RSA 算法中的代数结构

司光东,杨加喜,谭示崇,肖国镇
(西安电子科技大学 ISN 综合业务网国家重点实验室,陕西西安 710071)

摘 要: 本文首次应用二次剩余理论对 RSA 中的代数结构进行了研究.计算出了 Z_n^* 中模 n 的二次剩余和二次非剩余的个数,对它们之间的关系进行了分析,并用所有二次剩余构成的群对 Z_n^* 进行了分割,证明了所有陪集构成的商群是一个 Klein 四元群.对强 RSA 的结构进行了研究,证明了强 RSA 中存在阶为 $\phi(n)/2$ 的元素,并且强 RSA 中 Z_n^* 可由三个二次非剩余的元素生成.确定了 Z_n^* 中任意元素的阶,证明了 Z_n^* 中所有元素阶的最大值是 $lcm(p-1,q-1)$,并且给出了如何寻找 Z_n^* 中最大阶元素方法.从而解决了 RSA 中的代数结构.

关键词: RSA 算法; 代数结构; 二次剩余; 欧拉函数
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0242-05

Algebra Structure of RSA Arithmetic

SI Guang-dong, YANG Jia-xi, TAN Shi-chong, XIAO Guo-zhen
(*State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Based on the theory of quadratic residues, the algebra structure of RSA arithmetic is researched in this paper. This work calculates numbers of quadratic residues and non-residues in the group Z_n^* and investigates their relationship. Z_n^* is divided up by the group made up with all quadratic residues in Z_n^* and all cosets form a quotient group of order 4 which is a Klein group. Studyed the structure of strong RSA further, it shows that the element of order $\phi(n)/2$ exists and the group Z_n^* can be generated by three elements of quadratic non-residues. Let the facterization $n = p \cdot q$, the order of each element can be calculated, and the biggest order of all element is $lcm(p-1, q-1)$ in Z_n^*. It also shows how to find the element of the biggest order. So the algebra structure of RSA arithmetic is solved.

Key words: RSA arithmetic; algebra structure; quadratic residues; euler's phi function

1 引言

自从 1976 年 W Diffie 和 M Hellman 提出公钥密码体制以来[1],以数学为基础的非对称加密算法取得了突破性进展.这一体制的最大特点就是采用两个密钥将加密与解密能力分开,公开的密钥作为加密密钥,保密的密钥作为解密密钥,实现了通信双方无需事先交换密钥就可以进行保密通信.这些算法都是基于某个数学上的困难问题,在有限的计算资源和有限的储存空间下要从公开的密钥或密文中分析出私有密钥是不可行的.如果把私有密钥作为加密密钥而把公开密钥作为解密密钥,就可实现由一个用户加密的消息使多个用户解读,从而实现了代替手写签名的数字签名.公钥密码体制的提出为解决计算机信息网络中的安全和用户的身份认证提供了新的理论和技术基础.

1978 年,三位年青数学家 R L Rivest, A Shamir 和 L Adleman 提出了一种基于大整数分解困难问题的密码算法,称为 RSA 算法[2].这种算法既可以用于加密,又可以用作数字签名,并可构造其它的签名方案[3,4],是目前最能被人们接受也是最被广泛使用的算法.国际上一些标准化组织 ISO, ITU, SWIFT 等都已接受 RSA 体制作为标准.在 Internet 中,电子邮件是最常用的一种网络服务,广泛采用的 PGP(Pretty Good Privacy)技术就是用 RSA 算法作为传送会话密钥和数字签名的标准算法来保证电子邮件中的机密性和身份认证.

在 RSA 算法中,$n = p \cdot q$,其中 p, q 是长度约为 512 比特的大素数.其困难性基于:知道两个大素数 p, q,容易计算 $n = p, q$.反之仅知道 n,分解 $n = p, q$ 在计算上是不可行的.D Boneh 证明了 RSA 算法中私有密钥长度小于 $n^{0.292}$时方案容易被攻破[5],并对 20 年中 RSA 算法的攻击进行了总结[6].目前为止 RSA 算法还未遇到太大的挑战,这也是人们普遍认可该算法的原因之一.

