費馬最後定理 (一)

梁子傑
香港道教聯合會青松中學

大約在 1637 年，當法國業餘數學家費馬 (Pierre de Fermat, 1601-1665) 読
讀古希臘名著《算術》時，在書邊的空白地方，他寫下了以下的一段說話：「將
個立方數分成兩個立方數，一個四次冪分成兩個四次冪，或者一般地將一個高
於二次冪的數分成兩個相同次冪，這是不可能的。 我對這個命題有一個美妙
的證明，這裏空白太小，寫不下。」換成現代的數學術語，費馬的意思就即
是：「當整數n>2時，方程x^n+y^n=z^n
沒有整數解。」

費馬當時相信自己已發現了對以上命題的一個數學證明。可惜的是，
當費馬死後，他的兒子為他收拾書房
時，並沒有發現費馬的「美妙證明」。

費馬這個命題並不難理解，如果大家用計算機輸入一些數字研究一下，
(注意：費馬的時代並未發明任何電子
計算工具，) 那麼就會「相信」費馬這
個命題是正確的。由於費馬在生時提
出的數學命題，都逐步被實證或否
定，就只剩下這一要看正確，但無法
證明的命題未能獲證，所以數學家就稱
它為「費馬最後定理」。

說也奇怪，最先對「費馬最後定理」
的證明行出第一步的人，就是費馬本人。
有人發現，在費馬的書信中，曾經
提及方程x^n+y^n=z^n
無正整數解的證明。

費馬首先假設方程x^n+y^n=z^n
有解這個想法不成立，亦即是說方程
x^n+y^n=z^n
無整數解。

又由於方程x^n+y^n=z^n
無解的，方程x^n+y^n=(z^n)
亦必定無解。否則將
後者的解寫成x^n+y^n=(z^n)
就會變
成前一個方程的解，從而導出矛盾。

由此可知，當n=4時，「費馬最後定理」
成立。

為「費馬最後定理」踏出另一步的
人，是瑞士大數學家歐拉 (Leonhard Euler, 1707-1783)。他利用了複數a+b
的立方根必定可以再次寫成
方程x^n+y^n=z^n
無解的，但由於歐拉在他的證明中，在沒有
足夠論据的支持下，認為複數a+b
的立方根必定可以再次寫成
a+b
的立方根，因此他的證明未算圓滿。

歐拉證明的缺憾，又過了近半個
世紀，才由德國數學家高斯 (Carl Friedrich Gauss, 1777-1855) 成功地補
充。 同時，高斯更為此而引進了「複
整數」的概念，即形如a+b√-k
的複數，其中k為整數，a和b為整數。

1823年，七十一歲高齡的法國數
學家勒讓德 (Adrien Marie Legendre, 1752 - 1833) 提出了「費馬最後定理」
的證明。 1828年，年青的德
國數學家狄利克雷 (Peter Gustav Lejeune Dirichlet, 1805-1859) 亦獨立地
1839 年，另一位法國人拉梅 （Gabriel Lamé, 1795 -1870）就證到 $n = 7$。1847 年，拉梅更宣稱他已完成了「費馬最後定理」的證明。拉梅將 $x^n + y^n = z^n$ 分解成 $(x + ζ^k y)(x + ζ^{k+1} y)\ldots(x + ζ^{n-1} y)$，其中 $ζ = \cos\left(\frac{2π}{n}\right) + i \sin\left(\frac{2π}{n}\right)$，即方程 $r^n = 1$ 的複數根。如果 $x^n + y^n = z^n$，那麼拉梅認為每一個 $(x + ζ^k y)$ 都是 $n$ 次幂乘以一個複數單位，從而可導出矛盾，並能證明「費馬最後定理」成立。不過，拉梅的證明很快便證實為無效，這是因為拉梅所構作的複數，並不一定滿足「唯一分解定理」。

為了解決未能滿足「唯一分解定理」所帶來的問題，德國數學家庫默爾 （Ernst Edward Kummer, 1810 -1893）就提出了「理想數」的想法。已知 $n$ 爲一個質數。假設 $ζ = \cos\left(\frac{2π}{n}\right) + i \sin\left(\frac{2π}{n}\right)$，即方程 $r^n = 1$ 的複數根，則稱

$$a_0 + a_1ζ + a_2ζ^2 + \ldots + a_{n-1}ζ^{n-1}$$

為「分圓整數」，其中 $a_i$ 爲整數。並非每一個分圓整數集合都滿足「唯一分解定理」，但如果能夠加入一個額外的「數」，使到該分圓整數集合滿足「唯一分解定理」，則稱該數為「理想數」。

庫默爾發現，當 $n$ 爲一些特殊的質數時，（他稱之為「正規質數」），就可以利用「理想數」來證明「費馬最後定理」在這情況下成立。

庫默爾證明了當 $n < 100$ 時，「費馬最後定理」成立。德國商人沃爾夫斯凱爾 （Paul Friedrich Wolfskehl, 1856 -1908）在他遺囑上訂明，如果有人能夠在他死後一百年內證實「費馬最後定理」，則可以獲得十萬馬克的獎金。自此，「費馬最後定理」就吸引到世上不同人仕的注意，不論是數學家或者是業餘學者，都紛紛作出他們的「證明」。在 1909 至 1934 年間，「沃爾夫斯凱爾獎金」的評審委員會就收到了成千上萬個「證明」，可惜的是當中並沒有一個能夠成立。自從經過了兩次世界大戰之後，該筆獎金的已大幅貶值，「費馬最後定理」的吸引力和熱潮，亦慢慢地降低了。如果能夠滿足「唯一分解定理」，那麼當 $ζ = ab$ 時，我們就確信可以找到兩個互質的整數 $a$ 和 $b$，使得 $a = u^r$ 和 $b = v^s$ 了。但如果未能滿足「唯一分解定理」，以上的推論就不成立了。例如：$6^2 = 2 \times 3 \times (1 - \sqrt{5}) \times (1 + \sqrt{5})$，而 $a + b\sqrt{5}$ 的複數整數中，$2, 3, (1 + \sqrt{5})$ 和 $(1 - \sqrt{5})$ 都是互不相同的質數。換句話說，形如 $a + b\sqrt{5}$ 的複數整數，並不一定滿足「唯一分解定理」。

其實，研究「費馬最後定理」有甚麼好處呢？首先，就是可以滿足人類的求知慾。 「費馬最後定理」是一道簡單易明的命題，但是它的證明卻並非一般人所能理解，這已經是一個非常之有趣的事情。其次，在證明該定理的過程之中，我們發現了不少新的數學現象，產生了不少新的數學工具。同時亦豐富了我們對數學，特別是數論的知識。有數學家更認為，「費馬最後定理」就好像一隻會生金蛋的母雞，由它所衍生出来的數學理論，例如：「唯一分解定理」、「分圓整數」、「理想數」等等，都是人類思想中最珍貴的產物。

(to be continued next issue)
Problem Corner

We welcome readers to submit solutions to the problems posed below for publication consideration. Solutions should be preceeded by the solver’s name, home address and school affiliation. Please send submissions to Dr. Kin Y. Li, Department of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon. The deadline for submitting solutions is October 1, 1999.

Problem 86. Solve the system of equations:
\[
\begin{cases}
\sqrt{3x} \left( 1 + \frac{1}{x+y} \right) = 2 \\
\sqrt{7y} \left( 1 + \frac{1}{x+y} \right) = 4\sqrt{2}.
\end{cases}
\]
(Source: 1996 Vietnamese Math Olympiad)

Problem 87. Two players play a game on an infinite board that consists of 1x1 squares. Player I chooses a square and marks it with an O. Then, player II chooses another square and marks it with a X. They play until one of the players marks a row or a column of 5 consecutive squares, and this player wins the game. If no player can achieve this, the game is a tie. Show that player II cannot prevent player I from winning. (Source: 1995 Israeli Math Olympiad)

Problem 88. Find all positive integers n such that \(3^{n-1} + 5^n - 1 \div 3^n + 5^n\). (Source: 1996 St. Petersburg City Math Olympiad)

Problem 89. Let O and G be the circumcenter and centroid of triangle ABC, respectively. If R is the circumradius and r is the inradius of ABC, then show that \(OG \leq \sqrt{R(R-2r)}\). (Source: 1996 Balkan Math Olympiad)

Problem 90. There are n parking spaces (numbered 1 to n) along a one-way road down which n drivers \(a_1, a_2, ..., a_n\) drive. Each driver has a favorite parking space and parks there if it is free; otherwise, he parks at the nearest free place down the road. (Two drivers may have the same favorite space.) If there is no free space after his favorite, he drives away. How many lists \(a_1, a_2, ..., a_n\) of favorite parking spaces are there which permit all of the drivers to park? Here \(a_i\) is the favorite parking space number of \(d_i\). (Source: 1996 St. Petersburg City Math Olympiad)

***************

Solutions

Problem 81. Show, with proof, how to dissect a square into at most five pieces in such a way that the pieces can be reassembled to form three squares no two of which have the same area. (Source: 1996 Irish Math Olympiad)

Solution. SHAM Wang Kei (St. Paul's College, Form 4).

In the following diagram, A and B can be reassembled to form a 20x20 square and E and F can be reassembled to form a 12x12 square.

Other recommended solvers: CHAN Man Wai (St. Stephen's Girls' College, Form 4).

Problem 82. Show that if \(n\) is an integer greater than 1, then \(n^4 + 4^n\) cannot be a prime number. (Source: 1977 Jozef Kurschak Competition in Hungary)

Solution. Gary NG Ka Wing (STFA Leung Kau Kui College, Form 6) and NG Lai Ting (True Light Girls' College, Form 6).

For even \(n\), \(n^4 + 4^n\) is an even integer greater than 2, so it is not a prime. For odd \(n > 1\), write \(n = 2k - 1\) for a positive integer \(k > 1\). Then \(n^4 + 4^n = (n^2 + 2^n)^2 - 2^n + 1 = (n^2 + 2^n - 2k)^2 + 2^{2k-2} + 1\). Since the smaller factor \(n^2 + 2^n - 2k = (n-2^{k-1})^2 + 2^{2k-2} > 1\), \(n^4 + 4^n\) cannot be prime.

Other recommended solvers: FAN Wai Tong (St. Mark's School, Form 6), LAW Ka Ho (Queen Elizabeth School, Form 6), SHAM Wang Kei (St. Paul's College, Form 4), SIU Tsz Hang (STFA Leung Kau Kui College, Form 4) and TAM Siu Lung (Queen Elizabeth School, Form 6).

Problem 83. Given an alphabet with three letters a, b, c, find the number of words of \(n\) letters which contain an even number of a’s. (Source: 1996 Italian Math Olympiad).

Solution I. CHAO Khek Lun Harold (St. Paul's College, Form 4) and GARY NG KA WING (STFA Leung Kau Kui College, Form 6).

For a nonnegative even integer \(2k \leq n\), the number of \(n\) letter words with \(2k\) a’s is \(C_{2k}^n 2^{n-2k}\). The answer is the sum of these numbers, which can be simplified to \((2 + 1)^n + (2 - 1)^n)/2\) using binomial expansion.

Solution II. TAM SIU LUNG (Queen Elizabeth School, Form 6).

Let \(S_n\) be the number of \(n\) letter words with even number of a’s and \(T_n\) be the number of \(n\) letter words with odd number of a’s. Then \(S_n + T_n = 3^n\). Among the \(S_n\) words, there are \(T_{n-1}\) words ended in a and \(2S_{n-1}\) words ended in b or c. So we get \(S_n = T_{n-1} + 2S_{n-1}\). Similarly \(T_n = S_{n-1} + 2T_{n-1}\). Subtracting these, we get \(T_n - T_{n-1} = S_{n-1} - T_{n-1}\). So \(S_n - T_n = S_1 = T_1 = 2 - 1 = 1\). Therefore, \(S_n = (3^n + 1)/2\).

Problem 84. Let \(M\) and \(N\) be the midpoints of sides \(AB\) and \(AC\) of \(\triangle ABC\), respectively. Draw an arbitrary line through \(A\). Let \(Q\) and \(R\) be the feet of the perpendiculars from \(B\) and \(C\) to this line, respectively. Find the locus of the intersection of the lines \(QM\) and \(RN\) as the line rotates about \(A\).

Solution. CHAO KHEK LUN HAROLD (St. Paul's College, Form 4).

Let \(S\) be the midpoint of side \(BC\). From midpoint theorem, it follows \(\angle MSN = \angle ABC\). Since \(M\) is the midpoint of the hypotenuse of right triangle \(AQW\), we get \(\angle BAC = \angle AQM\). Similarly, \(\angle CAR = \angle ARN\).

If the line intersects side \(BC\), then either \(\angle MNQ = \angle QPR\) or \(\angle MPN + \angle QPR = 180^\circ\). In the former case, \(\angle MPN = 180^\circ - \angle QPR - \angle QPR = 180^\circ - \angle AQM - \angle QPR\).
\[ \angle ARN = 180^\circ - \angle BAC. \] So \[ \angle MPN + \angle MSN = 180^\circ. \] Then, \( M, N, S, P \) are concyclic. In the latter case, \[ \angle MPN = \angle PQR + \angle PRQ = \angle AQR + \angle ARM = \angle BAC = \angle MSN. \] So again \( M, N, S, P \) are concyclic. Similarly, if the line does not intersect side \( BC \), there are 2 cases both lead to \( M, N, S, P \) concyclic. So the locus is on the circumcircle of \( M, N, S \). Conversely, for every point \( P \) on this circle, draw line \( MP \) and locate \( Q \) on line \( MP \) so that \( QM = AM \). The line \( AQ \) is the desired line and \( AQ, RN \) will intersect at \( P \).

Comments: The circle through \( M, N, S \) is the nine point circle of \( \triangle ABC \). As there are 4 cases to deal with, it may be better to use coordinate geometry.

Other commended solvers: FAN Wai Tong (St. Mark's School, Form 6) and TAM Siu Lung (Queen Elizabeth School, Form 6).

Problem 85. Starting at \((1, 1)\), a stone is moved in the coordinate plane according to the following rules:

(a) Form any point \((a, b)\), the stone can be moved to \((2a, b)\) or \((a, 2b)\).

(b) From any point \((a, b)\), the stone can be moved to \((a-b, b)\) if \(a > b\), or to \((a, b-a)\) if \(a < b\).

For which positive integers \(x, y\), can the stone be moved to \((x, y)\)? (Source: 1996 German Math Olympiad)

Solution. Let \(gcd(x, y)\) be the greatest common divisor (or highest common factor) of \(x\) and \(y\). After rule (a), the gcd either remained the same or doubled. After rule (b), the gcd remain the same. So if \((x, y)\) can be reached from \((a, b)\), then \(gcd(x, y) = 2^n gcd(a, b)\) for a nonnegative integer \(n\). If \(a = b = 1\), then \(gcd(x, y) = 2^n\).

Conversely, suppose \(gcd(x, y) = 2^n\). Of those points \((a, b)\) from which \((x, y)\) can be reached, choose one that minimizes the sum \(a + b\). If \(a + b\) is even, then \((x, y)\) can be reached from \((2a, 2b)\) or \((a, 2b)\) with a smaller sum. So \(a + b\) is odd. If \(a > b\) (or \(a < b\)), then \((x, y)\) can be reached from \((a-b, 2b)\) or \((a, a+b)\) with a smaller sum. So \(a = b\).

Since \(2^n = gcd(x, y)\) is divisible by \(a = gcd(a, b)\) and \(a\) is odd, so \(a = b = 1\). Then \((x, y)\) can be reached from \((1, 1)\).

Olympiad Corner

(continued from page 1)

Problem 4. Determine all pairs \((a, b)\) of integers with the property that the numbers \(a^2 + 4b\) and \(b^2 + 4a\) are both perfect squares.

Problem 5. Let \(S\) be a set of \(2n+1\) points in the plane such that no three are collinear and no four concyclic. A circle will be called good if it has 3 points of \(S\) on its circumference, \(n-1\) points in its interior and \(n-1\) in its exterior. Prove that the number of good circles has the same parity as \(n\).

Equation \(x^4 + y^4 = z^4\)

Recall the following theorem, see Mathematical Excalibur, Vol. 1, No. 2, pp. 2, 4 available at the web site www.math.ust.hk/mathematical_excalibur/

Theorem. If \(u, v\) are relatively prime positive (i.e. \(u, v\) have no common prime divisor), \(u > v\) and one is odd, the other even, then \(a = u^2 - v^2\), \(b = 2uv\), \(c = u^2 + v^2\) give a primitive solution of \(a^2 + b^2 = c^2\) (i.e. a solution where \(a, b, c\) are relatively prime). Conversely, every primitive solution is of this form, with a possible permutation of \(a\) and \(b\).

Using this theorem, Fermat was able to show \(x^4 + y^4 = z^4\) has no positive integral solutions. We will give the details below.

It is enough to show the equation \(x^4 + y^4 = w^2\) has no positive integral solutions. Suppose \(x^4 + y^4 = w^2\) has positive integral solutions. Let \(x = a\), \(y = b\), \(w = c\) be a positive integral solution with \(c\) taken to be the least among all such solution. Now \(a, b, c\) are relatively prime for otherwise we can factor a common prime divisor and reduce \(c\) to get contradiction. Since \((a^2)^2 + (b^2)^2 = c^2\), by the theorem, there are relatively prime positive integers \(u, v\) (one is odd, the other even) such that \(a^2 = u^2 - v^2\), \(b^2 = 2uv\), \(c = u^2 + v^2\). Here \(u\) is odd and \(v\) is even for otherwise \(a^2 \equiv -1 \pmod{4}\), which is impossible.

Now \(a^2 + v^2 = u^2\) and \(a, u, v\) are relatively prime. By the theorem again, there are relatively prime positive integers \(s, t\) such that \(a = s^2 - t^2\), \(v = 2st\), \(u = s^2 + t^2\). Now \(b^2 = 2uv = 4st(s^2 + t^2)\). Since \(s^2, t^2, s^2 + t^2\) are relatively prime, we must have \(s = e^2\), \(t = f^2\), \(s^2 + t^2 = g^2\) for some positive integers \(e, f, g\). Then \(e^4 + f^4 = g^2\) with \(g \leq g^2 = s^2 + t^2 = u \leq u^2 < c\). This contradicts the choice \(c\) being least. Therefore, \(x^4 + y^4 = w^2\) has no positive integral solutions.

IMO1999

This year the International Mathematical Olympiad will be held in Romania. Based on their performances in qualifying examinations, the following students are selected to be Hong Kong team members:

Chan Ho Leung (Diocesan Boys' School, Form 7)
Chan Kin Hang (Bishop Hall Jubilee School, Form 5)
Chan Tsz Hong (Diocesan Boys’ School, Form 7)
Law Ka Ho (Queen Elizabeth School, Form 6)
Ng Ka Wing (STFA Leung Kau Kui College, Form 6)
Wong Chun Wai (Choi Hung Estate Catholic Secondary School, Form 6)

Both Chan Kin Hang and Law Ka Ho were Hong Kong team members last year. This year the team leader is Dr. Tam Ping Kwan (Chinese University of Hong Kong) and the deputy leader will be Miss Lok Mee Lin (La Salle College).

Corrections

In the last issue of the Mathematical Excalibur, the definition of power given in the article Power of Points Respect to Circles should state "The power of a point \(P\) with respect to a circle is the number \(d^2 - r^2\) as mentioned above." In particular, the power is positive when the point is outside the circle. The power is 0 when the point is on the circle. The power is negative when the point is inside the circle.