第7卷 无锡轻工业学院学报 Vol.7
第3期 JOURNAL OF THE WUXI INSTITUTE OF LIGHT INDUSTRY 1988 No.3

关于商高数 $(n+h)^2-n^2$, $2n(n+h)$, $(n+h)^2+n^2$

李晓莲
(基础课部)

摘　　要

本文解决了一类商高数的Jes′manowicz猜测，即证明下列定理：设 $a=(n+h)^2-n^2$、$b=2n(n+h)$、$C=(n+h)+n^2$，此处正整数 n、h 满足 $h^2=2n^2-1$，则丢番图方程 $a^x+b^y=c^z$ 仅有正整数解 $x=y=z=2$。

主题词：商高数；正整数解；奇偶数；猜测；同余式；模

熟知，3、4、5为一组商高数，1956年，Sierpinski[1]证明了方程 $3^x+4^y=5^z$ 仅有正整数解 $X=Y=Z=2$。接着，Jes′manowicz[2]猜测：如果正整数 a、b、c、x、y、z 满足 $a^2+b^2=c^2$，$a^x+b^y=c^z$，则必有 $x=y=z=2$。同时，对正整数 $a=2n+1$，$b=2n(n+1)$，$C=2n(n+1)+1$ $(n>0)$，他证明了当 $2\leqslant n\leqslant 5$ 时，这个猜测成立。此后，不少数学家对这个问题作了大量工作，如见文[3]-[6]。其中苏联数学家Demj′anenko[3]于1965年完全解决了商高数为 $a=2n+1$，$b=2n(n+1)$，$c=2n(n+1)+1$ 时的Jes′manowicz猜测。

本文探讨了商高数为

$$(n+h)^2-n^2,\ 2n(n+h),\ (n+h)^2+n^2 \tag{1}$$

的Jes′manowicz猜测，其中

$$h^2=2n^2-1 \tag{2}$$

证明了此时这个猜测是正确的。

由于 $h=n=1$ 时，由(1)给出商高数为3、4、5，即为Sierpinski的结果，故下文将恒设 $n>1$。

引理　设 $a=(n+h)^2-n^2$，$c=(n+h)^2+n^2$，这里 n、h 均为正整数，且满足 $h^2=2n^2-1$，则 $a\equiv -1\pmod{2n}$，$c\equiv -1\pmod{2n}$，$a^2\equiv 1\pmod{2n(n+h)}$，$c^2\equiv 1\pmod{2n(n+h)}$

证：由式(1)及式(2)有

$$a=2nh+h^2=2nh+2n^2-1=2n(n+h)-1,$$

$$c=2n^2+2nh+h^2=2n^2+2nh+2n^2-1=2n(2n+h)-1,$$

本文1987年7月25日收到

因此，$a\equiv-1\pmod{2n}$，$c\equiv-1\pmod{2n}$，
又有

$$a^2=(2n(n+h))^2-4n(n+h)+1=4n(n+h)(n(n+h)-1)+1,$$

$$c^2=4n(2n+h)[n(2n+h)-1]+1=4nh(2n+h)(n+h)+1,$$

所以

$a^2\equiv(\bmod 2n(n+h))$，$c^2=1\pmod{2n(n+h)}$，证毕。

定理　设$a=(n+h)^2-n^2$，$b=2n(n+h)$，$c=(n+h)^2+n^2$，其中正整数n、h满足$h^2=2n^2-1$，则方程

$$a^x+b^y=c^z \tag{3}$$

仅有正整数解　$x=y=z=2$。

证：设上述的商高数a、b、c满足方程(3)，即有：

$$[(n+h)^2-n^2]^x+[2n(n+h)]^y=[(n+h)^2+n^2]^z,$$

利用关系式（2），上式可化为

$$[2n(n+h)-1]^x+[2n(n+h)]^y=[2n(2n+h)-1]^z \tag{4}$$

对式(4)取$2n$为模，得到

$$(-1)^x\equiv(-1)^z\pmod{3n} \tag{5}$$

因$n>1$，故由式（5）知，数x、z具有相同的奇偶性（$n=1$时，x、z的奇偶性可不同）若x、z同为奇数，则对式（4）取$2n(n+h)$为模，由引理得到

$$-1\equiv 2n(2n+h)-1\pmod{2n(2n+h)},$$

即　$2n[n+(n+h)]\equiv0\pmod{2n(n+h)}$，
故有　$2n^2\equiv0\pmod{2n(n+h)}$，因此，$n\equiv0\pmod{(n+h)}$，而$h>1$，故此显然为不可能，从而，$x$、$z$必同为偶数。

