Open Access Library Journal
2025, Volume 12, e13181
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Semi-Primitive Roots and Information Security

Zhongqi Zhou

Hubei Coal Geology Bureau, Wuhan, China
Email: zhouzongqi1058@163.com

How to cite this paper: Zhou, Z.Q. (2025) Semi-Primitive Roots and Information Security. *Open Access Library Journal*, **12**: e13181.
https://doi.org/10.4236/oalib.1113181

Received: February 28, 2025
Accepted: April 21, 2025
Published: April 24, 2025

Abstract

In this paper, a new concept is proposed: semi-primitive root. The basic theory system of semi-primal roots is established, and the congruence equations and propositions of indefinite equations are solved by the theory of semi-primal roots. The security problem of using the same value to digitally sign multiple different information in discrete logarithm encryption is solved.

Subject Areas

Integral Equation, Mathematics, Number Theory

Keywords

Semi-Primitive Roots, Solving Congruence Equations, Proving Propositions of Indeterminate Equations, Encryption and Digital Signatures, Information Security

1. 引言

文中提出了一个新的概念：半原根。此概念是相对原根提出来的，所以，半原根得出的很多结论与原根的相类似。文章前半部分，建立了半原根的基本理论体系。后半部分给出了半原根的三方面的应用：

1) 用半原根理论解同余方程。

2) 用半原根理论证明不定方程的有关命题。

3) 用半原根加密和解密，解决了离散对数加密时用同一个值对多个不同的信息进行数字签名的安全问题。

2. 半原根的定义

设 $m \geq 3, (g,m)=1$，若 $g^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$ 且 $1 \leq k < \frac{\varphi(m)}{2}, g^k \not\equiv \pm 1 \pmod{m}$ 时称 g 为 m 的半原根。

为区别起见，将 $(a,m)=1$， $a^{\varphi(m)}\equiv 1(\bmod m)$ 且当 $1\le k<\varphi(m)$ 时，$a^k \not\equiv 1(\bmod m)$ 则称 a 为 m 的原根。

3. 半原根存在的必要条件

设 g 是 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ 的半原根， $p_1,p_2,\cdots p_r$ 为不同的素数，因 $(g,m)=1$，所以

$\left(g,p_i^{\alpha_i}\right)=1,1\le i\le r$，则

$$g^{\varphi\left(p_i^{\alpha_i}\right)}\equiv 1\left(\bmod p_i^{\alpha_i}\right)$$

令 $h=\left[\varphi\left(p_1^{\alpha_1}\right),\cdots,\varphi\left(p_r^{\alpha_r}\right)\right]$，则

$$g^h\equiv 1\left(\bmod p_i^{\alpha_i}\right)\text{和}\ g^h\equiv 1(\bmod m)$$

所以 $\dfrac{\varphi(m)}{2}\mid h$，或者

$$\frac{\left(\varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)\cdots\varphi\left(p_r^{\alpha_r}\right)\right)}{2}\mid\left[\varphi\left(p_1^{\alpha_1}\right),\varphi\left(p_2^{\alpha_2}\right),\cdots,\varphi\left(p_r^{\alpha_r}\right)\right]$$

而 $\varphi\left(2^k\right)=2^{k-1},\varphi\left(p_i^{\alpha_i}\right)=p^{\alpha_i-1}\left(p_i-1\right)$，于是， m 的不同奇素因子不能多于 2 个，若偶素因子 2 与两个奇素因子 p,q 同时存在，那么，2 的幂次不能大于 1，且 $(p-1,q-1)=2$；如果偶素因子 2 与一个奇素因子同时存在，且 2 的幂次大于 2，则奇素因子不能为 $4n+1$；若只有两个奇素因子 p,q 同时存在，则 $(p-1,q-1)=2$。

4. 哪些数有半原根

根据以上半原根存在的必要条件，并用证明存在原根的数的充分条件相类似的方法可以证明以下形式的数存在半原根：

2^k $k\ge 2$

$2^k p^\alpha$ p 为素数， $p\equiv -1(\bmod 4),0\le k\le 2$。

$4p^\alpha$ p 为素数， $\alpha\ge 1$。

$p^\alpha q^\beta$ p,q 均为素数， $\alpha\ge 1,\beta\ge 1,(p-1,q-1)=2$。

$2p^\alpha q^\beta$ p,q 均为素数， $\alpha\ge 1,\beta\ge 1,(p-1,q-1)=2$。

下面仅就 $m=p^r$ 和 $m=p^rq^s$ 存在半原根进行证明，其余的证明可参考文献[1]：

1) 设 g 模 p 之阶为 λ，并设 $g^\lambda=1+tp,(g-p)^\lambda=1+\mu p$，则 t 和 μ 这两个数中

至少有一个不是 p 之倍数。

证：若 $p\nmid t$，则结论已明，若 $p\mid t$，则

$$(g-p)^\lambda\equiv g^\lambda-\lambda pg^{\frac{p-3}{2}}\equiv 1-\lambda pg^{\frac{p-3}{2}}\left(\bmod p^2\right)$$

即

$$(g-p)^\lambda=1-\lambda pg^{\frac{p-3}{2}}+p^2x=1+\left(px-\lambda g^{\frac{p-3}{2}}\right)p$$

则 $\mu = px - \lambda g^{\frac{p-3}{2}}$。由于 $(\lambda, p) = (g, p) = \left(g^{\frac{p-3}{2}}, p\right) = 1$，所以 $p \nmid \mu$，得证。

2) $p \equiv -1 \pmod 4$ 为奇素数，$m = p^r$，设 $r > 1$，g 是 p 的半原根，并设 $g^{\frac{p-1}{2}} = 1 + tp$，$(g-p)^{\frac{p-1}{2}} = 1 + \mu p$，则

① 若 $p \nmid t$ 则 g 是 p^r 的半原根。

② 若 $p \mid t$，则 $g - p$ 是 p^r 的半原根。

证：① 设 $p \nmid t$，由 $g^{\frac{p-1}{2}} = 1 + tp$

得 $\left(g^{\frac{p-1}{2}}\right)^p = (1+tp)^p = 1 + tp^2 + \frac{p(p-1)}{2} t^2 p^2 + \cdots$

