证明数m，是斐波那契数当且仅当 $5m^2 \pm 4$是完全平方数

2024 年 11 月 10 日

目录

1 前置知识

1.1 定义：斐波那契数列

斐波那契数列$F_0, F_1, \cdots$的定义如下：令$F_0 = 0$，$F_1 = 1$，则对所有的整数$n \geq 2$，有$F_n = F_{n-1} + F_{n-2}$。

则斐波那契数列是: $0, 1, 1, 2, 3, 5, 8, 13, \cdots$

1.2 定义：同余和同余类

若两个整数a, b除以某个正整数M得到的余数相等，则我们说a和b模M同余，记作$a \equiv b \mod M$。

当我们说一个集合是同余类的时候，这是再说集合内的所有整数除以M都剩下同样的余数。一般选取集合内一个元a为表示元，将同余类记为$[a]_M$，在模同一个数M的情况下，我们可以简写为$[a]$

1.3 命题1：

用F_n表示斐波那契数列的第n项，则对所有的$n \geq 0$有：

$$F_n = \frac{1}{\sqrt{5}}(\gamma^n - \delta^n)$$

其中$\gamma = \frac{1}{2}(1 + \sqrt{5})$，而$\delta = \frac{1}{2}(1 - \sqrt{5})$

证明： 我们使用归纳法来证明，对于基础步骤，当$n = 0$的时候，就有$\frac{1}{\sqrt{5}}(\gamma^0 - \delta^0) = 0 = F_0$，并且公式对于$n = 1$也是成立的：

$$\begin{aligned}\frac{1}{\sqrt{5}}(\gamma^1 - \delta^1) =& \frac{1}{\sqrt{5}}\left[\frac{1}{2}(1 + \sqrt{5} - 1 + \sqrt{5})\right] \\ =& 1 = F_1\end{aligned}$$

现在，对归纳步骤，我们假定$n > j \geq 2$都是成立的。当$j \geq 2$的时候有$\gamma + 1 = \gamma^2$，$\delta + 1 = \delta^2$

$$
\begin{aligned}
F_n =& F_{n-1} + F_{n-2} \\
=& \frac{1}{\sqrt{5}} \ \left(\gamma^{n-1} - \delta^{n-1}\right) + \frac{1}{\sqrt{5}} \left(\gamma^{n-2} - \delta^{n-2}\right) \\
=& \frac{1}{\sqrt{5}} \left[\gamma^{n-2}\left(\gamma + 1\right) \ - \ \delta^{n-2}\left(\delta + 1\right)\right] \\
=& \frac{1}{\sqrt{5}} \left[\gamma^{n-2}\left(\gamma^2\right) \ - \ \delta^{n-2}\left(\delta^2\right)\right] \\
=& \frac{1}{\sqrt{5}} (\gamma^n - \delta^n)
\end{aligned}
$$

Q.E.D.

现在，我们引入完全平方数的概念：

1.4 定义：完全平方数

设$n \in \mathbb{Z}$，完全平方数指的是形如n^2的数。
换句话说，对任意的$n \in \mathbb{Z}$，若n是一个完全平方数，则$\sqrt{n} \in \mathbb{Z}$
接着，引入一个和斐波那契数列相关的数列。

2 斐波那契数列之外有关的一事实

2.1 定义：卢卡斯数列

若数列$\{L_n\}$,$n = 1, 2, \cdots$称为卢卡斯数列，则

$$
L_n = L(n) = \begin{cases} 2 & n = 0 \\ 1 & n = 1 \\ L(n-2) + L(n-1) & n > 1 \end{cases}
$$

2.2 命题

卢卡斯数列的通项公式为：

$$
L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n
$$

证明： 对基础步骤$n=0,n=1$有$L(0)=(\frac{1+\sqrt{5}}{2})^0+(\frac{1-\sqrt{5}}{2})^0=2$，而$L(1)=\frac{1+\sqrt{5}+1-\sqrt{5}}{2}=1$成立。

现在我们进行归纳步骤

假设对$n>1$步骤成立，$L(n)=L(n-2)+L(n-1)$，则

$$\begin{aligned}L(n-2)+L(n-1)&=\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}+\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}+\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}+\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\\&=\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(1+\frac{1+\sqrt{5}}{2}\right)+\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(1+\frac{1-\sqrt{5}}{2}\right)\end{aligned}$$

注意在上述斐波那契数列通项的证明中有:当$j\geq 2$的时候有$\gamma+1=\gamma^2$，$\delta+1=\delta^2$.其中$\gamma=\frac{1}{2}(1+\sqrt{5})$，而$\delta=\frac{1}{2}(1-\sqrt{5})$，则上述式子又可以重写为：

$$\begin{aligned}L(n-2)+L(n-1)=&\gamma^{n-2}\gamma^2+\delta^{n-2}\delta^2\\=&\gamma^n+\delta^n\\=&\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n\\=&L(n)\end{aligned}$$

Q.E.D.

