Advances in Applied Mathematics 应用数学进展, 2021, 10(8), 2733-2738
Published Online August 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.108284

Hans汉斯

从阿基米德分牛问题得出的Pell方程的最小正整数解

冯贝叶

中国科学院数学与系统科学研究院应用数学所，北京
Email: fby@amss.ac.cn

收稿日期：2021年7月4日；录用日期：2021年7月23日；发布日期：2021年8月9日

摘　要

本文借助于数学软件Mathematica11.0用个人计算机求出了从阿基米德分牛问题得出的Pell方程的最小正整数解。

关键词

阿基米德方程，Pell方程，最小正整数解，Mathematica11.0，个人计算机

The Smallest Positive Integer Solution of the Pell Equation Derived from Archimedes's Cattle Problem

Beiye Feng

Institute of Applied Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing
Email: fby@amss.ac.cn

Received: Jul. 4th, 2021; accepted: Jul. 23rd, 2021; published: Aug. 9th, 2021

Abstract

In this paper, with the help of the mathematical software Mathematica11.0, a personal computer is used to obtain the smallest positive integer solution of the Pell equation from Archimedes's cattle problem.

文章引用: 冯贝叶. 从阿基米德分牛问题得出的 Pell 方程的最小正整数解[J]. 应用数学进展, 2021, 10(8): 2733-2738.
DOI: 10.12677/aam.2021.108284

Keywords

Smallest Positive Integer Solution, Pell Equation, Mathematica11.0, Personal Computer

1. 引言

古希腊数学家Archimedes (阿基米德，公元前287~前212年)曾提出一个所谓的太阳神分牛问题，此问题最后可归结为求解一个二元二次的不定方程:

$$x^2 - 410286423278424y^2 = 1 \tag{1}$$

为节省篇幅，关于Archimedes分牛问题的原始形式，确切表述和如何将其化成上述方程的问题，请参见文献[1] [2] [3] [4]。方程(1)就是所谓的Pell方程。它的一般形式为 $x^2 - Dy^2 = 1$，其中D是一个不是完全平方数的正整数。这一方程现在已有了相当完整的理论和解法，但对于具体的D，特别是较大的D，求出它的具体的最小正整数解仍需具体的计算。

2. 用连分数解 Pell 方程的理论基础

在这一节中，我们首先简要回顾一下用连分数解 Pell 方程的主要结果。

定理 1. 设 D 是一个不是完全平方数的正整数，则 Pell 方程

$$x^2 - Dy^2 = 1 \tag{2}$$

具有无穷多组整数解，其所有的正整数解可用以下公式表出

$$x_n + y_n\sqrt{D} = \left(x_0 + y_0\sqrt{D}\right)^n \tag{3}$$

其中 (x_0, y_0) 表示方程(2)的最小的正整数解(必定存在，其具体求法可见下面的引理 1，定理 2)。

证明可见[5] [6]。

从公式(3)容易导出下面的递推公式和解得矩阵表达式

$$\begin{aligned} x_{n+1} &= x_0x_n + Dy_0y_n, (n \geq 2), x_1 = x_0 \\ y_{n+1} &= y_0x_n + x_0y_n, \ (n \geq 2), y_1 = y_0 \end{aligned} \tag{4}$$

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_0 & Dy_0 \\ y_0 & x_0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{5}$$

以上两式的优点是避免了使用根号，但递推公式(4)依赖了两个变量，从上面的公式我们易于导出下面的仅依赖于一个变量的二阶递推公式。

$$\begin{aligned} x_{n+2} &= 2x_0x_{n+1} - x_n \ (n \geq 3), x_1 = x_0, x_2 = x_0^2 + Dy_0^2 \\ y_{n+2} &= 2x_0y_{n+1} - y_n \ (n \geq 3), y_1 = y_0, y_2 = 2x_0y_0 \end{aligned} \tag{6}$$

引理 1. 设 D 是一个不是完全平方数的正整数，则 $\sqrt{D}$ 一定可表示成如下形式的无限循环连分数

$$\sqrt{D}=\left[a_0,\{a_1,a_2,\cdots,a_{n-1},2a_0\}\right]$$

其中 $a_0=\left[\sqrt{D}\right]$ ($\left[\sqrt{D}\right]$表示$\sqrt{D}$的整数部分)，$\{a_1,a_2,\cdots,a_{n-1},2a_0\}$表示$\sqrt{D}$的循环节。

证明可见[5]第七章推论 9。

定理 2 设 D 是一个不是完全平方的正整数，$\sqrt{D}=\left[a_0,\{a_1,a_2,\cdots,a_{n-1},2a_0\}\right]$

$$\frac{p}{q}=\left[a_0,a_1,a_2,\cdots,a_{n-1}\right]$$

则 p^2-Dq^2 必等于+1 或−1。如果 $p^2-Dq^2=1$，则 $x_0=p$，$y_0=q$ 就是方程 $x^2-Dy^2=1$ 的最小的正整数解，如果 $p^2-Dq^2=-1$，则 $x_0=2p^2+1$，$y_0=2pq$ 就是方程 $x^2-Dy^2=1$ 的最小的正整数解。证明可见[5] [6]。

3. 阿基米德方程的最小解

对从Archimedes分牛问题得出的Pell方程(1)，[7]和[8]曾用大型计算机算出了它的正整数解，后来[3]又借助于数学软件Mathematica4.0予以解决，不过[3]在其发表的论文中对利用Mathematica解决此问题中的一些相关问题表述不太清楚，也未指出一些应注意的细节，因此其计算过程经本文作者检验有些无法重复。本文详细给出了用Mathematica解决此问题的所有过程和有关细节，利用个人计算机中得出了本文的所有结果。所有过程读者均可自己重复。

Archimedes所提出的一些问题的解都是非常巨大的数，比如国际象棋问题的解答就是一个很大的数$2^{64}-1$。同样，本文所涉及的最后解答也是十万位级别的数，因此不可能在本文中完全写出，为了清楚地展示得出解答的过程，我们用两种方法求出解答。

方法1.

为了减少数据的大小，首先考虑410286423278424是否有平方因子，经过计算，发现

$$410286423278424=9314^2\times 4729494$$

因此方程(1)可化为方程

$$x^2-4729494z^2=1 \tag{7}$$

其中

$$z=9314y \tag{8}$$

现在，我们在Mathematica中键入命令

```
In[1]:= ContinuedFraction[Sqrt[4729494]]
```

然后得到答案

```
Out[1]= {2174, {1, 2, 1, 5, 2, 25, 3, 1, 1, 1, 1, 1, 1, 15, 1, 2, 16, 1, 2, 1, 1, 8, 6, 1, 21, 1, 1, 3,
>        1, 1, 1, 2, 2, 6, 1, 1, 5, 1, 17, 1, 1, 47, 3, 1, 1, 6, 1, 1, 3, 47, 1, 1, 17, 1, 5, 1, 1, 6, 2,
>        2, 1, 1, 1, 3, 1, 1, 21, 1, 6, 8, 1, 1, 2, 1, 16, 2, 1, 15, 1, 1, 1, 1, 1, 1, 3, 25, 2, 5, 1, 2,
>        1, 4348}}
```

根据定理2，我们应当把上述连分数修改成一个有限连分数如下

```
R = {2174,1, 2, 1, 5, 2, 25, 3, 1, 1, 1, 1, 1, 1, 15, 1, 2, 16, 1, 2, 1, 1, 8, 6, 1, 21, 1, 1, 3,
1, 1, 1, 2, 2, 6, 1, 1, 5, 1, 17, 1, 1, 47, 3, 1, 1, 6, 1, 1, 3, 47, 1, 1, 17, 1, 5, 1, 1, 6, 2,
2, 1, 1, 1, 3, 1, 1, 21, 1, 6, 8, 1, 1, 2, 1, 16, 2, 1, 15, 1, 1, 1, 1, 1, 1, 3, 25, 2, 5, 1, 2,
1}
```