则 $\left(g^{\frac{p-1}{2}}\right)^p = 1 + tp^2 \pmod{p^3}$

$$\left(g^{\frac{p-1}{2}}\right)^{p^{r-2}} \equiv 1 + tp^{r-1} \pmod{p^r} \tag{1}$$

$$\left(g^{\frac{p-1}{2}}\right)^{p^{r-1}} \equiv 1 \pmod{p^r} \tag{2}$$

设 g 模 p^r 其阶为 n，即 $g^n \equiv 1 \pmod{p^r}$，则 $n \mid p^{r-1}(p-1) = \varphi(p^r)$，因 $g^n \equiv 1 \pmod{p^r}$ 和 $g^n \equiv 1 \pmod{p}$，所以 $\frac{p-1}{2} \mid n$，如果 $n < p^{r-1}\left(\frac{p-1}{2}\right)$，则 n 必须是 $\frac{p^{r-2}(p-1)}{2}$ 的约数，则应有 $g^{p^{r-2}\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p^r}$，但根据(1)和 $p \nmid t$，此不可。如果 $n > \frac{p^{r-1}(p-1)}{2}$，那么必有：$g^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$，但根据(2)此亦不可。只有 $n = \frac{p^{r-1}(p-1)}{2} = \frac{\varphi(p^r)}{2}$。再若 $g^k \equiv -1 \pmod{p^r}$，$0 < k < \frac{\varphi(p^r)}{2}$，则有 $g^{2k} \equiv 1 \pmod{p^r}$，从而 $\frac{p^{r-1}(p-1)}{2} \mid 2k$，因 $2k < \varphi(p^r)$，只有 $k = \frac{\varphi(p^r)}{4}$，因 p 有半原根，$p \equiv -1 \pmod 4$，$k = \frac{\varphi(p^r)}{4} = \frac{p^r(p-1)}{4}$ 不为整数，故 g 是 p^r 的半原根。

② 若 $p \mid t$，则由 1)得知：$p \nmid \mu$，因 $g - p$ 也是 p 的半原根，同理可证，$g - p$ 是 p^r 的半原根。

3) $m = p^r q^s$，p, q 均为奇质数，r, s 为自然数。若 g 既是 p 的半原根，也是 q 的原根，且 $(\varphi(p), \varphi(q)) = 2$，则 g 是 m 的半原根。

证：因为 g 是 p 的半原根，根据(2)可知 g 或 $g - p$ 为 p^r 的半原根，所以就有 $g^{\frac{p^{r-1}(p-1)}{2}} \equiv 1 \pmod{p^r}$，也有 $g^{\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{2}} \equiv 1 \pmod{p^r}$。又因 g 也是 q

的原根，那么，g 或 $g-q$ 为 g^s 的原根，所以有 $g^{q^{s-1}(q-1)}\equiv 1\left(\mathrm{mod}\, q^s\right)$，也有 $g^{\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{2}}\equiv 1\left(\mathrm{mod}\, q^s\right)$，所以 $g^{\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{2}}\equiv 1\left(\mathrm{mod}\, p^r q^s\right)$。若存在：$n<\frac{\varphi(m)}{2}$ 使得 g 模 m 之阶为 n，即 $g^n\equiv 1(\mathrm{mod}\, m)$，就会有 $g^n\equiv 1\left(\mathrm{mod}\, p^r\right)$ 和 $g^n\equiv 1\left(\mathrm{mod}\, q^s\right)$，所以有 $\frac{p^r(p-1)}{2}\mid n$ 和 $q^{s-1}(q-1)\mid n$。即 $\left[\frac{p^{r-1}(p-1)}{2},\frac{q^{s-1}(q-1)}{2}\right]\le n$ 因 $\left(\varphi(p),\varphi(q)\right)=2$，所以 $n\ge\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{2}$，显然与原设矛盾。故 g 模 m 之阶为 $\frac{\varphi(m)}{2}$。再若存在 $n<\frac{\varphi(m)}{2}$，使得 $g^n\equiv -1(\mathrm{mod}\, m)$，就会有 $g^{2n}\equiv 1(\mathrm{mod}\, m)$。

则 $\frac{\varphi(m)}{2}\mid 2n$，因 $n<\frac{\varphi(m)}{2}$，只有 $n=\frac{\varphi(m)}{4}=\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{4}$ 或 $g^{\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{4}}\equiv -1(\mathrm{mod}\, m)$，并推出：$g^{\frac{p^{r-1}(p-1)q^{s-1}(q-1)}{4}}\equiv -1(\mathrm{mod}\, p)$。但由于 g 是 p 的半原根，所以 $g^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}\, p)$，$g^{\frac{\varphi(m)}{2}}\equiv 1(\mathrm{mod}\, p)$。

当 g 为奇数时：$\left(g^{\frac{\varphi(m)}{4}}+1,g^{\frac{\varphi(m)}{4}}-1\right)=2$

当 g 为偶数时：$\left(g^{\frac{\varphi(m)}{4}}+1,g^{\frac{\varphi(m)}{4}}-1\right)=1$

又因 p 为奇素数，所以 $g^{\frac{\varphi(m)}{4}}\not\equiv -1(\mathrm{mod}\, p)$，故 $g^{\frac{\varphi(m)}{4}}\not\equiv -1(\mathrm{mod}\, m)$。

得证。

5. 半原根的相关定理

定理 1. 若 a 是 m 的半原根，则 $\pm a,\pm a^2,\cdots,\pm a^{\frac{\varphi(m)}{2}}$ 为 m 的简化剩余系。

证：$\pm a,\pm a^2,\cdots\pm a^{\frac{\varphi(m)}{2}}$ 共有 $\varphi(m)$ 个数，如果 $\pm a^i\equiv\pm a^j(\mathrm{mod}\, m),1\le i<j\le\frac{\varphi(m)}{2}$，则会有 $a^{j-i}\equiv 1(\mathrm{mod}\, m)$ 或 $a^{j-i}\equiv -1(\mathrm{mod}\, m)$，由于 $j-i<\frac{\varphi(m)}{2}$，由半原根的定义，因此不可；如果 $a^i\equiv -a^i(\mathrm{mod}\, m)$，因 $(a,m)=1$，则会有 $2\equiv 0(\mathrm{mod}\, m)$，也不可。

定理 2. 设 $m\ge 3$ 为正整数，$\overline{\varphi(m)}$ 为所有小于 m 且与 m 互素的正整数之积，如果 m 存在半原根，则

$$\overline{\varphi(m)}\equiv(-1)^{\frac{\varphi(m)}{2}}(\mathrm{mod}\, m)$$

证：设 a 是 m 的半原根，因 $\pm a,\pm a^2,\cdots,\pm a^{\frac{\varphi(m)}{2}}$ 是 m 的简化剩余系，则有

$$aa^2\cdots a^{\frac{\varphi(m)}{2}}(-a)\left(-a^2\right)\cdots\left(-a^{\frac{\varphi(m)}{2}}\right)\equiv\overline{\varphi(m)}\left(\mathrm{mod}\,m\right)$$

$$(-1)^{\frac{\varphi(m)}{2}}\times a^{\frac{\varphi(m)}{2}\left(\frac{\varphi(m)}{2}+1\right)}\equiv\overline{\varphi(m)}\left(\mathrm{mod}\,m\right)$$

