

# 费尔马最后定理的证明

汪家诤<sup>1</sup>

(1995年4月10日收到)

## 摘要

(i) 我们用  $(x-b)^n + x^n = (x+a)^n$  (0.1)

来代替  $x^n + y^n = z^n$  作为费尔马最后定理(FLT)的普遍方程式。其中  $a$  及  $b$  是两个任意自然数。应用二项展开式, (0.1)可以写成

$$x^n - \sum_{r=1}^n \binom{n}{r} x^{n-r} [a^r - (-b)^r] = 0 \quad (0.2)$$

因为  $a^r - (-b)^r$  始终包含  $a+b$  作为它的因数, (0.2)可写成

$$x^n - (a+b) \sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r = 0 \quad (0.3)$$

其中  $\phi_r = [a^r - (-b)^r] / (a+b)$  对于  $r=1, 2, \dots, n$ 。都是个整数。

(ii) 令  $s$  是  $a+b$  的一个因数, 并令  $a+b = sc$ 。

我们可用  $x = sy$  来变换(0.3)成为下列(0.4)

$$(sy)^n - sc \left[ \sum_{r=1}^{n-2} \binom{n}{r} (sy)^{n-r} \phi_r + n sy \phi_{n-1} \right] = sc \phi_n \quad (0.4)$$

(iii) 将(0.4)除以  $s^2$ , 我们得

$$s^{n-2} y^n - c \left[ \sum_{r=1}^{n-2} \binom{n}{r} s^{n-r-1} y^{n-r} \phi_r + n y \phi_{n-1} \right] = \frac{c \phi_n}{s} \quad (0.5)$$

(0.5)式的左边, 是  $y$  的整系数多项式, 而右边是个常数  $c\phi/s$ 。若  $c\phi/s$  不是个整数, 那末我们不能求得能适合(0.5)的整数  $y$ , 这样FLT对这场合是对的。若  $c\phi_n/s$  是个整数, 我们可以改变  $s$  和  $c$ , 使  $c\phi_n/s =$  整数。

**关键词** 因式分解 共轭因数 互质 gcd 组合式 代数式除法 费尔马最后定理

## 一、引 论

(a) 费尔马最后定理的叙述: 方程式

$$x^n + y^n = z^n \quad (1.1)$$

其中  $n$  是大于 2 的一个自然数, 则上列方程式不存在  $x, y, z$  都不为 0 的正整数解。

(b) 二个重要限制

<sup>1</sup> 浙江大学, 杭州 310027.

(i)  $\gcd(x, y, z) = 1$

(ii) 证明FLT, 只需证明 $n$ 是个质数的场合.

(c) 费尔马的傅略, 和他的FLT

Pierre de Fermat (1601~1665)是个法国数学家. 他提出FLT 约在1637年, 他只证明了 $n=4$ 的一种情况. 即 $x^4+y^4=z^4$ 不存在 $x, y, z$ 的正整数解, 用的原则是“无限逐降法”这是他自己提出的原则(参考1).

我们知道, 任何正整数总是属于下列四种之一:  $4m, 4m+1, 4m+2, 4m+3$ . 费尔马证明了 $n=4$ , 那末由于 $x^{4m}+y^{4m}=z^{4m}$ 可以写成 $(x^m)^4+(y^m)^4=(z^m)^4$ , 所以FLT对于 $n=4m$ 也成立. 这样只剩下三种情况,  $4m+1, 4m+2, 4m+3$ 待证明.

但是由于 $4m+2=2(2m+1)$ , 所以我们要证明 $x^{4m+2}+y^{4m+2}=z^{4m+2}$ , 只需证明

$$(x^2)^{2m+1}+(y^2)^{2m+1}=(z^2)^{2m+1}.$$

现在 $4m+1, 2m+1, 4m+3$ , 它们都是奇整数. 所以我们只需证明 $n$ 是个奇质数的情况.

