的素数生成/素性检验算法
- Miller-Rabin算法(1986)：
- M-R算法输出素数的概率$\geq 1 - 4^{-N}$.
- 参阅N.Koblitz第五章。
- 应　用：RSA密码方案的参数生成、各类基于DLP难解性安全方案和安全协议的参数生成等，参见讲义第二部分。

二次剩余理论(14)

- 二次方程 $x^2 = a \bmod p$的解及其计算复杂性
- (a) 与可解性的判定问题不同，求解二次方程具有内在的计算复杂性，
- 即不存在普适的多项式复杂度算法求解二次同余方程。
- (b) 对特殊的素数p，方程有以下的显式解：
- (1) 素数$p=3 \bmod 4$, Legend符号$(a/p)=1$，则$\pm a^{(p+1)/4}$是方程$x^2=a \bmod p$的解。

  事实上，直接计算有$(a^{(p+1)/4})^2=a^{(p+1)/2}=a^{(p-1)/2}a=(a/p)a=a \bmod p$。

  (2) 素数$p=5 \bmod 8$, $(a/p)=1$，首先注意这时$a^{(p-1)/4}=\pm 1 \bmod p$ 且$y^2=-1 \bmod p$总存在解β，前者成立是因为$0=a^{(p-1)/2}-1=(a^{(p-1)/4}-1)(a^{(p-1)/4}+1) \bmod p$，后者成立是因为$(-1/p)=(-1)^{(p-1)/2}=1 \bmod p$因此-1是p的二次剩余。根据这些性质不难验证：

  若$a^{(p-1)/4}=1 \bmod p$则$\pm a^{(p+3)/8}$是方程$x^2=a \bmod p$的解；

  若$a^{(p-1)/4}=-1 \bmod p$则$\pm \beta a^{(p+3)/8}$是方程$x^2=a \bmod p$的解。

二次剩余理论(13)

- 其他的素数生成/素性检验算法
- Miller-Rabin算法(1986)：
- M-R算法输出素数的概率$\geq 1 - 4^{-N}$.
- 参阅N.Koblitz第五章。
- 应　用：RSA密码方案的参数生成、各类基于DLP难解性安全方案和安全协议的参数生成等，参见讲义第二部分。

二次剩余理论(14)

- 二次方程 $x^2 = a \bmod p$的解及其计算复杂性
- (a) 与可解性的判定问题不同，求解二次方程具有内在的计算复杂性，
- 即不存在普适的多项式时间复杂度算法求解二次同余方程。
- (b) 对特殊的素数p，方程有以下的显式解：
- (1) 素数$p=3 \bmod 4$, Legend符号$(a/p)=1$，则$\pm a^{(p+1)/4}$是方程$x^2=a \bmod p$的解。

  事实上，直接计算有$(a^{(p+1)/4})^2=a^{(p+1)/2}=a^{(p-1)/2}a=(a/p)a=a \bmod p$。

  (2) 素数$p=5 \bmod 8$, $(a/p)=1$，首先注意这时$a^{(p-1)/4}=\pm 1 \bmod p$ 且$y^2=-1 \bmod p$总存在解β，前者成立是因为 $0=a^{(p-1)/2}-1=(a^{(p-1)/4}-1)(a^{(p-1)/4}+1) \bmod p$，后者成立是因为$(-1/p)=(-1)^{(p-1)/2}=1 \bmod p$因此−1 是p的二次剩余。根据这些性质不难验证：

  若$a^{(p-1)/4}=1 \bmod p$则$\pm a^{(p+3)/8}$是方程$x^2=a \bmod p$的解；

  若$a^{(p-1)/4}=-1 \bmod p$则$\pm \beta a^{(p+3)/8}$是方程$x^2=a \bmod p$的解。