神奇的拉丁方与欧拉猜想（一）

翁林宸　彭小令　方开泰

1. 引言——下一个费马问题的候选者

从人类开始观察和认识自然，对数学的思考和追求就没有停止过。一些早期的数学家在洞察当时现象的过程中提出了自己基于直觉的猜想，而看似朴素易懂的结论，却可能需要接下来几个世纪数学家们前仆后继地努力，不断地发展和运用新的理论才能证明或推翻它们。这些看上去简单直白的问题，却开启或深深地影响了看似风马牛不相及的研究领域。最后不禁令人感叹，在数学世界中的无限奇妙。

1637 年法国数学家费马在阅读《算术》（*Arithmetica*），这本出自古希腊数学家丢番图的著作时，提出了他的伟大猜想：当 $n > 2$ 时方程 $x^n + y^n = z^n$ 无正整数解，后来成为闻名世界的费马大定理。

以费马大定理为主题的纪念邮票（Doménech, 2019）[1]

如此简洁易懂的算式，却引众多数学家竞折腰。18 世纪瑞士数学家欧拉仅仅给出了 $n = 3$ 的证明；19 世纪德国数学家高斯也终因证而不得选择放弃；20

[1] Doménech, F. (2019). Fermat and the greatest problem in the history of mathematics. *BBVA OpenMind*. https://www.bbvaopenmind.com/en/science/leading-figures/fermat-and-the-greatest-problem-in-the-history-of-mathematics/.

世纪德国数学家希尔伯特被劝去破解它时，他却说自己不愿意杀死这只会下金蛋的鹅。

希尔伯特之所以这么说，是因为在对费马大定理长达 3 个多世纪的艰辛研究中，推动了数学许多领域的发展，如扩充了“整数”的概念；扩展了“无穷递降法”和虚数的应用；德国数学家库默尔（Eduard Kummer）因此提出了“理想数”并开创了现代数学分支——代数数论，等等。即使在费马大定理被证明之后的 2008 年，这只鹅仍然在非对称加密领域孵出了“椭圆加密算法”，并应用于今日大行其道的比特币。

而它最引人注目的一个金蛋，无疑是 20 世纪 90 年代英国裔美国数学家怀尔斯[2]和他的学生泰勒（Richard Taylor）[3]关于费马大定理的证明。当中怀尔斯历时 8 年，最终在泰勒的帮助下通过代数里的伽罗瓦表示，建立了椭圆曲线与自守形式的对应。它表明谷山 - 志村 - 韦伊猜想在一类特殊情形下（即被称为半稳定的椭圆曲线）是成立的，因而实现费马大定理的证明。这样间接的证明方式，揭示了现代数学中不同领域之间的深刻联系，可能也是费马当初无论如何都想象不到的结局。

在欣赏费马大定理和它身后的数学世界之际，《量子》杂志（*Quanta Magazine*）的特约作家，美国数学家和新闻记者克拉瑞奇（Erica Klarreich）通过描绘一座神秘莫测的桥，深情地展示了她眼里的数学之美。桥的一边连接着数论中最简单的一类方程，即丢番图方程。它是一些变量、指数和系数的组合，且只允许解以整数形式存在。对于椭圆曲线而言，它的左右两边分别是 y^2 和一些最高次幂为 3 的变量组合，例如 $y^2 = x^3 + 4x + 7$。桥的另一边是分析中的一种特殊函数——自守形式，它和荷兰画家艾舍尔（Maurits Escher）的画一样，具有某种重复和对称性。这座桥即是著名的朗兰兹纲领，它连接着数学海洋中看似毫不相关的领域。许多数学问题在桥的一侧似乎很困难，但把它当转移到桥的另一侧时却能迎刃而解。正是通过这座桥，怀尔斯和泰勒将费马大定理转化为了一个和自守形式相关的问题，从而利用它的性质完成证明。最后他们的一系列工作，以两篇论文的形式发表在《数学年鉴》（*Annals of Mathematics*），它是数学世界最负盛名的期刊之一。

1994 年 2 月在美国数学协会（MAA）旗下的《聚焦》（*Focus*）杂志上面，英国裔美国数学家和科学作家德夫林（Keith Devlin）报道了费马大定理终于被解决的新闻。同时他也提到，如果一个研究主题想要成为下一个费马问题，