## 二、定理1 变数 $x, y, z$ 不能有二个相等

证 若 $z=x$ , 则方程式 $x^n+y^n=z^n$ 变成 $y=0$ . 这是违反 $x, y, z$ 都不为零的前题. 若 $z=y$ , 则 $x=0$ , 同样不行. 若 $x=y$ , 则有 $2x^n=z^n$ , 于是 $z=(2)^{1/n}x$ . 即使 $x$ 是个整数, 由这式知 $z$ 不能是个整数. 由此可知,  $x, y, z$ 三个整数是相互不同的整数. 因此FLT方程式可以写成

$$(x-b)^n+x^n=(x+a)^n \quad (0.1)$$

其中  $a$ 和 $b$ 是两个任意自然数.

## 三、三个FLT的启发式问题

(a)  $(x-1)^3+x^3=(x+1)^3$  其中  $x-1, x, x+1$ 是三个相邻整数. 于是我们有

$$x^3-3x^2+3x-1+x^3=x^3+3x^2+3x+1$$

或  $x^3-6x^2-2=0$  或  $x^3=2(3x^2+1)$

它表示 $x$ 必须是个偶数.

让我们使行变换式  $x=2y$  (3.1)

于是我们有  $(2y)^3=2[3(2y)^2+1]$

或  $8y^3-24y^2=2$  (3.2)

将(3.2)除以8, 我们得  $y^3-3y^2=\frac{1}{4}$  (3.3)

若 $y$ 是个整数, 则(3.3)的左边是个整数, 但右边是个分数 $\frac{1}{4}$ . 因此这整数 $y$ 必须不存在.

于是这偶数 $x$ 也不存在. 现在我们已经证明了对这场合FLT是真实的.

(b) 证明 $(x-1)^n+x^n=(x+1)^n$  (3.4)

它的FLT真确, 应用二项展开式

$$(x-1)^n=x^n+\sum_{r=1}^n \binom{n}{r} x^{n-r}(-1)^r$$

及 
$$(x+1)^n = x^n + \sum_{r=1}^n \binom{n}{r} x^{n-r} (1)^r$$

将上两式代入(3.4), 我们得到

$$x^n + \sum_{r=1}^n \binom{n}{r} x^{n-r} [(-1)^r - 1] = 0 \quad (3.5)$$

当 $r$ 是偶数时,  $(-1)^r - 1 = 0$ , 又当 $r$ 是奇整数时 $(-1)^r - 1 = -2$ . 让我用符号 $\sum_{r=1}^n$ 来表只对 $r$ 取奇整数之和, 我们能将(3.5)写成

$$x^n = 2 \sum_{r=1}^n \binom{n}{r} x^{n-r} \quad (3.6)$$

(3.6)显示 $x$ 必须是一个偶整数. 令

$$x = 2y \quad (3.7)$$

将(3.7)代入(3.6), 这(3.6)式成为

$$(2y)^n - 2 \left[ \sum_{r=1}^{n-4} \binom{n}{r} (2y)^{n-r} + \frac{n(n-1)}{2} (2y)^2 \right] = 2 \quad (3.8)$$

上式左边这多项式的系数有 $\text{gcd} = 2^3$ . 将(3.8)除以8, 我们得到

$$2^{n-3} y^n - \sum_{r=1}^{n-4} \binom{n}{r} 2^{n-r-2} y^{n-r} - \frac{n(n-1)}{2} y^2 = \frac{1}{4} \quad (3.9)$$

(3.9)式的左边, 是个 $y$ 的多项式, 而右边是个分数 $\frac{1}{4}$ , 这样的方程式不存在 $y$ 的整数解. 因此也不存在 $x$ 的偶数解. 由此我们已经证明(3.4)对于 $n$ 大于2的任何整数都没有整数解而不论它是奇数或偶数. 以上这个叙述是我们的重要判别原则.