因 $a^{\frac{\varphi(m)}{2}\left(\frac{\varphi(m)}{2}+1\right)}\equiv 1\left(\mathrm{mod}\,m\right)$，所以

$$\overline{\varphi(m)}\equiv(-1)^{\frac{\varphi(m)}{2}}\left(\mathrm{mod}\,m\right)$$

定理 3. 设 $n\geq 0,k\geq 3$，则 $8n+3,8n+5$ 均为 2^k 的半原根。

证：先设 $8n+3<2^k$，$8n+5<2^k$，此时 n 可取 2^{k-3} 个数，n 分别为：$0,1,2,\cdots,2^{k-3}-1$，共 $2\times 2^{k-3}=2^{k-2}$ 个数。而 $(8n+1)^{2^{k-3}}\equiv 1\left(\mathrm{mod}\,2^k\right)$，$(8n+7)^{2^{k-3}}\equiv 1\left(\mathrm{mod}\,2^k\right)$。因 $2^{k-3}<\dfrac{\varphi\left(2^k\right)}{2}$，所以，$8n+1,8n+7$ 均不为 2^k 的半原根。而不大于 2^k 的 $8n+1$ 和 $8n+7$ 的数也有 2^{k-2} 个，根据下面“半原根的个数”知 2^k 的半原根有 $\varphi\left(\varphi\left(2^k\right)\right)=2^{k-2}$ 个，且无偶数，所以 $8n+3,8n+5$ 均为 2^k 的半原根。

又因当 $8m+3,8m+5$ 均大于 2^k 时，总可以找到 i 使得

$$m\equiv i\left(\mathrm{mod}\,2^{k-3}\right),\quad 0\leq i\leq 2^{k-3}-1。$$

即有

$8n+3\equiv 8m+3\left(\mathrm{mod}\,2^k\right),8n+5\equiv 8m+5\left(\mathrm{mod}\,2^k\right)$。所以全体 $8n+3,8n+5$ 均为 2^k 的半原根，得证。

定理 4. 设 g 为 m 的半原根，a,b,c 均为已知整数，$(a,m)=(b,m)=(c,m)=1$，

$1\leq i,j,k\leq\dfrac{\varphi(m)}{2}$，则同余式

$$ac^x\equiv b\left(\mathrm{mod}\,m\right)\tag{5}$$

① 当 $a\equiv\pm g^i,b\equiv\pm g^j,c\equiv g^k\left(\mathrm{mod}\,m\right)$，则(5)式有解的充要条件为 $d=\left(k,\dfrac{\varphi(m)}{2}\right)\mid(j-i)$；

② 当 $a\equiv\pm g^i,b\equiv\pm g^j,c\equiv -g^k\left(\mathrm{mod}\,m\right)$，则同余式有解的充要条件 $x\equiv 0\left(\mathrm{mod}\,2\right)$ 且 $d=\left(k,\dfrac{\varphi(m)}{2}\right)\mid(j-i)$；

③ 当 $a\equiv\pm g^i,b\equiv\mp g^j,c\equiv -g^k\left(\mathrm{mod}\,m\right)$，则同余式有解的充要条件 $x\equiv 1\left(\mathrm{mod}\,2\right)$ 且 $d=\left(k,\dfrac{\varphi(m)}{2}\right)\mid(j-i)$；

④ $a\equiv\pm g^i,b\equiv\mp g^j,c\equiv g^k\left(\mathrm{mod}\,m\right)$，则同余式无解。

证：① (5)式可变形为：

$$kx\equiv j-i\left(\mathrm{mod}\,\frac{\varphi(m)}{2}\right),\tag{6}$$

(6)有解的充要条件为 $d=\left(k,\frac{\varphi(m)}{2}\right)\mid(j-i)$，且若有解，恰有 d 个不同余的解，

(5)式也有 d 个不同余的解。

② (5)式可变为：

$$x\left(ind_g(-1)+k\right)\equiv j-i\left(\mathrm{mod}\frac{\varphi(m)}{2}\right)$$

或

$$ind_g(-1)^x+xk\equiv j-i\left(\mathrm{mod}\frac{\varphi(m)}{2}\right),\tag{7}$$

当 $x\equiv 0(\mathrm{mod}\,2)$ 且 $d=\left(k,\frac{\varphi(m)}{2}\right)\mid(j-i)$，则(7)有 d 个不同余的解，(5)也有 d 个不同余的解。当 $x\equiv 1(\mathrm{mod}\,2)$ 或 $d=\left(k,\frac{\varphi(m)}{2}\right)\nmid(j-i)$，则(7)无解，(5)也无解。

③ (5)可变为：

$$x\left(ind_g(-1)+k\right)\equiv ind_g(-1)+j-i\left(\mathrm{mod}\frac{\varphi(m)}{2}\right)$$

或

$$(x-1)\left(ind_g(-1)\right)+xk\equiv j-i\left(\mathrm{mod}\frac{\varphi(m)}{2}\right),\tag{8}$$

当 $(x-1)\equiv 0(\mathrm{mod}\,2)$ 且有 $d=\left(k,\frac{\varphi(m)}{2}\right)\mid(j-i)$，则(8)有解且有 d 个不同余的解，(5)也有个不同余的解；当 $(x-1)\not\equiv 0(\mathrm{mod}\,2)$ 或 $d=\left(k,\frac{\varphi(m)}{2}\right)\nmid(j-i)$，则(8)无解，(5)也无解。