本文中所述的 RSA 代数结构就是指 Z_n^*(表示与 n 互素且在模 n 下的剩余类)的代数结构,因为 RSA 算法

收稿日期:2007-12-26;修回日期:2008-04-11
基金项目:国家自然科学基金(No.60773003, No.60603010)

是在 Z_n^* 中进行讨论的.通过研究 Z_n^* 的代数结构,计算出了 Z_n^* 中模 n 的二次剩余和二次非剩余的个数,对它们之间的关系进行了分析,并用二次剩余集合对 Z_n^* 进行了分割,证明了所有陪集构成的商群是一个 Klein 四元群.同时对强 RSA 的结构进行了分析,证明了强 RSA 中存在阶为 $\phi(n)/2$ 的元素,并且强 RSA 中 Z_n^* 可由三个二次非剩余的元素生成.本文同时给出了如何确定了 Z_n^* 中任意元素的阶,证明了 Z_n^* 中所有元素阶的最大值是 $t = lcm(p-1, q-1)$,并且给出了如何寻找 Z_n^* 中最大阶元素的方法.最后计算出了随机选取 Z_n^* 中元素恰好是最大阶元素的概率.

本文中采用的记号:Z_n 表示模 n 下的剩余类,Z_n^* 表示与 n 互素且在模 n 下的剩余类,$\phi(\cdot)$表示欧拉函数,$\gcd(x,y)$表示 x, y 的最大公约数,$lcm(u,v)$表示 u, v 的最小公倍数.$\langle a\rangle$表示由元素 a 生成的循环群,$|b|$表示元素 b 的阶,$|A|$表示集合 A 中元素的个数,xA 表示元素 x 与集合 A 中每个元素左乘所得的集合.当 m 为素数时,符号$\left(\frac{a}{m}\right)$表示 a 对 m 的勒让德符号(m 为素数时),当 m 为合数时,符号$\left(\frac{a}{m}\right)$表示 a 对 m 的雅可比符号.

2　RSA 算法

选取两个大素数 p, q 使 $n = p\cdot q$,其中 p, q 是长度大约为 512 比特的大素数.计算出 $\phi(n) = \phi(p\cdot q) = (p-1)(q-1)$.选取公开密钥 e.$1 \leqslant e \leqslant \phi(n)$,$\gcd(e, \phi(n)) = 1$ 在模 $\phi(n)$下计算出私有密钥 d,使 $ed = 1(\mathrm{mod}\phi(n))$.

加密算法:任取消息 $m \in Z_n^*$(必要时可对消息进行分块),计算出密文 $y = m^e(\mathrm{mod}n)$.

解密算法:恢复出明文 $y^d = (m^e)^d = m^{ed} = m(\mathrm{mod}n)$.

3　RSA 的代数结构

在 RSA 算法中,运算都是在集合 $Z_n^* = \{x = \bar{x}(\mathrm{mod}n) \mid \bar{x} \in Z, n = p\cdot q, \gcd(\bar{x}, n) = 1\}$中进行的,共有 $\phi(n) = \phi(p\cdot q) = (p-1)(q-1)$个元素.下面主要讨论 Z_n^* 的代数结构.

易知,Z_n^* 在普通乘法和模运算下构成一个群.

定义 1[7]　设整数 $m>0$,在 Z_m^* 中,$\gcd(g, m) = 1$,如果整数 g 对 m 的次数为 $\phi(m)$,则 g 叫做 m 的一个原根.

定义 2[8]　对于整数 n,整数 a 叫做模 n 的二次剩余,如果 $\gcd(a, n) = 1$,并且存在整数 x,使 $x^2 = a(\mathrm{mod}a)$成立.否则就称为 a 为模 n 的二次非剩余.

引理 1[7]　在 Z_m^* 中,设 $m>1$,则 m 有原根的充要条件是,m 必为下列诸数之一:$2, 4, p^l, 2p^l$,这里 $l \geqslant 1$,p 是奇素数.

定理 1　在 RSA 算法中,$n = p\cdot q$,其中 p, q 是大素数且 $p \neq q$,Z_n^* 中元素的阶最大可能为 $(p-1)(q-1)/2$.