命$x=2x_1$，$z=2z_1$，x_1、z_1为正整数，以此代入式(4)得到

$$[2n(n+h))^y=\{[2n(2n+h)-1]^{z_1}+[2n(n+h)-1^{x_1}\}\}[2n(2n+h)-1]^{z_1}$$
$$-[2n(n+h)-1]^{x_1}\} \tag{6}$$

现分$z_1\equiv0\pmod 2$与$z_1\equiv1\pmod 2$两种情形讨论。

（Ⅰ）若$z_1\equiv0\pmod 2$，设$A=[2n(2n+h)-1]^{z_1}$，　$B=[2n(n+h)-1]^{x_1}$，则由引理可得

$$A+B\equiv1+(-1)^{x_1}\pmod{2n(n+h)} \tag{7}$$

$$A-B\equiv1-(-1)^{x_1}\pmod{2n(n+h)} \tag{8}$$

(i）当$x_1\equiv1\pmod 2$）时，由式(7)与(8)得

$$A+B\equiv0\pmod{2n(n+h)},$$

$$A-B\equiv2\pmod{2n(n+h)},$$

因为$C=a+2n^2$，故$(c,a)=(2n^2,a)=1$，由此容器推出$(A,B)=(c^{z_1},a^{z_1})=1$，

又因$A+B$、$A-B$均为偶数，故由$(A,B)=1$，易得$(A+B,A-B)=2$，由(6)、(7)、(8)可得

$$A+B=2^{y-1}[n(n+h)]^y \tag{9}$$

$$A-B=2 \tag{10}$$

将(9)、(10)两式相加得

$$2[2n(2n+h)-1]^{z_1}=2^{y-1}[n(n+h)]^y+2,$$

即

$$[2n(2n+h)-1]^{z_1}=2^{y-2}[n(n+h)]^y+1.$$

令　$z_1=2r$，r为正整数，则

$$\{[2n(2n+h)-1^2\}^r=[4n^2(2n+h)^2-4n(2n+h)+1]^r$$

$$=\{4n(2n+h)[n(2n+h)-1]+1\}^r=[4n(2n+h)(2n^2-1+nh)+1]^r$$

$$=[4n(2n+h)h(n+h)+1]^r\equiv 1 \pmod{4nh(n+h)(2n+h)},$$

即

$$2^{y-2}[n(n+h)]^y\equiv 0 \pmod{4nh(n+h)(2n+h)} \tag{11}$$

若　$h(2n+h)\mid 2^{y-2}[n(n+h)]^y$，则　$h\mid 2^{y-2}[n(n+h)]^y\equiv 2^{y-2}n^{2y} \pmod h$，即$h\mid 2^{y-2}n^{2y}$，但因$h^2=2n^2-1$，$h$为大于1的奇数，且易知$(n,h)=1$，故知$h$不能整除$2^{y-2}n^{2y}$，这个矛盾说明了$h(2n+h)$不能整除$2^{y-2}[n(n+h)]^y$，这说明式(11)为不可能。

