费马大定理的简捷证明

梁增勇

前言

费马是一位法国的法官和业余数学家。1637 年，费马无意中被古希腊数学家丢番廷的算术中描述的毕达哥拉斯著作所吸引。他对能否找到毕达哥拉斯方程的不定方程的解心血来潮。

原始毕达哥拉斯方程可以表示为方程：

$$x^n + y^n = z^n$$

的正整数解。

费马在《算术》一书中解释道：不可能把一个立方数分成两个立方数，把一个四次方分成两个四次方，或者把一个高于二次方的幂分成两个相同指数的幂。在这方面，我确信我找到了一个极好的证明。不幸的是，这里的空白太小，写不下来。这个问题后来被称为“费马最后定理”。

三个多世纪以来，历史上最好的数学家一直试图证明这一点，但一无所获。1994 年，英国数学家怀尔斯（Wiles）利用现代数学方法，如模形式、Gushan-Zhicun 猜想和 Galois 群椭圆曲线的性质，间接证明了费马大定理。但他的证明长达 130 页，而且相当深奥，这显然不是费马所说的简短证明。正如费马所说，人们仍在寻求一个简洁的费马大定理证明。

该方程如果 x，y 和 z 有公因子，我们可以消除它们。那么方程就变成了

$$A^n + B^n = C^n$$

其中，$n \geq 3$,A、B 和 C 无公共因子。

第 1 个证明

费马大定理：方程

$$A^n + B^n = C^n \tag{1}$$

没有正整数解。

证　假设（1）成立，那么令 $A=C-a, B=C-b$，　可得

$$A^n=(C-a)^n= C^n -n C^{n-1}a+\ldots+ (-1)^{n-1} n Ca^{n-1}+(-1)^n a^n \tag{2}$$

$$B^n=(C-b)^n= C^n -n C^{n-1}b+\ldots+(-1)^{n-1} n C b^{n-1}+(-1)^n b^n \tag{3}$$

(2)+(3):

$$A^n+ B^n =(C^n-n C^{n-1}a+\ldots+(-1)^{n-1} n Ca^{n-1}+a^n)+(C^n-nC^{n-1}b+\ldots+(-1)^{n-1} n C b^{n-1}+(-1)^n b^n),$$

$$A^n+ B^n =2 C^n -n C^{n-1}(a+ b)+\ldots+(-1)^{n-1} n C(a^{n-1}+b^{n-1})+ (-1)^n (a^n +b^n) \tag{4}$$

由 (4) −(1)可得

$$C^n -n C^{n-1}(a+ b)+\ldots+ (-1)^{n-1} n C(a^{n-1}+b^{n-1})+ a^n +(-1)^n b^n = 0 \tag{5}$$

另外，有方程：

$$\mathrm{C}^n -\mathrm{n}\, \mathrm{C}^{n-1}\mathrm{q}+\ldots+ (-1)^{n-1} \mathrm{n}\, \mathrm{Cq}^{n-1}+(-1)^n \mathrm{q}^n = 0 \tag{6}$$

比较（5）和（6）得

$$a + b \rightarrow q,$$

$$a^2+b^2 \to q^2,$$

$$\ldots\ldots$$

$$a^n+b^n \to q^n.$$

再由定理 1 可知，如果（6）成立，必须 $q = C$ ，因此若要求（5）成立，也必须：

$$a+b = C,$$

$$a^2+b^2= C^2,$$

$$\ldots\ldots$$

$$a^n+b^n \to C^n.$$

很显然，以上的方程组是互相矛盾的（不可能同时成立）。

那么，方程（5）不可能成立，假设不为真，方程（1）也不可能成立。

定理 1. 如果

$$C^n - nC^{n-1}q+\ldots+(-1)^{n-1}nC\,q^{n-1}+(-1)^n q^n=0,$$

则必须 $C=q$.

证 因为

$$(C-q)^n = C^n - nC^{n-1}q+\ldots+(-1)^{n-1}nC\,q^{n-1}+(-1)^n q^n ,$$

则方程仅当 $C=q$ 才成立.

第 2 个证明

费马大定理：方程

$$A^n+ B^n = C^n \tag{1}$$

没有正整数解。

证 令 $C= A+ c$,

$$A^n+ B^n = (A+ c)^n$$

$$A^n+ B^n = A^n + n A^{n-1} c +\ldots+n A c^{n-1}+c^n,$$

$$B^n = n A^{n-1} c +\ldots+n A c^{n-1}+c^n,$$

$$B^n = c\left(n A^{n-1}+\ldots+n A c^{n-2}+c^{n-1}\right), \tag{2}$$

则 B 含 c, $c|B$.

令 $B = c\,k$, 代入（2）:

$$c^n k^n = c\left(n A^{n-1}+\ldots+n A c^{n-2}+c^{n-1}\right),$$

$$c^{n-1} k^n = n A^{n-1}+\ldots+n A c^{n-2}+c^{n-1},$$

$$c^{n-1}(k^n-1) = n\left(A^{n-1}+\ldots+A c^{n-2}\right) 。\tag{3}$$

那么，就要求 n 含 c^{n-1}，这是不可能的。所以方程（3）不成立，方程（2）和（1）也不成立。