证明　根据引理 1 知,$n \neq 2, 4, p^l, 2p^l$,故 n 没有原根.又由于对于任何的 $a \in Z_n^*$,有 $a^{\phi(n)} = 1(\mathrm{mod}n)$,$a$ 的阶是 $\phi(n)$的因子,而 $(p-1)(q-1)/2$ 是 $\phi(n)$的最大真因子,所以 Z_n^* 中元素的阶最大可能为 $(p-1)(q-1)/2$.　得证

注　通常元素的阶达不到 $(p-1)(q-1)/2$.比如 $n = p\cdot q = 7\times 13$,$Z_n^*$ 中元素的阶最大为 12,其中 5 就是阶为 12 的元素.

引理 2[9]　在强 RSA 算法中,$n = p\cdot q$,$p = 2p' + 1$,$q = 2q' + 1$,其中 p, p', q, q'是大素数且 $p \neq q$,Z_n^* 中元素的阶为 $\{1, 2, p', q', 2p', 2q', p'q', 2p'q'\}$之一.并且元素 $a \in Z_n^*$ 的阶为 $p'q'$或 $2p'q'$的充要条件是 $\gcd(a \pm 1, n) = 1$.

推论　设 n 满足引理 2 的条件,对于任意的 $a \in Z_n^*$,且 $\gcd(a \pm 1, n) = 1$,则 $\langle a^2\rangle \subset Z_n^*$ 是阶为 $p'q'$ 的循环子群.

引理 3[10]　若 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数,$m = m_1\cdot m_2\cdots m_k$,则同余式

$$f(x) \equiv 0(\mathrm{mod}m) \tag{1}$$

与同余式组 $f(x) = 0(\mathrm{mod}m_i)$,$i = 1, 2, \cdots, k$ 等价.并且若用 T_i 表示

$$f(x) = 0(\mathrm{mod}m_i),\ i = 1, 2, \cdots, k$$

对模 m_i 的解数,用 T 表示(1)对模 m 的解数,则 $T = T_1\cdot T_2\cdots T_k$.

定理 2　在 RSA 中,设 n 满足定理 1 的条件,则在 Z_n^* 中模 n 的二次剩余有 $\phi(n)/4$ 个.

证明　首先,设 a 是模 n 的一个二次剩余,Z_n^* 中模 n 的二次剩余所成的集合为:

$$\{a \mid a = x^2(\mathrm{mod}n), x \in Z_n^*, n = pq\}$$

故 Z_n^* 中每个元素都是某个二次剩余的根.

而由于 $x^2 = a(\mathrm{mod}n)$与

$$x^2 = a(\mathrm{mod}p) \tag{2}$$

$$x^2 = a(\mathrm{mod}q) \tag{3}$$

等价.同余方程组中每个方程都有 2 个不等根,根据引理 3 知,

$$x^2 = a(\mathrm{mod}n) \tag{4}$$

在 Z_n^* 中有 4 个根.下证这四个根不相等.

设 $x_1, p - x_1$ 是方程(2)的两个根,$x_2, q - x_2$ 是方

程(3)的两个根.易知由$\begin{cases}x=x_1(\mathrm{mod}p)\\x=x_2(\mathrm{mod}q)\end{cases}$确定了方程(4)的唯一根,同理,由$(x_1,q-x_2),(p-x_1,x_2),(p-x_1,q-x_2)$确定了方程(4)的另三个根,这四个根显然不相等.$Z_n^*$ 中每 4 个不同的元素对应唯一的一个二次剩余,故可得出以上结论. 得证

例 1 当 $n=7\times13$ 时,Z_n^* 中元素的阶最大为 12.并且它的全部二次剩余:1,4,9,16,25,36,64,81,30,53,43,74,51,88,29,79,22,23 共 18 个.即$(p-1)(q-1)/4$个.表 1 列出了全部二次剩余对应的平方根($1\leqslant x\leqslant 45$).当然,如果 1 是平方根,则 90 也是这个二次剩余的平方根,同理 x 是某个二次剩余的平方根,$91-x$ 也是它的平方根.所以表 1 中每个二次剩余对应 4 个平方根.