④ (5)可变为：

$$xk\equiv ind_g(-1)+j-i\left(\mathrm{mod}\frac{\varphi(m)}{2}\right)\text{或}$$

$$ind_g(-1)\equiv j-i-xk\left(\mathrm{mod}\frac{\varphi(m)}{2}\right),\tag{9}$$

因 j,i,x,f 均为整数，所以(9)无解，(5)也无解。得证。

6. 半原根的个数

若 m 存在半原根，其个数必为 $\varphi(\varphi(m))$ 个。

我们知道：存在半原根的 m 必为以下形式的数：

$2^k\quad(k\geq 2)$

$p^\alpha,2p^\alpha\quad p$ 为奇素数，$p\equiv -1(\mathrm{mod}\,4)$，$\alpha$ 自然数。

$4p^{\alpha}$ p为奇素数，α自然数。

$p^{\alpha}q^{\beta},2p^{\alpha}q^{\beta}$ p,q为奇素数，$(p-1,q-1)=2$，α,β为自然数。

现分别加以证明：

① 设$m=2^{k}$（$k\geq 2$）

当$k=2$时，$m=4$，其半原根仅有一个1，而$\varphi(\varphi(4))=1$。

当$k=3$时，$m=8$，其半原根为3和5，而$\varphi(\varphi(8))=2$。

当$k>3$时，设g为m的半原根，则$g,g^{2},\cdots,g^{\frac{\varphi(m)}{2}}$模$m$两两互不同余，若$\left(i,\frac{\varphi(m)}{2}\right)=1,i=1,2,\cdots,\frac{\varphi(m)}{2}-1$，则$g^{i}$模$m$之阶也为$\frac{\varphi(m)}{2}$，而不大于$\frac{\varphi(m)}{2}$且与$\frac{\varphi(m)}{2}$互质的数有$\varphi\left(\frac{\varphi(m)}{2}\right)$个，即在$g,g^{2},\cdots,g^{\frac{\varphi(m)}{2}}$中共有$\varphi\left(\frac{\varphi(m)}{2}\right)$个$g^{i}$关于$m$之阶为$\frac{\varphi(m)}{2}$。若$\left(g^{i}\right)^{\frac{\varphi(m)}{2}}\equiv 1(\mathrm{mod}\,m)$ $\left(i,\frac{\varphi(m)}{2}\right)=1$，还存在$n<\frac{\varphi(m)}{2}$，使$\left(g^{i}\right)^{n}\equiv -1(\mathrm{mod}\,m)$，则$\left(g^{i}\right)^{2n}\equiv 1(\mathrm{mod}\,m)$，就会有$\frac{\varphi(m)}{2}\mid 2n$，可得$n=\frac{\varphi(m)}{4}=2^{k-3}$，或$\left(g^{i}\right)^{2^{k-3}}\equiv -1\left(\mathrm{mod}\,2^{k}\right)$，由于$g$为奇数，$g^{i}$也为奇数，设$g^{i}=2q+1$，$q$为整数，则

$\left(g^{i}\right)^{2^{k-3}}=(2q+1)^{2^{k-3}}=1+2^{k-2}q+2^{k-2}q^{2}\left(2^{k-3}-1\right)+2^{k}t$，$t$为整数。

若$\left(g^{i}\right)^{2^{k-3}}\equiv -1\left(\mathrm{mod}\,2^{k}\right)$，则有$2\left(1+2^{k-3}\left(q+q^{2}\left(2^{k-3}-1\right)\right)\right)\equiv 0\left(\mathrm{mod}\,2^{k}\right)$，显然不可，即$g^{i}$为$m$的半原根。

又因$\frac{\varphi(m)}{2}$为偶数，显然有：$\left(-g^{i}\right)^{\frac{\varphi(m)}{2}}\equiv 1(\mathrm{mod}\,m)$，

若存在$n<\frac{\varphi(m)}{2}$，使$\left(-g^{i}\right)^{n}\equiv\pm 1(\mathrm{mod}\,m)$，此时若$n$为偶数，则有$\left(g^{i}\right)^{n}\equiv 1(\mathrm{mod}\,m)$此不可；若$n$为奇数，则有$\left(g^{i}\right)^{n}\equiv\mp 1(\mathrm{mod}\,m)$，也不可，所以，$-g^{i}$也为$m$的半原根，显然在$\pm g$，$\pm g^{2}$，$\cdots$，$g^{\frac{\varphi(m)}{2}}$中再无其他半原根，所以$2^{k}$共有$2\varphi\left(\frac{\varphi\left(2^{k}\right)}{2}\right)=\varphi\left(\varphi\left(2^{k}\right)\right)$个半原根。

② 设$m=p^{\alpha}$，p为奇素数，$p\equiv -1(\mathrm{mod}\,4)$，$\alpha$为自然数。并设$g$为$m$的半原根，则

g，g^{2}，$\cdots$，$g^{\frac{\varphi(m)}{2}}$模m两两互不同余，设$i=1,2,\cdots,\frac{\varphi(m)}{2}-1$。若$\left(i,\frac{\varphi(m)}{2}\right)=1$，则$g^{i}$模$m$之阶为$\frac{\varphi(m)}{2}$，且有$\varphi\left(\frac{\varphi(m)}{2}\right)$个，再若存在$n<\frac{\varphi(m)}{2}$，使得$\left(g^{i}\right)^{n}\equiv -1(\mathrm{mod}\,m)$，就有$n=\frac{\varphi(m)}{4}=\frac{p^{\alpha-1}(p-1)}{4}$，因$p\equiv -1(\mathrm{mod}\,4)$，则$n$不为整数，故不可，即$g^{i}$为$m$之半原根，且在$g$，$g^{2}$，

…，$g^{\frac{\varphi(m)}{2}}$ 中共有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个半原根。因 $\frac{\varphi(m)}{2}$ 为奇数，若有 $\left(-g^i\right)^{\frac{\varphi(m)}{2}}\equiv 1\left(\mathrm{mod}\, m\right)$，则 $\left(g^i\right)^{\frac{\varphi(m)}{2}}\equiv -1\left(\mathrm{mod}\, m\right)$，因 g^i 为 m 之半原根，此不可。即 $-g^i$ 不为 m 之半原根，显然，在 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 中，仅有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个为 m 的半原根，又因当 $p\equiv -1\left(\mathrm{mod}\, 4\right)$ 时，有 $\varphi\left(\varphi(m)\right)=\varphi\left(\frac{\varphi(m)}{2}\right)$，故 p^α 有 $\varphi\left(\varphi\left(p^\alpha\right)\right)$ 个 m 的半原根。

$m=2p^r$ 的半原根个数，p 为奇素数，$p\equiv -1\left(\mathrm{mod}\, 4\right)$，可仿②证明之。

③ 设 $m=4p^\alpha$，p 为奇素数，α 为自然数，设 g 为 m 的半原根，同上理，在 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 中有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个数模 m 之阶为 $\frac{\varphi(m)}{2}$，设 $\left(i,\frac{\varphi(m)}{2}\right)=1$，$i=1,2,\cdots,\frac{\varphi(m)}{2}-1$。若存在 $n<\frac{\varphi(m)}{2}$，使得：$\left(g^i\right)^n\equiv -1\left(\mathrm{mod}\, m\right)$，则必有：$\left(g^i\right)^{2n}\equiv 1\left(\mathrm{mod}\, m\right)$，也必有：$n=\frac{\varphi(m)}{4}=\frac{p^{\alpha-1}(p-1)}{2}$，若 $p\equiv 1\left(\mathrm{mod}\, 4\right)$，因 g 为奇数，n 为偶数，则 $\left(g^i\right)^n\not\equiv -1\left(\mathrm{mod}\, 4p^\alpha\right)$；