(c) 证明 $(x-a)^n + x^n = (x+a)^n$  它的FLT是正确的

$$(x-a)^n + x^n = (x+a)^n \quad (3.10)$$

让我们取变换式  $x = aw$ , 则(3.10)成为

$$(aw-a)^n + (aw)^n = (aw+a)^n \quad (3.11)$$

将(3.11)两边的 $a^n$ 约去, 它成为

$$(w-1)^n + w^n = (w+1)^n \quad (3.12)$$

(3.12)与(3.4)具有同样算式, 而(3.4)我们已经证明它的FLT是对的, 所以(3.12)的FLT也是正确的. 即(3.10)也是正确的.

#### 四、一般方程 $(x-b)^n + x^n = (x+a)^n$ 的变化式

对 $(x-b)^n$ 及 $(x+a)^n$ 应用二项展开式, 我们有

$$(x-b)^n = x^n + \sum_{r=1}^n \binom{n}{r} x^{n-r} (-b)^r \quad (4.1)$$

及

$$(x+a)^n = x^n + \sum_{r=1}^n \binom{n}{r} x^{n-r} a^r \quad (4.2)$$

将(4.1)的 $(x-b)^n$ 及(4.2)的 $(x+a)^n$ 代入方程(0.1), 我们得

$$x^n - \sum_{r=1}^n \binom{n}{r} x^{n-r} [a^r - (-b)^r] = 0 \quad (4.3)$$

当  $r=2m+1, a^r - (-b)^r = a^{2m+1} - (-b)^{2m+1} = a^{2m+1} + b^{2m+1}$

$$= (a+b)(a^{2m} - a^{2m-1}b + a^{2m-2}b^2 - \dots + a^2b^{2m-2} - ab^{2m-1} + b^{2m}) \quad (4.4)$$

当  $r=2m, a^r - (-b)^r = a^{2m} - b^{2m} = (a+b)(a^{2m-1} - a^{2m-2}b + a^{2m-3}b^2$

$$- \dots + a^3b^{2m-4} - a^2b^{2m-3} + ab^{2m-2} - b^{2m-1}) \quad (4.5)$$

所以  $a^r - (-b)^r$  总是包含  $a+b$  为它的因数. 我们可以写出

$$a^r - (-b)^r = (a+b)\phi_r \quad (r=1, 2, \dots, n) \quad (4.6)$$

其中  $\phi_r (r=1, 2, 3, \dots, n)$  都是整数.

于是方程(4.3)成为

$$x^n - (a+b) \left[ \sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r \right] = 0 \quad (4.7)$$

或将它写成更有用的方程式如下

$$x^n - (a+b) \left[ \sum_{r=1}^{n-2} \binom{n}{r} x^{n-r} \phi_r + nx\phi_{n-1} \right] = (a+b)\phi_n \quad (4.8)$$

其中 
$$\phi_n = \frac{a^n - (-b)^n}{a+b} = a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1} \quad (4.9)$$

现在列出一些  $\phi_r$  表如下:

$$\phi_1 = 1, \quad \phi_2 = a - b, \quad \phi_3 = a^2 - ab + b^2$$

$$\phi_4 = a^3 - a^2b + ab^2 - b^3, \quad \phi_5 = a^4 - a^3b + a^2b^2 - ab^3 + b^4$$

$$\phi_6 = a^5 - a^4b + a^3b^2 - a^2b^3 + ab^4 - b^5$$

$$\phi_n = a^{n-1} - a^{n-2}b + a^{n-3}b^2 - a^{n-4}b^3 + \dots - a^3b^{n-4} + a^2b^{n-3} - ab^{n-2} + b^{n-1}$$

对于  $n=7$  的FLT方程式可以写成下式

$$\begin{aligned} & x^7 - (a+b) \left[ 7x^6 + \binom{7}{2}x^5(a-b) + \binom{7}{3}x^4(a^2 - ab + b^2) \right. \\ & \quad + \binom{7}{4}x^3(a^3 - a^2b + ab^2 - b^3) + \binom{7}{5}x^2(a^4 - a^3b + a^2b^2 - ab^3 + b^4) \\ & \quad \left. + \binom{7}{6}x(a^5 - a^4b + a^3b^2 - a^2b^3 + ab^4 - b^5) \right] \\ & = (a+b)(a^6 - a^5b + a^4b^2 - a^3b^3 + a^2b^4 - ab^5 + b^6) \end{aligned} \quad (4.10)$$

