# Catalan 猜想的简捷证明

唐子周 唐世杰

（新疆.且末县中学 841900）

**摘要** 针对凯特兰（Catalan）猜想采用了反证法、命题转化法，根据阿贝尔群理论及数论定理简捷的证明了该猜想成立。

**关键词** 凯特兰猜想；勾股数定理；命题转化法；阿贝尔群

## 引言

凯特兰于 1842 年提出：除了 $8=2^3$，$9=3^2$ 以外没有两个连续数都是正整数乘幂的猜想。即不定方程 $x^p+1=y^q$，其中 $p$，$q$ 均是素数，除了 $8=2^3$，$9=3^2$ 以外没有其它的正整数解。

160 多年来数学家们证明了下列定理：

欧拉(Euler)首先证明了不定方程 $x^2-1=y^q$，当 $q$=3 时猜想成立；大约 1961 年卡塞尔斯证明了不存在三个相邻的正整数是完全幂[1]。

1962 年柯召证明了当 $q>3$ 时，不定方程 $x^2-1=y^q$ 无正整数解[2]。

另外，《数学猜想集》的定理 **1.3.16** “不定方程 $x^2+1=y^q$，$q$ 是奇素数，没有 $x>0$，$y>0$ 的正整数解”。定理 **1.3.18** “不定方程 $x^p+1=y^q$，$q$ 是素数，$p$ 是奇素数，有正整数解的充分必要条件是：

$$x+1=p^{sq-1}y_1^q,\frac{x^p+1}{x+1}=py_2^q,y=p^sy_1y_2,(y_1,y_2)=1,$$

$$p\dagger y_1y_2,$$

$$y-1=q^{tp-1}x_1^p,\frac{y^q-1}{y-1}=qx_2^p,x=q^tx_1x_2,(x_1,x_2)=1,$$

$$q\dagger x_1x_2,$$

其中 $s,t,x_1,x_2,y_1,y_2$ 均是正整数”[1]。

2004 年 P.Mihailescu 给出了 Catalan 猜想的一种证明方法，见 J.reine angew.Math. volume 572（2004）。

对于曾经困惑数学界一百六十多年的重大课题、本文另辟蹊径，对 Catalan 猜想采取了有效的转化，并采用了简捷的方法给出了该猜想成立的完全证明。

## 猜想的证明

## 2.1 猜想的部分情况

不定方程$x^p+1=y^q$，当$p$=$q$=2时，若$x^2+1=y^2$有正整数解，显然不符合《数学猜想集》中的勾股数定理，$x=2mn, y=m^2-n^2, z=m^2+n^2$，$m>n$,( $m$,$n$)=1 [1]；所以$x^2+1=y^2$无正整数解。

对于$p$=2，$q$>2时的情况已被柯召等数学家证明了。

## 2.2 猜想的完全证明

**假定：**凯特兰猜想不成立，那么必存在（除了8=$2^3$，9=$3^2$以外的）正整数$a$，$b$，$p$，$q$满足$a^p+1=b^q$①成立；$a,b\in N_+$，$N_+$表示正整数集合；$q$是素数，$p$是奇素数。

根据假定得（$a$, $b$）=1，且$a\neq 1$；否则，$a^p+1=b^q$不成立。

由《数学猜想集》的定理 **1.3.18** [1] 得：$a+1=p^{sq-1}b_1^{\,q}$，$b-1=q^{sp-1}a_1^{\,p}$；$a=q^t a_1 a_2, b=p^s b_1 b_2$，$p|b$, 得（$p$,$a$）=1，否则$a^p+1=b^q$不成立；而且得$a+1\equiv 0(\mathrm{mod}\ p)$，$a\equiv -1(\mathrm{mod}\ p)$；由此推得$a^p\equiv -1(\mathrm{mod}\ p)$

因为$b^{q-1}-1=(b-1)(b^{q-2}+b^{q-3}+b^{q-4}+\cdots\cdots+b+1)$

$=(b^2-1)(b^{q-3}+b^{q-5}+b^{q-7}+\cdots\cdots+b^2+1)$

所以，$b^{q-1}-1$能被$b^2-1$整除；令$b^{q-1}-1=t(b^2-1)$，则($t$,$b$)=1，否则$b^{q-1}-1=t(b^2-1)$不成立；由$b^q-b=tb(b^2-1)$，$a^p+1=b^q$得$a^p+1=tb^3+b(1-t)$, $t\in N_+$;即$tb^3+b(1-t)-(a^p+1)=0$;