我们引入一些新的概念和定义：

如果我们只对一个方程去求解它的整数（或者有理数解），则我们称该方程为**丢番图方程**(diophantine equation)，例如$x^2+y^2=z^2$就是丢番图方程，它的整数解是直角三角形的边长所满足的方程。

3 佩尔方程和其可解性

3.1 定义：佩尔方程

形如

$$x^2-dy^2=1$$

的丢番图方程称为佩尔方程，其中d是非完全平方数。

当$d=2$或者较小的数时，有一些比较容易发现的解，例如$x=1,y=0$是一个平凡解，算到$x=3,y=2$或者$x=17,y=12$也是一组解。

这引出了一个问题，是否对某个$d \in \mathbb{Z}$，佩尔方程是不存在非平凡解的。而且这关乎方程$x^2 - 5y^2 = \pm 4$，若这个只有平凡解，那么我们的问题就直接解决了。可惜问题没这么简单

上述提出的问题其实是拉格朗日定理(下面)，证明是非构造性的，因此我们先引入一个引理，内容是关于接近整数的$\sqrt{d}$的整数倍。

3.2 引理

对每个非完全平方正数d，这里存在无穷多个正整数x, y使得$\mid x - y\sqrt{d} \mid < 1/y$

证明： 我们将使用鸽笼原理来证明，对每个$m \geq 2$的整数考虑下述长度为$m+1$的序列：

$$0, \sqrt{d}, 2\sqrt{d}, \cdots, m\sqrt{d} \tag{1}$$

而式(1)中的小数部分位于$[0,1)$，将该开区间分割为一些小区间:
$[0, 1/m), [1/m, 2/m), \cdots, [(m-1)/m, 1)$。那么由于现在有$m$个$\sqrt{d}$，但区间有$m-1$个，因此式(3)中必定有两个值$a\sqrt{d}$和$b\sqrt{d}$，他们的小数部分在同一个区间内。不妨假设$a < b$，那么我们可以转

$$a\sqrt{d} = A + \epsilon,\ b\sqrt{d} = B + \delta \tag{2}$$

其中$A, B \in \mathbb{Z}$，且$\epsilon, \delta \in [i/m, (i+1)/m]$。那么

$$\mid \epsilon - \delta \mid < \frac{1}{m}$$

我们使用的是半开区间，所以该不等式是严格的。现在，利用式(2)，我们有

$$\mid \epsilon - \delta \mid < \frac{1}{m} \Rightarrow \mid (a\sqrt{d} - A) - (b\sqrt{d} - B) \mid < \frac{1}{m} \Rightarrow \mid (B - A) - (b - a)\sqrt{d} \mid < \frac{1}{m}$$

只需要令$x = B - A$和$y = b - a$，其中x, y是整数，并且由于$0 < y \leq m$，所以我们有不等式

$$\mid x - y\sqrt{d} \mid < \frac{1}{m} \leq \frac{1}{y} \tag{3}$$

从上述不等式我们可以发现，x是关于$y\sqrt{d}$严格小于1的。那我们有$x > y\sqrt{d} - 1 > 0 \geq \sqrt{d} - 1 > 0$。可以得到$x \geq 1$

先取一正整数对(x, y)使得$\mid x - y\sqrt{d} \mid < 1/y$。为了得到满足方程的其他数，我们选择正整数$m'$使得$1/m' < \mid x - y\sqrt{d} \mid$。这样的$m'$的存在性由$\sqrt{d}$是无理数保证。接着用$m'$去找到$x', y' \in \mathbb{Z}^+$满足$\mid x' - y'\sqrt{d} \mid < 1/m'$，接着因为$m' > y'$就可以有$\mid x' - y'\sqrt{d} \mid < 1/y'$。那么就找到了另一对答案$(x', y')$。接着不断的重复上述过程可以继续找到其他答案。

Q.E.D.

