P-6

平方ピラミッド問題と楕円曲線の整数点

石井　夕紀子[1]

Abstract

E. Lucas challenged to prove that a square pyramid of cannon-balls consists of a square number of balls only when it has 24 balls along its base. In this talk, we describe an elementary proof of this fact, that is the equation $1^2+2^2+\cdots+x^2=y^2$ has the only solution $(x,y)=(24,70)$ when x is an even positive integer.

1　平方ピラミッド問題

平方ピラミッド問題とは、球をピラミッド状に x 段積み上げるとその球の総数が平方数になるかどうかという問いである。つまり

$$1^2+2^2+\cdots+x^2=\frac{x(x+1)(2x+1)}{6}$$

が整数の平方数に等しいかどうかという問題である。$y^2=\dfrac{x(x+1)(2x+1)}{6}$ は楕円曲線とよばれる曲線であり、その整数点すなわち $(x,y)\in\mathbb{Z}^2$ となる点を求める問題と同値である。
$x=0,\ y=\pm1$ は自明解であるが、自明解以外にどのような解があるかという問題を考えよう。
今 $x>0,\ y>0,\ x,y\in\mathbb{Z}$ とすると非自明解は $x=24,\ y=70$ に限ることが 1875 年に E. Lucas [4],1876 年に M. Moret-Blanc, G. N. Watson らによって考察され、そして 1952 年に W. Ljunggren [6] によって証明された。1966 年には A. Baker-H. Davenport [2] らの超越数論による別証明が与えられた。1990 年に W. S. Anglin [1] が初等的証明を構築した。即ち次の定理を初等的に証明したことに相当する。

定理 1. $x,y\in\mathbb{Z},\ x,y>0$ とする。方程式

$$1^2+2^2+\cdots+x^2=y^2$$

の非自明解は $x=24,\ y=70$ に限る。

本稿では [1] の証明を紹介する。楕円曲線 $y^2=x^3-Ax-B$ $(A,B\in\mathbb{Q})$ において，整数点とは点 $(x,y)\in\mathbb{Z}^2$ を指すとすると、整数点全体が有限個であるという一般的結果は C. L. Siegel らによって確立されているが、ここでは非自明解が $x=24,\ y=70$ のみであることを示す。

2　定理の証明

補題 1. 3 辺とも整数の直角三角形の面積は整数の平方数にはならない。

この証明は [1] にある。

補題 2. $2x^4+1=y^2$ となるような正整数 x は存在しない。

証明. $(x,y)\in\mathbb{Z}^2,x>0,y>0$ を $2x^4+1=y^2$ の整数解のうち、y が最小の解と仮定する。$s\in\mathbb{Z}$ に対し $y=2s+1$ とおくと $x^4=2s(s+1)$ となる。もし s が奇数であるとすると、

$$\gcd(s,2(s+1))=1\quad(\because\gcd(s,s+1)=1,\ s:\text{奇数})$$

となり、ある $u,v\in\mathbb{Z}$ が存在して

$$s=u^4,\ 2(s+1)=v^4$$

と書ける。これより

$$2(u^4+1)=v^4\quad(u:\text{奇数、}v:\text{偶数})$$

が得られ $2(1+1)\equiv0\pmod 8$ となって矛盾。
従って s が偶数となり $\gcd(2s,s+1)=1$ 故に $u,v\in\mathbb{Z}$ $(u,v\geq1)$ が存在して

$$2s=u^4,\ s+1=v^4\ (u,v\geq1)$$

と表せる。u は偶数、v は奇数なので

$$\exists w,\ a\in\mathbb{Z}\quad s.t.\quad u=2w,\ v^2=2a+1$$

と書ける。即ち $\dfrac{u^4}{2}+1=v^4$ つまり $2w^4=a(a+1)$ となる。
v が奇数であることから v を mod 4 で分けると a は偶数。また、$2w^4=a(a+1)$ から $a=2b^4,\ a+1=c^4$ となるような正整数 b,c が存在する。すると

$$2b^4+1=(c^2)^2$$

となり、y の最小性より

$$y\leq c^2$$

これに対して

$$c^2\leq a+1<v^2\leq s+1<y$$

よって矛盾。
$\therefore 2x^4+1=y^2$ となるような正整数 x は存在しない。
□

補題 3. $8x^4+1=y^2$ をみたす正整数 x は 1 に限る。

[1]日大理工・院 (前)・数学

証明. $8x^4+1 = (2s+1)^2$ となる正整数 s をとる。
$2s^4 = s(s+1)$ である。
(i) s が偶数だと仮定する。$\gcd(s, s+1) = 1$ より

$$\exists u, v \in \mathbb{Z} \;\; s.t. \;\; s = 2u^4, \; s+1 = v^4$$

と表せる。従って $2u^4+1 = (v^2)^2$ となり補題 2 から $u = 0$ となる。故に $x = 0$.
(ii) s が奇数であると仮定する。$\gcd(s, s+1) = 1$ より

$$\exists u, v \in \mathbb{Z} \;\; s.t. \;\; s = u^4, \; s+1 = 2v^4$$

となり $u^4+1 = 2v^4$ が得られる。
u が奇数（s が奇数より）であることから mod 4 で分けると v も奇数である。
また $u^4+1 = 2v^4$ の両辺を 2 乗することにより $v^8 - u^4 = \dfrac{u^8 - 2u^4 + 1}{4}$ より $(v^4+u^2)(v^4-u^2) = \left(\dfrac{u^4-1}{2}\right)^2$
が従い右辺は整数の平方数となる。$\gcd(v^4, u^2) = 1$ より $\gcd\left(\dfrac{v^4-u^2}{2}, \dfrac{v^4+u^2}{2}\right) = 1$ から

$$\exists X, Y \in \mathbb{Z} \quad s.t. \quad \frac{(v^4-u^2)}{2} = X^2, \; \frac{(v^4+u^2)}{2} = Y^2$$