因为必存在整数$c$,满足$b$+$c$=$a$, $c\in\mathbf{Z}$,（$b$，$c$）=1;

所以，由$a^p+1=b^q$得$(b+c)^p+1=b^q$;$(c,\ p)=1$,

因为$p$是奇素数，二项式的系数$C_p^k$（$k$=1,2,3……$p$−1）都可以被$p$整除, 见《代数数理论讲义》47页 [3]，又因为$p|b$, 由二项式定理将$(b+c)^p+1=b^q$展开后可知$c^p+1\equiv 0(\mathrm{mod}\ p)$，$c^p+1\equiv 0(\mathrm{mod}\ b)$；由费马定理 [4] $c^{p-1}-1\equiv 0(\mathrm{mod}\ p)$，因为（$c$，$p$）=1，所以，（$c^{p-1}$，$p$）=1，$c+1\equiv 0(\mathrm{mod}\ p)$，$c+1=pl$，$l\in\mathbf{Z}$(整数集合)；

由定理 **1.3.18**: 可知$b$=$qh$+1, $h\in\mathbf{Z}$;所以，由$(b+c)^p+1=b^q$得

$(qh+1+c)^p+1=(qh+1)^q$；由二项式定理展开可知$(c+1)^p\equiv 0(\mathrm{mod}\ q)$，所以，$c+1\equiv 0(\mathrm{mod}\ q), c+1=qm$，$m\in\mathbf{Z}$; 由$pl=qm$得$l=nq, m=rp$; 所以，$npq=rpq$，$n=r$，$n,r\in\mathbf{Z}, c=npq-1$；

由$tb^3+b(1-t)-(a^p+1)=0$，$b+c=a$，得$tb^3+b(1-t)-[(b+nqp-1)^p+1]=0$；

由二项式定理将$[b+(nqp-1)]^p+1$展开后，根据“任意整系数方程的整根必为常数项的约数”的定理（见《数学手册》91页[5]）可知：

方程$tb^3+b(1-t)-[(b+nqp-1)^p+1]=0$中，$b$须整除$(nqp-1)^p+1$；把$(nqp-1)^p+1$按二项式定理展开后最高项$(npq)^p$须满足$(npq)^p\equiv 0(\mathrm{mod}\ p_i)$（见《代数数理论讲义》14页[3]），$p_i$表示$b$的任意一个素因子，得$npq\equiv 0(\mathrm{mod}\ p_i)$，因为$c^p\equiv -1(\mathrm{mod}\ q)$，$c^p\equiv -1(\mathrm{mod}\ p)$，由《初等数论》$n$次剩余定理[4]可知$c$的值是唯一的；根据定理“若同余式组$x\equiv a_1(\mathrm{mod}\ n_1), x\equiv a_2(\mathrm{mod}\ n_2), \cdots\cdots x\equiv a_k\ (\mathrm{mod}\ n_k)$的模两两互素，则同余式组正好只有一个解$\mathrm{mod}\ n_1\cdots n_k$。”[3]；得$npq$的值也是唯一的，因为$c=npq-1$，所以也可得$c$的值是唯一的；又因为$c^p+1\equiv 0(\mathrm{mod}\ b)$，所以$c^p+1\equiv 0(\mathrm{mod}\ p_i^{\alpha_i})$，$p_i^{\alpha_i}$表示$b$的任意一个因子，$p_i$是素数（$i$=1,2,3……）；若$c\equiv -1(\mathrm{mod}\ p_i^{\alpha_i})$，则必有$c^p+1\equiv 0(\mathrm{mod}\ p_i^{\alpha_i})$；表明了这唯一的$c$值必满足$c+1\equiv 0(\mathrm{mod}\ p_i^{\alpha_i})$成立；否则$c$的值不是唯一的，与$n$次剩余定理及上述定理皆矛盾；由《初等数论》同余的性质辛[4]可知$c+1\equiv 0(\mathrm{mod}\ b)$。

