关于不定方程组 $6x^2-4y^2=2$，$20y^2-6z^2=14$

李 杨
（濮阳职业技术学院，数学与信息工程系，河南 濮阳 457000）

摘要：用初等的证明方法，即递归数列的方法，对一个不定方程组 $6x^2-4y^2=2$，$20y^2-6z^2=14$ 进行了较深入的研究。证明了该方程组有且仅有两个正整数解，这两个正整数解分别为 $(x,y,z)=(1,1,1)$ 和 $(x,y,z)=(89,109,199)$。

关键词：不定方程组；正整数解；递归序列；二次互倒律
中图分类号：O156　　**文献标志码**:A

不定方程组

$$\begin{cases} a_2x^2-a_1y^2=a_2-a_1, \\ a_3y^2-a_2z^2=a_3-a_2, \end{cases}$$

（设 a_1,a_2,a_3 为正整数且其中任两数之积与 1 的和均为平方数）的求解是数论中一直研究的一个问题。1969 年 Baker 和 Davenport[1] 证明了：当 $(a_1,a_2,a_3)=(1,3,8)$ 时，不定方程组的正整数解只有 $x=y=z=1$ 和 $x=11,y=19,z=31$，这一结论在 1975 年又被 Kanagasabathy 和 Ponnudurai 用另一种方法加以证明。1980 年 Veluppillai[2] 又证明了：当 $(a_1,a_2,a_3)=(2,4,12)$ 时，不定方程组的正整数解只有 $x=y=z=1$ 和 $x=29,y=41,z=71.$ 1992 年郑德勋[3] 证明了：当 a_1,a_2,a_3 为正整数且其中任两数之积与 1 的和均为平方数时，有异于 $x=y=z=1$ 且满足 $x^2\equiv 1(\mathrm{mod}\,a_1)$ 的正整数解存在，并给出了这种解的表达式，但并没有具体给出全部解。2007 年李杨[4] 给出了此方程组的上界。本文将运用递归数列这一初等方法，证明当 $(a_1,a_2,a_3)=(4,6,20)$ 时，此不定方程组仅有两组正整数解：$(x,y,z)=(1,1,1),(89,109,199)$。

不定方程组

$$\begin{cases} 6x^2-4y^2=2 \\ 20y^2-6z^2=14 \end{cases} \tag{1}$$

将(1)式的第一个式子 $\times 4y^2+1$，整理变形得到如下形式

$$(4y^2+1)^2-24(xy)^2=1 \tag{2}$$

容易知道 Pell 方程[5] $u^2-24v^2=1$ 的全部正整数解是：$u_n+v_n\sqrt{24}=\left(5+\sqrt{24}\right)^n$，$n\in Z$，其中 $5+\sqrt{24}$

---

* 收稿日期：2013-12-20　　修回日期：2015-01-09
作者简介：郭辉，女，讲师，研究方向为数论，E-mail: yuling1981@126.com

是 Pell 方程$u^2-24v^2=1$的基本解。

于是不定方程组(1)的解应满足$\begin{cases}u_n=4y^2+1\\20y^2-6z^2=14\end{cases}$，得到

$$5u_n-19=6z^2 \tag{3}$$

由$u_n+v_n\sqrt{24}=\left(5+\sqrt{24}\right)^n$可以容易地推导出下列关系式：

$$u_{n+1}=10u_n-u_{n-1},\quad u_0=1,\quad u_1=5, \tag{4}$$

$$v_{n+1}=10v_n-v_{n-1},\quad v_0=0,\quad v_1=1, \tag{5}$$

$$u_{2n}=2u_n^2-1=u_n^2+24v_n^2,\quad v_{2n}=2u_nv_n, \tag{6}$$

$$u_{n+2h}\equiv -u_n(\bmod u_h),\quad v_{n+2h}\equiv -v_n(\bmod u_h) \tag{7}$$

1 主要引理

引理 1 设$n\equiv\pm1(\bmod 160)$，且$n\neq\pm1$，则（3）不成立。

证明 $n\neq1$，令$n=1+2\cdot2\cdot2\cdot5\cdot3^t\cdot k$，其中$k\equiv\pm4(\bmod 12)$，$t\geq0$。根据（7）有

$$u_n\equiv u_{1\pm4m}\equiv -u_{1\mp2m}\equiv -(5u_{\mp2m}+24v_{\mp2m})\equiv -5u_{2m}\pm24v_{2m}\left(\bmod u_{3m}\right)$$