表 1

二次剩余	1	4	9	16	25	36	64	81	30
平方根	1,27	2,37	3,10	4,17	5,44	6,20	8,34	9,30	11,24
二次剩余	53	43	74	51	88	29	79	22	23
平方根	12,40	15,41	16,23	18,31	19,33	22,43	25,38	29,36	32,45

定理 3 在强 RSA 中,设 n 满足引理 2 的条件,则 Z_n^* 中全部二次剩余构成一个循环群.

证明 根据定理 2 知,Z_n^* 中模 n 的二次剩余有$\phi(n)/4$个.又根据引理 2 推论知,对于任意的 $a\in Z_n^*$,且 $\gcd(a\pm1,n)=1$,则$\langle a^2\rangle\subset Z_n^*$ 是阶为 $p'q'=\phi(n)/4$ 的循环子群.显然 a^2 是一个二次剩余,同时由 a^2 生成的所有元素都是二次剩余.故$\langle a^2\rangle\subset Z_n^*$ 生成了 Z_n^* 中的全部二次剩余,是一个循环群.

定理 4 在强 RSA 中,设 n 满足引理 2 的条件,则 Z_n^* 中存在阶为 $\phi(n)/2$ 的元素,且该元素为二次非剩余.

证明 对于任意的二次非剩余 $b\in Z_n^*$,且 $\gcd(b\pm1,n)=1$(易知元素 b 是存在的),根据引理 2 推论知$\langle b^2\rangle\subset Z_n^*$ 是阶为 $p'q'$ 的循环子群.而$\langle b^2\rangle$包含了 Z_n^* 的全部二次剩余,故 $b\notin\langle b^2\rangle$.所以$\langle b^2\rangle<\langle b\rangle<Z_n^*$.从而 b 的阶大于 $p'q'$.由于 Z_n^* 中元素的阶大于 $p'q'$ 中只有$\phi(n)/2=2p'\cdot q'$.故$|b|=\phi(n)/2$,$\langle b\rangle$就是阶为$\phi(n)/2$的循环群. 得证

强 RSA 的 Z_n^* 中全部二次剩余构成阶为$\phi(n)/4$ 的循环群,可知任意二次剩余元素的阶都是 $\phi(n)/4$ 的因子.故阶为 $\phi(n)/2$ 的元素必然是一个二次非剩余.并且在由 Z_n^* 中二次非剩余生成的阶为$\phi(n)/2$ 的循环群中,二次剩余和二次非剩余各占 $\phi(n)/4$ 个.

定理 5 在 RSA 中,设 n 满足 $n=p\cdot q$,其中 p,q 是大素数且 $p\neq q$,令

$$A=\left\{a\mid a\in Z_n^*,\left(\frac{a}{p}\right)=1\text{ and }\left(\frac{a}{q}\right)=1\right\}$$

$$X=\left\{x\mid x\in Z_n^*,\left(\frac{x}{p}\right)=-1\text{ and }\left(\frac{x}{q}\right)=1\right\}$$

$$Y=\left\{y\mid y\in Z_n^*,\left(\frac{y}{p}\right)=1\text{ and }\left(\frac{y}{q}\right)=-1\right\}$$

$$S=\left\{s\mid s\in Z_n^*,\left(\frac{s}{p}\right)=-1\text{ and }\left(\frac{s}{q}\right)=-1\right\}$$

则$|A|=|X|=|Y|=|S|=\phi(n)/4$,$A\cup X\cup Y\cup S=Z_n^*$ 且 A,X,Y,S 两两交集为空集.

证明 对于任意元素 $b\in Z_n^*$,故$\left(\frac{b}{p}\right)=\pm1$ 以及$\left(\frac{b}{q}\right)=\pm1$ 都是唯一的,从而 b 必然属于且唯一属于以上四个集合之一,易知 $A\cup X\cup Y\cup S=Z_n^*$ 且 A,X,Y,S 两两交集为空集.从而由 A,X,Y,S 构成 Z_n^* 的一个分割.