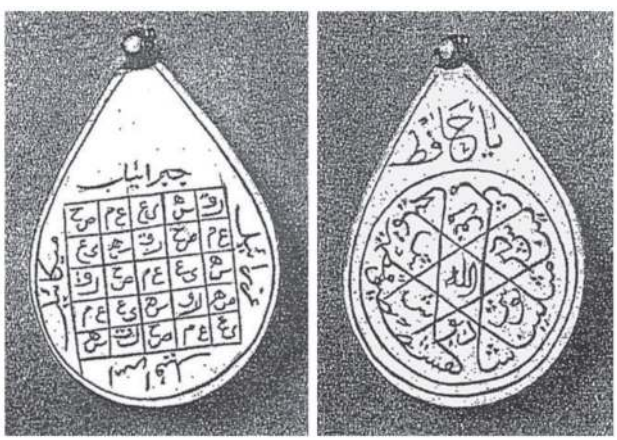
[2] 怀尔斯赢得 1995 年到 1996 年间沃尔夫奖（被誉为数学领域内的最高奖之一）和 1997 年柯尔数论奖（被视为数论领域内的最高奖）以及 1998 年菲尔兹奖银质奖章（被誉为数学领域内的最高奖之一。因为当时怀尔斯已经超过菲尔兹奖只授予 40 岁及以下数学家的规定，但是国际数学联盟 (IMU) 破例为他颁发了菲尔兹特别奖作为致敬）还有 2016 年阿贝尔奖（被誉为数学领域内的最高奖之一）。

[3] 泰勒赢得 2002 年柯尔数论奖，后来又在 2015 年荣获数学突破奖（被视为科学界的奥斯卡奖，分为生命科学，基础物理和数学三个领域），亦是该奖项的首届得主之一。

它必须形式简单而又容易描述，以便外行理解。但是最终可能需要使用艰深的数学方法，并且经过长年累月的努力才能得到彻底解决。德夫林在评论中讨论了各种各样的候选者，包括赫赫有名的哥德巴赫猜想、孪生素数猜想和梅森素数猜想、冰雹猜想以及他的最爱——矩形砖问题。1995 年美国数学家马伦（Gary Lee Mullen）也提出了他心目中的下一个费马问题：关于正交拉丁方的素数幂猜想。在古老的拉丁方世界里，漫长的探索旅程先后吸引着包括欧拉在内的一系列数学家的极大兴趣。而且当中不断涌现出的全新问题，也和其它很多数学领域产生了奇妙联系。那么它将是另一只下金蛋的鹅吗？让我们从充满神秘色彩的拉丁方说起。

2. 拉丁方的前世今生

早期有关拉丁方的记录似乎可以追溯至公元前 1000 年，它和幻方经常一起出现在某些阿拉伯和印度族群的护身符和仪式上。拉丁方和幻方代表了人类早期对一些特殊排列组合的关注。拉丁方要求将不同的符号排列在方阵中使得各行各列的符号都不相同；而幻方则要求填充进方阵的数字满足行和、列和甚至主对角线上的和都相等。人们很自然地认为这些特殊排列的矩阵应该具有某种神奇的魔力，比如早期的拉丁方护身符和幻方护身符被认为是可以对抗邪恶的灵魂，或是表达对神的崇敬等等。在中世纪关于魔法和拉丁方的书籍中，它们常常出现在一些奇特的装饰中，下图展示了在中东最古老的城市大马士革发现的银护身符，其中一面是拉丁方，另一面是七位沉睡者的名字，传说从公元 250 年开始，他们在一个山洞里沉睡了 200 年。



在大马士革发现的银护身符（MacDonald, 1912; Seligmann, 1914）[4]

[4] MacDonald, D. B. (1912). Description of a silver amulet. *Zeitschrift für Assyriologie und Vorderasiatische Archäologie*, 26(1-3):267–269. Seligmann, S. (1914). Das siebenschläfer-amulett (mit einem beitrage von erich graefe.) mit 7 abbildungen. *Der Islam*, 5(4):370–388.

除了宗教，拉丁方的身影也出现在了艺术领域。康沃尔郡圣马根教堂的铜板上曾经出现了一个拉丁方，它将四个单词按照不同的方式进行排列，然后得到了一首四行诗，用来纪念死于 1709 年的巴塞特（Hanniball Basset）：

Shall	wee	all	dye
Wee	shall	dye	all
All	dye	shall	we
Dye	all	wee	shall

按照拉丁方排列的古诗（Wilson and Watkins, 2013）[5]

从中我们不禁也能感受到，拉丁方的排列方式在语言艺术中也有一定的妙用。

尽管这些有趣的方阵大小不同，它们在排列上的共同特点是每个元素在每行中刚好出现一次，在每列中亦是如此。将行和列包含的元素数量称为阶数，可给出拉丁方的定义：

定义 1.

