密码理论与技术
–计算机密码学理论与应用

田园

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

有限域的基本性质与应用(11)

- 求解素域F_p上的DLP问题 $y = g^x \mod p$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$z^2 = a \mod p$ 的某个算法。
- (3) 对DLP问题，设x的二进制表示为$x=x_0 + 2x_1 + 2^2x_2 +\ldots+ 2^nx^n$,
- $x_i = 0, 1$, 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
- $y^{(p-1)/2} \mod p$ = -1还是+1，因此通过计算$y^{(p-1)/2} \mod p$能完全确定x的最低位x_0.
- (ii) 确定x_0后，注意到$y = g^x \mod p = g^{x_0} (g^{x_1+2x_2+\cdots+2^{n-1}x_n})^2 \mod p$,
- 因此$(g^{x_1+2x_2+\cdots+2^{n-1}x_n})^2 \mod p = yg^{-x_0} \mod p$, 再通过调用算法
- $B(yg^{-x_0} \mod p, p)$解出出$y_1 = g^{x_1+2x_2+\cdots+2^{n-1}x_n} \mod p$。
- (iii) 应用与(i)同样的方法，确定出次低位x_1 = 1还是0。
- (iv) 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。**

有限域的基本性质与应用(12)

【思考题】这一习题的目的是证明因子分解问题与求平方根问题难度等价。N=pq，p和q是(很大的)素数，a是与N互素的整数且使x^2=a mod N存在解。

(1) 若有算法A使A(N)输出素因子p和q，证明x^2=a mod N的解可以由以下过程得到：

第一步：分别求解u^2 =a mod p 和 v^2=a mod q，得解u_1,u_2,v_1,v_2；

第二步：对每一个组合(u_i,v_j)由中国剩余定理计算x：$x=u_i \bmod p$, $x=v_j \bmod q$。

由以上算法可以看到，x^2=a mod N一般地有四个解。

(2) 若存在一个算法B，任给与N互素的整数a且x^2=a mod N存在解(这由其他方法判定)，B(a,n)输出以上方程的四个解，证明以下算法可以得到N的素因子：

第一步：任取与N互素的y，计算$a=y^2 \bmod N$；

第二步：调用算法B(a,N)输出x_1, x_2, x_3, x_4，设其中$x_3=+y \bmod N$, $x_4=-y \bmod N$；

第三步：由Euclid算法计算(n, x_1+x_3)，则输出必是p或q之一。

习 题

- *Stallings*教程第四章习题：
- 4.6~4.13、4.23、4.24：
- 该组问题和我们前面已做过的习题类似，数值答案可自行验证，不提交。
- 4.16~4.18：
- 该组习题为算法分析题，下周提交。

- 下页是本单元的综合型例题，基于本单元的全部知识，论证Solovay-Strassen
- 随机算法每轮循环的差错概率不大于50%。请使自己清晰地理解全部细节。

第一单元的学习要点

- 主题　整数的算术运算及其基本规律
- 一、基本概念：
- 整数的同余等价关系、互素、素数的原根、离散对数、
- Euler函数、群、子群、素域F_p、扩域，Legender符号和Jaccobi符号；
- 离散对数问题、判定性和计算型Diffie-Hellman问题、
- 因子分解问题；
- 二、基本规律/定理：
- Euclid第一定理
- Euclid第二定理
- Euclid第三定理/线性同余式$ax=b \bmod N$的可解性判定条件
- 中国余数定理/求解公式
- Euler函数的基本性质、Euler公式和Fermat公式
- 二次同余式$x^2=a \bmod p$的可解性判定条件
- *Legender*符号和*Jaccobi*符号的形式计算规则/二次互反律；
    - 群的Lagrange定理：有限群的阶是其任何子群的阶的整数倍。
    - 多项式的基本运算
    - 多项式的同余等价关系
    - 多项式的相关Euclid定理
- 红色：重点内容

例题(Solovay-Strassen算法概率的理论依据)

- n是正奇整数，G(n)≡{a: a ∈Z_n^*, $(\frac{a}{n}) = a^{(n-1)/2} mod\ n$}，证明以下结论：
- (1) G(n)及其上面的mod n的乘法运算构成Z_n^*的子群，进而由Lagrange
- 定理，如果G(n)≠Z_n^*则
- $|G(n)| \leqq |Z_n^*|/2 \leqq (n-1)/2$ (为什么？)
- 证明： 对任何a和b ∈G(n), 由$(\frac{a}{n}) = a^{(n-1)/2}$mod n和$(\frac{b}{n}) = b^{(n-1)/2}$mod n 有
- $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n}) = (a^{(n-1)/2} \bmod n)(b^{(n-1)/2} \bmod n) \bmod n = (ab)^{(n-1)/2} \bmod n.$
- 因此G(n)对$mod\ n$乘法运算封闭。
- 如果a∈G(n), 则有b ∈Z_n^*使ab = 1 mod n，于是由$1= (\frac{1}{n})= (\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$
- $= a^{(n-1)/2}(\frac{b}{n})$ mod n (为什么？) 有$(\frac{b}{n}) = b^{(n-1)/2}$mod n(为什么？)，即a在G(n)中
- 有逆元素。
- 显然1是乘法中性元素，综上所述，故G(n)是群。
-