在 Z_n^* 中,集合 A 包含了全部二次剩余,且$|A|=\phi(n)/4$,从而二次非剩余共有$|X|+|Y|+|S|=3\phi(n)/4$个.任意取一个二次非剩余,不妨设 $x_0\in X$,用 $x_0Z_n^*$ 表示 x_0 乘以 Z_n^* 所成的集合.由于 Z_n^* 是一个乘法群,元素与元素的积封闭,$x_0Z_n^*\subseteq Z_n^*$.反之,对于任意的元素 $a_1a_2\in Z_n^*$,如果 $x_0a_1=x_0a_2$,两边同乘以 $x_0^{-1}\in Z_n^*$,可得 $a_1=a_2$,也就是说,$x_0Z_n^*$ 中的元素和 Z_n^* 的元素一样多.故可知 $x_0Z_n^*=Z_n^*$.

对于集合 $x_0Z_n^*$ 来说,任取元素 $x\in X$,由于

$$\left(\frac{x_0x}{p}\right)=\left(\frac{x_0}{p}\right)\left(\frac{x}{p}\right)=(-1)(-1)=1$$

$$\text{and }\left(\frac{x_0x}{q}\right)=\left(\frac{x_0}{q}\right)\left(\frac{x}{q}\right)=1,$$

故 $x_0x\in A$,即 $x_0X\subseteq A$,从而有$|X|=|x_0X|\leqslant|A|$.

对于集合 x_0A 来说,任取元素 $a\in A$,

$$\left(\frac{x_0a}{p}\right)=\left(\frac{x_0}{p}\right)\left(\frac{a}{p}\right)=(-1)\times1=-1$$

$$\text{and }\left(\frac{x_0a}{q}\right)=\left(\frac{x_0}{q}\right)\left(\frac{a}{q}\right)=1,$$

$x_0x\in X$,故 $x_0A\subseteq X$,从而有$|A|=|x_0A|\leqslant|X|$.所以有$|X|=|A|$.

同理,可得$|A|=|X|=|Y|=|S|=\phi(n)/4$. 得证

定理 6 在强 RSA 中,设 n 满足引理 2 的条件,则 Z_n^* 可由三个二次非剩余的元素生成.

证明 由定理 5 知,由 A,X,Y,S 构成 Z_n^* 的一个分割.任选二次非剩余 $x\in X$,且 $\gcd(x\pm1,n)=1$.根据定理 4 知$\langle x\rangle$是阶为 $\phi(n)/2$ 的循环群.因为对于任意的 $m\in Z$,有 $x^{2m}\in A$,$x^{2m+1}\in X$,所以$\langle x\rangle\subseteq A\cup X$.由于

$$|\langle x\rangle|=|A\cup X|=\phi(n)/2,$$

知$\langle x\rangle=A\cup X$.

同理$\langle y\rangle=A\cup X$,$\langle s\rangle=A\cup S$,这里 $y\in Y,s\in S$ 分别是阶为$\phi(n)/2$ 元素.从而有$\langle x,y,s\rangle=Z_n^*$. 得证

定理 7　在 RSA 中,设 n 满足 $n = p \cdot q$,其中 p, q 是大素数且 $p \neq q$,则

$$A = \left\{ a \mid a \in Z_n^*, \left(\frac{a}{p}\right) = 1 \text{ and } \left(\frac{a}{q}\right) = 1 \right\}$$

是 Z_n^* 中的不变子群,并且由子群 A 在 Z_n^* 中作成的陪集刚好是 A, X, Y, S,由陪集作成的商群 Z_n^*/A 是一个 Klein 四元群.

证明　由于 A 是群 Z_n^* 的一个子集,对于任意的 $a, b \in A$,易知 $a \cdot b \in A$.设 $a^{-1} \in Z_n^*$ 是 a 的乘法逆元,

由 $\left(\frac{a}{p}\right)\left(\frac{a^{-1}}{p}\right) = \left(\frac{aa^{-1}}{p}\right) = \left(\frac{1}{p}\right) = 1$

and $\left(\frac{a^{-1}}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{aa^{-1}}{q}\right) = \left(\frac{1}{q}\right) = 1$

知 $a^{-1} \in A$,故 A 是群 Z_n^* 的一个子群,由于 Z_n^* 中元素对乘法满足交换律,所以 A 是群 Z_n^* 的一个不变子群.