## 五、应用条件: $\gcd(a, b) = 1$ 弃除FLT的平庸解

当我们用  $x^n + y^n = z^n$  作为FLT的方程式时, 我们用  $\gcd(x, y, z) = 1$  以弃除平庸解  $(cx, cy, cz)$ , 若  $a$  和  $b$  有一公因数  $c$ , 那么  $a = \bar{a}c$ , 及  $b = \bar{b}c$ , 因此  $a + b = (\bar{a} + \bar{b})c$ . 从(4.7)我们有

$$x^n = (\bar{a} + \bar{b})c \sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r \tag{5.1}$$

于是 $x^n$ 包含 $c$ 作为它的因数。但 $x^n$ 是个整数，所以 $x$ 的本身必须包含 $c$ 为它的因数。令

$$x = \bar{x}c, \text{ 则 } y = x - b = \bar{x}c - \bar{b}c = (\bar{x} - \bar{b})c$$

$$z = x + a = \bar{x}c + \bar{a}c = (\bar{x} + \bar{a})c, \text{ 于是}$$

$$\gcd(x, y, z) = \gcd(\bar{x}c, \bar{y}c, \bar{z}c) = c \neq 1.$$

上式和条件 $\gcd(x, y, z) = 1$ 相背。所以我们必须有 $\gcd(a, b) = 1$ ，或写成

$$\gcd(a, b, a+b) = 1 \tag{5.2}$$

六、定理2  $\frac{a^n + b^n}{(a+b)^2}$ 是个整数，当且仅当  $a + b = n$

$$\begin{aligned} \frac{a^n + b^n}{(a+b)^2} &= \frac{a^n + b^n}{a+b} \bigg/ (a+b) = \left[ \sum_{r=1}^n a^{n-r} (-b)^{r-1} \right] \bigg/ (a+b) \\ &= (a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) / (a+b) \end{aligned} \tag{6.1}$$

现在用除法求 $(a^n + b^n)/(a+b)^2$ 。也就是求

$$\begin{array}{r} (a^{n-1} - a^{n-2}b + a^{n-3}b^2 \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) / (a+b) \\ \underline{a^{n-1} - 2a^{n-2}b + 3a^{n-4}b^3 - 4a^{n-5}b^3 + 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ a^{n-1} + a^{n-2}b \\ \hline -2a^{n-2}b + a^{n-3}b^2 \\ \underline{-2a^{n-2}b - 2a^{n-3}b^2} \\ 3a^{n-3}b^2 - a^{n-4}b^3 \\ \underline{3a^{n-3}b^2 + 3a^{n-4}b^3} \\ -4a^{n-4}b^3 + a^{n-5}b^4 \\ \underline{-4a^{n-4}b^3 - 4a^{n-5}b^4} \\ +5a^{n-5}b^4 - a^{n-6}b^5 \\ \underline{+5a^{n-5}b^4 + 5a^{n-6}b^5} \\ -6a^{n-6}b^5 + a^{n-7}b^6 \\ \dots \end{array}$$

于是，我们有

$$\frac{a^n + b^n}{(a+b)^2} = a^{n-2} - 2a^{n-3}b + 3a^{n-4}b^2 - 4a^{n-5}b^3 + 5a^{n-6}b^4 - 6a^{n-7}b^5 \tag{6.2}$$

对于 $n=7$ 作为例题，我们有

$$\frac{a^7 + b^7}{(a+b)^2} = a^5 - 2a^4b + 3a^3b^2 - 4a^2b^3 + 5ab^4 - 6b^5 + \frac{7b^6}{a+b} \tag{6.3}$$