3.3 定理：拉格朗日

对所有$d \in \mathbb{Z}^*$，d是非完全平方数，方程$x^2 - dy^2 = 1$都有非平凡解

证明： 一般来说，该定理是用连分数证明的，但在这里我们换种方法。在这里，我们先证明存在一个非零整数M使得方程$x^2 - dy^2 = M$在$\mathbb{Z}^+$中有无穷多个解，这就需要用到上述定理，接着我们将其和模运算结合起来，证明$x^2 - dy^2 = 1$在$\mathbb{Z}^+$上与一个解，而在这个证明中我们会应用两次鸽巢定理。

利用引理3.2，$\mid x - y\sqrt{d} \mid < 1/y$在$\mathbb{Z}^+$存在无穷多个$x, y$满足条件，我们来证明

$$\mid x^2 - dy^2 \mid < 1 + 2\sqrt{d}$$

但注意的是上界不应该由x, y干涉。

首先，我们根据y来约束x的上限：

$$x = x - y\sqrt{d} + y\sqrt{d} \leq \mid x - y\sqrt{d} \mid + y\sqrt{d} < \frac{1}{y} + y\sqrt{d} \leq 1 + y\sqrt{d}$$

就有

$$\mid x^2 - dy^2 \mid = (x + y\sqrt{d}) \mid x - y\sqrt{d} \mid < (1 + y\sqrt{d} + y\sqrt{d})\frac{1}{y} = \frac{1}{y} + 2\sqrt{d} \leq 1 + 2\sqrt{d}$$

因此存在无限对正整数(x, y)满足上述不等式。利用鸽笼原理，这里存在$M \in \mathbb{Z}$且满足$\mid M \mid < 1 + 2\sqrt{d}$使得

$$x^2 - dy^2 = M \tag{1}$$

有无穷多组正整数(x, y)满足，因为$\sqrt{d}$是有理数。则$M \neq 0$。

对于满足上述式(1)的$x, y \in \mathbb{Z}^+$。我们将x, y除$\mid M \mid$，再次利用鸽笼定理，我们可以得到无穷多对$x \mod \mid M \mid$和$y \mod \mid M \mid$是有重复的（更一般的说，存在一个关于x, y的$\mod \mid M \mid$同余类），因为对于$\mod \mid M \mid$是有限个的。那么我们就可以找到其它正整数解(x_1, y_1)和(x_2, y_2)，使得$x_1 \equiv x_2 \mod \mid M \mid$和$y_1 \equiv y_2 \mod |M|$，并且$x_1 \neq x_2$，$y_1 \neq y_2$

因此，我们重写$x_1 = x_2 + Mk$和$y_1 = y_2 + Ml$，其中$k, l \in \mathbb{Z}$，则

$$
\begin{aligned}
x_1 + y_1\sqrt{d} = &\quad x_2 + y_2\sqrt{d} + M(k + \ell\sqrt{d}),\\
x_1 - y_1\sqrt{d} = &\quad x_2 - y_2\sqrt{d} + M(k - \ell\sqrt{d}).
\end{aligned}
$$

由于$M = x_2^2 - dy_2^2 = (x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d})$。而上述等式给出了

$$
x_1 + y_1\sqrt{d} = (x_2 + y_2\sqrt{d})(1 + (x_2 - y_2\sqrt{d})(k + \ell\sqrt{d})) \tag{2}
$$

和

$$
x_1 - y_1\sqrt{d} = (x_2 - y_2\sqrt{d})(1 + (x_2 + y_2\sqrt{d})(k - \ell\sqrt{d})) \tag{3}
$$

最后，只需要将式2, 3等号右边的第二个因子重写为$x + y\sqrt{d}$和$x - y\sqrt{d}$，其中$x, y \in \mathbb{Z}$。就有

$$
\begin{aligned}
x_1 + y_1\sqrt{d} = &\quad (x_2 + y_2\sqrt{d})(x + y\sqrt{d})\\
x_1 - y_1\sqrt{d} = &\quad (x_2 - y_2\sqrt{d})(x - y\sqrt{d}).
\end{aligned}
$$

接着把式子乘在一起，就有$M = M(x^2 - dy^2)$。因此$x^2 - dy^2 = 1$，最后我们证明$(x, y) \neq (\pm 1, 0)$。用反证法，首先设$(x, y) = (1, 0)$，则$x_1 = x_2$和$y_1 = y_2$，但我们刚才知道，这俩是属于同一个同余类的不同数，这是个矛盾。其次，若$(x, y) = (-1, 0)$，则$x_1 = -x_2$。但x_1, x_2是正整数，矛盾。所以存在无穷多解

Q.E.D.