(ii)　当$x_1\equiv 0 \pmod 2$时，同理有

$$A+B\equiv 2 \pmod{2n(n+h)},$$

$$A-B\equiv 0 \pmod{2n(n+h)},$$

故由式(6)易得

$$A+B=2 \tag{12}$$

$$A-B=2^{y-1}[n(n+h)]^y \tag{13}$$

显然，上述两式不能同时成立。

(Ⅱ)　若$z_1\equiv 1 \pmod 2$，则由引理有

$$A+B\equiv 2n^2-1+(-1)^{x_1} \pmod{2n(n+h)} \tag{14}$$

$$A-B\equiv 2n^2-1-(-1)^{x_1} \pmod{2n(n+n)} \tag{15}$$

(i)　当$x_1\equiv 0 \pmod 2$时，上述两式化为

$$A+B\equiv 2n^2 \pmod{2n(n+h)} \tag{16}$$

$$A-B\equiv 2(n^2-1) \pmod{2n(n+h)} \tag{17}$$

由上述讨论及关系式(2)知h为奇数，设$h=2k+1$，则$n^2=(h^2+1)/2=2k^2+2k+1=2k(k$

+1)+1为奇数，故得

$$n\equiv 1 \pmod 2。$$

因为$(n, h)=1$，故由式(6)、(16)、(17)知

$$A+B=2n^y \tag{18}$$

$$A-B=2^{y-1}(n+h)^y \tag{19}$$

若$y=1$，将(18)、(19)两式相加得：

$$[2n(2n+h)-1]^{z_1}=(n+h)/2+n<2n(2n+h)-1$$

因此，$z_1<1$，此与z_1为正整数矛盾，故必$y>1$，此时，由于

$$z^{y-1}(n+h)^y>2n^y$$

$$A+B>A-B$$

显然，式(18)、(19)不可能成立。

(ii) 当$x_1\equiv 1 \pmod 2$时，则式(14)、(15)化为

$$A+B\equiv 2n^2-2 \pmod{2n(n+h)},$$

$$A-B\equiv 2n^2 \pmod{2n(n+h)}。$$

由情形(i)的讨论可知

$$A+B=2^{y-1}(n+h)^y \tag{20}$$

$$A-B=2n^y \tag{21}$$

因为

$$2n(2n+h)-1=C,$$

$$2n(n+h)-1=a,$$

故式(20)与(21)可化为

$$c^{x_1}+a^{x_1}=2^{y-1}(n+h)^y \tag{22}$$

$$c^{x_1}-a^{x_1}=2n^y \tag{23}$$

若$y\equiv 0 \pmod 2$，由式(22)、(23)可得

$$C^{x_1}=2^{y-2}(n+h)^y+n^y \tag{24}$$

$$a^{x_1}=2^{y-2}(n+h)^y-n^y \tag{25}$$

由$y\equiv 0 \pmod 2$可设$y=2y_1$，又$x_1\equiv 1 \pmod 2$设可$x_1=2x_2+1$，则由式(25)得

$$[(n+h)^2-n^2]^{2x_2+1}=[2^{y_1-1}(n+h)^{y_1}+n^{y_1}][2^{y_1-1}(n+h)^{y_1}-n^{y_1}],$$

因n是奇数，且$(n, h)=1$，所以$(2^{y_1-1}(n+h)^{y_1}, n^{y_1})=1$，于是$(2^{y_1-1}(n+h)^{y_1}+n^{y_1}, 2^{y_1-1}(n+h)^{y_1}-n^{y_1})=1$，由此即得

$$2^{y_1-1}(n+h)^{y_1}+n^{y_1}=u^{2x_2+1},\quad 2^{y_1-1}(n+h)^{y_1}-n^{y_1}=v^{2x_2+1},$$
$$uv=(n+h)^2-n^2,\quad (u, v)=1,$$

因为$u^{2x_2+1}=2^{y_1-1}(n+h)^{y_1}+n^{y_1}>2^{y_1-1}(n+h)^{y_1}-n^{y_1}=v^{2x_2+1}$,

故　$u>v$，又u、v均为奇数，所以$u\geqslant v+2$，又 $u^{2x_2+1}+v^{2x_2+1}=2^{y_1}(n+h)^{y_1}$，$u^{2x_2+1}-v^{2x_2+1}=2n^{y_1}$，由　$2^{y_1}n^{y_1}=2^{y_1-1}2n^{y_1}$，即得

$$u^{2x_2+1}+v^{2x_2+1}=2^{y_1}(n+h)^{y_1}>2^{y_1}n^{y_1}=2^{y_1-1}(u^{2x_2+1}-v^{2x_2+1}),$$

所以

$$(2^{y_1-1}+1)v^{2x_2+1}>(2^{y_1-1}-1)u^{2x_2+1}\geqslant(2^{y_1-1}-1)(v+2)^{2x_2+1}$$

$$=(2^{y_1-1}-1)v^{2x_2+1}+2(2^{y_1-1})(2x_2+1)v^{2x_2}+\cdots\cdots,$$

化简得

$$v>(2^{y_1-1}-1)(2x_2+1)+\cdots\geqslant 2^{y_1-1} \tag{26}$$

另一方面，由式(25)及　$(n+h)^2\equiv n^2$　$(\bmod((n+h)^2-n^2))$　可得

$$[(n+h)^2-n^2]^{2x_2+1}=2^{2y_1-2}(n+h)^{2y_1}-n^{2y_1},$$

再由

$(2^{2y_1-2}-1)(n+h)^{2y_1}$　$(\bmod((n+h)^2-n^2))$及$uv=(n+h)^2-n^2$　得：

$$(2^{2y_1-2}-1)(n+h)^{2y_1}\equiv 0 \quad (\bmod uv)。$$

因为$(n,h)=1$，　故

$(uv,\ n+h)=((n+h)^2-n^2,\ n+h)=(n^2,\ n+h)=1$，

由此，$2^{2(y_1-1)}-1\equiv 0$　$(\bmod uv)$。

故当$y_1>1$时，$uv\leqslant 2^{2(y-1)}-1$，但因$u\geqslant v+2$，故得　$v^2\leqslant 2^{2(y_1-1)}-1$，