且由$(b+nqp-1)^p+1$可知须$nqp\equiv 0(\mathrm{mod}\ b)$；又因为$(b,q)=1$，

所以，$npq=ubq$，$u\in Z$；

由$tb^3+b(1-t)-[(b+nqp-1)^p+1]=0$，$b^q=tb^3+b(1-t)$，

得$[b(1+uq)-1]^p+1=b^q$。

因为从$[b(1+uq)-1]^p+1=b^q$也可以推出$a^p+1=b^q$，即二者是等价的；

当$u<0$时，$[b(1+uq)-1]^p+1=b^q$式子左负右正不成立；

当 $u$=0 时，只有 $a$=2，$p$=3，$b$=3， $q$=2 满足 $[b\ (1+uq)-1]^p+1=b^q$，用反证法可以给出证明；

当 $u>0$ 时，由 $[b\ (1+uq)-1]^p+1-b^q=0$ 可知：$b$ 是方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 的根、也是方程 $x^q-(a^p+1)=0$ 的根。

下面讨论方程 $x^q-(a^p+1)=0$ 与 $[x\ (1+uq)-1]^p+1-x^q=0$ 根的情况；这一点可以根据复变函数论的知识及阿贝尔群理论来解决；“每个 $n$ 次代数方程在复数域中有 $n$ 个根，而且只有 $n$ 个根” [5]。对于方程 $x^q-(a^p+1)=0$ 的任意一个根 $b_i$ 都存在对应的 $u_i$ 值满足方程 $[x\ (1+u_iq)-1]^p+1-x^q=0$，$u_i$ 的值可由 $b_i+c_i=a$ 按照上述方法推出。

根据阿贝尔群理论的四条公理 [3]、把一切 $u_i$ 值 $u,u_2,u_3\cdots u_i$ 所对应的各个方程 $[x\ (1+uq)-1]^p+1-x^q=0$，$[x\ (1+u_2q)-1]^p+1-x^q=0$，$[x\ (1+u_3q)-1]^p+1-x^q=0\cdots\cdots[x\ (1+u_iq)-1]^p+1-x^q=0$ 的所有根 $x$ 值的全体，在复数域中按乘法复合关系构成一个群 $\wp$；而且，把方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 的根也按同样的条件及复合规则构成一个群 $\wp_1$；在构成群时，不仅要考虑方程的根，还必须要把任意两根之间转化的元素（例如：$a_1,a_2\in\wp$，$xa_1=a_2$，$x\in\wp$），单位元（为 1），逆元以及任意两元之积等元素也考虑在内，否则不符合阿贝尔群理论的四条公理。显然 $\wp_1$ 是 $\wp$ 的子群；再分析 $\wp_1$ 与 $\wp$ 是否是同一个群呢？

由同态群的定义：“有两个群 $G$，$G'$，与一个映射 $f$: $G\to G'$，设 $x\in G$，$x'\in G'$，若满足 $(ab)'=a'b'$；则称 $f$ 为一个同态” [5]，且 $\wp_1\subseteq\wp$；可知存在映射 $\varphi$：$\wp_1\to\wp$，其中：$\varphi(x)=x$，即 $\wp_1$ 中的元素 $x$ 在 $\wp$ 中对应的元素仍为 $x$，$\varphi$ 是 $\wp_1$ 到 $\wp$ 的同态映射。

由 “一个群和它的商群同态，并且抽象地看，一个群只能和它的商群同态” （《离散数学》254 页） [6]，可知 $\wp$ 是 $\wp_1$ 的商群；由定理：“设 $G$ 为群，而 $M$ 是 $G$ 的任一个不变子群，那么必有群同态满射 $\varphi:G\to\frac{G}{M}$，其中：$\varphi(x)=xM$” [7]（也可参考《离散数学》定理 17.23），可知 $\varphi$ 是 $\wp_1$ 到 $\wp$ 的同态满射。

再由《离散数学》253 页的定理：“若 $\varphi$ 是群 $\langle G,\times\rangle$ 到群 $\langle\overline{G},\overline{\times}\rangle$ 的同态映射，那么 $\varphi$ 的

核 ker（φ）是 $G$ 的不变子群，而且，$\frac{G}{\ker(\varphi)} \cong \overline{G}$”[6]，“在同态之下，单位元映到单位元、逆元映到逆元”[5]；“$\overline{G}$ 的单位元 $\bar{e}$ 的全部原象（逆象）作成的集合 $\{x \in G \mid \varphi(x) = \bar{e}\}$ 叫做φ的核，记为 $Ker(\varphi)$”。