注意到$u_{3m}=u_m\left(u_m^2+72v_m^2\right)$，所以$u_n\equiv -5u_{2m}\pm24v_{2m}\left(\bmod u_m^2+72v_m^2\right)$。因为$u_n\equiv1(\bmod d)$，$2\nmid n, v_n\equiv\pm1(\bmod 5)$，$2\mid n, v_n\equiv0(\bmod 5)$，$u_n{}^2+72v_n{}^2\equiv1(\bmod 8)$。于是由（4）～（7）式有

$$\left(\frac{5u_n-19}{u_m^2+72v_m^2}\right)=\left(\frac{-5\cdot5u_{2m}\pm5\cdot24v_{2m}-19}{u_m^2+72v_m^2}\right)=\left(\frac{-25u_{2m}\pm120v_{2m}-19}{u_m^2+72v_m^2}\right)=$$

$$\left(\frac{-25\left(u_m^2+24v_m^2\right)\pm240u_mv_m-19\left(u_m^2-24v_m^2\right)}{u_m^2+72v_m^2}\right)=\left(\frac{-44u_m^2-144v_m^2\pm240u_mv_m}{u_m^2+72v_m^2}\right)=$$

$$\left(\frac{3\ 024v_m{}^2\pm240u_mv_m}{u_m{}^2+72v_m{}^2}\right)=\left(\frac{\pm48v_m}{u_m^2+72v_m^2}\right)\left(\frac{5u_m\pm63v_m}{u_m^2+72v_m^2}\right)=\left(\frac{\pm3v_m}{u_m^2+72v_m^2}\right)\left(\frac{5u_m\pm63v_m}{u_m^2+72v_m^2}\right)=\left(\frac{u_m^2+72v_m^2}{5u_m\pm63v_m}\right)$$

1) 若 $2\nmid m,\ v_m\equiv\pm1\ (\bmod 5)$，则

$$\left(\frac{5u_n-19}{u_m^2+72v_m^2}\right)=\left(\frac{u_m^2+72v_m^2}{5u_m\pm63v_m}\right)=\left(\frac{63^2v_m^2+72\times5^2v_m^2}{5u_m\pm63v_m}\right)=\left(\frac{641}{5u_m\pm63v_m}\right)=\left(\frac{5u_m\pm63v_m}{641}\right)$$

2) 若 $2\mid m$，$v_m\equiv0\ (\bmod 5)$，则

$$\left(\frac{5u_n-19}{u_m^2+72v_m^2}\right)=\left(\frac{u_m^2+72v_m^2}{5u_m\pm63v_m}\right)=\left(\frac{63^2v_m^2+72\times5^2v_m^2}{u_m\pm63\times\frac{v_m}{5}}\right)=\left(\frac{641}{5u_m\pm63\times\frac{v_m}{5}}\right)=\left(\frac{5u_m\pm63\times\frac{v_m}{5}}{641}\right)=$$

$$\left(\frac{5}{641}\right)\left(\frac{5u_m\pm 63v_m}{641}\right)=\left(\frac{5u_m\pm 63v_m}{641}\right)$$

1)，2)两情形结果相同。

因为$\{5u_m\pm 63v_m\}$对 mod 641 的剩余类序列的周期为 642，$\{3^t\}$对 mod 642 的剩余类序列的周期为 53，

选取l,m使　$n=1+l\cdot m=1+2\cdot 2\cdot 2\cdot 5\cdot 3^t\cdot k$，以下分两种情况讨论。

如果$k\equiv 4\pmod{12}$则

$$m=\begin{cases}3^t, & 当t\equiv 3,5,13,14,15,19,20,22,27,28,32,34,39,40,45,46\pmod{53}, & l=40k\\ 2\cdot 3^t, & 当t\equiv 2,4,7,8,9,11,16,21,26,29,30,33,35,36,37,38,44,47,51\pmod{53}, & l=20k\\ 4\cdot 3^t, & 当t\equiv 6,17,18,23,25,31,41,42,43,48,49,52\pmod{53}, & l=10k\\ 5\cdot 3^t, & 当t\equiv 0,1,10,12,24\pmod{53}, & l=8k\\ 8\cdot 3^t, & 当t\equiv 50\pmod{53}, & l=5k\end{cases}$$