从而$v<2^{y_1-1}$，这与式(26)矛盾。于是$y_1=1$，由此$y=2$，以此代入式(24)及(25)立得：

$$c^{z_1}=c,\qquad a^{x_1}=a,$$

因此，$x_1=z_1=1$，从而$x=y=z=2$

若$y\equiv 1$　$(\bmod 2)$，　令$z_1=2k+1$，$x_1=2l+1$，

则由引理知

$$A=C^{z_1}=(C^2)^kC\equiv C=2n[n+(n+h)]-1$$

$$=(2n^2-1)+2n(n+h)\equiv 2n^2-1 \quad (\bmod 2(n+h)),$$

$$B=a^{x_1}=(a^2)^la\equiv a=2n(n+h)-1\equiv -1 \quad (\bmod 2(n+h)),$$

故由式(20)与(21)得到

$$2^{y-1}(n+h)^y\equiv 2(n^2-1) \qquad (\bmod 2(n+h)) \tag{27}$$

$$2n^y\equiv 2n^2 \qquad (\bmod 2(n+h)) \tag{28}$$

由式(27)得

$n^2\equiv 1$　$(\bmod (n+h))$，代入式(28)得$n^y\equiv 1$　$(\bmod (n+h))$。

若$y=1$，则$n\equiv 1$　$(\bmod (n+h))$此显然不可能。故必有$y>1$，此时，由$n^y\equiv 1\equiv n^2$ $(\bmod (n+h))$ 可知，$n+h|n^y-n^2$，即$n+h|n^2(n^{y-2}-1)$，因 $(n,\ n+h)=1$、故有 $n+h|n^{y-2}-1$，所以

$$n^{y-2}\equiv 1\equiv n^2 \pmod{(n+h)}$$

如此总可经有限次(设为k次)手续，使$y-2k=1$。因此，

$$n=n^{y-2k}\equiv n^2 \quad (\bmod\ (n+h)),$$

即 $n+h|n(n-1)$，因$(n,\ n+h)=1$，故$n+h|n-1$，

即 $n\equiv 1\ (\bmod\ (n+h))$，此不可能。故知$y\equiv 1(\bmod\ 2)$时为不可能。

综上所述，仅当$x=y=z=2$时等式$a^x+b^y=c^z$ 才成立。证毕。

参 考 文 献

[1] Sierpinski W.O ro'wnaniu $3^x+4^y=5^z$, Roczn, Polsk, towarz, mat, 1956; Ser.2, 1, 2, 194~195

[2] Jes'manowicz L.Kilke uway O liczlach Pitagorejskich, Roczn, Polsk. towarz.mat, 1956; Ser.2, 1, 2, 196~202

[3] Demj'anenko V.A. On Jes'manowicz Problem for Pythagorean numbers, Izv. Vyss.Ucebn.Zaved, Matematika, 1965; 5 (48), 52~56

[4] 柯召. 关于丢番图方程 $(a^2-b^2)^x+(2ab)^y=(a^2+b^2)^z$. 四川大学学报. 1959; 3, 24~34

[5] 陈景润. 关于 Jes'manowicz 的猜测. 四川大学学报. 1962; 2, 19~25

[6] 曹珍富. 关于商高数猜想的一个结论. 数学通讯. 1982; 6, 35~36

On the pythagorean numbers $(n+h)^2-n^2$, $2n(n+h)$, $(n+h)^2+n^2$

Abstract

This paper has solved Jes'manowicz's conjecture of a class of the pythagorean numbers. We have proved the following theorem: If $a=(n+h)^2-n^2$ $b=2n(n+h)$、$c=(n+h)^2+n^2$, where positive integer numbers n、h suffices $h^2=2n^2-1$, then the Diephantine equation $a^x+b^y=c^z$ has only a positive integer solution $x=y=z=2$.

subjectwords: pythagorean number; positive integer solution; odevity; conjecture; congruence; modulus