因为 $\wp_1$ 与 $\wp$ 的单位元都是 1 ，显然，这里讨论的映射 φ： $\wp_1 \to \wp$ 的核为 $N$={1}即“$N = \{e\}$”，根据上述定理得 $\frac{\wp_1}{N} \cong \wp$，因而 $\wp_1 \cong \wp$;即 $\wp_1$ 与 $\wp$ 是同构群。

由同构群的定义：“设两个群 $G_1$，$G_2$ 若使 $G_1$ 中任意两元 $a$，$b$ 的乘积与 $G_2$ 中的相应元的乘积对应，而且只与这个乘积对应，即 $(ab)' \to a'b'$；具有这个性质的 $G_1$ 到 $G_2$ 上的一对一的对应，称为一个同构”[5]；根据“在同构之下，一个群的单位元、逆元、子群分别对应到另一个群的单位元、逆元、子群”[5]，因为存在映射 φ： $\wp_1 \to \wp$，其中：$\varphi(x) = x$，即 $\wp_1$ 中的元素 $x$ 在 $\wp$ 中对应的元素仍是 $x$，φ 是 $\wp_1$ 到 $\wp$ 的同构映射、属于一一映射（已知 $\wp_1$ 与 $\wp$ 有一个共同元素 $b$、逆元同为 $b^{-1}$、单位元同为 1）；由此推得 $\wp_1$ 与 $\wp$ 的元素是以相等的对应关系（可逆的对应法则）一一对应的、即一一对等。

“凡一个群具有者，其同构群亦满足”[3]；这里 $\wp_1$ 与 $\wp$ 既是同构的，所有元素又是共同的，所以 $\wp_1$ 与 $\wp$ 有相同的与代数运算有关的性质。

因为满足方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 与方程组 $[x\ (1+uq)-1]^p+1-x^q=0$，

$[x\ (1+u_2q)-1]^p+1-x^q=0$，$[x\ (1+u_3q)-1]^p+1-x^q=0\cdots\cdots$

$[x\ (1+u_iq)-1]^p+1-x^q=0$ 也是按上述方法构成的群的一种与代数运算有关的性质;由于 $\wp_1$ 与 $\wp$ 是同构群，所以，$\wp_1$ 的哪些位置上的元素满足方程 $[x\ (1+uq)-1]^p+1-x^q=0$，那么，$\wp$ 中对应的那些位置上的元素也满足方程 $[x\ (1+uq)-1]^p+1-x^q=0$。同理 $\wp$ 的哪些位置上的元素满足上述方程组，则 $\wp_1$ 中对应的那些位置上的元素也满足上述方程组。

由此可知：若 $\wp_1$ 中的某个位置上的元素是由哪些位置上的元素按照代数运算而得到的，则 $\wp$ 中这个位置上的元素也是这样[8]。根据上述推理可知 $\wp_1$ 与 $\wp$ 的元素次序也相同；所以，

$\wp_1$ 与 $\wp$ 是同一个群、同一个排队集合。

由于 $\wp_1$ 与 $\wp$ 都是由方程的根 、任意两根之间转化的元素、单位元（为 1）、逆元以及任意两元之积等元素构成的，若方程组 $[x\ (1+uq)-1]^p+1-x^q=0$，

$[x\ (1+u_2q)-1]^p+1-x^q=0$，$[x\ (1+u_3q)-1]^p+1-x^q=0\cdots\cdots$

$[x\ (1+u_iq)-1]^p+1-x^q=0$ 与方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 有一个或若干个不同的根，那么 $\wp_1$ 与 $\wp$ 二者任意一个相同位置上的元素、不可能都是由某些相同位置上的二者共同的元素、按相同的代数运算而得到的；也就是说二者与代数运算有关的性质不可能完全相同；这与上述结论矛盾。所以方程组 $[x\ (1+uq)-1]^p+1-x^q=0$，

$[x\ (1+u_2q)-1]^p+1-x^q=0$，$[x\ (1+u_3q)-1]^p+1-x^q=0\cdots\cdots$

$[x\ (1+u_iq)-1]^p+1-x^q=0$ 与方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 的所有根都是一致的。