若 $p\equiv -1\left(\mathrm{mod}\, 4\right)$，$\left(g^i\right)^n\equiv g^{\frac{p^{\alpha-1}(p-1)i}{2}}\equiv 1\left(\mathrm{mod}\, p^r\right)$，从而有 $\left(g^i\right)^n\not\equiv -1\left(\mathrm{mod}\, p^\alpha\right)$，也有 $\left(g^i\right)^{\frac{p^{\alpha-1}(p-1)}{2}}\not\equiv -1\left(\mathrm{mod}\, 4p^\alpha\right)$。若 g 为 p^α 的原根，则 $g\equiv 1\left(\mathrm{mod}\, 4\right)$，所以 $\left(g^i\right)^{\frac{p^{\alpha-1}(p-1)}{2}}\equiv 1\left(\mathrm{mod}\, 4\right)$，$\left(g^i\right)^{\frac{p^{\alpha-1}(p-1)}{2}}\not\equiv -1\left(\mathrm{mod}\, 4p^\alpha\right)$。即 g^i 为 m 的半原根，且在 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 中共有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个。

显然 $\left(-g^i\right)^{\frac{\varphi(m)}{2}}\equiv 1\left(\mathrm{mod}\, m\right)$，若存在 $n<\frac{\varphi(m)}{2}$，使 $(-g)^n\equiv\pm 1\left(\mathrm{mod}\, m\right)$ 则当 n 为偶数时，$\left(g^i\right)^n\equiv\pm 1\left(\mathrm{mod}\, m\right)$，当为奇数时，$\left(g^i\right)^n\equiv\mp 1\left(\mathrm{mod}\, m\right)$，均不可，故在 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 中也有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个 m 的半原根。又因 $\varphi\left(\varphi(m)\right)=2\varphi\left(\frac{\varphi(m)}{2}\right)$，故 $4p^\alpha$ 共有 $\varphi\left(\varphi\left(4p^\alpha\right)\right)$ 个半原根。

④ 设 $m=p^\alpha q^\beta$，$(p-1,q-1)=2$，α,β 为自然数，设 g 是 m 的半原根，则 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 模 m 两两互不同余，若 $\left(i,\frac{\varphi(m)}{2}\right)=1$，$i=1,2,\cdots,\frac{\varphi(m)}{2}-1$。则 g^i 模 m 之阶为 $\frac{\varphi(m)}{2}$，而不大于 $\frac{\varphi(m)}{2}$ 且与 $\frac{\varphi(m)}{2}$ 互

质的数有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个，即在 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 中，共有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个 g^i 关于 m 之阶为 $\frac{\varphi(m)}{2}$。再若 $\left(g^i\right)^{\frac{\varphi(m)}{2}}\equiv 1(\bmod m)$，$\left(i,\frac{\varphi(m)}{2}\right)=1$ 时，还存在 $n<\frac{\varphi(m)}{2}$，使 $\left(g^i\right)^n\equiv -1(\bmod m)$，则应有 $n=\frac{\varphi(m)}{4}=\frac{p^{\alpha-1}(p-1)q^{\beta-1}(q-1)}{4}$，即有 $\left(g^i\right)^{\frac{\varphi(m)}{4}}\equiv -1(\bmod m)$，但因 $\left(\varphi\left(p^\alpha\right),\varphi\left(q^\beta\right)\right)=2$，则必有 $p\equiv -1(\bmod 4),q\equiv -1(\bmod 4)$ 或 $p\equiv -1(\bmod 4),q\equiv 1(\bmod 4)$ 或 $p\equiv 1,q\equiv -1(\bmod 4)$。现设 $p\equiv -1(\bmod 4),q\equiv -1(\bmod 4)$，则 $\left(g^{q^{\beta-1}(q-1)}\right)^{\frac{p^\alpha(p-1)i}{4}}\equiv 1\left(\bmod p^r\right)$，$\left(g^i\right)^{\frac{\varphi(m)}{4}}\equiv 1\left(\bmod p^r\right)$，则有 $\left(g^i\right)^{\frac{\varphi(m)}{4}}\not\equiv -1(\bmod m)$，同理若 $p\equiv -1,q\equiv 1(\bmod 4)$，也有 $\left(g^i\right)^{\frac{\varphi(m)}{4}}\not\equiv -1(\bmod m)$。

再若 $p\equiv -1,q\equiv -1(\bmod 4)$，则 g 为 p^α 的半原根或为 q^β 的半原根，不妨设 g 为 p^α 的半原根，则 $g^{\frac{p^{\alpha-1}(p-1)}{2}}\equiv 1\left(\bmod p^\alpha\right)$，也有 $\left(g^{\frac{p^{\alpha-1}(p-1)}{2}}\right)^{\frac{q^{\beta-1}(q-1)i}{2}}\equiv 1\left(\bmod p^\alpha\right)$，即 $\left(g^i\right)^{\frac{\varphi(m)}{4}}\equiv 1\left(\bmod p^\alpha\right)$，则 $\left(g^i\right)^{\frac{\varphi(m)}{4}}\not\equiv -1(\bmod m)$。

同理若 g 是 q^β 的半原根，也有 $\left(g^i\right)^{\frac{\varphi(m)}{4}}\not\equiv -1(\bmod m)$，也就是说 g^i 为 m 的半原根，且在 g，g^2，…，$g^{\frac{\varphi(m)}{2}}$ 中有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个 m 的半原根。

显然，$\left(-g^i\right)^{\frac{\varphi(m)}{2}}\equiv 1(\bmod m)$，若存在 $n<\frac{\varphi(m)}{2}$，使得 $\left(-g^i\right)^n\equiv \pm 1(\bmod m)$，当 n 为偶数时有 $\left(g^i\right)^n\equiv \pm 1(\bmod m)$；当为奇数时有 $\left(g^i\right)^n\equiv \mp 1(\bmod m)$，均不可，即在 $-g$，$-g^2$，…，$-g^{\frac{\varphi(m)}{2}}$ 中也有 $\varphi\left(\frac{\varphi(m)}{2}\right)$ 个 m 的半原根。又因 $\varphi\left(\varphi\left(p^\alpha q^\beta\right)\right)=2\varphi\left(\frac{\varphi\left(p^\alpha q^\beta\right)}{2}\right)$，故在 $\pm g$，$\pm g^2$，…，$g^{\frac{\varphi(m)}{2}}$ 中有 $\varphi\left(\varphi(m)\right)$ 个半原根。