对于任意的 $a \in A, x \in X, y \in Y, s \in S$ 有 $aA = A, xA = X, yA = Y, sA = S$,知由子群 A 在 Z_n^* 中作成的陪集刚好是 A, X, Y, S.易知这四个陪集作成的商群 Z_n^*/A 是一个四元群.下证是 Klein 四元群.

在陪集中定义以下乘法:对于任意的 $u, v \in Z_n^*$, $uA \circ vA = uvA$(由陪集的相关知识知,此定义对新的乘法。是合理的).设这四个元素分别是 A, xA, yA, sA,对于任意的 $x \in X, y \in Y, s \in S$.因为

(1)结合律成立:$u, v, t \in Z_n^*$, $(uA \circ vA) \circ tA = uvA \circ tA = uvtA$, $uA \circ (vA \circ tA) = uA \circ vtA = uvtA$,

(2)$A \circ A = A, A \circ xA = xA, A \circ yA = yA, A \circ sA = sA \Rightarrow A$ 是单位元.

(3)$x \cdot x, y \cdot y, s \cdot s \in A \Rightarrow xA \circ xA = A, yA \circ yA = A, sA \circ sA = A$,即 xA, yA, sA 是二阶元素,是自身的逆元.

(4)$x \cdot y \in S, y \cdot s \in X, x \cdot s \in Y \Rightarrow xA \circ yA = sA, yA \circ sA = xA, xA \circ sA = yA$

故以上的陪集作成的四元群是一个 Klein 四元群.

得证

下面讨论如何确定 Z_n^* 中元素的阶,如何确定 Z_n^* 中所有元素阶的最大值,如何寻找 Z_n^* 中阶最大的元素.

定理 8　在 RSA 中,设 n 满足 $n = p \cdot q$,其中 p, q 是大素数且 $p \neq q$,设 Z_n^* 中元素 a 在群 Z_p^*, Z_q^* 中的阶分别为 u, v,则元素 a 在群 Z_n^* 中的乘法阶为 $t = lcm(u, v)$, $lcm(u, v)$ 表示 u, v 的最小公倍数.

证明　由于元素 a 在群 Z_p^*, Z_q^* 中阶分别为 u, v,则有 $a^u = 1 (\mathrm{mod} p)$ 和 $a^v = 1 (\mathrm{mod} q)$ 成立,故 $a^t = 1 (\mathrm{mod} p)$ 和 $a^t = 1 (\mathrm{mod} p)$ 同时成立.从而 $a^t = 1 (\mathrm{mod} n)$.

设 a 在群 Z_n^* 中的乘法阶为 t',可知 $t' \mid t$.并且 $a^{t'} = 1 (\mathrm{mod} n)$.

故 $a^{t'} = 1 (\mathrm{mod} p)$ 和 $a^{t'} = 1 (\mathrm{mod} q)$ 成立.又因为 u, v 是元素 a 在群 Z_p^*, Z_q^* 中阶,则 $u \mid t'$, and, $v \mid t'$,从而 $t \mid t'$.所以 $t = t'$.　得证

例 2　当 $n = 19 \times 23$ 时,元素 2 是 Z_{19}^* 的生成元,阶为 18,在 Z_{23}^* 中阶为 11.经过验证知 2 在 Z_{437}^* 中阶为 198.

定理 9　在 RSA 中,设 n 满足 $n = p \cdot q$,其中 p, q 是大素数且 $p \neq q$,则 Z_n^* 中所有元素的阶最大为 $t = lcm(p-1, q-1)$,且 Z_n^* 中所有元素的阶都是 t 的因子.

证明　对于任意的元素 $a \in Z_n^*$,由于 $a^{p-1} = 1 (\mathrm{mod} p)$ 及 $a^{q-1} = 1 (\mathrm{mod} q)$ 成立.从而有 $a^t = 1 (\mathrm{mod} p)$ 和 $a^t = 1 (\mathrm{mod} q)$ 成立.故 $a^t = 1 (\mathrm{mod} n)$,即 Z_n^* 中元素的阶不超过 t.