例子　我们讲一个简单的例子，方程$x^2 - 7y^2 = 29$的一个解为$(6, 1)$，其次，方程$x^2 - 7y^2 = 1$的解为$(8, 3)$。在证明中我们提到另一个解的构成为原方程的解乘上$x^2 - 7y^2 = 1$的一个解即可得到一个新的解。这意味着

$$
(6 + \sqrt{7})(8 + 3\sqrt{7}) = 69 + 26\sqrt{7}
$$

是方程$x^2 - 7y^2 = 29$的一个新的解$(69, 26)$

然后，我们来证明一个比较重要的定理，首先引入一些其他引理

注：　接下来的引理都来自***kconrad***[1][2]

[1] https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf

[2] https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf

3.4 引理

若$x^2-dy^2=1$的一个解为(x,y)，则$(x+y\sqrt{d})^k$的系数也是一个解，其中$k\in\mathbb{Z}$。特别的，若该方程有一个非平凡解，则存在无穷多组解。

利用这个引理可以证明下述定理：

3.5 定理：

设$x^2-dy^2=1$有一个正整数解(x_1,y_1),其中y_1是所有解中最小的，那么$x^2-dy^2=1$的所有整数解（考虑符号）都可以由(x_1,y_1)通过对$x_1+y_1\sqrt{d}$取幂得到：

$$x+y\sqrt{d}=\pm(x_1+y_1\sqrt{d})^k$$

其中$k\in\mathbb{Z}$。正整数解满足$k\geq 1$并且带正号。

更进一步的，若对方程$x^2-dy^2=\pm 1$，则我们可以有下面的拓展定理：

3.6 定理：

设方程$x^2-dy^2=-1$有一个正整数解(x_1,y_1)且y_1是最小的。则方程$x^2-dy^2=\pm 1$的整数解可以由(x_1,y_1) 通过$x_1+y_1\sqrt{d}$的幂次生成，即：

$$x+y\sqrt{d}=\pm(x_1+y_1\sqrt{d})^k$$

其中的符号为正或负，而方程$x^2-dy^2=-1$的整数解对应k为奇数的情况，$x^2-dy^2=1$的整数解对应k为偶数的情况。

最后，我们针对形如$x^2-dy^2=n$，$n\in\mathbb{Z}$的广义佩尔方程做一些引理的引入。

3.7 定理：

固定$u=a+b\sqrt{d}$，满足$a^2-db^2=1$，其中$a,b\in\mathbb{Z}^+$，对每个$n\in\mathbb{Z}-\{0\}$，每个$x^2-dy^2=n$的整数解是$(x'+y'\sqrt{d})u^k$，其中$x'^2-dy'^2=n$,$k\in\mathbb{Z}$且

$$|x'|\leq\frac{\sqrt{|n|}(\sqrt{u}+1/\sqrt{u})}{2}\quad 和\quad |y'|\leq\frac{\sqrt{|n|}(\sqrt{u}+1/\sqrt{u})}{2\sqrt{d}}.$$

若$n > 0$，则我们取$|y'| \leq \sqrt{n}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{d}) < \sqrt{nu}/(2\sqrt{d})$.

