丢番图方程 $x^2=4.3^n+13$ 的正解

The Solution of Diophantine Equation $x^2=4.3^n+13$

黎进香

Li Jinxiang

(广西民族学院数学系,广西南宁 530006)

(Dept. of Math., Guangxi Univ. for Nationalities, Nanning, Guangxi, 530006, China)

摘要:用完全初等的方法证明丢番图方程 $x^2=4.3^n+13$ 仅有 3 组正解.

关键词:丢番图方程 Pell 方程 最小非负剩余 正解

中图法分类号:O156.7

Abstract: An elementary solution of the Diophantine equation in the title is given.

Key words: diophantine equation, Pell'equation, mininal non-negative residue, solution

A. Bremner 等[1]在研究编码理论时得到 1 个丢番图方程

$$x^2=4.3^n+13. \tag{1}$$

A. Bremner 等[2]将方程(1)变成 3 个椭圆曲线

$$\begin{cases} y^2=4x^3+13, \\ y^2=12x^3+13, \\ y^2=36x^3+13. \end{cases} \tag{2}$$

从而给出 1 个用到较高深的代数数论和 P-adic 方法的解法. 本文给出 1 个仅仅用到 Pell 方程和同余性质的初等解法.

定理 方程(1)仅有正整数解 $(n,x)=(1,5),(2,7),(3,11)$.

证明

首先,若 n 为偶数,设 $n=2k$,则(1)式给出

$$x+2.3^k=13, x-2.3^k=1,$$

两式相减得 $4.3^k=12, k=1, n=2, x=7$.

再设 n 为奇数,设 $n=2k+1$,以下只需证明 $k>1$ 时方程无解即可. 本文考虑二次丢番图方程

$$x^2-3.(2.3^k)^2=13, \tag{3}$$

熟知文献[3],(3)式的解由下列式子给出

$$x+2.3^k\sqrt{3}=(4\pm\sqrt{3})(2+\sqrt{3})^m$$
$$=(4\pm\sqrt{3})(x_m+y_m\sqrt{3})(\text{对某些整数}m), \tag{4}$$

(4)式给出

$$2.3^k=x_m+4y_m=u_m, u_0=1, u_1=6 \tag{5}$$

或

$$2.3^k=4y_m-x_m=v_m, v_0=-1, v_1=2. \tag{6}$$

容易验证下列关系式:

$$x_{m+n}=x_mx_n+3y_my_n, y_{m+n}=x_my_n+x_ny_m(m,n\text{是任意整数}), \tag{7}$$

$$x_{-n}=x_n, y_{-n}=-y_n, \tag{8}$$

$$x_{2n}=x_n^2+3y_n^2=2x_n^2-1=6y_n^2+1, y_{2n}=2x_ny_n, \tag{9}$$

$$x_{n+2kr}\equiv(-1)^kx_n(\mathrm{mod}\ x_r), y_{n+2kr}\equiv(-1)^ky_n(\mathrm{mod}\ x_r), \tag{10}$$

$$x_{n+2kr}\equiv x_n(\mathrm{mod}\ y_r), y_{n+2kr}\equiv y_n(\mathrm{mod}\ y_r), \tag{11}$$

$$x_{n+2}=4x_{n+1}-x_n, x_0=1, x_1=2, \tag{12}$$

$$y_{n+2}=4y_{n+1}-y_n, y_0=0, y_1=1, \tag{13}$$

$$x_9=70226=2\cdot13\cdot37\cdot73.$$

在(5)式和(6)式中分别设 $x_m+4y_m=u_m, 4y_m-x_m=v_m$,有

$$u_{m+2}=4u_{m+1}-u_m, u_0=1, u_1=6, \tag{14}$$

$$v_{m+2}=4v_{m+1}-v_m, v_0=-1, v_1=2, \tag{15}$$

若 $k>1$,对(14)式和(15)式分别取(mod 9)得周期序列(对 $m=0,1,2,\cdots$,周期为 18)如下:

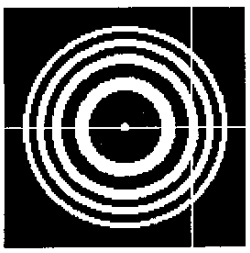
$(m,u_m,v_m)=(0,1,-1),(1,6,2),(2,5,0),(3,5,7),(4,6,1),(5,1,6),(6,7,5),(7,0,5),(8,2,6),(9,8,1),(10,3,7),(11,4,0),(12,4,2),(13,3,8),(14,8,3),(15,2,4),(16,0,4),(17,7,3);(18,1,-1),(19,6,2),\cdots(\mathrm{mod}(18,9,9))$.

由此可知仅当 $m=7+18t$ 或 $m=16+18t$ 时有 $9|u_m$, $m=2+18t$ 或 $m=11+18t$ 时有 $9|v_m$.

(下转第 54 页)

2003-08-01 收稿,2003-09-24 修回。

(d)



(e)

图 3 M_1 与 M_2 垂直的干涉图样

(a)～(e)为 d 由大变小至零，然后又反向变大的干涉图样

4.3 条纹移动及测量

通过对象（M_1）的 KeyDown 事件[5]上下移动 M_1，其象 M_1' 也关联水平移动，实现 d 的改变。每发生 1 个 KeyDown 事件，d 将改变 1 个数值。由式(2)知，对于同 1 个 r_k，Q 随 d 而变，因此用 Circle 方法所画的圆其亮度将改变，实现亮度的移动，其结果是明暗条纹的移动。当 d 增大时，可看到从干涉条纹中心，条纹不断涌出。当 d 变小时，最靠近中心的条纹将不断的陷入中心。记录 d 变化 Δd 后干涉条纹移过十字叉丝的个数，由 $\Delta d = N\lambda/2$，可以测量波长。

5 结束语

利用计算机模拟仿真物理实验，可以使学生对实验原理、实验过程、实验步骤有更好的理解。由于交互性强，能更好地培养学生的动手能力，从而极大地丰富了物理实验的教学方法和手段，起到物理实验辅助教学的作用。

参考文献：

1 母国光，战元龄. 光学. 北京：人民教育出版社，1978. 237～243.

2 Microsoft 公司. Visual Basic 6.0 中文版程序员指南. 希望图书创作室译. 北京：希望电子出版社，1998. 367～433.

3 王 宏，李 冬，付新苗. Windows API 常用技巧汇编. 北京：清华大学出版社，2000.

4 王克己. Visual Basic 4.0 参考手册. 北京：人民邮电出版社，1997. 51～52.

5 Microsoft 公司. Visual Basic 6.0 中文版语言参考手册. 希望图书创作室译. 北京：北京希望电子出版社，1998. 569～571.

（责任编辑：黎贞崇）

（上接第 51 页）

由(10)式有

$2.3^k = x_{18t+s} + 4y_{18t+s} \equiv \pm (x_s + 4y_s) \pmod{x_9}$，其中 $s = 7$ 或 -2， (16)

$2.3^k = 4y_{18t+s} - x_{18t+s} \equiv \pm (x_s - 4y_s) \pmod{x_9}$，其中 $s = -7$ 或 2. (17)

结合(8)式、(14)式和(15)式有

$$2.3^k \equiv \pm (x_7 \pm 4y_7) \pmod{x_9}$$

及 $2.3^k \equiv \pm (x_2 \pm 4y_2) \pmod{x_9}$

或 $2.3^k \equiv \pm u_2, \pm u_7, \pm v_2, \pm v_7 \pmod{x_9}$. (18)

注意到 $73 | x_9$，由(19)式和(18)式给出 $2.3^k \equiv \pm 23, \pm 42, \pm 9, \pm 32 \pmod{73}$.

$(n, u_n, v_n) \equiv (0,1,-1),(1,6,2),(2,23,9),(3,13,34),(4,29,54),(5,30,36),(6,18,17),(7,42,32),(8,4,38),(9,47,47),(10,38,4),(11,32,42),(12,17,18),(13,36,30),(14,54,29),(15,34,13),(16,9,23),(17,2,6),(18,72,1),(19,67,71),(20,50,64),(21,60,39),(22,44,19),(23,43,37),(24,55,56),(25,31,41),(26,69,35),(27,26,26),(28,35,69),(29,41,31),(30,56,55),(31,37,43),(32,19,44),(33,39,60),(34,64,50),(35,71,67);(36,1,-1),(37,6,2),(\mathrm{mod}(36,73,73))$. (19)

当 $k = 1,2,3,\cdots$，时，$2.3^k \pmod{73}$ 的最小非负剩余将形成 1 个周期为 12 的周期序列：

$(k, 2.3^k) \equiv (1,6),(2,18),(3,54),(4,16),(5,48),(6,71),(7,67),(8,55),(9,19),(10,57),(11,25),(12,2);(13,6),(\mathrm{mod}(12,73))$，

在这个周期序列里没有 1 个数等于 $23, 42, 9, 32, 73-23=50, 73-42=31, 73-9=64, 73-32=41$. 这说明在 $k > 1$ 时(5)和(6)式是不可能的. 而当 $k = 0,1$ 时显然分别给出解 $(n,x) = (1,5),(3,11)$. 证毕.

参考文献：

1 Bremner A, et al. Two-weight ternary codes and the equation. J Number Theory, 1983, 16: 212～234.

2 Bremner A, et al. The integer point on there related elliptic curves. Math Comp, 1982, 39: 235～238.

3 曹珍富. 丢番图方程引论. 哈尔滨：哈尔滨工业大学出版社，1989.

（责任编辑：黎贞崇）