拉丁方（*Latin square, LS*）：n 阶拉丁方是一个 $n \times n$ 的方阵，其中它的元素由 n 种不同符号代表，并且满足每个元素都只能在每行和每列分别出现一次。

在 18 世纪初期或更早，它们也经常被用于休闲娱乐之中。例如，一个古老的扑克牌游戏需要将一组 16 张的扑克牌排列成 4 × 4 的阵列。其中每行和每列都包含着 A, K, J, Q 四个点数，甚至连每条主对角线上都是如此，并且搭配黑桃、红桃、草花、方块四种花色，使得点数和花色的每个组合正好出现一次。实际上，它甚至提出了一个比单纯地构造拉丁方更高的要求。在不考虑对角线的情况下，这也已经涉及到一个全新的概念，即现在为人们所知的相互正交拉丁方。

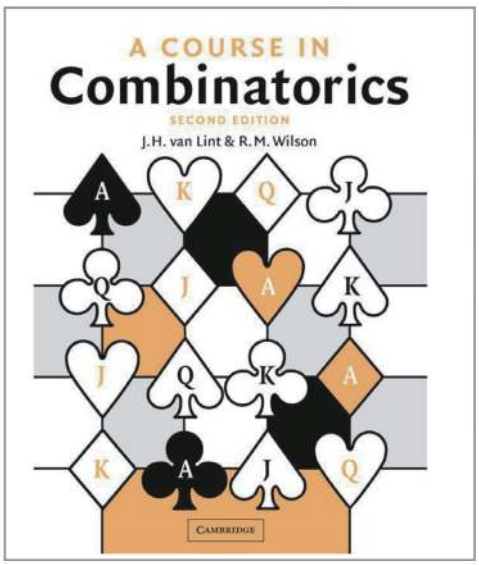
定义 2.

相互正交拉丁方（*mutually orthogonal Latin squares, MOLS*, 下面简称正交拉丁方）：设 A 和 B 是两个 n 阶拉丁方，a_{ij} 和 b_{ij} 分别表示 A 和 B 中的第 i 行和第 j 列元素。对于 A 和 B 来说，如果其中任何有序对 (a_{ij}, b_{ij}) 都不相同，则称它们是正交的。

因此，若将两个拉丁方叠加成一个以 (a_{ij}, b_{ij}) 作为元素的 n 阶方阵，那么一共

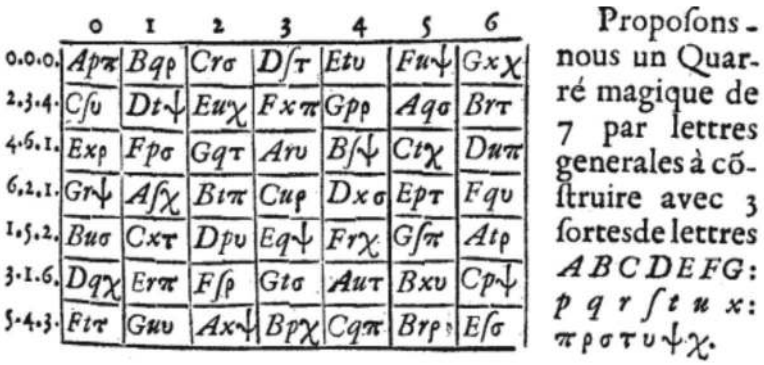
[5] Wilson, R. and Watkins, J. J. (2013). *Combinatorics: ancient & modern*. OUP Oxford.

存在 n^2 个元素，而且它们都只能分别出现一次。值得一提的是，印度尼西亚裔荷兰数学家，1996 年欧拉奖[6]得主范 • 林特（Jack van Lint）和美国数学家威尔逊（Richard Michael Wilson）在他们 2001 年所写的第二版书《组合数学教程》（*A Course in Combinatorics*）里，也将这款游戏作为这本经典著作的封面。



基于正交拉丁方的扑克牌游戏（van Lint and Wilson, 2001）[7]

当然我们需要知道，能够同时满足正交性质的拉丁方可能不止两个。例如，法国数学家和物理学家索沃尔（Joseph Sauveur）在他 1710 年发表的论文中展示了三个相互正交的 7 阶拉丁方。



Sauveur 的三个 7 阶正交拉丁方 (Sauveur, 1710)[8]

[6] 欧拉奖，被视为组合数学领域内的最高奖。

[7] van Lint, J. H. and Wilson, R. M. (2001). *A course in combinatorics*. Cambridge university press, 2 edition.

[8] Sauveur, J. (1710). Construction générale des quarrés magiques. *Mémoires de l'Academie Royales des Sciences*, pages 92–138.