如果$k\equiv -4\pmod{12}$则

$$m=\begin{cases}3^t & 当t\equiv 1,2,4,5,7,8,9,10,12,16,19,23,27,29,32,\\ & \quad 33,34,38,41,44,45,46,47,51,52\pmod{53}, & l=40k\\ 2\cdot 3^t & 当t\equiv 3,11,13,14,15,20,21,31,42,43,48\pmod{53}, & l=20k\\ 4\cdot 3^t & 当t\equiv 22,24,26,30,35,36,37,39,49,50\pmod{53}, & l=10k\\ 5\cdot 3^t & 当t\equiv 6,25,40\pmod{53}, & l=8k\\ 8\cdot 3^t & 当t\equiv 0,17,18\pmod{53}, & l=5k\\ 10\cdot 3^t & 当t\equiv 28\pmod{53}, & l=4k\end{cases}$$

容易验证，如此选取l,m满足以下两种情形之一：

1）　$l\equiv 4\pmod{12}$，此时$m \bmod 53$的剩余类的元素在 A 内：

$$A=\{27,243,237,69,207,75,225,99,303,267,441,117,183,549,513,255,348,390,528,546,420,588,\\ 168,504,228,192,576,144,54,552,474,138,414,450,66,294,252,114,96,435,525,177,222\}$$

2）　$l\equiv -4\pmod{12}$，此时$m \bmod 53$的剩余类的元素在 B 内：

$$B=\{18,162,522,282,204,552,600,66,630,318,312,78,60,180,540,336,342,246,24,219,15,567,609,\\ 603,3,9,81,243,261,141,423,627,507,621,75,297,303,159,441,117,489,363,171,513,255,123,333,\\ 357,396,354,618,624,120,360,438,90,576,444,102\}$$

情形 1）时，所有 A 中的数都使得$\left(\frac{5u_m+63v_m}{641}\right)=-1$，而$\left(\frac{6z^2}{u_m^2+72v_m^2}\right)=1$，矛盾！所以（3）式不成立。

情形 2）时，所有 B 中的数都使得$\left(\dfrac{5u_m-63v_m}{641}\right)=-1$，而$\left(\dfrac{6z^2}{u_m^2+72v_m^2}\right)=1$，矛盾！所以（3）式不成立。

当$n\equiv-1\left(\bmod 160\right)$时，由$u_{-n}=u_n$，$v_{-n}=-v_n$，而$-n\equiv1\left(\bmod 160\right)$，与上面的方法类似，可以容易的推出$u_n\equiv-5u_{2m}\mp24v_{2m}\left(\bmod u_m^2+72v_m^2\right)$，$\left(\dfrac{5u_n-19}{u_m^2+72v_m^2}\right)=\left(\dfrac{5u_m\mp63v_m}{641}\right)$，从而归结为上面的情形。　　证毕

引理 2 设$n\equiv\pm5\left(\bmod 132\right)$，且$n\neq\pm5$，则（3）式不成立。

证明 令$n=\pm5+2\cdot3\cdot11\cdot k\cdot2^t$，$t\geq1$，$2\nmid k$，取$m=2^t,3\cdot2^t,11\cdot2^t$，则$m\equiv0\left(\bmod 2\right)$，有$u_n\equiv1\left(\bmod 3\right)$，则由（7）式得

$$6z^2\equiv5u_n-19\equiv5u_{\pm5+2km}-19\equiv-5u_{\pm5}-19=-5u_5-19=-237\ 644\left(\bmod u_m\right)$$

即 $3z^2\equiv-118\ \ 822\left(\bmod u_m\right)$。有$\left(\dfrac{3z^2}{u_m}\right)=\left(\dfrac{-118\ \ 822}{u_m}\right)=\left(\dfrac{-1}{u_m}\right)\left(\dfrac{2}{u_m}\right)\left(\dfrac{11^2}{u_m}\right)\left(\dfrac{491}{u_m}\right)=\left(\dfrac{u_m}{491}\right)$，$\{u_m\}\bmod 491$的周期是 246，而$\{2^t\}$对 mod246 的剩余类序列的周期为 20，选取m如下

$$m=\begin{cases}2^t & 当\ t\equiv0,3,4,5,6,7,9,11,14,15,16,17\left(\bmod 20\right)\\ 3\cdot2^t & 当\ t\equiv2,19\left(\bmod 20\right)\\ 11\cdot2^t & 当\ t\equiv1,8,10,12,13,18\left(\bmod 20\right)\end{cases}$$