例题/续(Solovay-Strassen算法概率的理论依据)

- n是正奇整数，G(n)≡{a: a ∈Z_n^*, $(\frac{a}{n}) = a^{(n-1)/2} mod\ n$}，证明以下结论：
- (2) 设n=p^kq，p、q是奇数且p是素数，k≥2，(p,q)=1。如果a=1+$p^{k-1}q$，则
- $$(\frac{a}{n}) \neq a^{(n-1)/2} mod\ n$$

- 证明： $(\frac{a}{n}) = (\frac{1+p^{k-1}q}{p^kq}) = (\frac{1+p^{k-1}q}{p^{k-1}q})(\frac{1+p^{k-1}q}{p}) = (\frac{1}{p^{k-1}q})(\frac{1+p^{k-1}q}{p})$ (为什么？)
- 并注意到 $1+p^{k-1}q = 1 \bmod p$(为什么？)因此 $(\frac{1+p^{k-1}q}{p}) = (\frac{1}{p})=1$，进而
- $$(\frac{a}{n}) = (\frac{1}{p^{k-1}q}) = (\frac{1}{p})^{k-1}(\frac{1}{q}) = 1^{k-1}1 \text{ (为什么？) } = 1;$$
- 另一方面， $a^{(n-1)/2} = (1+p^{k-1}q)^{(n-1)/2} = 1 + \frac{1}{2}(n\text{-}1)p^{k-1}q + p^{k-1}q$的高次项，故
- $$a^{(n-1)/2} \bmod n = (1 + \frac{1}{2}(n\text{-}1)p^{k-1}q) \bmod n \text{ (为什么？)。}$$
- 但 $(1 + \frac{1}{2}(n\text{-}1)p^{k-1}q) \bmod n \neq 1 \bmod n$，否则将有 $\frac{1}{2}(n\text{-}1)p^{k-1}q = 0 \bmod n = 0 \bmod p^kq$,
- 进而必有p|(n-1)，然而这是不可能的(为什么？提示：$n= p^kq$)。 证毕。

例题/续(Solovay-Strassen算法概率的理论依据)

- n是正奇整数，G(n)≡{a: a ∈Z_n^*, $(\frac{a}{n}) = a^{(n-1)/2} mod\ n$}，证明以下结论：
- (3) 设$n=p_1...p_s$，p_j是不同的奇素数。u是满足$(\frac{u}{p_1})$ = -1的一个整数，a是满足
- $a=u$ mod p_1和a = 1 mod $p_2...p_s$的整数 (为什么这样的a必存在？)。证明
- $$(\frac{a}{n}) = -1$$
- 因此
- 证明： $(\frac{a}{n}) = (\frac{a}{p_1 p_2 ... p_s}) = (\frac{a}{p_1})(\frac{a}{p_2 ... p_s}) = (\frac{u}{p_1})(\frac{1}{p_2 ... p_s})$ = -1 (为什么？)；
- 推论：因为$a^{(n-1)/2} = 1\ mod\ p_2...p_s$ (为什么？) 故 $a^{(n-1)/2} \neq (\frac{a}{n})\ mod\ n$ (为什么？提示：
- 假若等式成立，即$a^{(n-1)/2}$ = -1 $mod\ n$，则必有$a^{(n-1)/2}$ = -1 $mod\ p_2...p_s$ (为什么？)从而有一个矛盾)。
- (4) 当n是奇合数时， |G(n)| ≦ (n-1)/2。
- 证：当n是奇合数时，n的因子分解结构或者具有形式$n=p^k q$，其中p、q是奇数且
- p是素数，k≥2，(p,q)=1；或者有 形式$n=p_1...p_s$，其中p_j是不同的奇素数(为什么？)。
- 从(2)和(3)的结论, 得到在每种情形下均存在a ∈Z_n^*\G(n), 因此这里的结论成立
- (请补全推理的细节)。

例题/续(Solovay-Strassen算法概率的理论依据)

- n是正整数，G(n)≡{a: a ∈Z_n^*, $(\frac{a}{n}) = a^{(n-1)/2} mod\ n$}，证明以下结论：

- (5) *Solovay-Strassen*算法在每次检验时发生差错的概率P≤1/2.

- 证：仅当n是奇合数、同时随机生成的a∈G(n)时，检验发生差错（为什么？）。
- 对奇合数n，前面已论证 |G(n)| ≦ (n-1)/2，因此差错的概率P≤1/2（为什么？）。