于是(6.2)的末项必须是  $\frac{nb^{n-1}}{a+b}$  (6.4)

由于条件 $\gcd(a, b, a+b) = 1$ ，我们知道  $\frac{b^{n-1}}{a+b}$  不是个整数。由此我们有下列定理2

$\frac{a^n + b^n}{(a+b)^2}$  是一整数当且仅当  $a+b=n$ ，此时  $\frac{nb^{n-1}}{a+b} = b^{n-1}$  成为一个整数。

$$\text{令 } \phi_n = \frac{a^n + b^n}{a+b} = a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1} \quad (6.5)$$

于是  $\frac{\phi_n}{a+b}$  将是一个整数仅当  $a+b=n$ .

### 七、定理3 $(a^n + b^n)/(a+b)^3$ 不是个整数

$$a+b \left/ \begin{array}{r} a^{n-3} - 3a^{n-4}b + 6a^{n-5}b^2 - 10a^{n-6}b^3 + 15a^{n-7}b^4 - \dots \\ a^{n-2} - 2a^{n-3}b + 3a^{n-4}b^2 - 4a^{n-5}b^3 + 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots \\ \hline a^{n-2} + a^{n-3}b \\ \hline -3a^{n-3}b + 3a^{n-4}b^2 \\ \hline -3a^{n-3}b - 3a^{n-4}b^2 \\ \hline +6a^{n-4}b^2 - 4a^{n-5}b^3 \\ \hline +6a^{n-4}b^2 + 6a^{n-5}b^3 \\ \hline -10a^{n-5}b^3 + 5a^{n-6}b^4 \\ \hline -10a^{n-5}b^3 - 10a^{n-6}b^4 \\ \hline 15a^{n-6}b^4 - 6a^{n-7}b^5 \\ \hline 15a^{n-6}b^4 + 15a^{n-7}b^5 \\ \hline -21a^{n-7}b^5 \end{array} \right. \quad (7.1)$$

注意, 让我们令  $S_m = 1 + 2 + 3 + \dots + (m-1) + m$

于是有  $S_1 = 1, S_2 = 1 + 2 = 3, S_3 = 1 + 2 + 3 = 6$

$S_4 = 1 + 2 + 3 + 4 = 10$  等等

因此  $\frac{\phi_n}{(a+b)^2}$  的商可以写成

$$\frac{\phi_n}{(a+b)^2} = S_1 a^{n-3} - S_2 a^{n-4}b + S_3 a^{n-5}b^2 - S_4 a^{n-6}b^3 + \dots \\ + \dots + S_m a^{n-m-2} (-b)^{m-1} + \dots \quad (7.2)$$

最后几项的除式可以求得如下:

$$a+b \left/ \begin{array}{r} (S_{n-4})a^2b^{n-5} - (S_{n-3})ab^{n-4} + (S_{n-2})b^{n-3} \\ \dots + (n-4)a^3b^{n-5} - (n-3)a^2b^{n-4} - (n-2)ab^{n-3} - (n-1)b^{n-2} + b^{n-1} \\ \hline - (S_{n-5})a^3b^{n-5} \\ \hline (S_{n-4})a^3b^{n-5} - (n-3)a^2b^{n-4} \\ \hline (S_{n-4})a^3b^{n-5} + (S_{n-4})a^2b^{n-4} \\ \hline - (S_{n-3})a^2b^{n-4} + (n-2)ab^{n-3} \\ \hline - (S_{n-3})a^2b^{n-4} - (S_{n-3})ab^{n-3} \\ \hline (S_{n-2})ab^{n-3} - (n-1)b^{n-2} \\ \hline (S_{n-2})ab^{n-3} + (S_{n-2})b^{n-2} \\ \hline - (S_{n-1})b^{n-2} + b^{n-1} \end{array} \right.$$