则有表 1，其中第一行表示$t(>1)\left(\bmod 20\right)$，第二行表示$m\left(\bmod 246\right)$，第三行表示$u_m\left(\bmod 491\right)$。

表 1　$k\equiv1\left(\bmod 4\right)$情况下的数据

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
124	22	12	8	16	32	64	128	110	20	194	80	38	76	148	50	100	200	218	186
486	285	261	193	356	115	426	102	86	200	76	347	66	364	216	21	390	270	343	439

若$t=1$，则$m=22,u_m\equiv285\left(\bmod 491\right)$。对此$m$及表中所有$m$均有$\left(\dfrac{u_m}{491}\right)=-1$。而当$m\equiv0\left(\bmod 2\right)$时，

$\left(\dfrac{3z^2}{u_m}\right)=\left(\dfrac{3}{u_m}\right)=\left(\dfrac{u_m}{3}\right)=\left(\dfrac{1}{3}\right)=1$,即：$1=\left(\dfrac{3z^2}{u_m}\right)=\left(\dfrac{u_m}{491}\right)=-1$，矛盾！（3）式不成立。

所以$n\equiv\pm5\left(\bmod 132\right)$，且$n\neq\pm5$时，（3）式不成立。　　证毕

推论 设$n\equiv\pm1，\pm5\left(\bmod 5\ 280\right)$，且$n\neq\pm1，\pm5$，则（3）式不成立。

引理 3 若（3）式成立，则必须$n\equiv\pm1，\pm5\left(\bmod 5\ 280\right)$。

证明 首先，对（4）式两边取模 3，则当$n\equiv0\left(\bmod 2\right)$时，$u_n\equiv1\left(\bmod 3\right)$，此时

$6z^2 \equiv 5u_n - 19 \equiv 1 \pmod 3$。不可能成立。排除了所有偶数。

下面采取对序列 $\{5u_n - 19\}$ 取模的方法来证明。

1）先证明 $n \equiv \pm 1$，$\pm 5 \pmod{66}$。

$\bmod 131$，$T = 22$，排除 $n \equiv 3, 7, 9, 11, 13, 15, (19\ \bmod)$，此时 $5u_n - 19 \equiv 117, 48, 13, 121, 80, 45, 129, 107 \pmod{131}$，剩 $n \equiv 1, 5, 17, 21 \pmod{22}$。等价于：剩 $n \equiv 1,5,17,21,23,27,39,43,45,49,61,65 \pmod{66}$。这里的 $\bmod 131$ 是对 $\{5u_n - 19\}$ 取的，$T = 22$ 指出所得剩余序列周期为 22。第三、四句话是“排除”的理由：$\left(\frac{117}{131}\right) = \left(\frac{48}{131}\right) = \left(\frac{13}{131}\right) = \left(\frac{121}{131}\right) = \left(\frac{80}{131}\right) = \left(\frac{45}{131}\right) = \left(\frac{129}{131}\right) = \left(\frac{107}{131}\right) = 1$，而 $\left(\frac{6z^2}{131}\right) = -1$，从而矛盾。

$\bmod 67$，$T = 66$，排除 $n \equiv 21, 45 \pmod{66}$，此时 $5u_n - 19 \equiv 34 \pmod{67}$，剩 $n \equiv 1,5,17,23,27,39,43,49,61,65 \pmod{66}$；$\bmod 859$，$T = 66$，排除 $n \equiv 17, 27, 39, 49 \pmod{66}$，此时 $5u_n - 19 \equiv 602\ 537 \pmod{859}$，剩 $n \equiv 1,5,23,43,61,65 \pmod{66}$；$\bmod 172\ 657$，$T = 66$，排除 $n \equiv 23, 43 \pmod{66}$，此时 $5u_n - 19 \equiv 41\ 848 \pmod{172\ 657}$，剩 $n \equiv 1, 5, 61, 65 \pmod{66}$，即 $n \equiv \pm 1, \pm 5 \pmod{66}$。