⑤ 设 $m=2p^\alpha q^\beta$，仿④可证：m 的半原根有 $\varphi\left(\varphi(m)\right)$ 个。

7. 半原根指数的性质

半原根指数和原根一样，也有类似对数的性质[2]，即下面的定理：

设 g 是 m 的半原根，如果 $(a,m)=(b,m)=1$，我们有

① $ind_g(ab)\equiv ind_g a+ind_g b\left(\mathrm{mod}\dfrac{\varphi(m)}{2}\right)$；

② $ind_g a^n\equiv nind_g a\left(\mathrm{mod}\dfrac{\varphi(m)}{2}\right),n\geq 1$；

③ $ind_g 1=0, ind_g g=1$；

④ 若 $n\equiv 0(\mathrm{mod}\,2), nind_g(-1)=0$；

若 $n\equiv 1(\mathrm{mod}\,2), nind_g(-1)=ind_g(-1)$；

⑤ 设 g_1 也是 m 的一个半原根，则

$$ind_g a\equiv(ind_{g_1}a)(ind_g g_1)\left(\mathrm{mod}\frac{\varphi(m)}{2}\right)。$$

证① 设 $ab\equiv g^{ind_g(ab)}(\mathrm{mod}\,m)$， $a\equiv g^{ind_g a}(\mathrm{mod}\,m), b\equiv g^{ind_g b}(\mathrm{mod}\,m)$。则有

$g^{ind_g(ab)}\equiv g^{ind_g a+ind_g b}(\mathrm{mod}\,m)$，故 $ind_g(ab)\equiv ind_g a+ind_g b\left(\mathrm{mod}\dfrac{\varphi(m)}{2}\right)$。

② 设 $a^n\equiv g^{ind_g a^n}(\mathrm{mod}\,m), a\equiv g^{ind_g a}(\mathrm{mod}\,m)$，则有

$g^{ind_g a^n}\equiv a^n\equiv\left(g^{ind_g a}\right)^n=g^{nind_g a}(\mathrm{mod}\,m)$，故 $ind_g a^n\equiv nind_g a\left(\mathrm{mod}\dfrac{\varphi(m)}{2}\right)$。

③、④显然。

⑤ 由于 $g_1\equiv g^k(\mathrm{mod}\,m), 1\leq k\leq\dfrac{\varphi(m)}{2}, \left(k,\dfrac{\varphi(m)}{2}\right)=1$，则

$$g^{ind_g a}\equiv a\equiv g_1^{ind_{g_1}a}\equiv g^{kind_{g_1}a}(\mathrm{mod}\,m)$$

故有

$$ind_g a\equiv kind_{g_1}a=(ind_g g_1)(ind_{g_1}a)\left(\mathrm{mod}\frac{\varphi(m)}{2}\right)。$$

8. 半原根的应用

应用一：解同余方程

根据定理 1 知 m 的简化剩余系可由 m 的半原根的幂表出，那么，同原根一样，可以建立半原

根 g 为底的指数组来解模 m 的同余方程，在全体正整数中，存在半原根的数的数量要比存在原根的数多，所以利用半原根的指数组来解同余方程或利用半原根和原根的指数结合起来解同余方程(在 100 以内有 85 个数存在半原根或存在原根)，其范围比单纯用原根要宽泛得多。

例：解同余方程

$$33x^3\equiv 19(\mathrm{mod}\,35)\tag{1}$$

这个同余式是不能直接用原根指数组的方式来求解的，因为 35 不存在原根，而只能将其化成同余方程组来解。而 $35=5\times 7, (\varphi(5),\varphi(7))=2$，故

35 存在半原根，$\frac{\varphi(35)}{2}=12$，计算可知 2 是 35 的半原根，并且有

$$2^1\equiv 2,2^2\equiv 4,2^3\equiv 8,2^4\equiv 16,2^5\equiv 32,2^6\equiv 29,2^7\equiv 23,2^8\equiv 11,2^9\equiv 22,2^{10}\equiv 9,2^{11}\equiv 18,2^{12}\equiv 1(\mathrm{mod}\,35)$$

$$-2^1\equiv 33,-2^2\equiv 31,-2^3\equiv 27,-2^4\equiv 19,-2^5\equiv 3,-2^6\equiv 6,-2^7\equiv 12,-2^8\equiv 24,-2^9\equiv 13,$$

$$-2^{10}\equiv 26,-2^{11}\equiv 17,-2^{12}\equiv 34(\mathrm{mod}\,35)$$

ind_2n 表

十 \ 个	0	1	2	3	4	5	6	7	8	9
0		12	1	I + 5	2		I + 6		3	10
1		8	I + 7	I + 9			4	I + 11	11	I + 4
2			9	7	I + 8		I + 10	I + 3		6
3		I + 2	5	I + 1	I + 12					

注：表中第一纵行是 n 的十位数字，第一横行是 n 的个位数字，$I=ind_2(-1)$。

由(1)可得：$ind_2 33+3ind_2 x\equiv ind_2 19\left(\mathrm{mod}\frac{\varphi(35)}{2}\right)$

或为 $3ind_2 x\equiv ind_2 19-ind_2 33(\mathrm{mod}12)$，查 ind_2n 表可得：

$ind_2 33=ind_2(-1)+1, ind_2 19=ind_2(-1)+4$，则有

$3ind_2 x\equiv ind_2(-1)+4-(ind_2(-1)+1)(\mathrm{mod}12)$

或 $3ind_2 x\equiv 3(\mathrm{mod}12), ind_2 x\equiv 1(\mathrm{mod}4)$

$ind_2 x\equiv 1,5,9(\mathrm{mod}12).$

再反查表得：$x\equiv 2,22,32(\mathrm{mod}35)$ 即为同余方程(1)的解。

应用二：证明相关不定方程的命题

1842 年卡塔兰 (Catalan, 1814~1894) 提出了一个著名的猜想：$x^m-y^n=1, m>1, n>1$ 的整数解只有 $x=3,m=2,y=2,n=3$。

1962 年，我国著名数学家柯召首先在卡塔兰猜想方面取得了突破，他证明了下述不定方程：$x^2-y^n=1$ 只有一组解：$x=3,y=2,n=3$。而方程 $x^m-y^2=1, m>1$ 没有正整数解。