下证 Z_n^* 中存在阶为 t 的元素.由于群 Z_p^*, Z_q^* 是循环群,设 a, b 分别是群 Z_p^*, Z_q^* 生成元,即 a, b 在群 Z_p^*, Z_q^* 中的阶分别为 $p-1, q-1$.根据中国剩余定理知,Z_n^* 中存在唯一的元素 x 使式(5)成立.

$$\begin{cases} x = a (\mathrm{mod} p) \\ x = b (\mathrm{mod} q) \end{cases} \tag{5}$$

易知 x 在群 Z_p^*, Z_q^* 中的阶分别为 $p-1, q-1$.由定理 8 可知,元素 x 在群 Z_n^* 中的阶为 t.从而证明了 Z_n^* 中所有元素的阶最大为 $t = lcm(p-1, q-1)$.

对于任意的元素 $a \in Z_n^*$,由上知 $a^t = 1 (\mathrm{mod} n)$ 成立,故 a 的阶是 t 的因子.　得证

定理 9 合理地解释了当 $n = 7 \times 13$ 时,例 1 中元素的最大阶为 12 的问题,同时也给出了如何寻找 Z_n^* 中阶最大的元素的方法.在实际操作中,由定理 8 知只要选在 Z_p^* 和 Z_q^* 中元素阶的最小公倍数等于 $lcm(p-1, q-1)$,同样能满足是 Z_n^* 中阶最大元素的要求.下面计算对于任意选择的元素 $x \in Z_n^*$ 是阶最大元素的概率.

由式(5)知 $x \in Z_n^*$ 与有序数对 $(a, b) \in Z_p^* \times Z_q^*$ 是一一对应的.由定理 8、9 知,只有当 a, b 在 Z_p^*, Z_q^* 的阶 $|a|, |b|$ 使

$$lcm(|a|, |b|) = lcm(p-1, q-1) \tag{6}$$

成立时,x 是 Z_n^* 中阶最大元素.设 $d = \gcd(p-1, q-1)$, $c_1, c_2 \in Z^+$ 且 $c_1 c_2 \mid d$,设 $|a| = (p-1)/c_1$, $|b| = (q-1)/c_2$,由式(6)可得:

$$\frac{|a| \cdot |b|}{\gcd(|a|, |b|)} = \frac{c_1|a| \cdot c_2|b|}{\gcd(c_1|a|, c_2|b|)}$$

$$\Leftrightarrow c_1 c_2 \gcd(|a|, |b|) = \gcd(c_1|a|, c_2|b|)$$

$$\Leftrightarrow \gcd(|a|, |b|) = \gcd\left(\frac{|a|}{c_2}, \frac{|b|}{c_1}\right)$$

$$\Leftrightarrow \gcd(c_1, c_2) = 1 \wedge \gcd(|a|, |b|) = \frac{d}{c_1 c_2}$$

令 $T = \{ c_1, c_2 \mid c_1, c_2 \in Z^+ \wedge c_1 c_2 \mid d \wedge \gcd(c_1, c_2) =$

$1 \wedge \gcd(|a|,|b|) = \frac{d}{c_1 c_2}\}$.

由于 a,b 分别在模 p,q 下生成了 $(p-1)/c_1,(q-1)/c_2$ 阶循环群.由循环群相关性质知,对于特定的 c_1c_2,上述 $(p-1)/c_1,(q-1)/c_2$ 阶循环群分别有 $\phi((p-1)/c_1),\phi(q-1)/c_2)$ 个生成元,从而 Z_p^*,Z_q^* 在中分别有 $\phi((p-1)/c_1),\phi(q-1)/c_2)$ 个 $(p-1)/c_1),(q-1)/c_2$ 阶元素.所以满足等式(6)的 $x \in Z_n^*$ 共有 $\phi((p-1)/c_1)\cdot\phi(q-1)/c_2)$ 个.当 c_1,c_2 遍历 T 时,满足等式(6)的 x 共有 $\sum_T \phi((p-1)/c_1)\cdot\phi(q-1)/c_2)$ 个.