と書けるので $(v^2-u)^2 + (v^2+u)^2 = \dfrac{4(v^4+u^2)}{2} = (2Y)^2$
となり直角三角形の 3 辺になるが、この面積は

$$\frac{(v^2-u)(v^2+u)}{2} = \frac{(v^4-u^2)}{2} = X^2.$$

補題 1 により、これは $v^2 = \pm u$ でないかぎり不可能。
$u^4+1 = 2v^4$ であることから、$u^4 - 2u^2 + 1 = 0$ となり $u^2 = 1$ であることがわかる。これより $s = 1$ となり $x = \pm 1$ となる。
$\therefore 8x^4+1 = y^2$ をみたす正整数 x は 1 に限る。

□

定理 1 の証明 .

x は偶数とする。
$\gcd(x, x+1) = 1, \;\; \gcd(x, 2x+1) = 1, \;\; \gcd(x+1, 2x+1) = 1$ であるから
$p, q, r \in \mathbb{Z}$ $(p, q, r > 0)$ に対して mod 3 で分けると

$$x = 6q^2, \; x+1 = p^2, \; 2x+1 = r^2$$

と表すことができる。
$x = (2x+1) - (x+1)$ より
$6q^2 = r^2 - p^2$.
p, r が奇数より
$6q^2 = r^2 - p^2$
$= (2m+1)^2 - (2n+1)^2 \quad (0 < m, n \in \mathbb{Z})$
$\equiv 0 \pmod 4$.
ゆえに q は偶数となる。
$q' \in \mathbb{Z}, \; q = 2q'$ とおくと
$6q^2 = (r-p)(r+p)$ より
$6q'^2 = \left(\dfrac{r-p}{2}\right)\left(\dfrac{r+p}{2}\right)$.
$\left(\dfrac{r-p}{2}, \dfrac{r+p}{2}\right) = 1$ より次の 4 つのケースを得る。

(i) $\dfrac{r-p}{2} = 6A^2, \; \dfrac{r+p}{2} = B^2 \;\; (A, B \in \mathbb{Z}, A, B > 0)$ のとき

$\dfrac{r-p}{2} - \dfrac{r+p}{2} = 6A^2 - B^2$ より
$p = B^2 - 6A^2$.
$r - p = 12A^2, \; r + p = 2B^2$ とすると
$6q^2 = 12A^2 \cdot 2B^2$ より
$q = 2AB$.
$6q^2 + 1 = x + 1 = p^2$ より
$24A^2B^2 = (6A^2 - B^2)^2$.
$\therefore (6A^2 - 3B^2)^2 - 8B^4 = 1$
となる。補題 3 より $B = 0, \; 1$ となり

$$x = 6q^2 = 0 \text{ もしくは } 24$$

となる。
(ii) $\dfrac{r-p}{2} = B^2, \; \dfrac{r+p}{2} = 6A^2 \;\; (A, B \in \mathbb{Z}, A, B > 0)$ のときも同様である。
(iii) $\dfrac{r-p}{2} = 3A^2, \; \dfrac{r+p}{2} = 2B^2 \;\; (A, B \in \mathbb{Z}, A, B > 0)$ のとき
$\dfrac{r-p}{2} - \dfrac{r+p}{2} = 3A^2 - 2B^2$ から
$p = 2B^2 - 3A^2$ である。
$r - p = 6A^2, \; r + p = 4B^2$ とすると
$6q^2 = 6A^2 \cdot 4B^2$ となり
$q = 2AB$.
よって $6q^2 + 1 = 24A^2B^2 + 1 = p^2 = (2B^2 - 3A^2)^2$.
$\therefore (3A^2 - 6B^2)^2 - 2(2B)^4 = 1$.
補題 2 より $B = 0$. 故に

$$x = 6q^2 = 0.$$

(iv) $\dfrac{r-p}{2} = 2B^2, \; \dfrac{r+p}{2} = 3A^2 \;\; (A, B \in \mathbb{Z}, A, B > 0)$ のときも同様である。

以上より x が偶数のとき解は $x = 24$ のみである。　□
x が奇数の場合の説明も同様の議論で導かれるので、本稿では省略する。

参考文献

[1] W. S. Anglin, *The Square Pyramid Puzzle*, The American Math. Monthly, Vol. 97, No. 2, (1990), 120–124.

[2] A. Baker and H. Davenport, The Equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quarterly J. of Math.*, ser. 2, Vol. 20, (1969) 129–37.

[3] B. Brindza and Á. Pintér, *On the number of solutions of the equation* $1^k + 2^k + \cdots + (x-1)^k = y^z$, Publ. Math. Debrecen, Vol. 56, (2000), 271–277.

[4] E. Lucas, Question 1180, *Nouvelles Annales de Mathématiques*, ser. 2, Vol. 14, (1875), 336.

[5] M. J. Jacobson, Jr., Á. Pintér and P. G. Walsh, *A Computational Approach For Solving* $y^2 = 1^k + 2^k + \cdots + x^k$, Math. Comp. Vol. 72, No. 244, (2003), 2099–2110.

[6] W. Ljunggren, New solution of a problem proposed by E. Lucas, *Norsk Mat. Tidsskrift*, Vol. 34, (1952), 65–72.