现在将其输入到Mathematica中去，再输入命令

FromContinuedFraction[R]

即得到

$$\text{Out[3]}= \frac{1099319867328297349798662328214335439010880 49}{5054948523431503307447781973554040898634 0}$$

令 $u=1099319867328297349798662328214335439010880 49$，

$v=5054948523431503307447781973554040898634 0$

由于 $u^2-4729494v^2=1$

因此(u,v)就是方程(7)的最小解，而(7)的所有正整数解可以根据公式(6)算出

$$v_{n+2}=219863973465659469959732465642867087802176098v_{n+1}-v_n \tag{9}$$

$$v_1=5054948523431503307447781973554040898634 0$$

$$v_2=1111401068026018560632955932851937225371941550212741643095177344694021579356635650 1320$$

显然，方程(1)的最小解包含在这些解中，但是它必须符合条件(8)，因此方程(1)的最小解就是v中能被9314整除的最小的v。这样通过一个循环程序就可找到这个最小解(循环程序应在$9314|v_n$时停止，而整除性可通过计算v_n除以9314所得的余数是否为0来判定，这一余数可通过公式

$$r_n=v_n-\text{IntegerPart}\left[v_n/9314\right]\times 9314$$

来计算。

最后结果是循环到 $n=2329$ 次即可得出答案 x_0,y_0。

方法2：直接对方程(1)进行计算，算法如下：

1. 计算 $\sqrt{410286423278424}$ 的连分数

在Mathematica中键入命令

ContinuedFraction[Sqrt[410286423278424]]

回车后即可得出一个如下形式的无限连分数

{20255528, {4, 1, 1, 1, 4, 1, 2,……, 2, 1, 4, 1, 1, 1, 4, 40511056}}

(全部连分数可见[9])。

2. 根据定理2，我们应当把上述连分数修改成一个有限连分数如下

R = {20255528,4, 1, 1, 1, 4, 1, 2,……, 2, 1, 4, 1, 1, 1, 4}

(全部连分数可见[10])并在Mathematica中输入它，即键入

R = {20255528,4, 1, 1, 1, 4, 1, 2,……, 2, 1, 4, 1, 1, 1, 4}

后再回车。

3. 计算p，q

在Mathematica中再键入命令

FromContinuedFraction[R]

并回车就得到一个分数，其分子就是p，分母是q，这两个数都是非常大的数。其中p是一个103,273位的正整数，它的开头100位是

3765344502347205884018786193550576892856610111171560836237851390311234167566480643694312349186281391，

最后100位是

1040818520976114141057706314714705096647940993314916269513956239940831835922232584777023371728320049

(所有数字可见[11])。q是一个103,266位的正整数，它的开头100位是

1858921901386913309458254208638757413523161201977027301065816550850027682269834724191861021631174425，

最后100位是

0600177126871130538492849382053917018667259351819528374696260428780278235279034092592107710208663490

(所有数字可见[12])。根据定理2， $p^2 - Dq^2$ 必等于+1或−1，利用上面的p,q的末位数可知 $p^2 - 410286423278424q^2$ 的值只能是+1 (在Mathematica中也可直接验证这一结论)，这就说明方程(1)的最小解就是 $x_0 = p, y_0 = q$ ，由方法1和方法2得出的答案是完全一致的。

注1：在向Mathematica中输入任何数据之前，必须把数字之间的换行符\。分行符>和空白全部去掉，否则Mathematica会认为你输入的是多个数据，从而得不到正确的结果。比如当你输入In[1]:= A=ContinuedFraction[Sqrt[4102865]]并回车后，Mathematica会显示如下结果

```
Out[1] = {2025, {1, 1, 4, 4, 1, 1, 1, 2, 3, 5, 1, 4, 7, 1, 2, 1, 1, 2, 2, 1, 2, 1, 115, 63, 3, 2, 4, 2,
>       5, 2, 3, 10, 1, 4, 3, 1, 10, 82, 1, 1, 2, 1, 1, 10, 1, 1, 1, 3, 3, 2, 1, 15, 7, 1, 6, 2, 1, 3, 1,
>       4, 2, 1, 1, 1, 2, 15, 3, 1, 5, 39, 1, 14, 1, 1, 1, 252, 1, 1, 6, 1, 2, 1, 2, 1, 21, 6, 18, 6, 21,
>       1, 2, 1, 2, 1, 6, 1, 1, 252, 1, 1, 1, 14, 1, 39, 5, 1, 3, 15, 2, 1, 1, 1, 2, 4, 1, 3, 1, 2, 6, 1,
>       7, 15, 1, 2, 3, 3, 1, 1, 1, 10, 1, 1, 2, 1, 1, 82, 10, 1, 3, 4, 1, 10, 3, 2, 5, 2, 4, 2, 3, 63,
>       115, 1, 2, 1, 2, 2, 1, 1, 2, 1, 7, 4, 1, 5, 3, 2, 1, 1, 1, 4, 4, 1, 1, 4050}}
```

如果想把上述无限连分数修改成定理2所要求的有限连分数，并将其重新输入Mathematica中，则必须先把它写成下面的形式

```
R = {2174,1, 2, 1, 5, 2, 25, 3, 1, 1, 1, 1, 1, 1, 15, 1, 2, 16, 1, 2, 1, 1, 8, 6, 1, 21, 1, 1, 3,
1, 1, 1, 2, 2, 6, 1, 1, 5, 1, 17, 1, 1, 47, 3, 1, 1, 6, 1, 1, 3, 47, 1, 1, 17, 1, 5, 1, 1, 6, 2,
2, 1, 1, 1, 3, 1, 1, 21, 1, 6, 8, 1, 1, 2, 1, 16, 2, 1, 15, 1, 1, 1, 1, 1, 1, 3, 25, 2, 5, 1, 2,
1}
```

本文参考文献中的[9] [10] [11]和[12]在储存数据后都进行了上述处理，因此文件中的数据都是可以直接输入Mathematica的。

注2：在 Mathematica中，对比较小的分数，它以下面的用虚线当做分数线的分数形式显示，例如

```
                109931986732829734979866232821433543901088049
Out[3] = ------------------------------------------------------------------------
                505494852343150330744778197355404089863 40
```

但对比较大的分数，则用/号把分子和分母分开。请读者注意区分换行符\和前面的分数线符号。

参考文献

[1] Lenstra Jr., H.W. (2008) Solving the Pell Equation. *Algorithmic Number Theory*, **44**, 1-24.

[2] Vardi, I. (1998) Archimedes' Cattle Problem. *The American Mathematical Monthly*, **105**, 305-319. https://doi.org/10.1080/00029890.1998.12004887

[3] 赵东方. 运用 Mathematica4 软件包求解 Pell 方程的方法[J]. 华中师范大学学报(自然科学版), 2003, 37(3): 301-303.

[4] 王念良, 杨全, 王辉. 关于阿基米德牛群问题及与之有关的 Pell 方程[J]. 商洛学院学报, 2011, 25(4): 3-5.

[5] 潘承洞, 潘承彪. 初等数论[M]. 北京: 北京大学出版社, 1992.

[6] 冯贝叶. Gauss 的遗产——从等式到同余式[M]. 哈尔滨: 哈尔滨工业大学出版社, 2018.

[7] Williams, H.C., German, R.A. and Zarnke, C.R. (1965) Solution of the Cattle Problem of Archimedes. *Mathematics of Computation*, **19**, 671-674.

[8] Nelson, H.L. (1981) A Solution to Archimedes' Cattle Problem. *Journal of Recreational Mathematics*, **13**, 162-176.

[9] 冯贝叶. 根号 410286423278424 的连分数[Z].

[10] 冯贝叶. 有限部分连分数[Z].

[11] 冯贝叶. p, word 文件[Z].

[12] 冯贝叶. q, word 文件[Z].