将上列各除式结合在一起, 我们可以得到

$$\frac{\phi_n}{(a+b)^2} = a^{n-3} - S_2 a^{n-4}b + S_3 a^{n-5}b^2 - S_4 a^{n-6}b^3 + S_5 a^{n-7}b^4 \\ + (S_{n-4})a^2b^{n-5} - (S_{n-3})ab^{n-4} + S_{n-2}b^{n-3} + \frac{-S_{n-1}b^{n-2} + b^{n-1}}{a+b}$$

让我们研究最后一个分式

$$\frac{- (S_{n-1})b^{n-2} + b^{n-1}}{a+b} = \frac{(-S_{n-1} + b)b^{n-2}}{a+b} \quad (7.3)$$

我们知道 $a+b$ 与 $b^{n-2}$ 是互质的,所以我们可以只考虑上列分数的一部分内容.

$$\frac{-S_{n-1}+b}{a+b}, \text{ 其中 } S_{n-1}=1+2+3+\dots+(n-2)+(n-1)=\frac{n(n-1)}{2}$$

因为我们有 $a+b=n$ ,所以我们有

$$\frac{-S_{n-1}+b}{a+b} = \frac{-\frac{n(n-1)}{2}+b}{n} = \frac{-n(n-1)}{2n} + \frac{b}{a+b} = \frac{-(n-1)}{2} + \frac{b}{a+b} \quad (7.4)$$

因为 $n \geq 3$ 及 $n$ 是一个奇质数, $\frac{n-1}{2}$ 是一个整数,但 $\frac{b}{a+b}$ 不是个整数.所以它们的和不是个整数.

于是我们已证明了定理3,如下:

**定理3**  $\frac{a^n+b^n}{(a+b)^3} = \frac{\phi_n}{(a+b)^2}$  不是个整数.

### 八、若 $a+b$ 是一个质数,则FLT对这场合正确

(A)  $a+b \neq n$

当 $a+b$ 是个质数,我们可用变换式 $x=(a+b)w$ .将 $x=(a+b)w$ 代入(4.8),我们得到

$$(a+b)^n w^n - (a+b) \left[ \sum_{r=1}^{n-2} \binom{n}{r} (a+b)^{n-r} w^{n-r} \phi_r + n(a+b)w\phi_{n-1} \right] = (a+b)\phi_n \quad (8.1)$$

在上列方程式中的左边的系数有 $\text{gcd}=(a+b)^2$ .将上式除以 $(a+b)^2$ ,我们得到

$$(a+b)^{n-2} w^n - \left[ \sum_{r=1}^{n-2} \binom{n}{r} (a+b)^{n-r-1} w^{n-r} \phi_r + n w \phi_{n-1} \right] = \frac{\phi_n}{a+b} \quad (8.2)$$

(8.2)式的左边,是个 $w$ 的整系数多项式,及右边是个分数 $\phi_n/(a+b)$ ,如在(6.4)中所示,当 $a+b \neq n$ 时这样的方程式没有整数解.于是对这场合FLT正确.

(B)  $a+b=n$

若 $n$ 是个质数,除了 $\binom{n}{n}=1$ 以外,所有 $\binom{n}{r}$ 都以 $n$ 为其因数.方程式(8.1)可以写成

$$n^n w^n - n \left[ \sum_{r=1}^{n-2} \binom{n}{r} n^{n-r} w^{n-r} \phi_r + n^2 w \phi_{n-1} \right] = n \phi_n \quad (8.3)$$

在(8.3)的左边,各系数有一 $\text{gcd}=n^3$ ,将(8.3)除以 $n^3$ ,我们得到

$$n^{n-3} w^n - \left[ \sum_{r=1}^{n-2} \binom{n}{r} n^{n-r-2} w^{n-r} \phi_r + w \phi_{n-1} \right] = \frac{\phi_n}{n^2} \quad (8.4)$$

在(8.4)式的左边,是 $w$ 的整系数多项式,但在(8.4)的右边是个分数,不是整数,所以(8.4)没有整数解.即FLT对这场合正确.

### 九、若 $a+b$ 是个偶数,则FLT正确

令 $a+b=2^m B$ ,其中 $B$ 是 $2^m$ 的共轭因数及 $B$ 是个奇整数,即 $B$ 不再包含因数2.

首先,我们必须讨论 $a$ 和 $b$ 的奇偶性.

(A) 若 $a$ 和 $b$ 都是偶数,则 $cd(a,b,a+b)=2$ 它与条件 $\gcd(a,b,a+b)=1$ 矛盾,不可!

(B) 若 $a$ 和 $b$ 有不同奇偶性,则 $a+b$ 不能是个偶数.这出于我们问题之外

(C) 于是 $a$ 和 $b$ 必须都是奇整数.

令  $a=2l+1$  及  $b=2m+1$ , 则  $a+b=2(l+m+1)$

其中  $l+m+1$  可以是个任意整数.我可令

$$a+b=2^{n_0} p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t} = 2^{n_0} E \quad (9.1)$$

其中

$$E = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t} \quad (9.2)$$

$p_1, p_2, \dots, p_t$  都是奇质数,  $n_1, n_2, \dots, n_t$  都是自然数. 将(9.1)代入(4.8), 我们得到

$$x^n - 2^{n_0} E \left[ \sum_{r=1}^{n-2} \binom{n}{r} x^{n-r} \phi_r + nx \phi_{n-1} \right] = 2^{n_0} E \phi_n \quad (9.3)$$

于是 $x$ 必须包含2为它的因数. 我们令 $x=2^m w$ 作为变换式, 则变换后的方程为

$$2^{mn} w^n - 2^{n_0} E \left[ \sum_{r=1}^{n-2} \binom{n}{r} 2^{m(n-r)} w^{n-r} \phi_r + n 2^m w \phi_{n-1} \right] = 2^{n_0} E \phi_n \quad (9.4)$$

如果我们选取整数 $m$ , 使  $m \geq \frac{n_0}{n-1}$ , 那末就有  $mn \geq n_0 + m$ . 于是(9.4)式的左边的各系数有最大公因数  $\gcd = 2^{m+n_0}$ . 将(9.4)除以  $2^{m+n_0}$ , 得

$$w^n 2^{mn-m-n_0} - E \left[ \sum_{r=1}^{n-2} \binom{n}{r} 2^{m(n-r)-m} w^{n-r} \phi_r + n w \phi_{n-1} \right] = \frac{E \phi_n}{2^m} \quad (9.5)$$

(9.5)式的左边是 $w$ 的整数系数的多项式, 而右边是个分数. 这样的方程式不存在一个整数 $w$ 来适合(9.5), 于是FLT对这个场合正确.

## 十、若 $a+b$ 包含一个因数 $p^t$ (其中 $p$ 是个质数, $t$ 是个自然数)则FLT正确

证 令  $a+b=p^t B$ , 其中 $B$ 是个整数, 它是 $p^t$ 在 $a+b$ 中的共轭因数. 于是这问题的FLT方程式成为

$$x^n - p^t B \left[ \sum_{r=1}^{n-2} \binom{n}{r} x^{n-r} \phi_r + nx \phi_{n-1} \right] = p^t B \phi_n \quad (10.1)$$

由于(10.1),  $x$ 必须包含 $p^s$ 为它的一个因数, 其中  $1 \leq s \leq t$ . 令  $x=p^s y$ . 将它代入(10.1)我们有

$$(p^s y)^n - p^t B \left[ \sum_{r=1}^{n-2} \binom{n}{r} (p^s y)^{n-r} \phi_r + n (p^s y) \phi_{n-1} \right] = p^t B \phi_n \quad (10.2)$$

现在我们选 $s$ , 使  $s \geq \frac{t}{n-1}$ , 则  $ns \geq t + s$ . 将(10.2)的等号两边都除以  $p^{t+s}$ , 则(10.2)成为

$$p^{s(n-t-s)} y^n - B \left[ \sum_{r=1}^{n-2} \binom{n}{r} p^{s(n-r)-s} y^{n-r} \phi_r + n y \phi_{n-1} \right] = B \phi_n / p^s \quad (10.3)$$

在(10.3)的左边,是 $y$ 的整系数的多项式,在它的右边是个分数 $B\phi_n/p^s$ .这样的方程式不存在 $y$ 的整数解,所以FLT对这问题是正确的.

### 十一、结 论

现在我们已经证明了FLT问题的以下的各种场合:(1)  $a=b$ , (2)  $a+b$ 是个质数, (3)  $a+b$ 是个偶数, (4)  $a+b$ 包含一个因数 $p^t$ , 其中 $p$ 是任何质数, 及 $t$ 是个任意自然数, 于是我们完全证实了FLT问题.

**注意1** 我们知道费尔马只证明了 $n=4$ 的场合, 欧拉(L. Euler)证明了 $n=3$ 的场合, 而他的证明尚有一个漏洞, 德利息列脱(G. L. Dirichlet)在1828年证明了 $n=5$ 的场合, 等等, 我们知道: 质数 $n$ 可以无限大, 所以我们若用已知值的整数( $>2$ )来证明FLT是不能完全证明的. 在这篇论文中, 我们用 $n$ 是个任何质数.

**注意2** 在这篇论文中我们用 $n$ 表示任何质数, “我们用一个分数 $\frac{n}{a+b}$ , 它仅当 $n=a+b$ 时它才是个整数 $n/(a+b)=1$ ”.

### 参 考 文 献

- [ 1 ] Raulo Ribenboim, 《费尔马最后定理的13份讲稿》. Springer-Verlog, New York(1979)
- [ 2 ] M. Harold, 《费尔马最后定理 (一种具有发展式引导的代数数论)》, Springer-Verlag (1977).

## The Proof of Fermat's Last Theorem

Wong Chiahe

(Zhejiang University, Hangzhou 310013, P. R. China)

### Abstract

(i) Instead of  $x^n+y^n=z^n$ , we use

$$(x-b)^n+x^n=(x+a)^n \tag{0.1}$$

as the general equation of Fermat's Last Theorem (FLT), where  $a$  and  $b$  are two arbitrary natural numbers. By means of binomial expansion, (0.1) can be written as

$$x^n - \sum_{r=1}^n \binom{n}{r} x^{n-r} [a^r - (-b)^r] = 0 \tag{0.2}$$

Because  $a^r - (-b)^r$  always contains  $a+b$  as its factor, (0.2) can be written as

$$x^n - (a+b) \sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r = 0 \tag{0.3}$$

where  $\phi_r = [a^r - (-b)^r] / (a+b)$  are integers for  $r=1, 2, 3, \dots, n$ .

(ii) Let  $s$  be a factor of  $a+b$  and let  $(a+b)=sc$ . We can use  $x=sy$  to trans-

form (0.3) to the following (0.4)

$$(sy)^n - sc \left[ \sum_{r=1}^{n-2} \binom{n}{r} (sy)^{n-r} \phi_r + nsy\phi_{n-1} \right] = sc\phi_n \quad (0.4)$$

(iii) dividing (0.4) by  $s^2$ , we have

$$s^{n-2}y^n - c \left[ \sum_{r=1}^{n-2} \binom{n}{r} s^{n-r-1}y^{n-r}\phi_r + ny\phi + ny\phi_{n-1} \right] = \frac{c\phi_n}{s} \quad (0.5)$$

On the left side of (0.5), there is a polynomial of  $y$  with integer coefficients and on the right side there is a constant  $c\phi_n/s$ . If  $c\phi_n/s$  is not an integer, then we cannot find an integer  $y$  to satisfy (0.5), and then FLT is true for this case. If  $c\phi_n/s$  is an integer, we may change  $s$  and  $c$  such that  $c\phi_n/s \neq$  an integer.

**Key words** factorization, cofactor, relative prime, gcd, combination, algebraic division, Fermat's Last Theorem