故任意选择的元素 $x \in Z_n^*$ 是阶最大元素的概率为:

$$\frac{\sum_T \phi((p-1)/c_1)\cdot\phi(q-1)/c_2)}{\phi(n)}$$

4 结束语

RSA 算法是二十世纪数学界和密码学界最为重要的发现之一,对非对称加密和数字签名影响深远,成为现实生活中最被广泛使用的算法.通过上述分析,已经完全解决了 RSA 中的代数结构.得出了 Z_n^* 中所有二次剩余和二次非剩余的个数,并且由所有二次剩余对 Z_n^* 进行了分割,所得的陪集构成了一个 Klein 四元商群.确定了 Z_n^* 中任意元素的阶,证明了 Z_n^* 中所有元素阶的最大值是 $t = lcm(p-1,q-1)$,并且给出了如何寻找 Z_n^* 中最大阶元素方法以及计算出了随机选择元素 $x \in Z_n^*$ 是阶最大元素的概率,这对于利用 RSA 算法构造加密和签名算法具有非同寻常的意义.

参考文献:

[1] W Diffie, M E Hellman. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 – 654.

[2] R L Rivest, A Shamir, L Adleman. A method for obtaining digital signatures and public key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[3] M Bellare, G Neven. Identity-Based Multi-signatures from RSA [A]//M. Abe (Ed.). CT-RSA 2007: LNCS 4377[C]. San Francisco, CA, USA, 2007. 145 – 162.

[4] 袁晓宇,张其善.基于智能卡的 RSA 数字签名实现关键问题解析[J].电子学报,2004,32(11):1897 – 1900.
Yuan Xiao-yu, Zhang Qi-shan. The key question analysis of RSA digital signature algorithm based on smart card[J]. Acta Electronica Sinica, 2004, 32(11): 1897 – 1900. (in Chinese)

[5] D Boneh, G Durfee. Cryptanalysis of RSA with private key d less than N0. 292[A]. Proceedings of the 17th International Couference on Theory and Application of Cryptographic Techniques[C]. 2000. 1339 – 1349.

[6] D Boneh. Twenty years of attacks on the RSA cryptosystem [J]. Notices of the AMS, 1999, 46(2): 203 – 213.

[7] 柯召,孙琦.数论讲义[M].第二版上.北京:高等教育出版社,1999.128.
Ke Zhao, Song Qi. Lectures on Number Theory[M]. Second Edition. Beijing: Higher Education Press, 1999. 128. (in Chinese)

[8] V Shoup. A Computational Introduction to Number Theory and Algebra[M]. Version 1. Cambridge: Cambridge University Press, 2005.

[9] G Ateniese, J Camenisch, M Joye, G Tsudik. A practical and provably secure coalition-resistant group signature scheme[A]. Advances in Cryptology-Crypto 2000[C]. Santa Barbara, California, USA, 2000. 255 – 270.

[10] 闵嗣鹤,严士健.初等数论[M].第三版.北京:高等教育出版社,2003.80.
Min Si-he, Yan Shi-jian. Elementary Number Theory[M]. Third Edition. Beijing: Higher Education Press, 2003. 80. (in Chinese)

作者简介:

司光东 男,1975 年 9 月出生于陕西省榆林市,2005 年 9 月至今在西安电子科技大学通信工程学院攻读密码学博士学位,研究方向为:信息安全与网络安全.
E-mail: siguangdong@126.com

杨加喜 男,1981 年 9 月出生于福建省莆田市,2005 年 9 月至今在西安电子科技大学通信工程学院攻读密码学博士学位,研究方向为:电子商务安全.
E-mail: jiaxiyang@126.com

谭示崇 男,1979 年 10 月出生于广西贵港市,2003 年 9 月至今在西安电子科技大学通信工程学院攻读密码学博士学位,研究方向为:信息安全与密码学.
E-mail: sctan@mail.xidian.edu.cn

肖国镇 男,1934 年 9 月生,吉林四平人,西安电子科技大学教授、博士生导师,西安电子科技大学信息安全与保密研究所所长.