因为方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 与方程 $[x\ (1+u_iq)-1]^p+1-x^q=0$ 的次数相同，复根个数也相同；若把每一个确定的 $u_i$ 值所对应的方程 $[x\ (1+u_iq)-1]^p+1-x^q=0$ 的根 $x$ 值，也按照与上述同样的条件及复合规则构成群，即 $u,u_2,u_3\cdots u_i$ 对应的群分别是 $\wp_1$，$\wp_2$，$\wp_3\cdots\wp_i$；则同理可得：所有这些群与 $\wp$ 都有相同的与代数运算有关的性质；都是同一个群、同一个排队集合；而且方程组 $[x\ (1+uq)-1]^p+1-x^q=0$，

$[x\ (1+u_2q)-1]^p+1-x^q=0$，$[x\ (1+u_3q)-1]^p+1-x^q=0\cdots\cdots$

$[x\ (1+u_iq)-1]^p+1-x^q=0$ 与每一个确定的 $u_i$ 值所对应的方程

$[x\ (1+u_iq)-1]^p+1-x^q=0$ 的所有根都是一致的。

所以，方程 $[x\ (1+uq)-1]^p+1-x^q=0$ 的根与每一个确定的 $u_i$ 值所对应的方程 $[x\ (1+u_iq)-1]^p+1-x^q=0$ 的根 $x$ 值也都是一致的。

也就是说，方程 $[x\ (1+uq)-1]^p+1-x^q=0$，$[x\ (1+u_2q)-1]^p+1-x^q=0$，

$[x\ (1+u_3q)-1]^p+1-x^q=0\cdots\cdots$ $[x\ (1+u_iq)-1]^p+1-x^q=0$ 中的 $u_i$ 值只有一个，即 $u_i=u$；而 $u_i$ 的值可由 $b_i+c_i=a$ 按照上述方法推出，表明方程 $x^q-(a^p+1)=0$ 只有一

个根 $b$；因为 $q\geqslant 2$，$p>2$，这与“每个 $n$ 次代数方程在复数域中有 $n$ 个根，而且只有 $n$ 个根”的定理矛盾；所以，假定不成立。

由此可知：除了 $8=2^3$，$9=3^2$ 以外，$q$ 是素数，$p$ 为奇素数时，不定方程 $x^p+1=y^q$ 无其它正整数解。而且找到了只有 $8=2^3$，$9=3^2$ 满足不定方程 $x^p+1=y^q$ 的根本原因。

## 结论

由上述证明可知：不定方程 $x^p+1=y^q$，其中 $p$，$q$ 均是素数时没有（除了 $8=2^3$，$9=3^2$ 以外的）正整数解；若 $x^k+1=y^j$，$k$、$j\in N_+$ 且 $k$、$j$ 不全是素数时，有正整数解，则可化为 $(x_1^v)^p+1=(y_1^w)^q$ 的形式，$v$、$w\in N_+$，与已证明的结果矛盾；所以凯特兰猜想已完全获证。

## 参考文献

[1] 徐本顺、解恩泽著《数学猜想集》[M] 湖南科学技术出版社，1999年4月2版 8、56-57页

[2] 柯召著《关于方程 $x^2=y^n+1$》[J] 四川大学学报(自然科学版)，1962 年 1-6 页

[3] 赫克著、王元 译《代数数理论讲义》[M] 科学出版社 2005年1月 1版 14、15、18、21、47页

[4] 闵嗣鹤、严士健著《初等数论》[M] 高等教育出版社 2003年7月3 版，37、49、50、61、134页

[5] 数学手册编写组《数学手册》[M] 高等教育出版社，1979年5月 1版 2004年3月10次印 91、467页

[6] 尹宝林、何自强、许光汉、檀风琴著<<离散数学>>[M] 高等教育出版社2004.7 2 版 252-254页

[7] 《同态与不变子群》http://www.gxtc.edu.cn/jpkc/dsx/UploadFiles/jx_15.doc

[8] 张禾瑞 著《近世代数基础》[M] 高等教育出版社，1978年修订本 24-25页

# The Simple and direct proof of Catalan conjecture

Tang Zizhou Tang Shijie

(The middle school of Qie Mo County in Xinjiang 841900)

**Abstract** Has used the reduction to absurdity for Catalan conjecture , the proposition changes method, according to Abel group theory and the theory of numbers theorem simple and direct proved the conjecture 。

**Key words** Catalan conjecture ; Pythagorean Numbers theorem; the proposition changes method ; Abel group