2）再证明 $n \equiv \pm 1, \pm 5 \pmod{60}$。

$\bmod 59$，$T = 30$，排除 $n \equiv 3,9,11,15,19,21,27 \pmod{30}$，此时 $5u_n - 19 \equiv 46, 7, 48, 35 \pmod{59}$ 剩 $n \equiv 1, 5, 7, 13, 17, 23, 25, 29 \pmod{30}$，即剩 $n \equiv 1, 5, 7, 13, 17, 23, 25, 29, 31, 35, 37, 43, 47, 53, 55, 59 \pmod{60}$。

$\bmod 1\ 901$，$T = 20$，排除 $n \equiv 3, 17 \pmod{20}$，此时 $5u_n - 19 \equiv 505 \pmod{1\ 901}$，剩 $n \equiv$ [illegible] $\pmod{20}$，即剩 $n \equiv 1,5,7,9,11,13,15,19,21,25,27,29,31,33,35,39,41,45,47,49,51,53,55, 59 \pmod{60}$。

至此，还剩 $n \equiv 1, 5, 7, 13, 25, 29, 31, 35, 47, 53, 55, 59 \pmod{60}$。

$\bmod 93\ 139\ 201$，$T = 60$，排除 $n \equiv 7, 53 \pmod{60}$，此时 $5u_n - 19 \equiv 23\ 284\ 806 \pmod{93\ 139\ 201}$。$\bmod 241$，$T = 120$，排除 $n \equiv 25, 35, 59, 61, 85, (95\ \bmod)$，此时 $35, 168, 197 \pmod{241}$，因此排除 $5u_n - 19 \equiv$ $n \equiv 25, 35 (\bmod 60)$；$\bmod 3\ 361$，$T = 120$，排除 $n \equiv 13, 47, 73, (107\ \mathrm{m})$，此时 $5u_n - 19 \equiv 3\ 013, 310 (\bmod 3\ 361)$，因此排除 $n \equiv 13, 47 \pmod{60}$。

综上所述，还剩 $n \equiv 1, 5, 29, 31, 55, 59 \pmod{60}$。

$\bmod 79,\ T=80$，排除 $n\equiv 9,15,27,53,65,71 \pmod{80}$，此时 $5u_n-19\equiv\ 50,4,9 \pmod{79}$。$\bmod 107\ 601\ 838\ 470\ 319$，$T=80$，排除 $n\equiv 11,13,25,29,31,49,51,55,67,69 \pmod{80}$，此时 $5u_n-19\equiv 223\ 580\ 887\ 206, 21\ 908\ 645\ 272\ 806, 5\ 213\ 113\ 556\ 736, 107\ 378\ 257\ 583\ 075, 107\ 599\ 556\ 795\ 075 \pmod{107\ 601\ 838\ 470\ 319}$。由 $\bmod 79$, $\bmod 107\ 601\ 838\ 470\ 319$ 可知：排除了 $n\equiv 9,11,13,15,25,27,29,31,49,51,53,55,65,67,69,71 \pmod{80}$。因此排除了 $n\equiv 29,31 \pmod{60}$。

综上：还剩 $n\equiv 1,5,55,59 \pmod{60}$，即 $n\equiv \pm 1,\pm 5 \pmod{60}$。

3）最后证明 $n\equiv \pm 1,\pm 5 \pmod{40}$。

$\bmod 92\ 188\ 801,\ T=40$,排除 $n\equiv 7,33 \pmod{40}$.此时 $5u_n-19\equiv\ 23\ 284\ 806 \pmod{92\ 188\ 801}$。由前面知：$\bmod 1\ 901, T=20$,排除 $n\equiv 3,17,23,37 \pmod{40}$; $\bmod 107\ 601\ 838\ 470\ 319$，$T=80$，排除 $n\equiv 11,13,25,29,31,49,51,55,67,69 \pmod{80}$; $\bmod 79,\ T=80$，排除 $n\equiv 9,15,27,53,65,71 \pmod{80}$。

综上：排除了 $n\equiv 3,7,9,11,13,15,17,23,25,27,29,31,33,37 \pmod{40}$，还剩 $n\equiv 1,5,19,21,35,39$ (m o 。

再由前面知：$\bmod 59$，$T=30$，可排除 $n\equiv 19,21,99,101 \pmod{120}$; $\bmod 241$, $T=120$, 排除 $n\equiv 59,61 \pmod{12}$，所以又排除了 $n\equiv 19,21 \pmod{40}$。

综合以上，可得：仅剩 $n\equiv 1,5,35,39 \pmod{40}$.即 $n\equiv \pm 1,\pm 5 \pmod{40}$。

由 1)可知，$n\equiv \pm 1$，$\pm 5 \pmod{66}$,2) $n\equiv \pm 1,\pm 5 \pmod{60}$ 和 3) $n\equiv \pm 1,\pm 5 \pmod{40}$，便可立得 $n\equiv \pm 1$，$\pm 5 \pmod{5\ 280}$。 证毕

根据前面的讨论，现在给出本文的主要结果。

2 定理及证明

定理 不定方程组(1)式仅有正整数解 $(x,y,z)=(1,1,1)$ 和 $(x,y,z)=(89,109,199)$。

证明 由推论和引理 3 可知，若（3）式成立，则 $n=\pm 1$，± 5。当 $n=\pm 1$ 时，$u_{-n}=u_n$，则 $6z^2=5u_1-19=5\times 5-19=6$，$4y^2+1=5$，计算得正整数 $z=1$，$y=1$，从而得出正整数 $x=1$；当 $n=\pm 5$ 时，$u_{-n}=u_n$，则 $6z^2=237\ 606$，$4y^2+1=47\ 525$，计算得正整数 $z=199$，$y=109$，从而得出正整

数 $x=89$。即得到不定方程组(1)式的正整数解是 $(x,y,z)=(1,1,1)$ 和 $(x,y,z)=(89,109,199)$。　　证毕

参考文献:

[1] Baker A. Davenport H. The equations $3x^2-2=y^2$ and $8x^2-7=z^2$ [J].Quart J Math Oxford,1969,20(2):129-137

[2] Veluppilai M . The equations $z^2-3y^2=-2$ and $z^2-6x^2=-5$ [M].A Collection of Manuscrips Related to the Fibonacci Sequence.Fibonacci Assoc.Santa Clara.Calif,1980:71-75.

[3] 郑德勋.关于不定方程组 $a_2x^2-a_1y^2=a_2-a_1,a_3y^2-a_2z^2=a_3-a_2$ [J].四川大学学报:自然科学版,1992,29(3):348-351.

Zheng D X.On the simultaneous Diophantine equations $a_2x^2-a_1y^2=a_2-a_1,a_3y^2-a_2z^2=a_3-a_2$ [J]. Si Chuan University:Natual Science:Natural Science,1992,29(3):348-351.

[4] 李杨.关于不定方程组 $6x^2-4y^2=2,20y^2-6z^2=14$ 正整数解的上界[J].重庆师范大学学报:自然科学版,2007(1):19-21.

Li Y.On the simultaneous Diophantine equations $6x^2-4y^2=2,20y^2-6z^2=14$ [J].Journal of Chongqing Normal University:Natual Science,2007(1):19-21.

[5] 罗明.关于不定方程组 $z=x^2+(x+1)^2,z^2=y^2+(y+1)^2$ [J].重庆师范学院学报:自然科学版,1994 (3):

Luo M.On the simultaneous Diophantine equations $z=x^2+(x+1)^2,z^2=y^2+(y+1)^2$ [J].Journal of Chongqing Normal University: Natual Science,1994(3):

[6] 柯召,孙琦.谈谈不定方程[M].上海:上海教育出版社,1980:28-65.

Ke Z,Sun Q.About indeterminate equation[M].Shanghai: Shanghai Education Press,1980:28-65.

On the Simultaneous Diophantine Equations

$$6x^2-4y^2=2,\quad 20y^2-6z^2=14$$

LI Yang

(Department of Mathematics and Information Engineering , Puyang vocational and technical college, Puyang Henan 457000, China)

Abstract：In this paper, with the method of recurrence sequences, we have shown that the only two solutions in positive integers of the simultaneous Diophantine equations $6x^2-4y^2=2$, $20y^2-6z^2=14$ are $(x,y,z)=(1,1,1)$ and $(x,y,z)=(89,109,199)$.

Key Words: Diophantine equation;　positive integer solution;　recurrence sequence; quadratic residue