2002 年 4 月，米哈伊列斯库大幅使用分园域和伽罗华模证明了此猜想。

下面用半原根及其指数理论来证明：

不定方程

$$n^x-2^y=1 \tag{2}$$

$x>1, y>1$ 的整数解只有 $x=2,n=3,y=3$。

证：当 $y\le 3$ 时，可以验证：$x=2,n=3,y=3$ 是(2)的整数解。

当 $y>3$ 时，根据(2)有：

$$n^x\equiv 1(\mathrm{mod}\,2^y) \tag{3}$$

设 $n=8m+3$ 和 $n=8m+5$。根据定理 3 知，n 为 2^y 的半原根。

对(3)两边取以 n 为底的指数得：

$ind_n 1 + x ind_n n \equiv ind_n 1 \left(\mathrm{mod}\, 2^{y-2}\right)$，又根据定理 4 知(3)有唯一解，

$$x \equiv 0 \left(\mathrm{mod}\, 2^{y-2}\right)。$$

得到 $x = 2^{y-2} t$，t 为整数。也就有：

$$n^{2^{y-2}t} = \left(8m+3\right)^{2^{y-2}t} = \left(2^3 m+3\right)^{2^{y-2}t} = 1 + 2^y l$$

$$n^{2^{y-2}t} = \left(8m+5\right)^{2^{y-2}t} = \left(2^3 m+5\right)^{2^{y-2}t} = 1 + 2^y h$$

l, h 均为正整数。

但 $3^{\frac{\varphi\left(2^y\right)}{2}} = \left(3^2\right)^{2^{y-3}} = \left(2^3+1\right)^{2^{y-3}} > 2^y + 1$ 和

$5^{\frac{\varphi\left(2^y\right)}{2}} = \left(5^2\right)^{2^{y-3}} = \left(2^3 \times 3 + 1\right)^{2^{y-3}} > 2^y + 1$，

所以当 $y > 3$ 时，$\left(8m+3\right)^x - 2^y = 1$ 和 $\left(8m+5\right)^x - 2^y = 1$ 不存在整数解。

又因：$\left(8n \pm 1, 2^y\right) = 1$，有 $\left(8n \pm 1\right)^{\varphi\left(2^y\right)} \equiv 1 \left(\mathrm{mod}\, 2^y\right)$，如果还有：

$\left(8m \pm 1\right)^k \equiv 1 \left(\mathrm{mod}\, 2^y\right), k < \varphi\left(2^y\right)$，则必有 $k \mid \varphi\left(2^y\right) = 2^{y-1}$。如果 $k \geq 2^{y-3}$，则 $m \geq 1$ 时 $\left(8m \pm 1\right)^k > 2^y + 1$ 方程(2)无正整数解。那么 k 只能是 2^r，$0 < r < y-3$。而当 $m \geq 1$ 时，设 $m = 2^j q$，$r \geq 0, q$ 为奇数，则

$$\left(8m \pm 1\right)^{2^r} = \left(2^{j+3} q \pm 1\right)^{2^r} \tag{4}$$

由(4)可知：

当 $r \geq y - j - 3$ 时，$\left(8m \pm 1\right)^{2^r} > 2^y + 1$；

当 $r < y - j - 3$ 时，$\left(8m \pm 1\right)^{2^r} \not\equiv 1 \left(\mathrm{mod}\, 2^y\right)$

则 $\left(8m \pm 1\right)^{2^r} \not\equiv 1 \left(\mathrm{mod}\, 2^y\right)$。所以 $\left(8m \pm 1\right)^x - 2^y = 1$ 无整数解。

再因 $\left(8n + 2l\right)^x - 2^y \neq 1$，$l$ 为整数。得证。

应用三：半原根所形成的离散对数公钥方案及数字签名

1) 加密和解密

用户 A 选取 $m = p \times q$，p 和 q 均为大素数，并 $\left(p-1, q-1\right) = 2$，此时 m 存在半原根，并选取 m 的一个半根 g，用户 A 再选取一个整数 $i, 0 \leq i \leq \frac{\varphi\left(m\right)}{2} - 1$，计算 $b \equiv \pm g^i \left(\mathrm{mod}\, m\right)$，把 m, g, b 均公开，而 i 作为用户 A 的私密而保密，b 为用户 A 的公钥。如果用户 B 将信息 x 发用户 A，$\left(1 \leq x \leq m-1\right)$，其加密和解密的方式为：[3]

① 加密：用户 B 随意选取一个整数 $k, 1 \leq k \leq \frac{m}{3} < \frac{\varphi\left(m\right)}{2}$，(当 p, q 均大于 5 时 $\frac{m}{3} < \frac{\varphi\left(m\right)}{2}$)

并计算

$a \equiv \pm g^k \left(\mathrm{mod}\, m\right)$ 和 $c \equiv b^k x \left(\mathrm{mod}\, m\right)$。

如果 k 为奇数

$a \equiv -g^k \left(\mathrm{mod}\, m\right)$，则将密文 $\left(a, c, -1\right)$ 传给 A；

$a \equiv g^k \left(\mathrm{mod}\, m\right)$，则将密文 $\left(a, c, 1\right)$ 传给 A；

如果 k 为偶数

$a \equiv -g^k \pmod{m}$，则将密文 $(a,c,0)$ 传给 A；

$a \equiv g^k \pmod{m}$，则将密文 $(a,c,2)$ 传给 A。

② 解密：用户 A 收到密文后，根据 $b \equiv \pm g^i \pmod{m}$ 的情况(用户 A 自己知道)，用私钥 i 进

行加密：

当用户 A 收到 $(a,c,-1)$ 后，用私钥 i 计算：

如果 $b \equiv g^i \pmod{m}$

$c(-a)^{-i} \equiv b^k x\left(-\left(-g^k\right)\right)^{-i} \equiv \left(g^i\right)^k x\left(g^k\right)^{-i} \equiv x \pmod{m}$

如果 $b \equiv -g^i \pmod{m}$

$(-1)^{1-i} ca^{-i} \equiv (-1)^{1-i}\left(-g^i\right)^k x\left(-g^k\right)^{-i} \equiv (-1)^{2(1-i)} x \equiv x \pmod{m}$

当用户 A 收到 $(a,c,1)$ 后，用私钥 i 计算：

如果 $b \equiv g^i \pmod{m}$

$ca^{-i} \equiv b^k x\left(g^k\right)^{-i} \equiv \left(g^i\right)^k x\left(g^k\right)^{-i} \equiv x \pmod{m}$

如果 $b \equiv -g^i \pmod{m}$

$-ca^{-i} \equiv -b^k x\left(g^k\right)^{-i} \equiv -\left(-g^i\right)^k x\left(g^k\right)^{-i} \equiv x \pmod{m}$

当用户 A 收到 $(a,c,0)$ 后，用私钥 i 计算：

如果 $b \equiv \pm g^i \pmod{m}$

$c(-a)^{-i} \equiv b^k x\left(-\left(-g^k\right)\right)^{-i} \equiv \left(\pm g^i\right)^k x\left(g^k\right)^{-i} \equiv x \pmod{m}$

当用户 A 收到 $(a,c,2)$ 后，用私钥 i 计算：

如果 $b \equiv \pm g^i \pmod{m}$

$c(a)^{-i} \equiv b^k x\left(g^k\right)^{-i} \equiv \left(\pm g^i\right)^k x\left(g^k\right)^{-i} \equiv x \pmod{m}$

以上计算可将用户 B 发来的密文恢复成明文 x，由于用户以外的人不知道 A 的私钥 i，而由

公钥 g,m,b 求 i 是困难的离散对数问题，所以，外人由密文很难算出明文。

2) 数字签名

用户 A 作数字签名和认证的过程为：

① 用户 A 随意取一个与 $\frac{\varphi(m)}{2}$ 互素的整数 r 并计算：

$$c \equiv g^r \pmod{m}, 1 \le r < \frac{\varphi(m)}{2} \tag{5}$$

而由 $b^c c^d \equiv g^x \pmod{m}$ 得

$$\left(g^r\right)^d \equiv c^d \equiv \frac{g^x}{b^c} \equiv \frac{g^x}{\left(g^i\right)^c} \equiv g^{x-ic} \pmod{m} \tag{6}$$

对(6)两边取指数得

$$rd \equiv (x-ic)\left(\bmod \frac{\varphi(m)}{2}\right)$$

或

$$d \equiv (x - ic) r^{-1} \left(\mathrm{mod} \frac{\varphi(m)}{2} \right), 0 \le d < \frac{\varphi(m)}{2}$$

则 (c,d) 就是用户 A 在信息 x 上的签名，用户 A 将信息 x 和签名 (c,d) 同时发给用户 B。

② 任何人都可认证信息 x 来自用户 A，因为由用户 A 的公钥 b 和签名 (c,d) 并根据(5)和(6)可知

$$b^c c^d \equiv g^{ic} g^{x-ic} \equiv g^x \pmod{m}$$

即由公开的 m, g, b 签名 (c,d) 和信息 x 直接验证同余式 $b^c c^d \equiv g^x \pmod{m}$ 成立，就可以认证信息 x 来自用户 A。

我们知道：使用由原根所形成的离散对数同样也可用来作信息加密和数字签名，但此时用户 A 不能用同一个值 r 对两个不同的信息 x_1 和 x_2 $\left(x_1 \not\equiv x_2 \left(\mathrm{mod}(p-1)\right)\right)$ 同时做签名，否则，存在私钥被破译的风险。[4]

而使用由半原根所形成的离散对数来作加密和数字签名时，用户 A 则可用同一个值 r 对多个不同的信息 $x_1, x_2, \cdots, x_n$ 同时做签名而不致于被破译，这是由于：

$$d_1 \equiv (x_1 - ic_1) r^{-1} \left(\mathrm{mod} \frac{\varphi(m)}{2} \right) \tag{7}$$

$$d_2 \equiv (x_2 - ic_2) r^{-1} \left(\mathrm{mod} \frac{\varphi(m)}{2} \right) \tag{8}$$

如果 $c_1 \equiv g^r \equiv c_2 \pmod{m}, (1 \le c_1, c_2 \le m-1)$

则由(7)-(8)可得

$$r(d_1 - d_2) \equiv x_1 - x_2 \left(\mathrm{mod} \frac{\varphi(m)}{2} \right) \tag{9}$$

由于 $\frac{\varphi(m)}{2} = \frac{(p-1)(q-1)}{2}$，当 p 和 q 都非常大时，分解 $m = p \times q$ 是非常困难的[5]，所以求解(9)中的 r 也是极其困难的，因此，用同一个值 r 对多个不同的信息 $x_1, x_2, \cdots, x_n$ 同时做签名也是很安全的，这也是使用由半原根所形成的离散对数来做加密和数字签名最大的优势。

9. 猜想

$Q(m)$ 表示所有小于 m 的半原根之和，$R(m)$ 表示所有小于 m 的原根之和。

下面的 $\mu(n)$ 表示 n 的麦比乌斯函数。$\varphi(m)$ 为关于 m 的欧拉函数。

猜想：

1) 设 $p > 3, p \equiv -1 \pmod{4}$ 为素数，$m = p, 2p$。则

$Q(m) \equiv \mu(\varphi(m)) \times (p-1) \pmod{m}$.

2) 设 $p \ge 3$ 为素数，$p \equiv -1 \pmod{4}, r \ge 2, m = p^r, 2p^r$，则

$$Q(m) \equiv -\mu(p-1) \times \frac{\varphi(m)}{p} \pmod{m}.$$

3) a) 设 p,q 为奇素数， α,β 为自然数， $(p-1,q-1)=2$， $k\geq 2$。
$m=3,6,2^k,p^\alpha\times q^\beta,2p^\alpha\times q^\beta.$
b) 设 p 为奇素数， α 为自然数。
$m=4p^\alpha,$
则

$$Q(m)\equiv -\mu(\varphi(m))(\mathrm{mod}\, m).$$

4) 任何大于 1 的自然数 m 都有下面的同余式：

$$Q(m)+R(m)\equiv 0(\mathrm{mod}\, m).$$

以上诸猜想，均已验证到 $m=5000$。

10. 结束语

从上文中可以看出：存在半原根的数比存在原根的数范围要大，例如 $p^\alpha q^\beta,2p^\alpha q^\beta$ 和 $2^k\ (k\geq 2)$ 都存在半原根，而它们是不存在原根的，所以可以充分利用它们的半原根性质来解决原根不能解决的问题。作者相信，一定还能找到半原根在其他方面的应用，这将是提出半原根的最好结果。

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Kenneth H. Rosen. 初等数论及其应用[M]. 夏鸿刚, 译. 北京: 机械工业部出版社, 2009: 255-258.

[2] 柯召, 孙琦. 数论讲义, 上册[M]. 北京: 高等教育出版社, 1986: 138-139.

[3] 游林. 初等数论及其在密码学中的应用与 Maple 实现[M]. 北京: 科学出版社, 2009: 189.

[4] 冯克勤. 数论与密码[M]. 北京: 科学出版社, 2007: 88-97.

[5] 纪建. 数论与应用[M]. 北京: 清华大学出版社, 2013: 217-225.

Appendix (Abstract and Keywords in Chinese)

半原根与信息安全

摘要：文中提出了一个新的概念：半原根。建立了半原根的基本理论体系,并用半原根理论解同余方程和证明不定方程的命题；解决了离散对数加密时用同一个值对多个不同的信息进行数字签名的安全问题。

关键词：半原根，解同余方程，证明不定方程的命题，加密与数字签名，信息安全