最后，我们有

3.8 定理

对广义佩尔方程$x^2 - dy^2 = n$，其中$n \neq 0$存在一个有限的解集，使得集合中每个解都是这些解中某个解的佩尔倍数。即，每个解(x, y)都可以表示为(x_1, y_1)的如下形式：

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

其中k是任意整数

现在，回到证明上来，我们要做的事情很简单。为了证明$5m^2 \pm 4 = x^2$，我们先还原成广义佩尔方程，然后找到一个其中的解即可$x^2 - 5m^2 = \pm 4$，这其实是两条不同的方程，即

$$\begin{aligned} x^2 - 5m^2 =& 4 \\ x^2 - 5m^2 =& -4 \end{aligned}$$

回到正题

4 命题：

给定数m，m是斐波那契数列数当且仅当对m，有$5m^2 \pm 4$是完全平方数

证明： 先证充分性，记$\gamma = \frac{1+\sqrt{5}}{2}$，$\delta = \frac{1-\sqrt{5}}{2}$

并且有$\delta + 1 = \delta^2, \gamma + 1 = \gamma^2$，则

$$\begin{aligned} 5m_n^2 - L_n^2 =& 5(\frac{1}{5}(\gamma^n - \delta^n))^2 - (\gamma^n + \delta^n)^2 \\ =& (\gamma^{2n} - 2\gamma^n\delta^n + \delta^{2n}) - (\gamma^{2n} + 2\gamma^n\delta^n + \delta^{2n}) \\ =& -4\gamma^n\delta^n \end{aligned}$$

最后，注意$(1+\sqrt{5})(1-\sqrt{5}) = -4$，就有$-4\gamma^n\delta^n = -4 \times \frac{1}{4^n} \times (-4)^n = 4(-1)^n$，因此$5m^2 \pm 4$是一个完全平方数

对必要性，我们实际上要解方程$f(x,y) = x^2 - 5y^2 = \pm 4 \Rightarrow g(x,y) = (x/2)^2 - (\frac{5}{2}y)^2 = \pm 1$. 对原方程$f(x,y) = 4$和$f(x,y) = -4$满足的一对解为$(3,1)$和$(1,1)$，那么要带入$g(x,y)$的一组解，则$(1,1)$的解$(1+\sqrt{5})/2$ 也是$g(x) = \pm 1$的解，利用定理3.6，则$(1+\sqrt{5})/2$生成一组解，通解形如$(x+y)/2 = \gamma^n$，当$n = 2n$时，为$g(x,y) = 1$的解，当$n = 2n-1$时，是$g(x,y) = -1$

然后，对$(x+y\sqrt{5})/2$，$1/(x+y\sqrt{5})/2 = (x-y\sqrt{5})/2$也应该是一个方程解。注意到$((x+y\sqrt{5})(x-y\sqrt{5}))/4 = (x^2-5y^2)/4 = \pm 1$，就是我们一开始定义的方程了。

因此，对$(x-y\sqrt{5})/2$，我们可以解的

$$y_{2n-1} = \frac{1}{\sqrt{5}}\ \left(\gamma^{2n-1} - \delta^{2n-1}\right) \quad 和 \quad y_{2n} = \frac{1}{\sqrt{5}}\left(\gamma^{2n} - \delta^{2n}\right)$$

接着，我们证明每个$g(x,y)$的解都是整数解：

思路很简单，若$(x+y\sqrt{5})/2$或$(x-y\sqrt{5})/2$非整数解，则上述y_n必定有非整数出现，由此可得x也是非整数的。所以，为了方便，我们依然是对$n=0$和$n=1$开始证明，则$y_0 = 0$，$y_1 = 1$，（实际上就是斐波那契数列的第一项和第二项）接着我们归纳的套用斐波那契的通项公式就可以证明完了。

利用定理3.7，我们可以得到一组解（可以计算$|\ y\ | < 1.7\cdots$ ）$(3,1),(2,0)$和$(1,1)$。其中$(3,1),(2,0)$ 是$f(x,y)=4$的解，另一个是$f(x,y)=-4$的解

而$(2,1)$是$f(x,y)=-1$的解，由定理3.6，该解生成所有$f(x,y)=\pm 1$的解，而$(2+\sqrt{5})=((1+\sqrt{5})/2)^3$，因此可以用它生成所有$f(x,y)=\pm 1$的解。其中$n=1$的时候，是$f(x,y)=-4$的解$(1,1)$，$n=2$是$f(x,y)=4$的解$(3,1)$，由于$g$是$f/4$得来的，这意味着能用$2(((1+\sqrt{5})/2)^3)^n$生成任意解。

Q.E.D.

参考文献

Rotman, J. J. (2000). *A first course in abstract algebra (2nd ed.).* Upper Saddle River, NJ: Pearson College Division.

Keith conrad. (n.d.). PELL’S EQUATION, I. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf

Keith conrad. (n.d.). PELL’S EQUATION, II. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf