Mathematical Culture

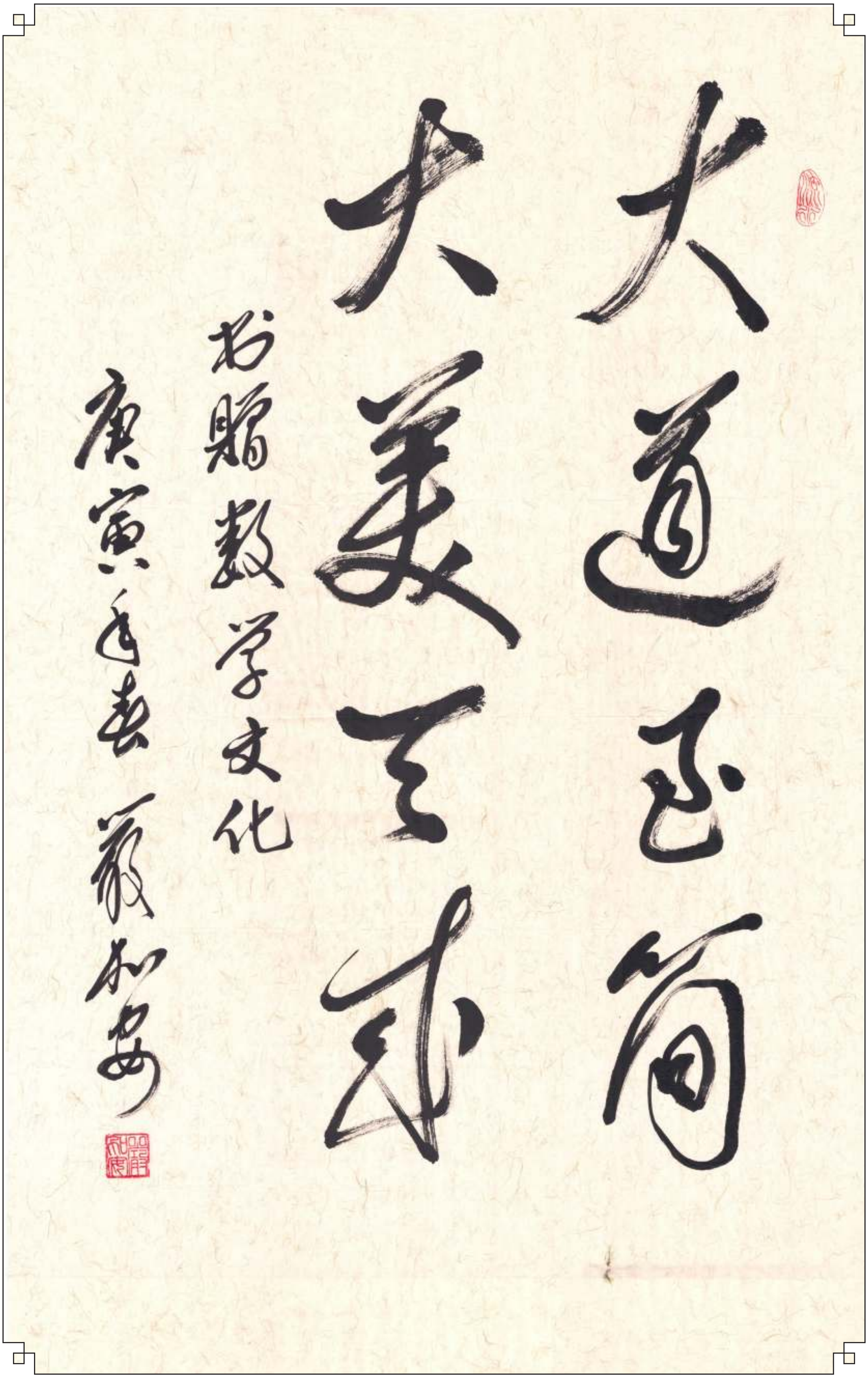
数学文化

冯·诺伊曼：因为他世界更加美好

- ★ 布拉格天文钟的数学原理
- ★ 作家笔下的数学与数学家
- ★ 十位伟大的数学家
- ★ 美国的数学推广月
- ★ 我读《数学恩仇录》
- ★ 谈数学职业
- ★ 数学与选举

2010/第1卷第2期

ISSN：2070－545X



中国科学院院士，著名数学家严加安题词

编委的话

关于【数学文化】期刊的一些我见我思

时代背景与创刊理念

廿一世纪初十年代，新中国建国业已一甲子，改革开放亦已卅年，经济上的蓬勃进展，成绩斐然，举世共睹。但是也到了亟待转型才能更上层楼的时候。而教育是立国之根基，是创新、知识型经济的命脉。这也正是数学教育工作者为国为民大有为的时代。我觉得我们所要开拓的期刊的理念就是为我们数学教育工作者提供一个相互切磋，深切研讨，共策群力，共勉互励的平台与园地；它将帮助我们在数学与文明的认知与修养上力求精进。

数学与理性文明

概括来说，理性文明乃是世代相承，人类认知大自然的成果与精华。宇宙中的事物现象是极其繁复多样的，但是它的本质与内在规律却又是既精且简的；可以说宇宙的至善、至美在于其“至精”以“至简”形式所展现的精简合一。自然科学世代相承所致力者，就是由表及里，由繁至简地探索本质，精益求精；而所用的基本方法就是定量分析与定性分析；其中数理分析是最具有洞察力的认知方法。所以自古到今，数学——特别是基础数学——在理性文明中一直是核心，扮演着重要的角色。

数学教育

基础数学教育大体可以分为普及和精英这样两个层面，而且两者应当配合互补，相辅相成。前者在于培训一般学生认识问题和解决问题的能力；而后者则在于启发与提升高材生解析思维的素质与能力，使他们能够成长为文明、科技上承先启后、继往开来的中坚力量。再者，基础数学是数学中最为简朴精要，也是最为易懂好用者。在初高中阶段则是至为重要的启蒙与奠基；在大一、大二阶段则是提升、深入和拓展其广阔之应用。基础数学教育是启蒙心智，培养人才的核心与重点。在廿一世纪的竞争中，一个国家的总体国力之强弱，将愈来愈取决于上述两个层面及两个阶段的基础数学教育的优劣。它是一个现代强国极为根本的基本建设，而此事的主导因素则取决于其数学教育工作者的素质与总体实力。唯有做好承先启后，才能发展、释放人口大国的人才潜力，才能展现波澜壮阔的继往开来。

数学教育工作者的任务与素养

要在人口众多的中国，革新和创造上述基础数学教育事业，我们数学教育工作者所要肩负的任务是巨大的。它对于献身于这一事业的教育者的学识和素养，也有很高的要求。他们不但要对于基础数学的精要和来龙去脉有简朴精到的认知；也要对于数学在理性文明中所扮演的核心角色有深入的理解。唯有如此，才能把基础数学教得平实近人，朴实精到，深入浅出，引人入胜。我们期望中华儿女的精英要有海阔天空，顶天立地的气概，以承先启后，继往开来为志趣。我等献身于教育工作者当然也应有此素养。最后，教育工作者还要有不争朝夕之长短，但求世代之永昌的抱负。

本人觉得，上述三者，就是我们对所要创建的期刊的期望，让我们同心协力做好播种与耕耘。希望大家以此共勉互励。

项武义
2010年于柏克利加州大学

从右至左：邓明立，罗懋康，贾朝华，汤涛，刘建亚，张智民，
蔡天新。左一是山东大学数学院鲁统超教授。

主　办　香港 Global Science Press
沙田新城市中央广场第一座 1521 室

《数学文化》旨在发表高质量的传播数学文化的文章；主要面向广大的数学爱好者。

本期刊欢迎投稿，来稿请寄：
Math.Cult@gmail.com; 或mc@global-sci.org

本刊欢迎订阅
订阅联络代理：北京中科进出口有限责任公司
电话：010-84039343转633；传真：010-84038202
电邮：periodical@bjzhongke.com.cn (中国)
info@global-sci.org (海外)
开户账号：中国银行金宝街支行
一行账户:810907911408091001

本期刊欢迎教育界，出版界，科技界的广告
本期刊网站：http://www.global-sci.org/mc/
本期出版时间：2010年7月

Contents | 目录

计算所三室上世纪六十年代初合影。二排左起第十二人为张克明，左十三为冯康。

冯康

—— 一位杰出数学家的故事（连载二）

汤涛 姚楠 / 文

那是一个英雄辈出的年代，
也是一段激情燃烧的岁月，
锋芒初现，再到带领团队奋力攻坚，
他开始为中国的计算数学踏开先河，
也开始为计算数学的未来运筹帷幄，
他习惯昼夜奋战，
也沉醉热火朝天，
他用澎湃的心赋予了时代最美的颜色……

第三章 火红年代

1945年抗战胜利后，一直在国外负责采购工作的大哥冯焕回到了重庆，冯康一家人终于再次聚到了一起。

这时的冯康虽然可以重新站立，但由于卧床久了，身体还处于虚弱的恢复期。尽管家人团聚让冯康的内心充满了欢喜，然而欢喜之外也平添了些许不安。敏感而细心的冯康察觉到由于家中人口增多，经济负担也随之加重。他并不想因为自己身体还没有完全恢复，需要照顾，而继续成为家人的负担。于是，他开始尝试寻找一些工作。他觉得自己必须工作。

1945年9月，经过中央大学介绍，冯康被在抗战中西迁至重庆北碚的复旦大学数理系聘为助教。1946年8月，随着西迁的众多高校纷纷迁回原址，冯康也随复旦大学迁回上海。不久后，他又经人推荐到北京担任清华大学物理系助教。一年半后，冯康转入清华大学数学系担任助教。

由此，冯康开始走上了深入钻研数学之路。

恩师喜相逢

“西山苍苍，东海茫茫”。1947 年初，冯康来到了中国著名的高等学府——清华大学任教。美丽优雅的清华园既是冯康神往已久的地方，也是冯康成就数学家梦想开始的地方。

在清华浓郁的学术氛围中，冯康结束了孤身一人的自学阶段。他不断地参加数学讨论班，拓展视野，更有幸师从陈省身、华罗庚等中国当代知名数学家，近距离聆听名家的亲身教诲。

1947 年到 1948 年，陈省身先生担任当时在南京的中央研究院数学研究所所长期间，曾经去北京清华大学主持过数学讲习班。热爱数学的冯康慕名参加了陈先生的讲习班。后来，中央研究院数学研究所迁往台湾，陈省身就转到美国芝加哥大学任教。

1948 年 12 月，地处北京西郊的清华大学已经先期解放。不久，整个北京城也和平解放。北京到处是花团锦簇与歌声笑语，而此时的冯康却静静地沉浸在数学研究的王国里。这是他期待已久的祥和与稳定，这种气氛可以让他全心地投入到数学领域的研究中。

冯康开始从基础数学的研究做起，他最初研究工作集中在殆周期拓扑群理论。他以其坚实的基础理论知识和良好的研究素养解决了极小殆周期群的表征问题，初步展露他的数学才能。

那段时间里，潜心研究拓扑群理论的冯康对外面世界似乎并没有太多的关心，然而 1950 年 3 月 16 日《人民日报》一篇“数学家华罗庚回国”的消息却令他激动不已。

华罗庚，中国解析数论、矩阵几何学、典型群、自守函数论等多方面研究的创始人和开拓者，世界著名数学家。他的许多数学科研成果，如“华氏定理”、“怀依—华不等式”、“华氏不等式”、“普劳威尔—加当—华定理”、“华氏算子”、“华—王方法”等在国际上均得以华氏命名。美国著名数学家贝特曼著文称华罗庚为“中国的爱因斯坦”、“足够成为全世界所有著名科学院院士”。芝加哥科学技术博物馆把华罗庚列为当今世界 88 位数学伟人之一。

早在 1946 年，华罗庚与两位鼎鼎大名的科学家吴大猷、曾昭抡一起被国民政府选派赴美考察。1946 年 9 月，华罗庚离开上海前往美国，先在普林斯顿高等研究所担任访问教授，后又被伊利诺大学聘为终身教授。

新中国成立的鞭炮锣鼓，敲响了华罗庚教授的爱国赤子之心。1950 年 3 月

冯康在北京第一个工作的地方，清华园。他在这里也得遇恩师华罗庚。

冯康曾于上世纪五十年代留学莫斯科斯捷克洛夫数学研究所

16 日，华罗庚留下一封慷慨激昂的万言长信，毅然带领家人回到祖国。“梁园虽好，非久居之乡……为了国家民族，我们应当回去。”至今，这些铿锵的话语仍回响在许多爱国学子的耳旁。

归去来兮！华罗庚归国的壮举不仅对冯康是个很大的鼓舞，更令他兴奋不已的是，华罗庚不但回到祖国，更回到美丽的清华园，担任清华大学数学系的主任。天涯咫尺，在冯康看来，他不仅有机会与崇敬的数学大师共同探讨数学难题，更可以面对面与数学大师交流共事。

事实证明，在接下来的几年间，华罗庚对冯康在数学领域的研究产生了巨大的影响。华罗庚成为引领冯康走进数学梦花园的重要师长。

华罗庚回到清华大学不久，受中国科学院院长郭沫若的邀请开始筹建数学研究所。直至 1952 年 7 月中国科学院数学研究所成立时，华罗庚出任中科院数学研究所第一任所长。

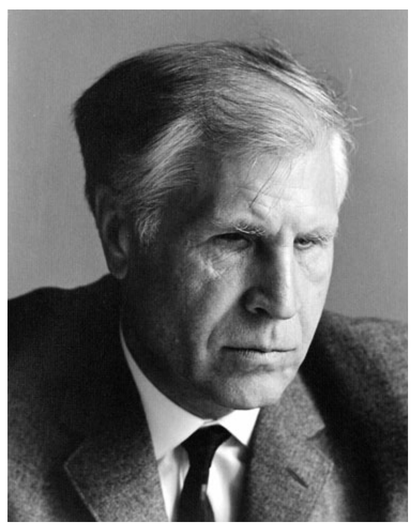
1951 年 3 月，数学研究所正在组建之时，在数学领域已经初显才华的冯康就被选调到研究所任助理研究员。

不久，作为新中国成立后第一批被选派到苏联留学的研究生，冯康又前往苏联莫斯科斯捷克洛夫（Steklov）数学研究所进修。斯捷克洛夫（1864-1926）是前俄国数学物理学派的创始人，主要从事热传导、旋转物理的平衡和静电问题的研究。他于 1921 年在圣彼得堡大学创立了物理数学研究所。斯捷克洛夫去世之后，研究所就以他的名字命名。八年后，数学部分从该所中分离出来，形成了现在的斯捷克洛夫数学所，并全面开展纯粹数学与应用数学各方面的研究工作。数学研究所的主要部分于 1940 年移到莫斯科，但圣彼得堡的分部依然存在。该所集中了前苏联最好的数学家，其中有许多具有国际声望。最近证明了庞加莱猜想的数学怪杰佩雷尔曼脱离数学界之前一直在位于圣彼得堡的斯捷克洛夫研究所工作。

苏联，这是一个可以勾起无数中国人复杂情感的国家。尽管今天，苏联作为国家的名字已经不复存在，然而停留在许多中国人心中那段中苏友谊的记忆却依然无法抹去。五十年代，中苏关系正处于“蜜月期”，作为第一个承认并与新中国建交的国家，苏联代表了中国美好的前进方向。高喊着“向苏联老大哥”学习的口号，中国在政治、经济、科技、文化和教育各方面都全力追赶着苏联的步伐。

1951 年，冯康来到了托尔斯泰的故乡。冯康深知这次留苏，并不能沉醉于他的文学梦想，而是追求他的数学理想。

到苏联后，冯康师从苏联著名的盲人数学家彭特亚金 (Pontryagin)。



彭特亚金（1908 - 1988），
冯康留学时的老师。

彭特亚金13岁那年，因一次汽炉的意外爆炸而双目失明，后来母亲帮助他树立起坚强的人生信念，他靠母亲在旁边读书给他听坚持学习数学，每次听完课后，立刻集中复习并加以熟记。他21岁毕业于莫斯科大学，28岁便成为莫斯科大学教授，31岁当选为苏联科学院的通讯院士。彭特亚金专攻拓扑群与拓扑几何学，他在数学上的最大贡献是拓扑学和最优控制理论。彭特亚金因其杰出的数学成就，曾获得罗巴切夫斯基奖，曾三次被授予列宁勋章，更获得社会主义劳动英雄金星奖章。在人们的眼中，彭特亚金出身社会下层，又双目失明，却传奇般地成了一代数学名家，简直就是一个奇迹。而他个人勤奋的励志故事更成为激励许多数学学子奋斗的榜样。

在去苏联留学之前，冯康对彭特亚金的数学研究工作有过一些了解。当他了解到彭特亚金作为盲人数学家的传奇经历后，或许是同样饱尝过身体残疾与疾病的折磨，冯康对彭特亚金更是崇拜有加。在他的心中，彭特亚金是一个数学上的英雄。

能够得到心目中数学英雄大师的亲自指点，冯康觉得确实是极其难得的机会。与彭特亚金在一起学习数学的日子更是冯康记忆中最美丽的一段时光。

然而，这种美好的时光延续得并不长久，不到一年，冯康的脊椎结核病又复发了。于是冯康只好住进莫斯科第一结核病院。

尽管冯康留苏的大部分时光都是在病榻上度过的，然而对数学有着敏锐嗅觉的他却很快地捕捉到苏联数学研究领域最活跃的分支——广义函数。

住院期间，他坚持通过大量阅读来广泛地涉猎了解苏联数学家的研究成果。他接触了彭特亚金的老师——苏联数学家、苏联科学院院士亚历山德罗夫（Aleksandrov）一些关于数论的著作，同时他也毫不隐讳地阐明自己对大师著作的一些观点。冯康说，真正让他钦佩的苏联数学家是被誉为“苏联数学大神”的柯尔莫哥洛夫（Kolmogorov）。实现了将概率论公理化的柯尔莫哥洛夫，在算法复杂性、随机数学、动力系统乃至于湍流理论等方面也取得了很大成功。柯尔莫哥洛夫因其工作的广泛性，不仅对数学学科，而且对物理学科也作出了重大贡献，这恐怕在二十世纪的科学家中也是不多见的。不但他本人获得了沃尔夫奖，他的学生阿诺德（V. Arnold）、盖尔范德（I. Gelfand）、辛赖（Y. G. Sinai）也都先后获得了沃尔夫奖。

病榻上，冯康除了获得了数学知识的增长，俄语也取得了突飞猛进的进步。据他后来说，这得益于他每天和俄罗斯女护士们的交谈。

柯尔莫哥洛夫（1903 - 1987），二十世纪最伟大的数学家之一，也是冯康最佩服的数学家。

1953年，在苏联先进的医疗条件和精心的护理下，经过一年多的治疗，冯康的脊椎结核病终于痊愈了。然而，他也不得不结束在苏联的学习，提前回国。

若干年后，冯康再次听到彭特亚金的消息是得知他卷入苏联科学界反犹太人的风暴，至此他觉得与当年的“恩师”走上了一条南辕北辙的道路，他大呼一声：“我爱我师，我更爱真理”，英雄的神话破灭了，绽放在心中的红梅花儿也凋谢了。

锋芒初显露

尽管冯康留苏的大部分时光都是在病榻上度过的，然而对数学有着敏锐嗅觉的他却很快地捕捉到苏联数学研究领域最活跃的分支——广义函数。广义函数是和物理有着密切联系的数学，在他认为，也是具有生命力的数学。

历史上第一个广义函数是由英国物理学家保罗·狄拉克引进的，他为了陈述量子力学中某些量的关系引入了德尔塔函数，而按20世纪前所形成的经典数学概念是无法理解这样奇怪的函数的。然而物理学上一切点量，如点质量、点电荷、偶极子、瞬时打击力、瞬时源等物理量用它来描述不仅方便、物理含义清楚，而且当它被当做普通函数参加运算，如对它进行微分和傅里叶变换，将它参与微分方程求解等所得到的数学结论和物理结论是吻合的。这个函数虽然行之有效，但缺乏

巩固的数学基础。后来法国数学家劳伦·席瓦兹（Laurent Schwatz）用泛函分析观点为德尔塔函数建立了一整套严格的理论，即广义函数论，恰恰弥补了这一缺陷。

冯康留苏期间，正是苏联广义函数理论盛行并异常活跃的时期，其领军人物便是盖尔范德，他也是那位冯康最钦佩的数学大师柯尔莫哥洛夫的弟子。盖尔范德是一位出生在乌克兰的苏联著名数学家，他在数学、数学物理及生物学等方面都取得了重要的成就，特别是在泛函分析上更有自己的独到专长，曾获1978年的沃尔夫奖。当时在莫斯科大学担任教授的盖尔范德经常会在莫斯科大学举办广义函数的研讨班，这种学术的思想碰撞给冯康带来了很大的启发与影响。

中国计算机事业的发展，最初孕育就是在冯康所工作的中国科学院数学研究所。而对于中国计算机事业初始发展作出重要贡献的也正是与冯康结下深厚师缘的华罗庚。

从苏联回国后，冯康继续在数学研究所担任助理研究员。此时他的工作兴趣全部集中在广义函数的研究上。

1955年，冯康将盖尔范德关于广义函数的文章翻译发表在刚刚创刊的《数学进展》上，题为“广义函数论”。这篇文章被公认为是国内介绍广义函数方面最具影响力的文章。文章发表后，引起了《数学进展》的创办人、也是时任《数学进展》主编的华罗庚的注意，华罗庚也由此对广义函数产生了极大的兴趣。

作为冯康心中敬佩的恩师，华罗庚对冯康在广义函数方面的研究大加赞赏。那个时候，人们经常会听到华罗庚在数学所举办的全国性广义函数讨论班上称赞冯康，他不但会引述一些冯康关于广义函数的说法，也会表扬冯康每次都能把他布置的问题做得很好。

熟悉华罗庚的人都知道他性格有些“专横霸道”，对待学生非常严厉，他很少去表扬别人，但对冯康却是例外。此时，冯康在学术上和工作中也尽显锋芒。

1956年冯康在数学研究所期间也曾给新分配的大学生们办讨论班，教习题课。那个时候冯康对学生要求也很严厉，批评学生不留情面，学生们都很敬畏他。

在华罗庚的启发引导下，冯康继续在梅林（Mellin）变换方面深入广义函数的研究。1957年，冯康在《数学进展》上发表了题为“广义函数的泛函对偶关系”的论文。同年，他还在《数学学报》上发表了另一篇题为“广义梅林变换”的论文。关于广义函数论文的发表标志着冯康的数学研究工作经过牛刀小试，已经初见成果。他所建立的广义函数空间的对偶定理和广义梅林变换，对于微分方程和解析函数论都有很大的应用，后来更加被广为流传。

冯康在广义函数方面的研究体现出一个数学家敏锐的嗅觉、非凡的眼光和极高的鉴赏能力，冯康也由此开始逐步走向成熟。

新中国成立以后，随着经济的逐步恢复，中国开始着手制定宏伟的经济建设发展目标。国家深知经济建设离不开科学技术的发展，于是针对中国科技工作发展薄弱的现状，1956年，在

刚刚建立中科院数学研究所时的华罗庚和他的学生们

计算所三室首任主任徐献瑜教授，
去年刚过百年华诞。

国务院总理周恩来的亲自领导下制定了《十二年科技规划》。这是建国以来国家制定的第一个科技规划，规划中将计算技术、半导体、电子学和自动化列为四项紧急措施重点发展，并提出立即筹建研究机构。

中国计算机事业的发展，最初孕育就是在冯康所工作的中国科学院数学研究所。而对于中国计算机事业初始发展作出重要贡献的也正是与冯康结下深厚师缘的华罗庚。

1946 年的情人节，当世界上第一台电子计算机 ENIAC 在美国宾夕法尼亚大学宣布问世，震撼全球，引起了全球科学工作者的极大关注。科学家们关注的焦点不仅在于 ENIAC 未来将如何改变世界，而在于那位被称为具有“天才大脑”的美国数学家冯·诺依曼的参与设计。不出所料，在接下来的几年，这位“电子计算机之父”在开发计算机的设计与制造的同时，也开创了现代科学计算的一片新天地。

当时正在美国学习考察的华罗庚亲历了这种科技的变革，也敏锐地发现数学发展的新方向，这段经历为他回国后开创中国的计算机事业奠定了重要基础。

1952 年，华罗庚筹建了数学研究所。1956 年，他又领衔担任国家《十二年科技规划》中计算技术和数学规划组的专家。同年 6 月，他牵头从中国科学院、第二机械工业部十局（后来的四机部）、军委总参三部、国防部五院（后来的七机部）和高等院校几个方面抽调干练的科技力量，从事计算技术研究所的筹备工作。1956 年 8 月 25 日，国务院正式批准成立中国科学院计算技术研究所筹备委员会，华罗庚出任主任委员，从此，中科院计算技术研究所诞生。

计算技术研究所成立初期，国内懂计算机专业的人员还很少，因此培训中国第一批计算技术的专业队伍迫在眉睫。计算所通过与清华、北大合作，抽调数学系四年级的学生及一部分刚刚大学毕业的大学生，办了计算机与计算数学两个训练班。这个训练班一共办了四期，共培养出 600 多人，不但充实了计算所自身的力量，也为很多大学培养了教学和科研的骨干。当时，冯康虽然还没有调到计算所工作，但他已经到计算所在北大办的培训班讲课。冯康讲课用的教材是苏联数学家米赫林写的《数学物理中的直接方法》。与冯康同在培训班讲课的教师还有清华大学的孙念增讲程序设计，北京大学的胡祖炽讲数值分析，张世龙讲无线电原理，何国伟讲微分方程数值解。其中胡祖炽在 1950 年末出版的《计算方法》是中国最早的一本计算方法教材，使得中国早期的计算数学和计算科学研究者受益匪浅。

冯康他自身通晓物理和工程，而纯数学的素养又使他不同于别的应用数学家。计算数学犹如一片全新的天空，可以让他没有任何阻碍，不受任何限制地任意驰骋。

在北大的课室中，有许多聆听冯康讲课的学子日后都成为与冯康共事的骨干。黄鸿慈，也是有限元方法早期的研究者之一，后来与冯康一起共事了三十多年，成为冯康重要的助手。黄鸿慈从香港培正中学毕业后，和很多爱国青年一样，回到了新中国念大学。培正中学是当时香港以中文为主的中学，曾任培正中学校长的林子丰先生后来创办了香港浸会学院（1990 年代改名为香港浸会大学）和香港浸会医院。由培正中学走出的学生后来成就了众多著名的专家学者，包括诺贝尔奖获得者，菲尔兹奖获得者和多位香港大学校长，这在两岸三地的中学里也算一个奇迹。

黄鸿慈回忆当年在北大听冯康讲课的情景，他说虽然冯康的课只讲了一个学期，但是让大家受益匪浅。通过这门课程，冯康引导大家利用变分方法解决数学物理的方程，这其中就包括了有限元概念的雏形。冯康的重要影响力在于他带领大家认识到了变分原理是一个方向。

而就在这一时期，冯康的数学研究领域也从纯数学转移到应用数学。数学领域一向有纯数学与应用数学之分。前者以研究数学自身的规律为目标，从精美的数学抽象中深化人们对客观世界的认识，努力攀登数学金字塔的最高峰。后者则致力于生产实践中大

量实际问题的解决，旨在通过建模、计算、运筹、优化、统计等数学工具寻找解决问题的办法。作为应用数学分支之一的计算数学，是随着电子计算机出现而兴起的一门应用性极强的学科，需要懂得实际应用背景及掌握交叉学科的知识。

当时的计算技术研究所非常需要具备数学、物理和工程方面的坚实基础又了解实际应用背景的学术带头人。冯康的大学学习经历，留苏的纯数学研究经历，以及多年的教学和研究工作，都使他成为最佳人选。对于冯康来说，计算数学是一个全新领域的工作。他自身通晓物理和工程，而纯数学的素养又使他不同于别的应用数学家。计算数学犹如一片全新的天空，可以让他没有任何阻碍，不受任何限制地任意驰骋。

据三室的同事回忆说，冯康和张克明的关系非常好，两个人的配合也相得益彰。关键时刻，张更会挺身而出，担当冯康的“政治保护伞”。

计算技术研究所成立初期主要肩负两项任务：一是尽快研制出电子计算机，二是利用电子计算机解决国防与经济建设中亟待解决的重大计算任务。计算所下设三个研究室，一室和二室分别负责整机与元件的研究，主要肩负研制计算机的重任，而三室则是从事计算数学与科学工程计算研究，承担解决国防与经济建设中重大问题的任务。

二十世纪五十年代中国开始筹划电子计算机的研制。当时世界上的计算机数量尚少，其作用主要是科学与工程计算。国外能用计算机的人，大多从数学专业转过来。刚于去年度过百年华诞的徐献瑜教授是中国计算数学的老一辈开拓者，他毕业于东吴大学，早年留美获华盛顿大学博士学位。回国后在燕京大学担任教授，1952 年大学院系调整后转到北京大学。50 年代，为了适应国家的需要，徐献瑜毅然从纯数学转到计算数学领域。1956 年 2 月，由徐献瑜、胡世华、闵乃大、吴几康、张效祥、林建祥参加了在莫斯科主办的“计算技术发展之路”的国际会议，在苏期间，与会者参观了苏联科学院的精密机械与计算技术研究所，计算中心以及莫斯科大学数学系计算中心，看到了苏联当时最先进的计算机，拜访了苏联科学院计算所所长列别杰夫院士、计算中心主任妥罗德尼称院士、莫斯科大学计算数学专业主任索波列夫院士，并从此开始了中国计算技术工作者的国际交往。从苏联回国后，徐献瑜即参加了周恩来总理领导制定的“中国科学发展 12 年规划”中“计算技术建立”的规划工作。他所在的计算技术和数学规划组，由 26 名有名望的数学家、计算机专家和电子技术专家组成，华罗庚领衔。

上世纪五十年代冯康与母亲和冯端夫妇摄于北京

1957 年初，冯康被调到中国科学院计算技术研究所三室工作。学术优秀的冯康很快就成了三室学术的掌舵人。

“三室”日与夜

“三室”，对于冯康来说，是一个让他激情燃烧的地方，也是一个让他施展才华的地方。

冯康调到三室的时候，只有 37 岁，正是年富力强的好年华。此时的冯康，无论在人生阅历还是学术研究方面都已经步入成熟。经过了数年的积累，冯康需要一片土壤，让他亲手浇种的计算数学可以开花；冯康也需要一个战场，让他可以统领三军，运用韬略，一展风华。事实上，三室正是这片土壤，这个战场。三室不但让冯康有了施展将才的空间，通过大量实践，也让冯康的学术研究得以升华。

计算所筹备和成立之初，临时的办公地点和实验室都设在中关村附近的西苑大旅社三号楼，当时的数学所也从清华园迁出至此。今天，这个作为中国计算数学最早发

计算所三室一组 1961 年合影。第一排左五为冯康，左六为张克明。

源地的地方几经翻修，已成为一座现代化的五星级的酒店——北京西苑饭店。

1958 年 2 月，一幢全新的科研楼在中关村落成。计算所与数学所由临时办公的西苑大旅社迁往这里，这幢后来被称为“北楼”的灰色办公楼成为计算所与数学所真正的“家”。冯康所在三室的办公地点就位于这幢“北楼”的三楼。

冯康调到计算所三室时担任三室主任的是徐献瑜，副主任是张克明。出生于安徽峰山乡前窑村的张克明，1934 年入清华大学数学系，得熊庆来教授指导。毕业后，他有着奔赴延安、担任华东野战军宣教干部的红色经历，解放后在中科院顾问办公室任主任。

徐献瑜与张克明早年都是计算所筹备委员会的委员，因此计算所成立后，都被委以重任。徐献瑜教授一直钟情教学，因此担任三室主任也只是兼职，他的主要工作仍在北大教书育人。张克明则由中科院的顾问办公室直接调入计算所担任三室副主任，主持工作并兼任三室的党支部书记。冯康调入三室后，负责三室业务的全面指导。

据三室的同事回忆说，冯康和张克明的关系非常好，两个人的配合也相得益彰。如同刘备与诸葛亮一般，开明的张克明十分欣赏冯康的学识才干，全力支持冯康在三室开展工作；冯康也需要张克明这样的权力保护，使得他的一些思路和做法畅通无阻。关键时刻，张克明更会挺身而出，担当冯康的“政治保护伞”。

三室成立之初根据不同的研究方向分为六个小组：其中一组负责初值问题、天气预报。初值问题一般是动态问题，物理状态随时间而变，其解依据“初始条件”。二组负责边值问题（以水坝计算为主）及大规模的矩阵计算（如大地测量）。边值问题一般是静态或平衡问题。其解由所关心的区域边界决

计算所三室二组摄于1961年。后排左七为张克明，左八为冯康。

定。三组负责与国防相关的计算问题，包括航空航天中遇到的激波计算等。四组负责程序设计自动化，这里也成为中国计算软件最早的发源地。五组负责一些微分方程以外的计算问题，包括公路设计、光学镜头设计等。六组则负责常微分方程和统计计算。常微分方程自变量只有一个，当时主要对象是卫星轨道的计算，对中国早期发射人造卫星提供重要的理论和计算支持。而统计计算是对一些不能用数学方程描述的物理现象进行模拟，或对有很多自变量的问题进行计算。其中最有代表性的方法是蒙特卡罗方法，至今仍在物理和金融预测中起着重要的作用。

今天中国计算数学和工程计算很多领域的优秀科学家、中科院院士当年都是和冯康在三室并肩战斗的同事。

石钟慈，1955年复旦大学数学系毕业后被分配到中科院数学所。1956年计算所筹备成立时，他被调到计算所，并派往苏联学习计算数学。1961年，三室迎来了最早一批留苏的大学生，毕业于莫斯科大学的张关泉、秦孟兆和马延文，他们为三室带来了新鲜的朝气与活力。次年，石钟慈也从苏联读研归来，分配到三室二组。与他同时来到三室的还有与张关泉等人在莫斯科大学就读时的同学邬华谟。张关泉1965年又被派到法国留学。

黄鸿慈，1957年北大毕业后被分配到计算所，1958年初在计算所三室正式开始工作，当时他在二组，主要进行水坝问题的相关计算。

黄兰洁，洋名Nancy，在美国长大和接受的教育，毕业于哥伦比亚大学，1957年回到北京，也来到了计算所三室。黄兰洁的丈夫吴承康先生与她同期回国，并长期在中科院力学所工作。吴承康先生1991年当选为中科院院士，是著名的高温气体动力学专家。

崔俊芝，1962年从西北工业大学数学力学系计算数学专业毕业，同年10月到计算所三室的二组工作。

上个世纪五十年代中国的首台计算机

朱幼兰、李子才，1963年毕业于清华大学工程力学系，毕业后分到计算所三室。朱幼兰、黄兰洁还有从苏联回来的邬华谟等主要从事计算流体力学的研究。

负责三室业务指导工作的还有董铁宝教授。董铁宝1917年生于江苏省武进县，1939年毕业于上海交通大学土木工程系。毕业后即奔赴抗日的大后方，参加抢修滇缅公路桥梁。他于二战结束那年赴美国留学，后来在伊利诺伊大学学习、参加研究工作，并于1949年获得博士学位。他在和纽克曼等著名学者一起工作时，有机会参与了第一代电子计算机伊利亚克机（ENIAC）的设计、编程和使用。1956年，当中国开始大规模向科学进军的时候，他放弃了已有的良好工作条件和优厚的生活待遇，携夫人梅镇安和三个年幼的孩子回到祖国，到北京大学任教授，同时兼职于计算所三室。由于董铁宝教授熟悉力学和计算，特别是结构工程与抗震，例如板壳和水坝的数学模型与应力分析，都能给予指导。董铁宝还在计算所指导研究生，周天孝、孙家昶都是他名下的研究生。

当时担任三室二组组长的是魏道政、副组长是林宗楷。先后担任四组组长的是1952年毕业于清华大学的许孔时，1956年毕业于吉林大学的董韫美，组员有张绮霞、仲萃豪、曹东启、李开德等。魏道政、许孔时等和冯康一样，也是从数学所调到计算所的。

冯康主要工作就是指导一、二组进行科学计算。与此同时，他还着手组建和培训计算数学队伍，除了与北大合作办培训班之外，在计算所内也办培训班积极培养年轻的计算数学人才。1957年9月至12月，苏联专家什梅格列夫斯基被邀请来讲课。

冯康在三室倾注了大量的心血，三室的实践也滋润了冯康的学术思想。在三室拼搏的日与夜，让冯康和他的同事们创造了事业的第一个巅峰。

在对年轻人培养期间，冯康邂逅了他人生的第一个红颜知己——李开德。李开德和冯康一样，都是从数学所转到计算所，她被分配到三室四组工作。和三室所有的年轻人一样，她经常要请教冯康补习数学知识。据三室的老同事回忆，那时的李开德年轻、有活力，长得很漂亮。李开德曾经和三室的一位同事发生过短暂的感情，但在当时极左的环境下却被误解为“不正常的男女关系”，给予严厉的处分，甚至要她调离单位。情急之中，她想到一直很敬仰的冯康，她认为以冯康的地位与影响可以帮她躲过一劫。

1959年，冯康与李开德结婚。那一年，刚好是中国历史上疯狂的大跃进时代。但这段婚姻维持了一段不长的时间。

见证了中国最早的计算机诞生和计算数学发展的计算所北楼，在一片拆迁的风声中也未能幸免。它已于2009年正式消失了。

1958 年 5 月，中共八大二次会议正式制定了“鼓足干劲、力争上游、多快好省地建设社会主义”的总路线。随后中国进入了历时三年之久的“大跃进”、“人民公社”时期。“大炼钢铁”、“大放卫星”的口号在全国铺天盖地的蔓延，中国的工业与农业出现了严重的浮夸风。

华罗庚给科大本科生上课

在当时的形势下，中科院数学所与计算所的领军人物华罗庚教授也在科学界大搞高指标的活动中违心地提出了 12 项数学指标，要在 10 年内赶上美国，并且提出要把计算技术、人造卫星、大型水坝等各方面的一切数学问题都承担下来的目标。尽管如此，华罗庚仍难逃厄运。不久在知识界兴起的“拔白旗运动”中，华罗庚被树为“白旗”的典型受到攻击，说他倡导研究哥德巴赫猜想是提倡搞“古人、洋人、死人”，毒害青年。

计算所中，当时盛行的风气也是人人不敢读书，读书即是图名图利的思想。于是大家只能专注实际的数学计算，动手算题目。在没有机器的情况下，大家只能靠手算。尽管条件艰苦，当时三室人员的工作热情却很高。人们经常看到“北楼”的灯光通宵点亮。

1958 年 8 月 1 日，中国第一台电子计算机 103 机终于试制成功。新华社在人民日报上发表了标题为“我国计算技术不再是空白学科，第一架通用数字电子计算机制成”的消息。虽然 103 机的内存容量很小，仅有 1024 个存储单元，但在冯康的带领下，三室利用自己编写的程序在这台机器上，进行了多项计算。

1959 年 9 月国庆十周年前夕，104 大型通用计算机研制成功，104 机在科学计算中发挥了重要作用，许多三室的同事对于运用 104 机进行计算还记忆犹新。到 1959 年底，三室利用这两台计算机完成了八十多项计算任务。

郭沫若（前排左二）、陈毅（左三）、聂荣臻（左四）和第一届中科大毕业生

值得一提的是，在三室担任兼职主任的徐献瑜教授也为三室的发展和成就付出了辛勤的汗水。他曾带领 70 多名计算数学培训班的学员为超音速飞机的设计作出了贡献。当时正值 1958 年科技跃进之际，国防部门设计超音速飞机时遇到小展弦比宽机身组合的翼身干扰问题，当时还没有建成跨音速风洞，所以要估算超音速飞机气动力只能借助数值计算。军事工程学院罗时钧教授提出计算方案，从苏联留学归国的北大青年教师黄敦教授画出了翼身图形，徐献瑜据此图形做出了数学公式。然后指导学员们用电动计算机算了一个月，得出了小展弦比宽机身机翼组合体的超音速干扰气动力，交出了一份出色的答卷。

1960 年代初，三室已经发展成为具有 200 多人的计算数学队伍（包括各地的进修人员）。在冯康的全面指导下，三室完成了国防与国民经济建设中亟待解决的数百个重大计算课题，其中包括数值天气预报、大型水坝应力分析、大地测量计算、核武器内爆分析与计算、火箭、导弹、卫星的高速空气动力学计算、卫星轨道计算、全国铁路布线及站点设立的最优化方案计算等等。与此同时，三室还为全国各地代培了近百名科学计算人才，其中不少人回去后担当了本单位的业务领导工作。

冯康在三室倾注了大量的心血，三室的实践也滋润了冯康的学术思想。在三室拼搏的日与夜，让冯康和他的同事们创造了事业的第一个巅峰。

今天，当我们再次来到位于中关村的中国科学院基础园区，已经看不到当年计算所三室所在的那幢灰色的六层楼房。如今那里变成了一片拆迁后的平地，据说不久会有一幢现代化的商务大楼在那里拔地而起。如今，在昔日三室“北楼”的对面，是一间装潢时尚，飘逸着海派菜香的苏浙汇餐馆；偶尔，我们还会在那里邂逅鹤发耄耋的院士，四十年多前，咫尺之遥，那曾是他们激情澎湃、热火朝天奋战的地方……

1963 年，中科大 58 届计算数学专业学生在计算所北楼前与实习指导老师合影。前排中为计算教研室主任冯康。

第七研究组

正当中国的“大跃进”在全国各地进行得如火如荼的时候，中国教育史和科学史上也发生了一项重大事件：中国科学技术大学在北京宣布成立。1958 年 9 月，在聂荣臻等老一辈领导人的积极倡导下，隶属于中科院的中国科技大学宣布成立，旨在为中国培养急需的高新科技人才。由科学院院长郭沫若兼创校校长，钱学森等一批颇有名望的科学家也纷纷到科大执教鞭。此时，经历了“拔白旗运动”在数学所遭受排挤的华罗庚将主要精力集中在科大数学系，担任中国科技大学副校长兼数学系主任。数学系的副主任则由冯康担任。从此，华罗庚虽然长期地在中国科学院数学所工作，在科大兼职，但却再也没有过问计算所的事情。

60 年代初，为了在科大搭建一个完整的教学平台，在冯康的倡导下，科大成立了计算数学教研室。冯康担任教研室主任。冯康除了选派三室富有经验的业务骨干如石钟慈、黄鸿慈等到科大任教之外，他还在三室专门成立科大教材编写组，为科大编写教材。当时在教材编写组的有黄鸿慈、李家楷、张关泉、秦孟兆等人。作为计算数学专业课程的设计师，冯康除了亲自撰写教学大纲、组织编写教材之外，有时还会亲自到科大作演讲、报告。冯康带领团队为科大编写的那些油印教材虽然最终没能出版，但却成为中国计算数学专业教学的宝贵资料。在同一时期，石钟慈正式调入中国科大工作。他逐渐由教研室主任，后来接替冯康升至数学系主任，在科大工作了二十余年。中国科技大学于 1970 年搬迁至安徽合肥市，他也随学校来到了合肥，直至八十年代中期又回到了北京，回到了科学院。

冯康一方面深入到七个研究组进行业务指导，一方面又带动大家在完成实际任务中开展理论研究工作。到文化大革命前夕，三室不仅完成了一批国家急需的重大任务，还写出了多篇高水平的学术论文。

1961 年，在广东省汕头召开了第二届全国计算技术经验交流会，冯康与三室副主任张克明等人参加了会议。会议后，冯康建议三室在解决实际任务的同时，要开展理论研究。他疾呼，形势逼人，开展理论研究已是刻不容缓。

在当时的条件下冯康提出这样的建议是顶着很大阻力的，因为当时普遍的观点认为，搞理论研究就是从文章到文章，是一种争名逐利的思想，因此受到很多人的批判。这时，与冯康搭档默契的张克明主动帮他解围，1963 年在张克明的支持下，三室成立了第

1962 年春，石钟慈（左一）与科大 1958 届计算数学专业师生在颐和园合影。

七研究组，进行理论方面的研究。黄鸿慈获任第七研究组的组长，张关泉担任副组长，组员大部分是冯康在 60 年代初期带的一批研究生，其中包括王烈衡等，李子才后期也调入第七研究组。

第七研究组的成立标志着三室在计算数学研究方面由理论到实践的框架已经搭建完成。今天看来，不得不令人钦佩冯康的远见卓识与高瞻远瞩。由此，冯康作为计算数学大家的风范逐步显露，他也开始在自己搭建的平台上施展才华。

冯康一方面深入到七个研究组进行业务指导，一方面又带动大家在完成实际任务中开展理论研究工作。到文化大革命前夕，三室不仅完成了一批国家急需的重大任务，还写出了多篇高水平的学术论文。无粘超音绕流数值计算和初边值问题差分方法研究工作在理论和实践上已经有所突破，获得了初阶段的成果，为国防部门计算出了大量有关数据，为中国早期的航空、航天事业作出了贡献，这一领域的数值计算问题是当时国际上公认的难题。原子能反应堆的物理计算，需要求解波尔兹曼方程，这个问题的难度也很大。冯康提出从积分守恒原理出发建立差分方程，并指导任务组推导出解决波尔兹曼方程的一系列守恒格式，在实际计算中获得了成功，并且在理论分析方面也做了一些研究，为我国早期的原子弹试制和第一艘核潜艇上核反应堆的设计提供了可靠数据。冯康还直接负责一项国防部门提出的解不定常冲击波问题计算方法研究课题，他指导课题组通过实际计算研究总结出各类方法的特点和适应的情况，以及如何选取各种参数，从实践和理论两个方面初步探索出了解决此类问题的途径和方法，对国防部门的有关试制研究工作起到了参考与指导作用。

第七研究组在计算数学理论方面取得的丰硕成果，也催生了中国第一本计算数学杂志《应用数学与计算数学》的诞生。

《应用数学与计算数学》最早萌芽于《计算机动态》中的计算数学专刊。《计算机动态》是由计算所主办的一本杂志，每月一期，以刊登一些介绍国外先进机器的文章为主。随着国内计算数学研究的兴起，《计算机动态》每年出版四期计算数学专刊，刊登计算数学方面的翻译文章及少量国内原创论文。这本期刊在 1960 年代初刊登过一篇北大的胡祖炽翻译的三位应用数学大家，库朗（纽约大学库朗研究所的创始人）、Friedrichs（拉克斯的博士导师）、Lewy (1984 年的沃尔夫奖获得者) 于 1920 年代用德文写的经典文章，题目是《差分方程和数学物理》。此文提出了经典的用三位作者第一个字母组成的 CFL 稳定性条件，至今仍是计算数学必知的条件。这篇三十年后的译文，仍对三室的研究起到很大的推动作用。由此也可看到当时参考文献水平的落后。

七组成立后，计算数学理论研究的文章多了起来。1964 年，在冯康的主持下，《应用数学与计算数学》创刊，每季一期。从此计算数学有了自己的一片研究天地，第七研究组发表的文章占了这一期刊文章的一半左右。

在当今资讯爆炸的年代，期刊的种类已经多得数不胜数，甚至成为研究者的负担。在美国《数学评论》注册的数学期刊就有上千种，在中国和数学有关的中英文期刊也有上千种。庞大的数目之后是水平的严重参差不齐。但在 1960 年代，数学期刊种类只有二、三十份，计算数学的刊物只有几个。当时有一个交流的平台是非常重要的。冯康在这方面的远见卓识和身体力行对中国计算数学的研究是有重要影响的。

好景不长，当文化大革命袭来的时候，随着七组解散，这个仅仅诞生了两年半的杂志也被迫停刊。直至 1978 年《应用数学与计算数学》复刊，更名为《计算数学》。《计算数学》目前是中国计算数学最权威的杂志。

尽管在整个中国计算数学的发展史上，第七研究组以及《应用数学与计算数学》都如同昙花一现，然而他们却是中国计算数学研究的一个良好的开端。

花儿谢了，美丽犹存。


1966年3月19日，中共中央总书记邓小平等抵刘家峡水电站建设工地视察。

曾经，
在神奇的数学王国中，
有一个并未被许多人认知的“美丽花园”，
人们称它为“有限元”。
遇上有限元，
有人说是他的一种偶然，
也有人说是时代的一种必然；
开发有限元，
让他有足够的自信与世界数学大师平等对话，
更让他成就了数学骄子的梦想……

第四章　数学骄子

在人的一生中，机遇与际遇如同两个孪生兄弟，如影相随。有时候，一个偶然的机遇会让人生的际遇改变；有时候，人生的际遇又会让失去的机遇重生。

也许，一个人曾经无数次地与机遇擦肩而过，无数次地与机遇失之交臂，但只要有一次握住了机遇的手，整个的人生际遇就会从此改变。

有限元对于冯康来说就是改变了他人生际遇的一次机遇。

没有有限元，冯康的名字在今天就不会被人们一次次地提起。

没有有限元，冯康也就不会傲然地站在世界级数学大师之列。

尽管有限元的发现蕴含了一个又一个曲折的故事，尽管有限元的开发凝结了太多太多科学工作者的心血与智慧，尽管有限元的发展引发了学术界的争议与个人的恩怨，然而，当我们逐步抽丝剥茧，试图还原有限元发现前后的真实故事，我们发现，原来所有的一切都无法遮挡冯康的光芒。

冯康以他独有的数学高度与思想，不但发现并找到了这片数学王国的“美丽花园”，并且还给出了关于有限元方法充足的理论根据。冯康的高度与深度是同时代的许多研究者所无法超越的，他也因此赢得了国际声望与多位世界级数学大师的尊敬。

重拾有限元的故事，我们依旧要回到那令冯康激情燃烧的火红年代……

刘家峡被“困”

“黄河的水哗啦啦地流，流过一个美丽的地方，流过一道神奇的峡谷……”大多数人对于刘家峡的记忆都始于小学的语文课本。2008年，一首迅速唱红的歌曲《美丽的刘家峡》再度勾起人们对于这颗“黄河明珠”的向往与回忆。

今天，当我们乘船沿着黄河溯流而上，行至甘肃省永靖县内，豁然见到两岸奇峰对峙、壁立千仞、风景奇伟壮观。九曲黄河水陡然在这里转了一个九十度的急弯，向西奔流入峡。这里就是著名的刘家峡。

人们记住刘家峡不仅仅是因为它阳刚

从空中俯瞰刘家峡水电站的景色

与阴柔兼备的奇特景观，更因为它包含了让许多中国人倍感自豪与骄傲的火红记忆。

刘家峡水电站是中国第一座超过百万千瓦级的大型水电站，也是中国第一个自己设计、施工、建造的超过百米的大型混凝土坝。从 1958 年 9 月 27 日刘家峡大坝红红火火地破土动工，到 1966 年 10 月刘家峡大坝顺利实现截流成功。1968 年 10 月水库正式蓄水，1969 年 4 月 1 日第一台机组发电……这一连串令人骄傲的事件曾经许久地激荡在人们的心中。

然而，人们也许还并不知道，这个令人骄傲的宏伟工程在建设中也不是一帆风顺的。50 年代末至 60 年代初，刘家峡大坝遇到了一系列设计计算和建设方面的难题，造成大坝工程进展缓慢。

在中科院计算所，三室二组的主要任务之一就是承担水坝工程的计算问题。三室二组最早进行水坝计算的是李旺尧。1958 年李旺尧下放劳动，未完成的计算由黄鸿慈接手。在刘家峡大坝工程计算之前，黄鸿慈已经进行过广东河源新丰江水坝、云南威信扎西坝等水坝工程的计算。他运用以往的计算经验与蔡中雄、詹重禧（在计算所进修）一起编写了两个计算标准程序。其数学模型主要是重调和方程。据崔俊芝介绍，黄鸿慈等人编写的十三点差分格式应力函数计算程序质量非常高，已经达到了指令级程序的最优化。这两个程序为其后二组其他同事进行水坝计算奠定了良好的基础。

1963 年，中科院对各科研单位提出了系统研究的要求，即以完成国家重大需求任务为目标，开展系统研究，解决国家发展中困难的科学问题。中科院提出的口号是“以任务带学科”。在当时的三室中，黄鸿慈应当说是既有超强的理论能力又有实战经验的骨干，深得冯康的欣赏，他也因此受命担当由冯康倡导成立的第七研究组的组长。黄鸿慈调任七组之后，二组接替他进行水坝计算任务的就是刚刚由西北工业大学分配来的年轻人崔俊芝。

1963 年 2 月，刚刚过了农历新年，刘家峡大坝设计组的副组长朱昭钧工程师找到了计算所三室，请求帮助解决刘家峡大坝的应力分析问题。研究室把这项计算任务交给了崔俊芝。

朱工首先向崔俊芝介绍了他们采用的弓冠量分配计算方法，崔俊芝很快发现用这种方法形成的系数矩阵是病态的，于是他转而使用主元素消去法去求解弓冠量方法导出的病态线性方程组。病态问题虽然解决了，但是对计算结果进行应力校核，发现局部应力总是不平衡。于是，崔俊芝对弓冠量计算方法产生了怀疑。接着，崔俊芝在蔡中熊的帮助下利用黄鸿慈等人编写的应力函数法标准程序进行了计算，但算出来的结果仍然不能做到局部区域应力平衡。

崔俊芝今天回忆起来仍然认为，当时之所以计算的结果不理想，是因为采用十三点差分格式的应力函数计算程序来进行水坝应力分析。得不到满意的结果的主要原因是全部采用了正方形网格，水坝的边界不可能与网格线重合。黄鸿慈回忆说，内节点用差分逼近，边界节点不得不使用外推插值处理，这种不统一、不协调的处理方式也是造成计算结果不理想的原因。

除了计算方法之外，计算机储存量的限制也是造成计算难题的重要原因，当时的计算机全部数据与程序加起来不能超过 2048 个内存单元。崔俊芝称那是一个很艰苦的程序设计年代，因为当时编

程序都用机器原码，输入都用纸带穿孔。

1950年代编写程序相当地辛苦。没有汇编，没有C，也没有C++。当时的那种编程并不是今天这样的“写”程序，也不是在自己家里或是办公桌上就可以做的，而是要用机器语言来编，要到保安极强的机房里换上白大褂去工作的！也就是说，编出程序除了写在纸上，更重要的是穿成纸带，即在纸带上打出一系列的小孔（修改程序就是给纸孔打补丁）。程序员需要先将计算机的指令换算成二进制数字，然后把二进制数字组成这些小孔，每个小孔代表一个信号；数十个小孔构成一条指令，驱使计算机做一个动作！这个方法一直延续到1980年初，笔者之一曾于1983年在北京大学的机房里穿过几个月的孔，在庞大的机房里体验过那时编程的艰辛。

正当崔俊芝对于水坝计算问题一筹莫展的时候，冯康在计算所的一次学术报告上重点讲述了一篇文章，这篇文章让崔俊芝茅塞顿开。经过了漫长的黑暗摸索，崔俊芝终于看到了光亮与希望。

破题刘家峡

作为三室全面的业务指导，冯康经常要在三室或者全所范围内作学术报告，分享一些他近期研究以及读书的心得。在一次报告中，冯康提到的是Synge的一篇文章，并提出把微分方程写成变分形式，用变分的原理来推导差分格式。

冯康提到的那篇文章是Prager和Synge于1947年发表在美国《应用数学季刊》上的一篇文章。Synge在应用数学和力学方面作过很多杰出的工作，也是钱伟长院士在多伦多大学读博士时的导师。他本人后来当选为英国皇家协会院士。他的二女儿Cathleen Morawetz是柯朗数学研究所的著名教授，曾任美国数学学会会长，并当选为美国科学院院士。他的叔父约翰·辛格（John M. Synge）是爱尔兰著名诗人，也是英国皇家协会院士，代表作品包括《西方世界的花花公子》和《骑马下海的人》。他的另外一个远亲曾获1952年诺贝尔化学奖。所以这也是一个传奇的文化世家。

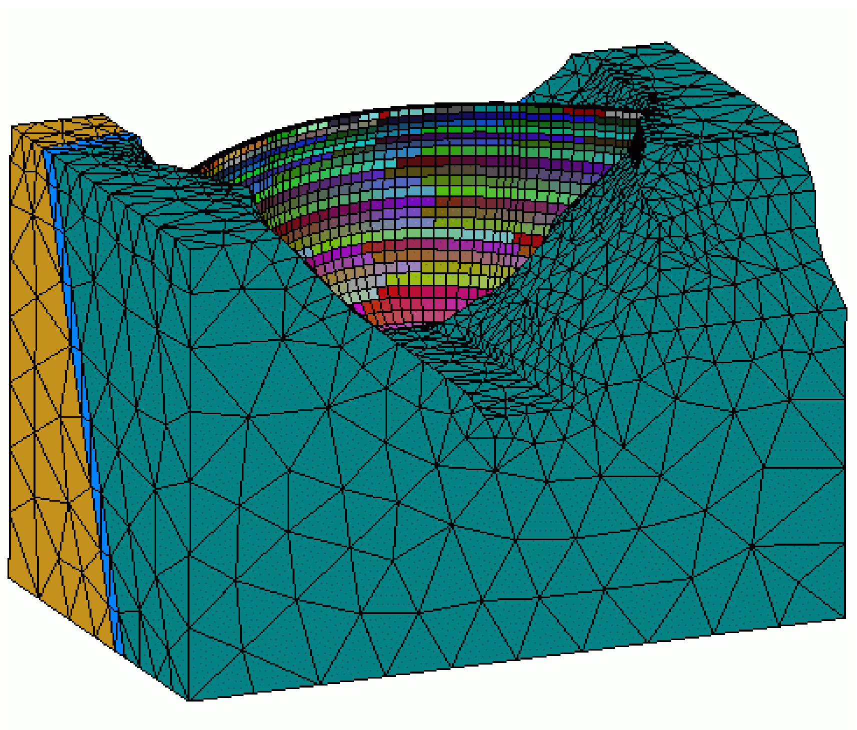
冯康的这次报告给了黄鸿慈和崔俊芝等人很大的启发，他提出的用变分原理进行差分计算的思想为许多年轻学者提供了新的研究方向。

1963年夏天，在冯康的带领下，三室的同事们掀起了钻研与探讨差分方法的热潮。他们从中科院的图书馆借来美国的Forsythe和Warsow二人于1960年写的一本书，叫做《偏微分方程的差分方法》。书中有两个关于椭圆方程计算的章节，讲到了变分差分格式。三室的同事们如饥似渴地争相阅读这本书，由于当时没有复印机，他们就自己抄公式、刻钢板，进行油印。

1963年水坝问题的计算已经由二组上升成为三室亟待解决的攻坚难题。

在冯康的筹划部署下，二组的水坝计算组分成三个小组，从三个不同方向对水坝计算进行系统研究。

三个小组的划分如下：二组副组长林



有限元计算大坝的三维网格。1960年代的网格仅仅是二维的。

忠楷带领一个小组，把大坝的基础砍掉，用应力函数的方法进行计算；二组组长魏道政带领一个小组，从平衡方程出发，把应力——应变关系代进拉梅方程进行计算，崔俊芝在这个小组。剩下的一个小组由蔡中熊带领，王荩贤在这个小组，从变分原理出发，直接用位移差商代替位移导数进行计算。三个小组要定期交流，并将结果向冯康汇报。

1963年10月，魏道政突发急性肝炎，住进了北京郊区潭柘寺医院。崔俊芝只好带着由魏道政指导毕业设计的科大64届毕业生魏学玲继续进行计算。为了尽可能地保证在坝体内部任意局部区域上的应力平衡性，崔俊芝与魏学玲采用了基于拉梅方程的积分守恒的差分格式，内部采取不等距矩形网格，边上采用三角形网格，使所有计算节点都落在坝体内部或边界上。二人分工合作，终于在1964年春天来临的时候算出了一组新的结果——利用积分守恒格式的计算结果。经过细致地应力校核，其结果不仅在边界节点附近应力是基本平衡的，且在坝体内部任意局部区域上的应力也是基本平衡的。

三室有关人员曾收到一份落款为“中共中央、国务院、中央军委、中央文革小组”的明码电报，祝贺和表彰计算所三室在刘家峡水电工程建设中的突出贡献。

当崔俊芝把这样的计算结果交给刘家峡水坝工程设计组的人员时，他们露出了满意的笑容。

在获得用户满意的计算结果之后，崔俊芝对原来由他和魏学玲合作编制的程序进行了重大的修改，采用标准化的信息格式，编制出了第一个平面应力分析标准程序（104计算机版本）；同年，崔俊芝还编制了平面应力分析标准程序（119计算机版本）。利用这两个程序，崔俊芝为刘家峡工程计算了多个（不少于十个）设计方案。

与此同时，崔俊芝和王荩贤一起，把基于积分守恒格式的差分格式和基于变分原理的差分格式一一进行了对比，发现在边界节点上其差分格式是一致的；它们正是后来“有限元法”得到的边界节点上的差分格式；对于内部节点的差分格式也进行了组合优化，形成了当时认为是最好的差分格式。以这些差分格式为基础，崔俊芝、王荩贤、赵静芳三人合作编制了另一个平面应力分析标准程序（109-乙计算机版本）。利用这个程序，他们为多个不同类型的结构工程进行了平面应力分析。

1964年“五·一”节，对于三室的同事来说心里是暖洋洋的，经过多年的刻苦攻关、废寝忘食，水坝计算的系统研究终于有了结果，刘家峡大坝的应力分析已经使用户满意。“五·一”过后不久，在计算所302房间，冯康、黄鸿慈、崔俊芝等人激动地向刘家峡大坝工程设计组的负责人员进行了汇报。

破解刘家峡大坝应力分析的计算难题是计算所三室对社会主义经济建设的一大贡献。1966年10月刘家峡大坝截流成功时，三室有关人员曾收到一份落款为“中共中央、国务院、中央军委、中央文革小组”的明码电报，祝贺和表彰计算所三室在刘家峡水电工程建设中的突出贡献。

发现有限元

人们原本以为，破解了刘家峡水坝的计算难题，事情就应该画上了一个圆满的句号。谁知，时隔不久，由刘家峡大坝的计算更引发了另一个美丽的结局。

冯康在指导与总结刘家峡水坝计算的过程中，发现了一整套求解偏微分方程边值问题的计算方法，一个用变分原理进行差分计算的方法。即通过剖分插值，构建分片多项式的函数空间，来求解偏微分方程。这就是著名的有限元方法。虽然冯康当时把它叫做基于变分原理的差分方法。这一方法的发现在计算数学领域中引起了强烈的震动。

早在1962年2月，黄鸿慈在《计算机动态》的《计算数学》专刊中发表了一篇题为“求解重调和方程最小特征值问题的一种差分方法”的论文，文中提出一种求解四阶微分方程的C1-元（即导数连续的分片多项式空间）方法。这篇文章被称为“具有早期有限元的思想”，后来也成为有限元方法报奖的四篇文章之一。当时，冯康对黄鸿慈的这篇文章大加赞赏，黄还因此被提升为助理研究员，获得了晋升两级工资的嘉奖。

1964年10月，为迎接即将在哈尔滨举行的全国计算机会议，三室先召开了一个预备会议。会上，黄鸿慈和崔俊芝分别作了关于理论和计算方面的报告。黄鸿慈的报告主要讲了拉普拉斯（Laplace）方程和平面弹性问题的离散方法的误差估计，但是在较强的解的光滑性条件下完成的。黄对这个

结果很满意，还专门向冯康单独汇报了这个结果并征求他的意见。令黄费解的是，冯康听后表现得很冷淡，并没有象两年前给他提工资那次那样热情。一年后，黄鸿慈了解到，其实冯康当时正有一个从广义函数出发的收敛性证明，也是他那篇伟大的开创性文章中讲述的工作。只不过这一次冯康并没有和黄交流。

1965 年 5 月，全国计算机会议在哈尔滨召开。由于当时黄鸿慈已经去河南信阳“四清”劳动，他没有机会听到冯康那篇精彩的报告。后来冯康的报告又以论文的形式发表在 1965 年第 4 期《应用数学与计算数学》期刊上，题为“基于变分原理的差分格式”。而根据张克明等三室领导决定，黄和崔俊芝两人需要把 1964 年 10 月在三室作的报告删改合并，发表于 1966 年第 1 期的同一个期刊上，题为“求解平面弹性问题的差分方法”，论文的合作者还有王荩贤、赵静芳、林宗楷。

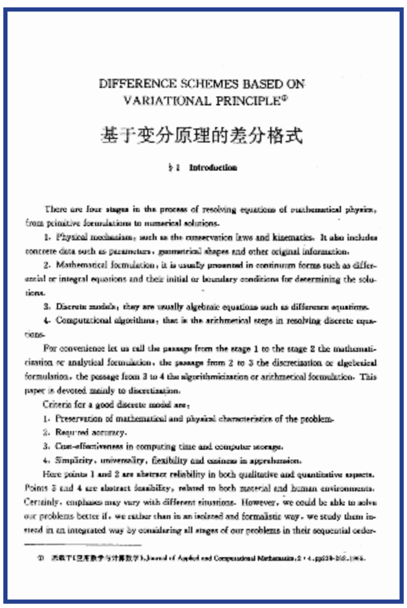
如同任何科学技术的创新都是社会和科技发展的必然结果一样，在那样一个令人激情燃烧的年代，在一个国家呼唤计算数学飞速发展的年代，冯康团队与他们的有限元方法呼之欲出。

黄鸿慈、王荩贤、崔俊芝等人的文章给出了有限元方法的误差估计，这是文献可查的非常早的误差估计结果，但是在较强的解的光滑性假定下获得的。而冯康在其论文中，用高深的数学理论，在极其广泛的条件下证明了方法的收敛性和稳定性，建立起有限元方法严格的数学理论框架，为有限元方法的实际应用提供了可靠的理论基础。这篇论文被公认为是中国学者先于西方创造有限元方法理论的标志。

由于黄鸿慈的文章没有单独发表，他也怀疑是冯康从中作梗，因此也为冯康与黄鸿慈多年后的恩恩怨怨埋下了伏笔。冯康的这篇文章与黄鸿慈等人的文章最终成为了有限元报奖的重要材料。

如同任何科学技术的创新都是社会和科技发展的必然结果一样，在那样一个令人激情燃烧的年代，在一个国家呼唤计算数学飞速发展的年代，冯康团队与他们的有限元方法呼之欲出。冯康在许多场合都反复提到他的那篇文章是在水坝计算的基础上写出来的，有限元方法的提出是集体智慧的结晶。

是的，应当说，如果没有三室同事水坝计算的大量实践，冯康就不会发展有限元方法的系统理论。然而，如果没有冯康的数学境界与思想高度，也不会有有限元方法的发现和理论化。冯康的贡献不仅仅是一个数学理论的证明，而是一个方法从数学角度的重新发现，并且使得这个方法得以更广泛地应用。



DIFFERENCE SCHEMES BASED ON
VARIATIONAL PRINCIPLE①

基于变分原理的差分格式

§1 Introduction

There are four stages in the process of resolving equations of mathematical physics, from primitive formulations to numerical solutions.

1. Physical mechanism, such as the conservation laws and kinematics. It also includes concrete data such as parameters, geometrical shapes and other original information.

2. Mathematical formulation, it is usually presented in continuum forms such as differential or integral equations and their initial or boundary conditions for determining the solutions.

3. Discrete models, they are usually algebraic equations such as difference equations.

4. Computational algorithms, that is the arithmetical steps in resolving discrete equations.

For convenience let us call the passage from the stage 1 to the stage 2 the mathematicization or analytical formulation, the passage from 2 to 3 the discretization or algebraical formulation, the passage from 3 to 4 the algorithmicization or arithmetical formulation. This paper is devoted mainly to discretization.

Criteria for a good discrete model are:

1. Preservation of mathematical and physical characteristics of the problem.

2. Required accuracy.

3. Cost-effectiveness in computing time and computer storage.

4. Simplicity, universality, flexibility and easiness in apprehension.

Here points 1 and 2 are abstract reliability in both qualitative and quantitative aspects. Points 3 and 4 are abstract feasibility, related to both material and human environments. Certainly, emphases may vary with different situations. However, we could be able to solve our problems better if, we rather than in an isolated and formalistic way, we study them instead in an integrated way by considering all stages of our problems in their sequential order.

① [illegible]《应用数学与计算数学》, Journal of Applied and Computational Mathematics, 2 : 4, [illegible], 1965.

冯康 1965 年论文的英译版

许多国际著名科学家对冯康的这一成果都给予极高赞誉和充分的肯定，也把这一成果摆到了它应该占有的地位上。

正如我们在故事的开篇提到的，法国著名科学家、法国科学院院长里翁斯(J. L. Lions)院士赞扬冯康是在对外隔绝的环境下独立创始了有限元方法，位列世界最早。曾任美国总统科学顾问及美国数学会会长的彼得·拉克斯（P. Lax)院士后来在纪念冯康的文章中也写道：冯康独立于西方并行地创造了有限元方法的理论，在方法的实现及理论基础的创立两方面都做出了贡献。

中国的国家领导人在讲话中多次提到有限元的成就。

2002 年 5 月 28 日，时任国家主席的江泽民在两院院士大会上发表了重要讲话，他说到：在当代世界科技发展的史册上，我国科技工作者也书写了光辉的篇章。在数学领域创立的多复变函数的调和分析，有限元方法和辛几何算法，示性类及示嵌类的研究和数学机械化与证明理论，关于哥德巴赫猜想的研究，在国际上都引起了强烈反响。

2008 年 12 月 15 日，胡锦涛主席在纪念中国科协成立 50 周年大会上发表讲话也别提到了有限元方法，并在新中国成立以后的众多科学成果中将其列在第一位。

有限元方法的发现和其数学理论让冯康攀上了数学研究的第一个巅峰。

有限元方法

提到二十世纪对人类具有重大影响的发明，人们自然会联想到飞机、电视、卫星、电子计算机、无线通讯技术等等这些与人们近在咫尺、息息相关的发明创造，事实上，人们可能并不知道，在工程设计领域还有一个直接关系到国计民生的重大发明，那就是有限元方法。

有限元方法对于数学界、物理学界、工程界的人士来说是再熟悉不过的，而对于普通人来说却显得陌生而遥远。其实，人们可以不知道有限元，却一定知道今天的飞机可以造得庞大而又安全；人们可以不知道有限元，却一定知道今天的大坝可以造得坚固而又伟岸；人们可以不知道有限元，却一定知道今天的手机可以让沟通变得畅快而又简单……有限元间接地与人们的生活发生着千丝万缕的联系。

有限元方法的早期发展有着较漫长的历史。

结构力学家在对飞机结构应力分析的研究中，最早导致有限元方法及其技术的诞生。飞机在载荷变化很大的环境下工作，会经受复杂的应力变化。这时，结构的承载能力、断裂疲劳寿命、结构的可靠性和耐久性，都需要有合理的分析。这些分析，直接影响设计与制造的成本。在计算机出现之前，这些问题的解答主要依赖各种形式的结构实验。由于这些实验基本上是采用和飞机的大小差不多尺寸的模拟，因此实验规模之大，花费之高是可想而知的。一架好端端的飞机在巨大的全机静力试验厂房内，通过液压传动的协调加载设备，在一声巨响之下，将其拉得支离破碎，真是非常可惜。

1950 年代中，美国飞机设计工程师 M.J. Turner 与大学教授 R.J. Clough 合作在 1956 年的《航空科学杂志》上提出了飞机结构分析的直接刚度法，同时欧洲的 Argyris 教授创导了飞机结构分析矩阵分析方法，他们被认为是当代有限元法诞生的起点。但作为一种求解数学物理问题的近似方法，这一方法的原型甚至可以从大数学家柯朗（R. Courant）1940 年代发表的论文中找到。但是由于当时计算机尚未发明，柯朗的方法因计算量太大并未引起科技界的重视。

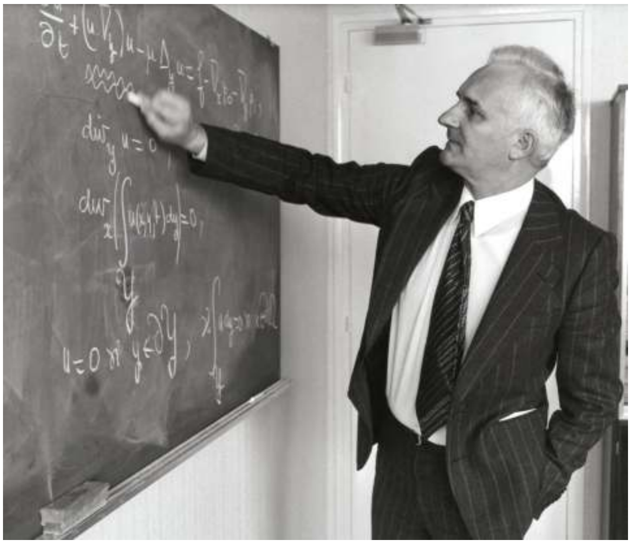
按力学应力平衡方法装配起来的有限元系统，被当作为复杂结构应力 - 应变分析的一个近似的数学模型，是有限元化繁为简指导思想的根本。由于几何形状简单，受力变形单纯，每一单元的应力—应变关系可根据有限的几个节点位移直接地表达出来。这种按力平衡原理组合可等价为单元刚度矩阵的某种叠加，于是一个复杂的应力 - 应变问题能够归结为一个线性代数方程组问题。也正是这个原因，力学家们一开始把有限元方法叫做直接刚度法或矩阵方法。

这是结构力学家发明的有限元法的思维路线。而真正对有限元方法有所突破，并使得有限元方法得以大范围、广泛应用的却是计算数学家们的贡献。特别是中国数学家对于有限元方法的创导和发展具有不可磨灭的贡献。

中科院计算所三室成立的主要任务是研究计算数学，计算数学作为数学的一个重要分支，研究的内容包括算法设计和算法分析。在三室，一组、二组和三组的主要研究工作是求解连续的偏微分方程问题，既把连续的偏微分方程转换为离散的数值代数问题。这样可以把极少可能找到解析解的连续问题转化为离散的有限维问题，进而计算得到近似解。这个过程叫数值偏微分方程方法。

2005 年，拉克斯从挪威王子手中接过约百万美元的数学大奖，阿贝尔奖。拉克斯对冯康的贡献非常赞赏。

微分方程的定解问题就是在满足某些定解条件下求解微分方程的解。在空间区域的边界上要满足的条件称为边值条件。如果问题与时间有关，在初始时刻所要满足的条件，称为初值条件。不含时间而只带边值条件的定解问题，称为边值问题（比如水坝应力分析问题）。与时间有关而只带初值条件的定



法国科学院院长里翁斯对冯康的工作给予高度评价

解问题，称为初值问题。同时带有两种定解条件的问题，称为初边值混合问题（如天气预报问题、石油勘测问题等）。

大多数微分方程问题往往求不出解析解，或者其解析解不易找到。所以要采用可行的数值解法。在1950年代以前，最主要的数值求解方法是有限差分方法，简称差分方法。它的基本思想是把问题的定义域进行矩形剖分，然后在网格点上以用网格节点上的函数值的差商替代控制方程中的导数进行离散，从而建立以网格节点上的值为未知数的代数方程组。该方法是一种直接将微分问题变为代数问题的近似数值方法，数学概念直观，表达简单。此外，还要研究差分格式的解的存在性和唯一性、求解方法、解的数值稳定性、差分格式的解与原问题的真解的误差估计，以及差分格式的解当网格尺寸充分小时是否趋于真解（即收敛性）等等。

在有限差分理论方面起到先驱作用的学者包括计算机之父冯·诺伊曼（von Neumann），他给出了基于傅立叶级数的稳定性分析方法。沃尔夫奖获得者彼得·拉克斯（Peter Lax）提出了等价性定理，建立了差分方法稳定性和收敛性的内在联系。还有俄国数学家萨马斯基（A.A. Smarskii）院士系统地发展了有限差分理论。另外，马尔丘克院士（G.I. Marchuk）提出了交替方向法，使高维度空间的差分方程求解变得更有效，后者于1980年代曾任苏联部长会议副主席和苏联科学院院长。

有限差分方法直观、理论成熟，精度容易预测。但是对区域的规则性要求较高，对于不规则区域处理繁琐。这些缺点已被证明可以用有限元方法来弥补。对于有限元方法，其基本思路可用下面六点说明：第一、根据变分原理建立与微分方程初边值问题等价的积分表达式，这是有限元的出发点。第二、区域剖分。根据求解区域的形状及实际问题的物理特点，将区域剖分为若干个相互联接但又不重叠的单元。第三，确定单元基函数。根据单元中节点数目及对近似解精度的要求，选择满足一定插值条件的函数作为单元基函数。第四，单元分析。将各个单元中待求解的函数用单元基函数的线性组合进行逼近；再将近似函数带入积分表达式，并在单元上进行数值积分，可以获得含有待定函数节点近似值的代数方程组，称为单元有限元方程。第五，总体合成。将区域中所有单元的有限元方程进行累加，形成总体有限元方程。第六，求解有限元方程。由于最后得到的是代数方程组，采用适当的数值代数方法，可求得各节点的函数值。这个方法最重要的优点之一是上述的第二步，其单元可以不是矩形，这样就可以应付任意形状的多边形区域。在实际计算中，有限元方法可以应用于任何的求解区域。

这些有限元方法的叙述，是我们今天在计算方法的教科书中常见的内容。

数学家与有限元

冯康曾用简单形象的比喻形容有限元方法：求解微分方程的定解问题好象是大海捞针，但有限元离散后，寻求近似解就好象是碗里捞针。

计算所三室的数学家们当时面临解决大坝受力问题，从不同的角度也达到了有限元法的统一形式。冯康和他的团队考虑的是一组描写物理力学问题的连续的偏微分方程的近似解，将这些偏微分方程用泛函分析的方法转化为求解能量极小的变分问题。再将所有可能的场变量局部近似，在场内每个简单的三角形或四边形区域上，假定场变量具有低阶多项式的近似表达式。这样，无穷自由度的问题就可以近似成有限自由度的Ritz-Galerkin问题。如前面描述的，在实际计算过程中，冯康和同事们发现现有的计算方法对许多问题的求解并不适用，难以满足工程应用的实际需求。他注意到同一个物理问题可以有

多个数学表达形式，而这些数学形式在理论上是等价的。过去人们在求同思维的驱使下，往往只注意早已广为人知的微分方程形式，而不注意其它形式。计算数学家往往也只研究已有的计算方法，或从微分方程形式去构造一些新的差分格式。但冯康并不满足于此。

求异思维使冯康决心创建和发展新的计算方法。既然一个物理问题可以有多个等价的数学表达形式，为什么非从微分方程形式出发呢？他注意到了久被忽视的变分形式。为了克服传统计算方法难以处理几何形状与材料的复杂性，难以保持物理问题的主要特征，冯康开辟了椭圆型方程计算方法的系统研究。在大量计算经验的基础上，通过系统的理论分析及总结提高，把变分原理与剖分逼近有机结合，既保持了物理问题的主要特征，又以“分整为零、裁弯取直、以简驭繁，化难为易”的新思路，妥善解决了几何形状和材料的复杂性问题，创造了一整套从变分原理出发求解偏分方程问题的数值方法。

美籍捷克裔数学家巴布什卡(Babuska)(左三)是有限元的大师之一。这是他上世纪八十年代初访问北京时和冯康(中)，黄鸿慈(右三)，林群(右二)等的合影。

冯康曾用简单形象的比喻形容有限元方法：求解微分方程的定解问题好象是大海捞针，成功的可能是微乎其微；但有限元离散后，寻求近似解就好象是碗里捞针，显而易见容易多了。

需要提出的是以冯康为首的中国科学院的研究集体在用计算机做水坝应力——应变分析的过程中，克服了传统方法的种种缺陷，创造性地提出基于变分原理的差分方法。当时中国和西方的交流几乎中断，这个方法和西方称为有限元的方法完全一样。他们不仅提出了方法，而且更重要的是在世界上最先给出了这一方法的可靠性理论，开辟了有限元数学的新篇章。冯康的论文是国际公认的最早有关有限元理论的奠基性工作；在对函数解析性质要求非常一般的情形下，给出了方法的稳定性和收敛性证明。需要指出的是，很多介绍冯康工作的文章中都提出冯康1965年的经典性文章（后由李波翻译的英文版本Difference Scheme Based on Variational Principle 全文可见 http://lsec.cc.cn/fengkangprize/article.html）给出了近似解的误差估计，但这是不符合实际的。冯康的论文并没有给出误差估计，这方面的工作由捷克的M. Zlamal于1968年给出（On the Finite Element Method，德国出版的《数值数学》，第12卷，394-409页）。Zlamal (1924-1997) 时任捷克布尔诺（Brno）科技大学教授。Zlamal的文章用到J. Céa于1964年用法文发表的一个重要不等式以及P. G. Ciarlet 1966年的博士论文。

意大利数学家Brezzi(左一)是有限元理论的重要代表人物。1983年，中法有限元会议在北京召开，这是冯康和黄鸿慈会议期间与Brezzi夫妇的合影。

由中国数学家冯康等开创的这一研究，在其后的数十年中，捷克/美国（代表人物I. Babuska）、美国（代表人物J. Douglas和J. Bramble）、法国（代表人物P. Ciarlet和P. Raviat）、意大利（代表人物F. Brezzi）等许多学者广泛参

法国科学院院士、中国科学院外籍院士、香港城市大学教授 P. G. Ciarlet

与，最终确定有限元的逼近性质、逼近精度、有限元尺寸和多项式阶次的关系，使有限元方法实现质的飞跃。在这些分析中，广义函数论、索波列夫空间理论、偏微分方程的希尔伯特空间方法等现代数学理论都起着重要的作用。顺便说一下，前面提到的法国人 P. Ciarlet 2003 年以后一直在香港城市大学工作，他是法国科学院院士，今年更锦上添花地成为中国科学院外籍院士。他于 1970 年代末写的有限元专著，成了研究有限元理论的学者们必读的参考书。

毋庸置疑，有限元法的发现让冯康成就了数学骄子的梦想，让他得以自信地步入世界级数学大师的殿堂。

时至半个世纪后的今天，有限元方法的理论不仅在应用数学领域被广为接受，即使在纯数学领域也得到认可。2002 年，在北京举行的世界数学家大会上，美国的 D. Arnold 作了一个小时的大会报告。在 2006 年西班牙马德里举行的世界数学家大会上，意大利的 A. Quarteroni 也作了一个小时的大会报告。两个人都是有限元方面的专家。在纯数学统治下的数学家大会上，连续两届有两个一个小时的报告，足见有限元这一研究方向受到的重视程度。

由于数学家揭示了有限元的普遍性，由于其 Ritz-Galerkin 方法的理论基础，使得有限元方法和技术已经成为当今科学与工程计算的重要方法，其应用更是早已跨越出航空航天和土木建筑，进入石油化工、电机工程、国防、风电能源等与国民经济密切相关的重大行业，以及与民生密切相关的电子电器、汽车制造等行业领域。近些年，随着社会现代化脚步的加快，有限元也应用于解决包括生物计算、医学计算、电磁场计算、数值天气预报、数值海洋预报等很多重大的问题。有限元方法将很多成功的数学方程转化为近似的数字式图象。

今天，在化工过程中，数值模拟的应用也相当普遍，它在优化原有的或设计新的工艺和原型上显示出越来越重要的作用。在医学方面，医学图像诊疗向导在当今的医学界已经有广泛的应用。医师们可通过定量分析与仿真模拟技术来制定治疗计划和外科手术。这些仿真模拟往往和有限元的应用是分不开的。

值得一提的是，有限元的精度问题目前也越来越受重视。事缘 1991 年 8 月 23 日挪威的一个海上钻井台，仅仅是因为一个有限元的计算结果不够精确，应力计算低估了百分之四十七，导致海上平台倒塌，损失超过七亿美元。虽然这二十年货币已经贬值很多，但即使是今天来看，七亿美元也是很惨重的损失。

毋庸置疑，有限元方法的发现对二十世纪乃至未来世界的经济都会产生重大的影响，有限元法的发现也让冯康成就了数学骄子的梦想，让他得以自信地步入世界级数学大师的殿堂。

尽管在有限元发现之初，冯康和他的团队并没有引起太多的重视与奖励，甚至还引来了不少的争议，但是经过历史时间的磨砺，经过科技进步的检验，有限元依然成为冯康最闪光的成就，而提到有限元我们自然会和冯康的名字连在一起。

未完待续

作者之一于 2010 年在北京采访崔俊芝院士

冯•诺伊曼：因为他世界更加美好

蔡天新

从爪子判断，这是一头狮子。

—— 丹尼尔•贝努利

一颗匪夷所思的大脑

他本是东欧一位富有的银行家的公子，放浪不羁喜欢逛夜总会，却成了二十世纪举足轻重的人物。二战以前他是一位杰出的数学家和物理学家，是美国普林斯顿高等研究院首批聘请的五位终身教授中最年轻的一位（二十九岁，最年长的爱因斯坦五十四岁）。二战期间盟军离不开他，无论陆军还是海军，美国还是英国，因为他是最好的爆炸理论专家，也是第一颗原子弹的设计师和助推人。二战以后，他创立的博弈论极大地开拓了数理经济学的研究，至少影响了十一位诺贝尔经济学奖得主的工作。而他贡献最大的则可能是在计算机理论和实践方面，被誉为“电子计算机之父”。简而言之，他是二十世纪美国引进的最有用的人才。此人不是别人，正是本文的主人公，匈牙利出生的美国犹太人约翰・冯・诺伊曼。

冯・诺伊曼身材敦实，有一双明亮的棕色眼睛和一张随时可以咧嘴一笑的脸。这些都寻常可见，可是，要取得如此丰富伟大的成就，必然有一颗奇异的大脑。首先，他对自己专注的事情，有着惊人的记忆力，能够整页背诵十五年前读过的英国作家狄更斯的

冯•诺伊曼

小说《双城记》和《大英百科全书》中有启示性的条目。至于数学常数和公式，更是塞满他的大脑，且随时可以提取出来。其次，他的阅读速度和计算能力也同样惊人。据说在少年时代，上厕所时他有时也要带着两本书，成名后他的助手或研究生经常会觉得自己像是在“骑着一辆自行车在追赶载着冯・诺伊曼博士的快速列车。”当他做计算时，样子有些古怪，往往眼睛盯着天花板，面无表情，此时他的大脑在高速运转着。如果是在快速运行的火车上，他的思想和计算速度也会加快。

他是一位杰出的数学家和物理学家，是美国普林斯顿高等研究院首批聘请的五位终身教授中最年轻的一位。他是二十世纪美国引进的最有用的人才。

如果说上述几种能力显示了他神奇的一面，那么下面一种能力并非那么高不可攀，那就是不断学习新事物的愿望和行动。在柏林大学求学期间的一个暑假，化学系本科生冯•诺伊曼返回布达佩斯家中，结识了一位准备去剑桥读经济学的小老乡，立刻向他咨询并要求推荐经济学的入门书籍，从此开始牵挂这门对他来说全新的学科。还有一次，他被邀请到伦敦，指导英国海军如何引爆德国人布下的水雷，却在那里学到了空气动力学的知识，同时对计算技术发生了浓厚的兴趣。前者使他成为研究斜冲击波的先驱，后者让他开数值分析研究的先河。而他对电子计算机的直接介入，则起因于月台上的一次邂逅，他在旅行途中尤其多产。让人惊叹的是，他的所有成就都是在他主要从事别的工作时取得的。

对一个经常需要与各种各样出类拔萃的科学家合作，有时甚至要与政治家、军事家打交道的人来说（从美国数学会主席到总统特别顾问他都担任过），还需要具备敏锐的政治嗅觉和平衡能力。二战以前冯・诺伊曼就曾预言，德国将会征服孱弱的法国，犹太

匈牙利首都布达佩斯：冯•诺伊曼度过青少年的地方

人会惨遭种族灭绝，如同一次大战期间土耳其的亚美尼亚人所遭受的屠杀一样;之后，乘着两个劲敌（德国和苏联）鹬蚌相争，美国会坐收渔利。他还认定，苏联人迟早会发明核武器，因为“原子弹的秘密很简单，受过教育的人都会研制”。至于平衡能力，对他来说可能是与生俱来的，而非雄心所致，他不需要花钱去改善公共关系。他还有一个显著的特点，不事张扬也不喜欢与人辩论，遇到紧张的气氛时善于利用讲段子和逸闻将其化解。

冯·诺伊曼天才的大脑也存在着不足。最主要的是，他不像爱因斯坦和牛顿那样有独创性。但他却能抓住别人原创的思想火花或概念，迅速进行深入细致的拓展，使其丰满、可操作，并为学术界和人类所利用。

当然，冯・诺伊曼天才的大脑也存在着不足。最主要的是，他不像同事爱因斯坦和牛顿那样有独创性。但他却能抓住别人原创的思想火花或概念，迅速进行深入细致的拓展，使其丰满、可操作，并为学术界和人类所利用。爱因斯坦来到美国之后，只是个象征性甚或装饰性的人物，没有发挥多大的作用，而冯・诺伊曼的所作所为却是无可替代的。鹰派成员、海军上将斯特劳斯认为，“他有一种非常宝贵的能力，能够抓住问题的要害，把它分解开来，最困难的问题也会一下子变得简单明了。我们都奇怪怎么自己没能如此清晰地看穿问题得到答案。”诺贝尔物理学奖得主维格纳在被问及冯・诺伊曼对美国政府制订科学和核政策的影响力时也曾谈到，“一旦冯・诺伊曼博士分析了一个问题，该怎么办就一清二楚了。”

当所有这些素质都加在一起，集中到一个人身上，他的优势便显得非常突出了。维格纳从小与冯・诺伊曼在布达佩斯一起长大，他承认在这位比自己低一届的中学校友面前怀有自卑情结，他在获得诺贝尔奖后接受了著名的科学史家、《科学革命的结构》一书作者库恩的采访。“您的记忆力很好，是吗？”“没有冯・诺伊曼好。不管一个人多么聪明，和他一起长大就一定有挫折感。”另一位诺贝尔奖得主、德裔美国物理学家贝特和维格纳一样，都是冯・诺伊曼在洛斯阿拉莫斯实验室的老同事，他曾经发出这样的感叹，“冯・诺伊曼这样的大脑是否意味着存在比人类更高一级的生物物种？” 在人类历史上，他属于那种在黑板上写几个公式就能改变世界的少数几个人之一。法国数学家、布尔巴基成员迪厄多内甚至相信，冯・诺伊曼是“最后一个伟大的数学家”。

午餐时分的家庭聚会

1903年12月28日，冯•诺伊曼出生在多瑙河畔的匈牙利首都布达佩斯，原名

冯•诺伊曼的少年时代

布达佩斯自由广场

多瑙河上的大桥

布达佩斯夜景

Neumann Janos（诺伊曼•亚诺什）。其时匈牙利和奥地利虽然组成了奥匈帝国，但那只是外交和军事上的联合，内政和经济各自独立，且有自己的国名、国王和语言。与绝大多数欧洲人不同而与中国人一样，匈牙利人的姓在前名在后，这成了学者们考证他们的祖先来自中亚或蒙古草原的重要依据。需要说明的是，亚诺什相当于英文里的约翰，它们的昵称分别是扬奇和约翰尼。冯•诺伊曼十岁那年，做银行家的父亲因为担任政府经济顾问有功，被授予贵族头衔，从此家族姓氏前面多了一个von，变成了冯•诺伊曼。而在他移居到美国以后，全名就成了约翰•冯•诺伊曼。

在冯•诺伊曼出生前的三十五年里，布达佩斯一直是欧洲发展最快的城市，如同纽约和芝加哥（内战战胜方）是美洲发展最快的城市。人口从全欧第十七名一举跃为第六名，仅次于伦敦、巴黎、柏林、维也纳和圣彼得堡。布达佩斯率先实现了电气化，铺设了欧洲第一条电力地铁，并用电车取代了公共马车（彻底清除了散布病菌的马粪）。就在冯•诺伊曼出生那年，横跨多瑙河的伊丽莎白大桥建成，那是当时世界上最长的单孔桥。那会儿匈牙利正处于黄金时代，布达佩斯颇有些巴黎的情调和氛围，仅咖啡馆就有六百多家，歌剧院的音响效果甚至超过了维也纳，来自世界各地可供挑选的保姆不计其数，夜总会里迷人的女郎耐心地倾听客人们的政治主张。

在一次大战爆发前的半个世纪里，布达佩斯和纽约是世界各国聪敏的犹太人优先考虑移民的城市。在这两处人间天堂里，他们迅速成为医生、律师那样的专业人士或成功的商人。相比之下，移民到纽约的犹太人大部分出身较为低下。这是由于当时交通工具的限制，横渡大西洋的船票惟下层的统舱比较低廉，能够乘坐豪华客轮的只有极少数的富豪，且漂洋过海生命无法保障。布达佩斯更为那些中产阶级和上层社会的犹太人向往和喜爱，那里还有理想的中学教育环境。尤其重要的是，在中欧其他国家犹太人仍低人一等的时候，在匈牙利已经有所改变。主要原因是当一些少数民族酝酿暴动的时候，犹太人坚定地站在主要民族马扎尔族一边，他们的先见之明后来得到了回报，歧视性的法令被逐一废除。值得一提的是，出生在布达佩斯的犹太人中，还包括犹太复国主义的创始人赫茨尔。

冯•诺伊曼的祖上来自俄罗斯，他的父亲出生于紧邻塞尔维亚的匈牙利南方小镇，他在故乡接受了良好的乡村教育，中学毕业后来到首都布达佩斯，通过律师资格考试后进入银行，开始了兴旺发达的事业。他广泛交际的朋友中有一位法学博士，后来成为上诉法庭的大法官。有趣的是，他们两人成了连襟，并通过联姻成为殷实的犹太家族的一员。冯•诺伊曼的外祖父与人合伙经营农业设备，成功借鉴了美国西尔斯公司的销售经验，四个千金全部招了入赘女婿，一家占据了布达佩斯一条繁华商业大街的两侧，底层是商铺，上面是住宅。冯•诺伊曼在店铺的楼上长大，比他晚二十多年出生的英国政治家撒切尔夫人也是这样。

在冯•诺伊曼十岁以前，他接受的是典型的犹太式教育，也就是请家庭教师授课。在那个年代，家庭教师和保姆也是中上层阶层的组成部分。外语学习特别受重视，不少家长认为，只会说马扎尔语的孩子将来连生存都成问题。先是德语，然后是法语和英语。年龄稍长以后，还要学拉丁语和

希腊语。说到拉丁语，她在匈牙利已经被教授了几百年。这是一种公理化的语言，会使人头脑条理化，逻辑性增强。可以说，正是早年的拉丁语训练，帮助冯•诺伊曼后来创造出计算机语言。当然，数学也至关重要。从小他就表现出计算方面的天赋，可以快速心算两个四位数或五位数的乘积，这方面的遗传来自他的外祖父。冯•诺伊曼注意到，数学并非抽象枯燥，而是有一定的规律可循。母亲的艺术素养帮助他发现数字的优雅，后来这成为他对学问境界的一个要求。

对历史，冯•诺伊曼也非常酷爱，据说他曾在极短的时间里，啃完一套四十四卷的《世界史》，且书中夹满了小纸条。当然，冯•诺伊曼并非万能，比如他在击剑和音乐方面才华平平，甚至因为击剑教练的称谓的缘故，他后来一直反感被人家叫“教授”。虽然家里请来出色的大提琴教师，但他似乎永远处于指法练习阶段。不过，匈牙利犹太人中不乏伟大的指挥家和钢琴家，移居美国的就有芝加哥的索尔蒂、费城的奥曼迪、克里夫兰的塞尔、达拉斯的多拉蒂。至于美语里的电影一词 movie，很有可能从匈牙利语 mozi 演变而来，后者是匈牙利第一家电影制片厂。正是移居美国的匈牙利人创造了好莱坞，其中包括福克斯和祖可，后者是派拉蒙公司的奠基人。而当老冯•诺伊曼的银行业取得成功以后，也开始投资电影业和戏剧。

冯·诺伊曼家有一个很好的传统，那就是午餐时分的家庭聚会。孩子们争相提出一个个问题供大伙讨论，比如海涅的某一首诗、反犹主义的危害性、“泰坦尼克”号的沉没、外祖父的成就，等等。

贝特(Hans Bethe, 1906-2005)，因在1938年解释了为什么恒星能够长时间向外释放如此之多的能量而获得1967年诺贝尔物理学奖。贝特对冯•诺伊曼极为佩服。

必须提及的是，冯•诺伊曼家有一个很好的传统，那就是午餐时分的家庭聚会。孩子们争相提出一个个问题供大伙讨论，比如海涅的某一首诗、反犹主义的危害性、“泰坦尼克”号的沉没、外祖父的成就，等等。（相比之下，如今中国大学学生餐厅里最不缺少的就是高清晰的电视机。）在那个时候，大人不会把自己的观点强加给孩子。有一天，小冯•诺伊曼提出，眼睛的视网膜成像原理不同于照相负片上的小颗粒，应该是多通道或多区域输入，而耳朵可能是单道或线性输入。综观他的一生，都对中枢神经系统的运转技术和人工输入机器或机器人的技术之间的区别感兴趣。当他第一次见到有声电影时，惊讶于声音明明是从银幕上看不到的扬声器里发出，看起来却好象是从演员的嘴巴里说出。冯•诺伊曼度过了幸福的童年，他后来娶到的两任夫人都是昔日一起玩耍的邻家女孩。

十岁那年，冯•诺伊曼上了中学，在英语和法语里一般叫公学或文法学校，在德语里叫 gymnasium。那些视德国为精神领袖的国家，包括奥匈帝国也用这个词，本意是体育馆或健身房。自古希腊以来，那里便是年轻人赤身裸体参与竞争的地方。那时候匈牙利采用精英教育，引入激烈的竞争机制，对十分之一高智商的学生精心培养，对其余的孩子听之任之。这项政策有利于犹太人的脱颖而出，对他们来说，研究理性的数据比与人打交道更容易。连爱因斯坦也承认，“自己喜欢从你我的世界逃脱，去物的世界。”二战结束后，日本模仿了匈牙利的精英教育模式，以考取东京大学学生多少衡量一所中学的水准，不仅迅速提升了经济实力，还培养出十多位诺贝尔奖和菲尔兹奖得主。日本人赶超的是战胜他们的美国人，正如匈牙利人希望超越“可恨的奥地利人”。相比之下，目前中国的教育可能缺乏这方面的动因。

冯•诺伊曼进了用德语授课的路德教会学校，在那前后，共有四位年龄相仿的犹太男孩进入布达佩斯三所最顶尖的学校，他们后来全部移居美国。除了冯•诺伊曼以外，还有齐拉特、维格纳和特勒，主要是依靠这四个匈牙利人，美国研制成功了原子弹和氢弹。正是后面这三位物理学家在 1939 年夏天说服爱因斯坦给弗兰克林•罗斯福总统写信（实为齐拉特执笔），建议发展原子弹，才有了“曼哈顿计划”。齐拉特的贡献在于率先提出了链式反应的理念，维格纳建立了中子吸收理论，并协助费米建成首座核反应堆，


Dennis Gabor


Georg von Békésy


Theodore von Kárman


John von Neumann


Leo Szilard

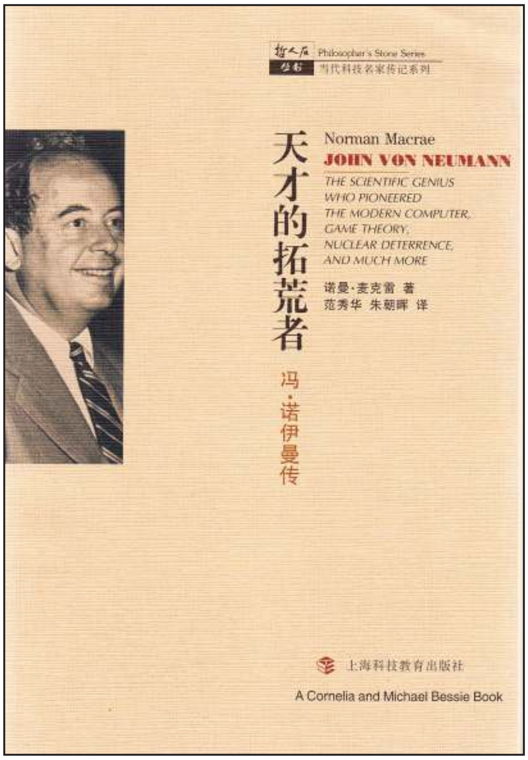

Edward Teller


Eugene Wigner

二战前从匈牙利走出的精英: 1971年诺贝尔物理学奖得主伽柏(Dennis Gabor);
1961年诺贝尔医学奖得主贝凯希(Georg von Bekesy); 超音速飞机之父, 钱学森的导师冯•卡门(Theodore von Karman);
冯•诺伊曼; 原子弹先驱齐拉特(Leo Szilard); 氢弹之父, 杨振宁的导师特勒(Edward Teller);
1963年诺贝尔物理学奖得主维格纳(Eugene Wigner)

而特勒（华裔物理学家杨振宁的博士导师）则被誉为“氢弹之父”。作为犹太人，这四位科学家对纳粹德国和昔日的沙皇帝国有一种恐惧和厌恶感，这促使他们奋不顾身地投入核武器的研制。

1914年也是一次大战爆发的年份，奥匈帝国因奥地利王储遇刺向塞尔维亚宣战，俄罗斯和德国迅速卷了进来。冯•诺伊曼家族因为地位高无人服兵役，战时仍可到威尼斯等地旅行。同盟国战败后，俄罗斯末代沙皇尼古拉二世被列宁的红色政权取代，匈牙利也被邻国瓜分走三分之二的土地。可是，精英教育并未受影响，中学校长十分赏识冯•诺伊曼的数学才华，把他推荐给布达佩斯大学的教授。十七岁那年，他与一位教授合作研究车比雪夫多项式根的求解，在一家德国杂志发表了处女作。1921年，冯•诺伊曼以获得厄特沃什奖圆满地结束了自己的中学时代，这个奖的得主还有齐拉特、特勒，以及工程学家、超音速飞机之父——冯•卡门，后者也是中国核工业奠基人钱学森的博士导师。



天才的拓荒者：数学天才冯•诺伊曼的故事

辗转在欧罗巴的土地上

中学的最后一年，老冯•诺伊曼便开始为儿子的前途操心。他征询过许多朋友的意见，包括当时担任共产党-社会民主党联合政府教育部次长的冯•卡门。最后决定，儿子要学化学工程。这就像新千年之交的中国，很多家长希望孩子读计算机和生物学一样，长辈的意志强加在了后辈身上。小冯•诺伊曼要去柏林大学和苏黎世联邦工学院（ETH）学习化学工程，但他真正感兴趣的却是数学，而数学家在匈牙利前景并不看好。结果，他一边在柏林和苏黎世学化工，一边在布达佩斯大学注册成为数学博士候选人。也就是说，尚且不满十八岁的年轻人要在相距遥远的三座城市兼读跨专业的本科生和研究生。由此可见，冯•诺伊曼父子是多么的自信和坚毅。

1921年秋天，冯•诺伊曼来到德国首都柏林。原先以为，他要拜著名的犹太化学家哈伯为师。这个哈伯非常了得，他在1915年发明了毒气，极大地帮助一战时期四面受敌的德国。1918年德意志战败，同年哈伯却因另一项发明——用氢和氮合成氨——获得诺贝尔化学奖（物理学奖的得主也是德国人、量子力学的开创者普朗克），他成了一战期间唯一的化学奖得主。这一点足以说明，瑞典确实保持了中立国的立场。可是，冯•诺伊曼到柏林以后，却意外地“失踪了两年”。他不仅没有去拜访哈伯，还时常在上化学课时逃学。那个年代柏林的性服务业臭名昭著，荒淫无度，对手持外币的年轻人来说又十分廉价，冯•诺伊曼夫妇对这些令人担忧的事耳有所闻。

事实上，这种担心有些多余，对于生性活跃而又有远大理想的冯•诺伊曼来说，既然不会满足于一个专业方向，更不会沉湎于一种娱乐或游戏的。那时他的主要兴趣在集合论方面，虽然他在柏林大学听过爱因斯坦关于统计力学的讲座，但更多的受到数学老师施密特教授的影响。施密特是希尔伯特早年的学生，也是策梅罗（Zermelo）的朋友。后者为消除著名的罗素悖论率先提出了一个公理化的集合论，可惜在明确性方面存在一个歧义。几年以后，另一位德国数学家弗兰克尔（Fraenkel）提出了替代公理，这个集合论因此被称为ZF集合论或ZF系统。当1931年哥德尔证明了不完备性定理以后，ZF系统成为康托尔连续统假设成立的惟一希望。直到1963年，这一希望才被美国数学家柯恩摧毁，后者因此得到了菲尔兹奖。

1923年，冯•诺伊曼终于完成了他的长篇论文，投给施密特担任编委的德国《数学杂志》，后者把它交给弗兰克尔审阅。弗兰克尔读后深感震惊，随即邀请二十岁的冯•诺伊曼到德国中西部的马伯里作客，最后建议他以《集合论的一种公理化》为题发表。冯•诺伊曼所建立的公理体系后经瑞士数学家贝尔纳斯（Bernays）和奥地利数学家哥德尔（Godel）的完善，形成了集合论中一个新的系统——NBG系统。现已证明，NBG系统是ZF系统的扩充，至今它仍是集合论最值得信赖的基础之一。值得一提的是，在文章的最后冯•诺伊曼写道，“没有一种已知的方法可以避开所有的困难。”换句话说，他已经隐约预见到哥德尔革命性成果的出现。

冯•诺伊曼画像

冯•诺伊曼在自家的客厅里

多年以后，已经移居以色列的弗兰克尔回忆起这段往事，说他自己当时就断定这是一篇了不起的文章。他还引用十八世纪瑞士数学家丹尼尔•贝努利读到牛顿的论文时说过的一句话，“从爪子判断，这是一头狮子。”这篇论文尚未发表，已经在重量级人物中间传阅，从那时起，这位化学系的本科生便时常受邀到哥廷根，成为数学大师希尔伯特家的常客。两位相差四十多岁的一老一少常在书房或花园里一待就是几个小时，弄得哥廷根一些教授心里不是滋味。可以说，冯•诺伊曼“失踪的两年”与十七世纪牛顿返回故乡躲避鼠疫的两年颇为相似，后者借机发明了近代科学。不同的是，牛顿是在静谧的农庄，而冯•诺伊曼却在繁华的都市。值得一提的是，也是在那两年里，现代主义文学的代表作——艾略特的《荒原》和乔伊斯的《尤利西斯》得以问世。

现在，让我们把目光转向苏黎世。冯•诺伊曼在柏林的两年，只是修了化学的一些基础课程，拿学位却要到苏黎世。1923年秋天，他在苏黎世联邦工业大学轻松通过了一年一度的入学考试（爱因斯坦考了两次），开始了第二阶段的学习。第一学期他的功课全优，包括有机化学、无机化学和分析化学，有意思的是，在数学方面成就斐然的他不得不修最基础的高等数学。两年以后，他勉强读完了化学工程的全部课程，摔破的实验室玻璃容器难以计数。其时，他早已经与这所大学两位最好的数学家——外尔和波利亚建立了密切的关系。外尔去外地讲学开会的时候，身为化学系本科生的冯•诺伊曼会替他代课。匈牙利老乡兼师兄波利亚回忆过一件往事，有一次他在课堂上提起一个悬而未决的数学问题，没想到下课时已经被冯•诺伊曼解决了。

从那时起，这位化学系的本科生便时常受邀哥廷根，成为数学大师希尔伯特家的常客。两位相差四十多岁的一老一少常在书房或花园里一待就是几个小时，弄得哥廷根一些教授心里不是滋味。

1925年夏天，冯•诺伊曼在苏黎世联邦工业大学获得化学工程学士学位。次年春天，他在布达佩斯大学通过数学博士论文答辩，年仅22岁。他名义上的博士导师是布大数学系主任费耶，师兄弟中除了波利亚还有爱多士和图拉。在希尔伯特的安排下，他来到哥廷根做访问学者，此时他已经被量子力学迷住了。在那以后，他被柏林大学聘为无薪讲师（privatdozent）。这是十九世纪德国为那些有意走学术之路的年轻人设置的岗位，也是取得教授席位的必由之路。不仅没有编制，连薪水也不发，所得酬劳全部来自修课学生的学费，迫使年轻人发奋图强。对冯•诺伊曼那样有钱人家的公子这不成问题，对家境贫寒的爱因斯坦来说无疑是一种折磨了，这应是他一直躲在伯尔尼做小小的专利员，迟迟未去大学工作的原因。

冯•诺伊曼在柏林大学待了两年以后，又转到了汉堡大学。在担任无薪讲师期间，他在集合论、代数学和量子理论方面取得了一系列重要的研究成果，受到了数学界的瞩目。例如，在测度论方面，冯•诺伊曼发表了《一般的测度理论》，把测度问题从欧氏空间推广到一般的非阿贝尔群，证明了所有可解群都是可测度的。可是，这项工作并不像他早先发表的《集合论的一种公理化》那样，在集合论中处于中心地位。在算

普林斯顿高等研究院大楼；研究院首批聘请的五名终身教授中有爱因斯坦和冯•诺伊曼。冯•诺伊曼是最年轻的终身教授，年仅29岁；当时常被误认为是研究生（刘建亚 摄）

子理论方面，冯・诺伊曼首先给出了希尔伯特空间的抽象定义；然后，把这个空间上的自共轭算子谱理论从有界推广到无界，从而建立起了自己的谱理论，这是"抽象数学之花"——泛函分析诞生的必要条件。相比之下，那段时间里冯・诺伊曼在量子理论方面的工作最出色也最重要。

迄今为止，牛顿力学仍统治着这个世界的大部分领域，适用于我们肉眼所能看见的一切事物。只有当物体运动速度太快时，爱因斯坦相对论的某些定律才开始起作用。而当物体太小时，量子力学起了支配作用，它使得我们能够描述分子、原子和电子的状态。"量子"一词的拉丁文含义是"多少"，如同普朗克所发现的，光、X射线以及其他的波只能一份份地发出，每一份称为"一个量子"。量子力学是理论物理学和现代技术的基础，它直接导致了电子革命和原子弹的诞生。量子力学的一个基本点是原子状态的数学描述，冯・诺伊曼赋予它以全新的形式：原子的状态是由希尔伯特空间中的单位向量表示，这就使得量子力学的两种表示方式——海森堡的矩阵力学和薛定谔的波动力学相互统一。

大萧条时期的美利坚

冯・诺伊曼之所以愿意接受汉堡大学无薪讲师的职位，是因为那里比柏林有更多升迁的机会（那年春天他的父亲去世了）。如果他真的做上汉堡大学的教授，那么几年以后中国留学生陈省身有可能成为他的学生。没想到当年秋天（1929），美国的普林斯顿大学便向他伸出橄榄枝，邀请他担任客座讲师。原来此前，他在苏黎世的老师外尔到普林斯顿做了一年的访问教授，适逢希尔伯特退休。外尔奉命返回哥廷根接替老师的职位，尽管师生两人的哲学观点相互背离。于是，外尔向美国人推荐了冯・诺伊曼。显而易见，客座讲师只是一个过渡职位。可以说，因为德国教授位置的稀缺，也因为战争的逼近，让美国获得一个不可多得的人才。冯・诺伊曼先是回了趟布达佩斯，皈依为天主教徒，完成了一桩

普林斯顿高等研究院用冯•诺伊曼命名了宿舍区的一条环形小径，叫做von Neumann Drive。图为von Neumann Drive宿舍的秋景。（刘建亚 摄）

人生大事——结婚。随后，他便携带着新婚妻子，在法国的瑟堡乘船渡过了大西洋。

虽然那会儿美国正处经济大萧条，但冯•诺伊曼第一眼就爱上了这个移民国家。这里的人讲究实效、言之有物，不墨守成规。果然第二年，他便顺利晋升教授。又过了两年，雄心勃勃的普林斯顿高等研究院成立，冯•诺伊曼成了首批聘请的终身教授。不过，这得感谢外尔的临时退出，虽然冯•诺伊曼原本就是考虑的对象，但由于年纪太轻，加上普林斯顿大学舍不得，一直没有敲定。外尔最终还是接受了高等研究院的邀请，那是在获知希特勒当上德国总理以后。加上爱因斯坦，普林斯顿高等研究院首批聘请的五位教授中，有三位来自德国。这三个人当中，只有外尔不是犹太人，但他是犹太人的女婿。有人作过统计，1933年及以后从德国移民到美国的科学家中，有十一人已获得或后来获得诺贝尔奖，十人参与“曼哈顿计划”。

说到普林斯顿高等研究院，人们的印象似乎只有羡慕和崇拜了。即便在大萧条时期，教授们仍拿着高薪，而不用承担任何义务。那里还有一些奇怪的规则，比如，从不招收研究生，只吸纳优秀的博士做博士后研究，为他们日后寻找工作提供跳板；又比如，虽然有物理学家，但不设任何实验室。对此，有不少人不以为然。“曼哈顿计划”的领导人奥本海默就不愿意当那里的教授（后来他不仅当了而且还做了院长），认为那是“一个疯人院：在那里，惟我独尊的星星们孤独、绝望地发着各自的光。”数学家柯朗（希尔伯特的另一个学生）和物理学家费恩曼（诺贝尔奖得主）都认为，在自己缺少灵感时，学生们“提出的相关问题”会刺激他们，“教学和学生使得生活有意义”。

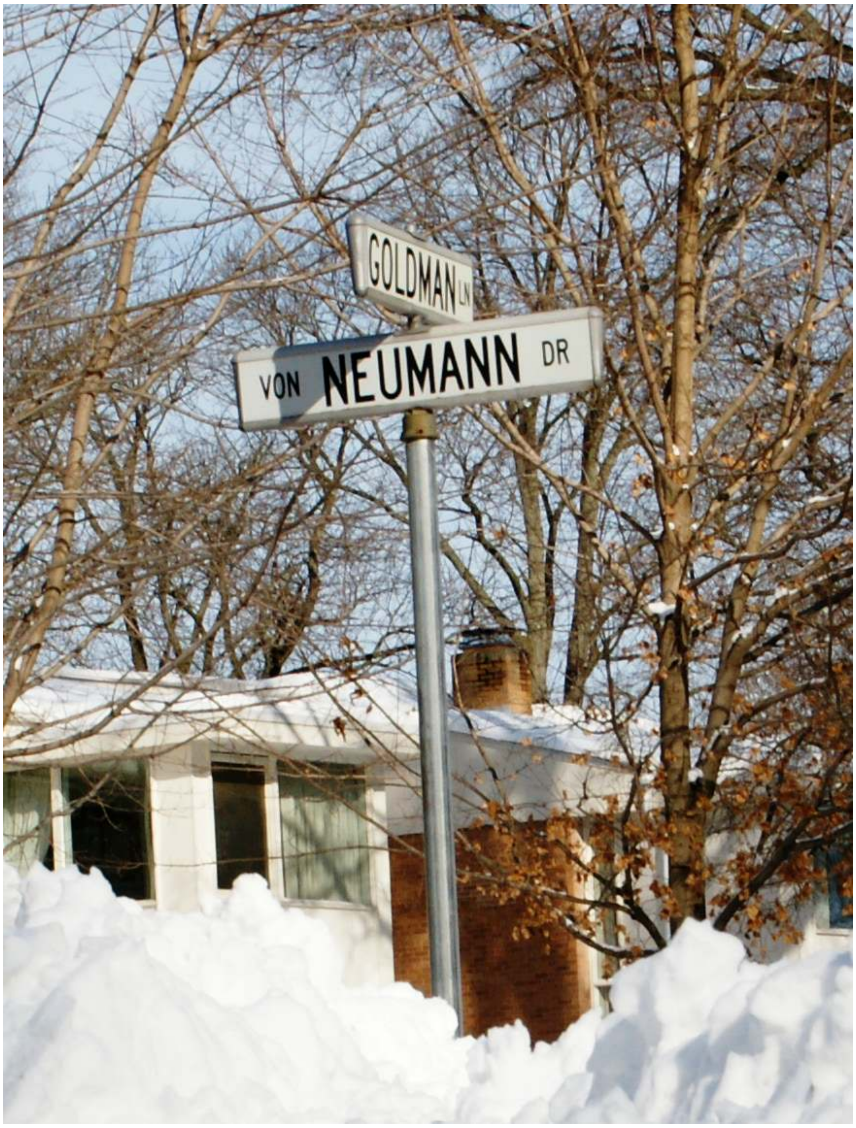
即便是爱因斯坦，也在普林斯顿高等研究院感受到了压抑的气氛。他在给爱丁堡的物理学家玻恩的信中写到，

“我觉得自己像是在穴中冬眠的熊。”当初他从欧洲抵达美国，纽约市长带着一支乐队到码头恭候，结果却吃了闭门羹，一艘汽艇直接把客人接到了新泽西海岸。甚至罗斯福总统夫妇邀请爱因斯坦共进晚餐时，也被高等研究院方面婉言谢绝。有些人以为，顶尖科学家都不食人间烟火，伟大的思想都出自真空。爱因斯坦依然勤奋，他试图找出量子理论中矛盾的地方（的确存在），却劳而无获。他在给比利时女王的信中写到，“一座古怪而死板的村庄，住着一群盛名之下其实难副的人”，落款地是“集中营，普林斯顿”。

冯·诺伊曼写出了“算子环”的系列论文。算子环是有限维矩阵代数的自然推广，后来成为量子物理学的强有力武器，并催生出连续几何学这一副产品。人们将其命名为冯·诺伊曼代数。

即便是冯·诺伊曼，在普林斯顿高等研究院过得也不开心，每到夏天来临，他都携带妻女迫不及待地返回欧洲。三年以后的那个夏天，他的妻子没有跟他回来，此前她在普林斯顿因为生活习惯不同频出洋相。他们唯一的女儿跟妈妈走了，直到上中学后才回到爸爸身边，那时冯·诺伊曼早已娶了另一位儿时伙伴。不过，他的学术研究从来没有停止过，且总是成绩卓著。上个世纪九十年代，当高等研究院快要迎来六十华诞时，院方认真总结了三个标志性的成果，分别是：哥德尔对连续统问题的研究，杨振宁和李政道推翻宇称守恒定律，冯·诺伊曼的工作。当然，现在必须加上怀尔斯对费尔马大定理的证明。

在普林斯顿大学期间，冯·诺伊曼从数学意义上总结了量子力学的发展，出版了《量子力学的数学基础》，至今依然是一部经典著作。此外，他还推出统计学中著名的弱遍历定理。受聘高等研究院的当年，他在群论方面的研究取得了突破，在紧致集情况下解决了希尔伯特第五问题。在年轻数学家默里的协助下，冯·诺伊曼写出了“算子环”的系列论文。算子环是有限维矩阵代数的自然推广，后来成为量子物理学的强有力武器，并催生出连续几何学这一副产品。人们为了纪念他，将其命名为冯·诺伊曼代数。在格论方面他率先发现了“布尔”代数中交与并的运算必然是无穷分配的，这种分配性又等价于连续性。这一切，应归功于他的年轻和持续的创造力，他是一个懂得如何放松思考的人。



普林斯顿高等研究院的von Neumann Drive大雪街景（刘建亚 摄）

水雷和“曼哈顿计划”

1937年，冯・诺伊曼宣誓加入了美国籍。同年，日本全面反动侵华战争。接下来的两年里，德国吞并了奥地利和捷克斯洛伐克，意大利吞并了阿尔巴尼亚。可是，在西方史学家看来，1939年9月才意味着二次大战的开始，其标志是希特勒军队侵入波兰，英国和法国对德宣战。不过此前，马里兰州东北部一个叫阿伯丁的滨海小镇早已经开始忙碌了，冯・诺伊曼被邀请来这里担任陆军机械部所属的弹道试验场实验室顾问（后来又成为科学咨询委员会委员）。迎接他的是一门新的学问——火炮弹道学，科学家们早就发现，炮弹穿越浓度变化的空气的运动阻力和轨迹是非线性方程，这类方程的求解并不容易。于是，冯・诺伊曼成了前计算机时代冲击波和弹道轨迹的计算者。

不过，直到1941年底日本偷袭珍珠港，冯•诺伊曼一直没有在阿伯丁花费太多的精力，他相信英国能够暂时抵御德国的入侵，美国不会太早宣战。他与普林斯顿高等研究院的助手继续合作，撰写有关算子环的论文。期间他还涉猎天体物理学，与印度（巴基斯坦）出生的物理学家钱德拉塞卡（1983年诺贝尔奖得主）联名发表了一篇题为《恒星的无规则分布引起的引力场统计》的论文。闲暇时，冯•诺伊曼开始革新经济学，不过这得等战后才能发挥更大的作用。当然，冯•诺伊曼也与人合作写下诸如《从逐次差分估计可能误差》的研究报告，并对这篇报告作了三次增补。看得出来，他的合作意愿越来越明显，这对他未来的工作将很有帮助。

冯•诺伊曼撰写的那些报告使他成为美国最重量级的爆炸理论专家，待到美国参战几个月以后，他更是声誉鹊起，成为复杂爆破（如碰撞爆破）的计算大师，阿伯丁实验室的指挥官西蒙上校（后为西蒙将军）对其尤为崇拜。在陆军机械部名声大振后，海军机械部很快盯上他了。相比陆军上将，冯•诺伊曼更喜欢海军上将，因为陆军将军们午餐时只喝冰水，海军将军一上岸就喝酒，而他本人喝起酒来从不上头。后来，冯•诺伊曼果然被转到水雷作战处工作。起初的三个月，他在华盛顿的海军部上班，那里离普林斯顿不远。接下来的半年，他被派到英国工作，他的第二任妻子与之同行，两人乘坐轰炸机飞越了大西洋。

英国之所以需要冯•诺伊曼，是因为德国人在英吉利海峡上布下了大量的磁性水雷。起初，这些水雷一感应到金属就被吸收，随即爆炸销毁。这样，利用金属拖网很容易发现它们的位置并将其引爆。后来，狡猾的德国人在水雷中设置了机关，不在第一次感应，而是在感应若干次以后才爆炸，每只水雷都不一样，其中的模式无法破解，于是英国人不得不请求盟军帮助。这对冯•诺伊曼来说可谓是小菜一碟，他运用数学技巧轻而易举地完成了这项任务，避免了无数海军官兵的无谓牺牲。除此以外，他还根据自己对空气中和水下破坏性最强的斜击波反射的了解，为英国海军设计了锥形爆炸的方程。

到了1943年5月，华盛顿方面就要求伦敦送他们最好的爆炸理论专家回国。冯•诺伊曼却希望在英国再待上一段时间，他在这里学到了许多空气动力学方面的知识，正与一些他认为有趣的实验物理学家合作，甚至觉得“我还

后立左起第三位是美国原子弹之父奥本海默，第五位是冯•诺伊曼

冯•诺伊曼和美国海军军官在一起；
左一是IBM的总裁托马斯•沃森(Thomas J•Watson)

对计算技术也有了不同寻常的兴趣”，最后一句话很可能意味着他已经见过图灵了。说到图灵这位确立了数字计算机基本模式的英国人，几年前在普林斯顿大学攻读数学博士时，就成为冯•诺伊曼挑中的助手之一。可是，等到年中的某个时候，美国还是强行召回了冯•诺伊曼。他的下一个任务令其无法抗拒，那牵涉到人类发明的份量最重的一个词——核。可是，返回美国之初，他仍沉浸在英国刚学到的知识中，帮助陆军改善了防空系统，扩展了高空爆炸理论，不久又将其应用到水下。接下来，情况发生了变化。

冯•诺伊曼被任命为新墨西哥州的洛斯阿拉莫斯实验室顾问，这个头衔看起来并不起眼，取得的成果却极其辉煌。从那以后，他便身兼四职了（几乎每一项都是全职）：普林斯顿高等研究院、陆军机械局、海军机械局、洛斯阿拉莫斯。更有甚者，那时他在英国还留有一些尾巴工作。因此，他的某一位朋友或同行读到下面这封发信地址不详的短函也就不足为怪了，“自从我从英国回来，每个星期都要辗转三四个不同的地方。现在我在西南部（指洛斯阿拉莫斯）……圣诞节前可能还要去一趟英国……何时去、待多久我也不清楚……没办法及时回信实在失礼。”可是，冯•诺伊曼对投放日本的两颗原子弹的贡献究竟有多大呢？

众所周知，核武器的研制要依靠集体的智慧和力量，第一个取得成功的美国人更不可能例外。先是冯•诺伊曼的布达佩斯老乡齐拉特在1933年“灵光乍现”，想到了链式反应。按照他的设想，以等比级数的数量形式释放中子，可以在几百万分之一秒内，在狭小的空间里释放出超出人类想象的巨大能量。可是当时，包括爱因斯坦、卢瑟福、玻尔在内的资深物理学家都轻视他的发现，爱因斯坦甚至开玩笑说，“原子能研究就如同在黑夜里开枪射中一只体形娇小且珍稀的鸟”。当在伦敦一家医学院工作的齐拉特要求到英国海军部任职时，同样也遭到了拒绝。其时，意大利物理学家费米在罗马正以中子轰击一切可能的物质，包括铝、铁、铜、银等金属和硅、碳、磷、碘等非金属，甚至水。

> **从那以后，他便身兼四职了（几乎每一项都是全职）：普林斯顿，陆军机械局，海军机械局，洛斯阿拉莫斯。**

自从十七世纪伽利略被迫在宗教裁判所上认罪，意大利的科学事业便走下坡路了，直到马可尼（发明无线电）和费米的出现才有了转机。1934年秋天，费米轰击铀时，中子穿过了原子核并开始改变原子。四年以后，费米“因认证出由中子轰击产生新的放射性元素以及他在这一研究中发现由慢中子引起的反应”而荣获诺贝尔奖，墨索里尼政府居然同意他去瑞典。结果，他在斯德哥尔摩领完奖后，携带着犹太妻子、一对儿女和奖金直接乘船去了纽约。有趣的是，当年晚些时候柏林威廉皇帝研究所的三位科学家用慢中子轰击铀，却发现所谓的新元素其实是已知的56号元素钡。也就是说，诺贝尔奖可能发错了。幸好费米还作出了其他重要的贡献，例如他发现，用降低速度的中子容易引起被辐射物质的核反应。这一点正如速度太快的篮球容易从框上弹出，速度慢的较容易进篮一样，这种方法很快被各国同行采用了。

柏林的那三位科学家中，有德国化学家哈恩和斯特拉斯曼，最年长的是奥地利犹太物理学家迈特纳，她是居里夫人之后又一位巾帼英雄，正是她命名了“裂变”。倘若不是希特勒种族歧视，蔑视犹太人，讨厌核物理学，认为那是一种“犹太物理”，德国有可能先于美国制造出原子弹。事实上，在那个微妙的时刻，物理学家海森堡曾经向希特勒政府装备部长的同僚郑重汇报过，但希特勒知道后却不为所动。当匈牙利被德国占领，迈特纳从外籍犹太人变成了德国犹太人，她时刻担心自己遭到清洗，于是被迫出逃丹麦。留在柏林的两位同事完成了后续工作，并赢得了大部分荣誉（1944年诺贝尔化学奖）。虽然终身未嫁的迈特纳没有移居美国，但她和同事们的研究成果后来通过哥本哈根学派的领袖、海森堡从前的导师玻尔带到了美国。

此时洛斯阿拉莫斯人才济济，除了“匈牙利四人帮”以外，还有玻尔、费米，以及实验室主任、土生土长的美国物理学家奥本海默，甚至混进来

一位克格勃间谍、德裔英籍物理学家富克斯。在一堆顶尖的物理学家队伍里，一个数学家能做什么呢？虽然冯•诺伊曼非常重视数学与物理学之间的内在关系，他本人也是出色的物理学家，但主要成就是在理论物理方面，确切地说，对量子力学的数学化作出了贡献，冯•诺伊曼却通过自己的努力，成为物理学家们最尊敬的数学家。他指导了原子弹最佳结构的设计，确保体积不大可以装进一架轰炸机，同时，他还探讨了实现大规模热核反应的方案。依照他的观念，炸药和其他事物一样，可以用数字代表实验中的物理元素，只要处理得当，这些数字就可以构成整个实验。这样一来，不仅节约了时间，也节约了财力和物力。据说，每次他来到实验室，都会被同行们团团围住，向他讨教某些计算中出现的问题。

冯·诺伊曼通过自己的努力，成为物理学家们最尊敬的数学家。他指导了原子弹最佳结构的设计，确保其体积不大可以装进一架轰炸机，同时，他还探讨了实现大规模热核反应的方案。

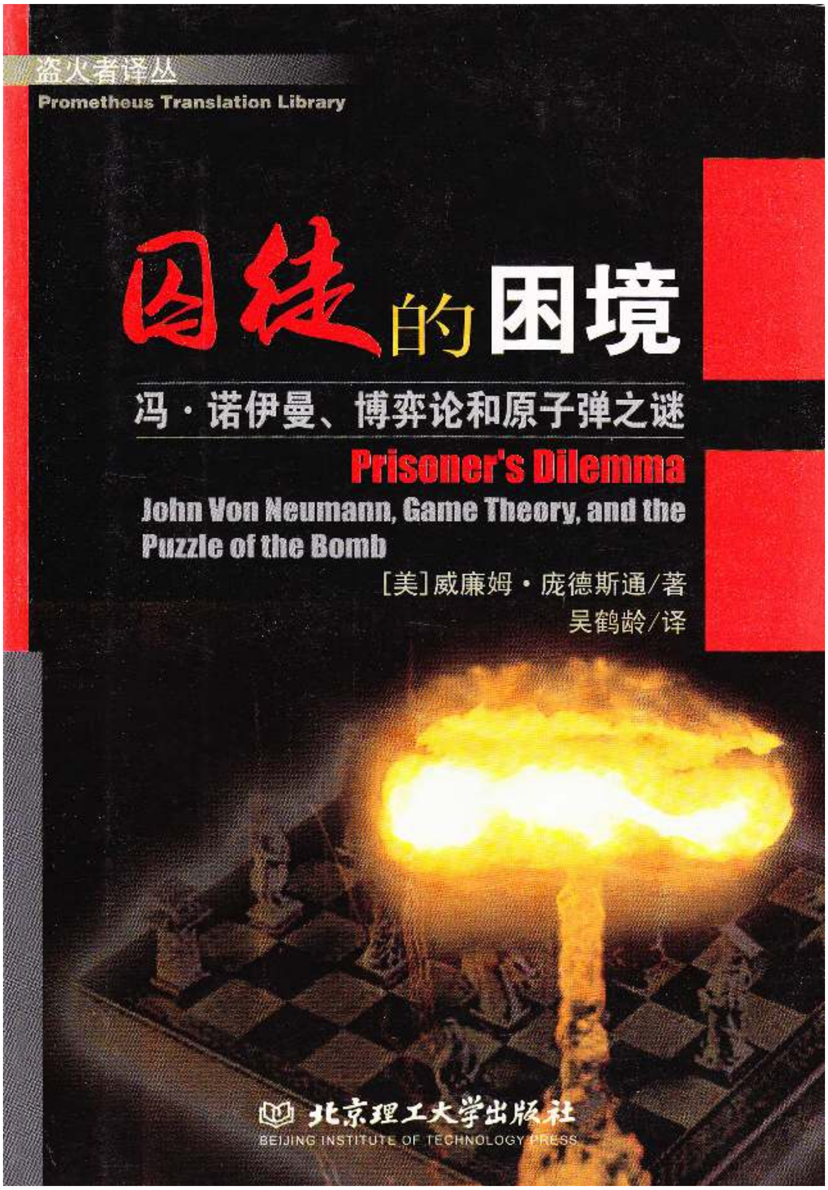
经过一段时间的协作努力，科学家们确认，铀-235和钚-239是裂变的最佳材料，投放广岛和长崎的两颗原子弹分别由这两种材料制成。（中国第一颗原子弹是铀弹，而朝鲜最近试爆的是钚弹。）两者的区别在于，钚可以通过化学方法分离获取，而铀因其同位素有着相同的化学性质，只能一个原子、一个原子地分离。这就是为何广岛原子弹投放三天以后，日本仍然没有投降的意思，因为次日有科学家报告，要制作另一颗同样的原子弹需要花费一年时间。可是，当三天后长崎也落下原子弹，天皇不得不宣布无条件投降了。钚弹的优越性在于，一个月就可以制作两到三枚。不过，当初曾遇到无法解决的难题，适用于铀弹的炮击法（用一块铀射击另一块铀）不适用于钚弹。冯•诺伊曼发挥了聚爆专家的作用，他亲自设计了一枚棱镜构成内爆装置，在第一次核试验中获得了成功（铀弹并未试爆）。

值得一提的是，当初美国计划在四座城市投放原子弹，空军列出了六个候选地点：京都、广岛、横滨、东京的皇宫、小仓军械库和新潟。冯•诺伊曼是决定投放地点的委员会成员，他圈出的四座城市与委员会的选择一致，没有皇宫和新潟。幸运的是，陆军部长对京都提出了异议，理由显而易见，京都既是故都，又是佛教和神道教圣地，摧毁它会引起公愤。否则的话，战后的政治格局和经济形势恐会改变。接着横滨也被排除了，理由是，以往轰炸得够多了，且离东京太近，改由九州的长崎代替。美国人意识到，投降的决定将在首都作出。1945年8月6日，铀弹“小男孩”投放广岛，三天以后，钚弹“胖子”投放长崎，二次大战由此结束。不难推想，战争每延续一天，包括中国在内的国家就会有更多的军人和百姓伤亡。笔者以为，广岛之所以始终在投放目标之列，原因在于它是本州最偏远的大城市。

商人如何赢取最大利润

原子弹在日本投放后，奥本海默引用了印度史诗《薄伽梵歌》里的诗句自我忏悔，“现在我成了死神，世界的毁灭者。”爱因斯坦也深感痛悔，他认为给罗斯福总统寄出的那封信，是自己一生所犯的最大的错误（由于那年四月罗斯福突然去世，投放原子弹的命令由继任的杜鲁门签署）。1954年，核反应堆的设计师费米因患癌症去世，

冯•诺伊曼在授课



囚徒的困境(Prisoner's Dilemma); 冯•诺伊曼、博弈论和原子弹之迷

冯•诺伊曼也因参与比基尼岛上的核试验遭受核辐射。稍后，苏联的马雷舍夫和中国的邓稼先也没有逃脱厄运，即便寿命较长的奥本海默，也只活到了 62 岁。冯•诺伊曼认为，既然原子弹可以制造出来，那么，寄希望于独裁者的良心发现是不足取的。冯•诺伊曼的亲人中有不少死于对纳粹的恐惧，有些是在他们移居美国以后。人类许多科学进步，从蒸汽机船到飞行器，从工业化到医药试验，从枪支弹药到坦克，都会有死亡事件的发生，然而这些进步却帮助人类提高生产率、延长寿命、节约时间或摆脱专制，赋予生命更多的意义。

对冯•诺伊曼那样曾服务于三届美国政府的实干家来说，有太多有关民生和建设的事情要做。即便在 1944 年，洛斯阿拉莫斯的同僚们最忙碌的时候，他也抽空对经济学作了全面的思考，那一年，他与经济学家摩根斯坦合著的《博弈论与经济行为》正式出版，立刻获得凯恩斯母校剑桥大学的经济学家斯通（1984 年诺贝尔奖得主）的赞誉，称其为凯恩斯的《通论》之后最重要的经济学教科书。说到博弈论（Game Theory，又译对策论），它本是应用数学的一个分支，后来在经济理论和应用中发挥了重要作用，并广泛深入到政治、军事、商业、法律、体育、生物学等领域。博弈论对于扩展和精炼战略思想具有较大的影响和指导意义，而对于商人来说，则教导他们如何运作以赢取最大利润。

最早提出博弈问题的是法国数学家波莱尔，他以创建实变函数论里的波莱尔集闻名，同时也是一位著名的政治家和教育家，曾担任巴黎高等师范学校的领导人、市长、议员和海军部长。上个世纪二十年代，波莱尔首先定义了策略的应对，考虑了最优策略、混合策略、均衡策略和无限对策，同时提出了解决个人对策与零和两人对策的数学方案。所谓两人对策是与多人对策相对应的，前者是完全对抗的，后者必须考虑结盟的可能性和稳定性。零和对策是与非零和对策相对应的，前者每次结局给竞争者（局中人）的支付总和为零或常数，而后者的支付总和是可变的。前者一个竞争者的所得恰好是另一个竞争者的所失，

最早提出博弈问题的是法国数学家波莱尔，他以创建实变函数论里的波莱尔集闻名，同时也是一位著名的政治家和教育家，曾担任巴黎高等师范学校的领导人、市长、议员和海军部长。

后者竞争者可以同时有所得或有所失。

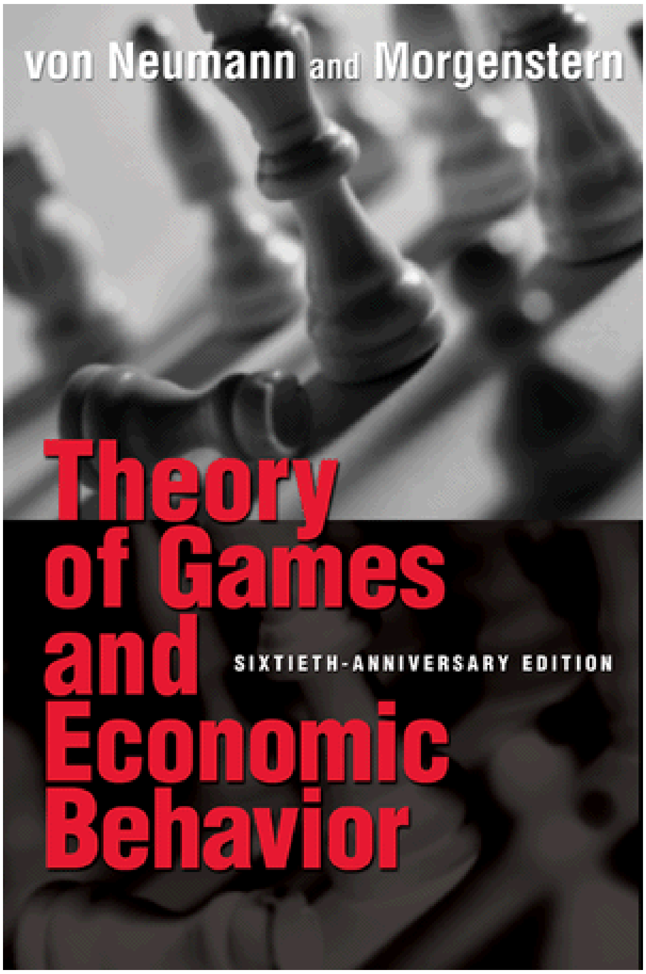
1928 年，还在柏林大学任无薪讲师的冯 • 诺伊曼发表了第一篇重要的博弈论文章《关于伙伴游戏理论》，利用一个表示讨价还价能力的矩阵建立了关于零和两人对策的极大极小定理，后来成为博弈论的基石和中心定理。作为一个应用，冯 • 诺伊曼讨论了合作对策问题，特别考虑了零和三人对策中有两方联合的情形。为此他引入了数学中的特征函数概念，明确给出了多个竞争者的一般博弈方案，并在附加条件下证明了，多人对策问题的解是存在并且惟一的。按照冯 • 诺伊曼的理论，福特公司的经济政策之所以正确，是因为它的制订不完全依赖于市场，而是同时考虑了通用、日本、德国以及其他汽车制造商实施的战略在市场上引起的变化。

1932 年，冯 • 诺伊曼在普林斯顿的一个数学研讨班上，做了一个没有讲稿的报告，标题叫《关于经济学的几个方程和布劳威尔不动点定理的推广》。这篇报告从数学的角度指出了经济问题的解决方案，可谓是一种新型的扩张经济模型：“所有商品以尽可能低的成本和尽可能大的量生产”。这是一种理想的模型，一旦达到最大的增长率，就会自动产生一个动态的平衡。四年以后，冯 • 诺伊曼本计划在维也纳的一次数学会议上再次报告这篇论文，结果却因婚姻破裂而改变旅行计划。因为无法前往，他在巴黎的旅店里用德文匆匆草书了九页，发表在随后出版的会议论文集上，也未受到特别的关注。1945 年，这篇文章被译成英文在英国重新发表，标题改为《普遍经济均衡的一个模型》。大约半个世纪以后，此文被公认为是数理经济学最重要的论文。

今天，冯 · 诺伊曼被公认为是博弈论的创立者，也是现代经济学的重要分支—数理经济学的开拓者。萨缪尔森发出由衷的赞叹，“冯 · 诺伊曼是无与伦比的，他不过在经济学领域蜻蜓点水，这一领域便今非昔比了。”这一结构一直使用至今，冯 · 诺伊曼也因此被誉为计算机之父。

冯 • 诺伊曼把经济学引入具有线性、非线性编程和未来发展动力模型的科学，使人们能够更好地理解计划经济和市场经济的无为及有为所在。迄今为止，至少有六位获诺贝尔奖的经济学家承认自己的工作受到了冯 • 诺伊曼的影响，他们是萨缪尔森、阿罗、坎托罗维奇、库普曼斯、德布勒、索洛，还有五位获奖者的工作是对冯 • 诺伊曼创立的博弈论的直接发展或应用，即 1994 年获奖的豪尔绍尼、纳什和泽尔敦，2005 年获奖的奥曼和谢林。这些经济学家来自美国、英国、德国、苏联和以色列，即使在日本，也有推崇冯 • 诺伊曼的经济学家遵循他倡导的模式，“如果要使动态平衡存在，就有必要最大限度增产。”战后日本的国家政策是，“努力在十年内将实际收入增加一倍”。当时有些西方经济学家断定那会导致严重的通货膨胀，结果证明他们是多虑了，日本的经济跳入了“良性循环”的轨道。

1938 年，德国经济学家摩根斯坦来到普林斯顿大学执教，这使得冯 • 诺伊曼的理论有了拓展的机会和空间，也使得他对诸如货物交换、市场控制和自由竞争等经济行为产生了兴趣。经过几年的合作，他们完成了那部六百多页的经济学巨著。



冯•诺伊曼《博弈论和经济行为》的专著

从左到右：波默林(James Pomerence)，比奇诺(Julian Bigelow)，冯•诺伊曼和戈德斯坦(Herman Goldstine)；他们是冯•诺伊曼计算机计划的主力。

虽然如此，战后仍有许多经济学家对冯·诺伊曼的理论不以为然，甚至心生怨恨，这部分是因为存在着种种误解，更主要的是因为他是经济学专业的一个闯入者。随着时间的推移和实践的检验，这些误解被逐渐消除。今天，冯·诺伊曼被公认为是博弈论的创立者，也是现代经济学的重要分支——数理经济学的开拓者。萨缪尔森发出由衷的赞叹，“冯·诺伊曼是无与伦比的，他不过在经济学领域蜻蜓点水，这一领域便今非昔比了。”

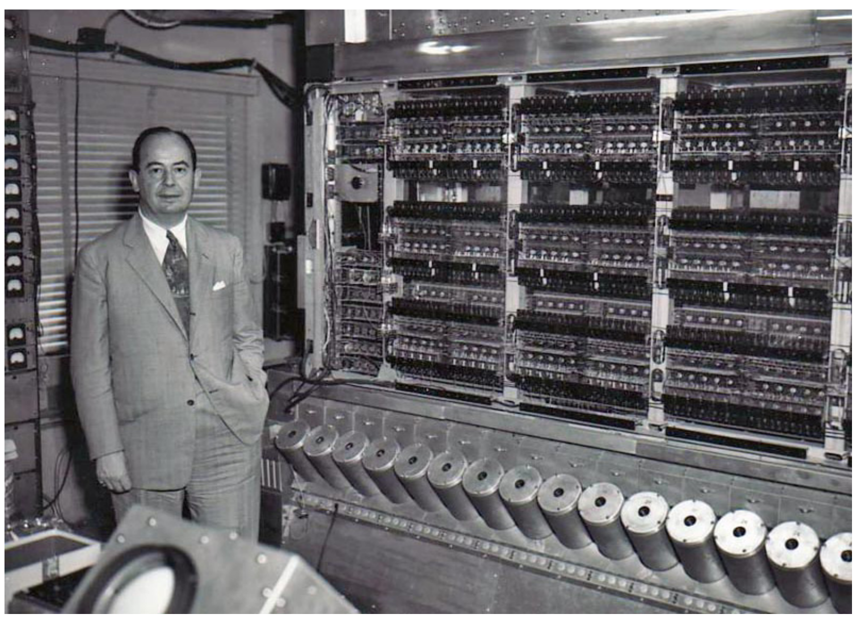
让人类生活得更加美好

自从牛顿发明了微积分，实现了物理学的数学化之后，科学家对数值列表的需求大大增加。除了一般的对数表和三角函数表等以外，更多特殊的数表是科学家在研究时临时产生的。牛顿的竞争对手莱布尼兹为此感叹，“一个优秀的人像奴隶一样把时间耗费在计算这一苦差事上，真是太不值得了。”莱布尼兹因此发明了一种类似机械化算盘的机器。只要摇动四周的轮子，就可以做加法或乘法运算。这种轮式的计算机比早些时候帕斯卡尔发明的台式加法计算器要高级一些，但十九世纪英国一位异想天开的数学家巴比奇并不满意。巴比奇利用当时最时髦的蒸汽技术驱动，结果未获成功。但他意识到了，计算机应该以精确的、数学形式的逻辑为基础。果然不久，自学成才的爱尔兰人布尔发明了新形式的数学——布尔代数。

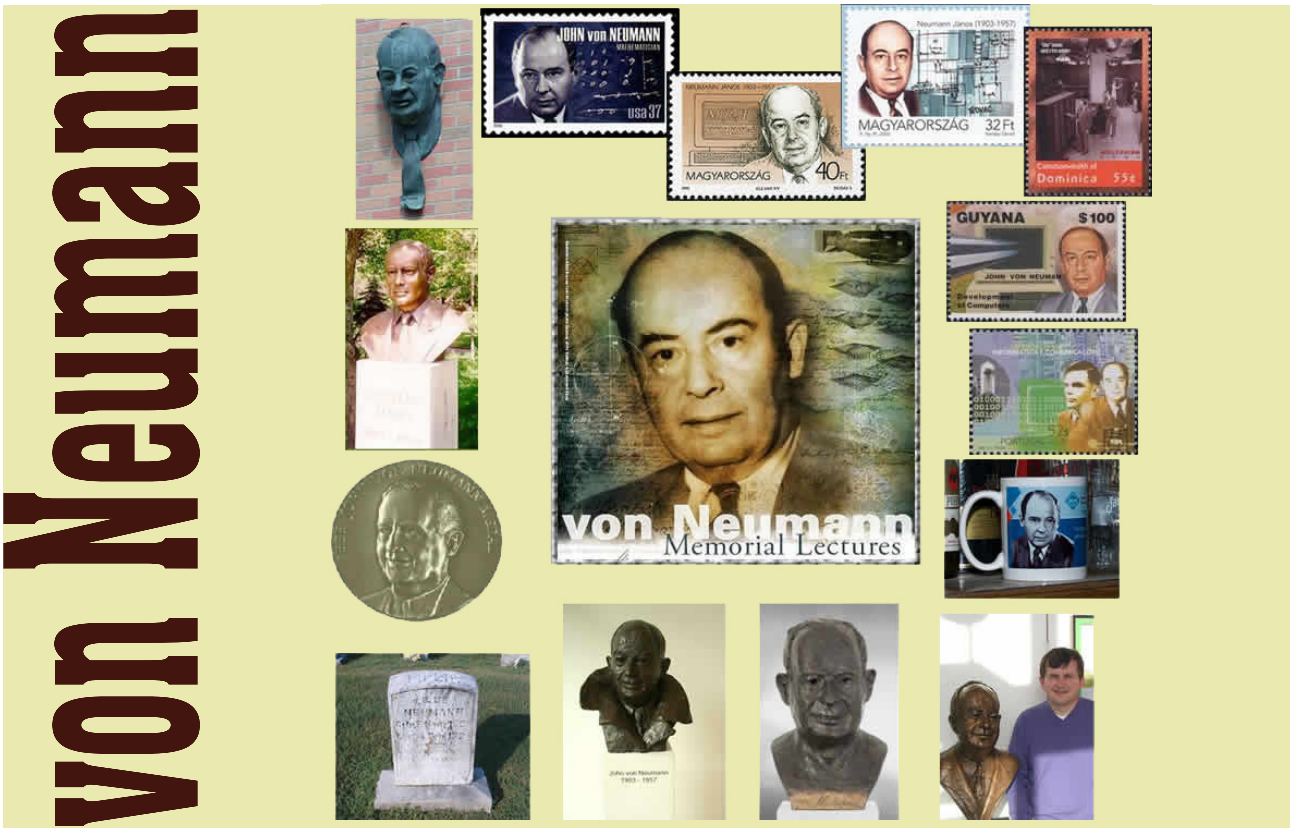
到了二十世纪中叶，情况又有了新的变化。在洛斯阿拉莫斯，原子核裂变过程中所提出的大量计算任务，促使冯·诺伊曼关注电子计算机的研制情况。《博弈论与经济行为》出版的当年，他在阿伯丁火车站的月台上遇到他的同事、参与第一台电子计算机ENIAC设计的戈德斯坦，后者向他作了汇报。当时冯·诺伊曼正准备去洛斯阿拉莫斯，立刻予以关注。他发现这台机器的主要缺陷是，仍采取以往机电式计算机的“外插型”。接下来的几年时间里，冯·诺伊曼亲自参与宾夕法尼亚大学和普林斯顿高等研究院两台计算机的设计，即EDVAC和IAS。他建立了计算机内部最主要的结构原理——储存程序原理，确定由五个部分组成，即计算器、控制器、储存器、输入和输出装置。

他建立了计算机内部最主要的结构原理——储存程序原理，确定由五个部分组成，即计算器、控制器、储存器、输入和输出装置。

与ENIAC相比，这两台机器有不少改进，最重要的是：将十进制改为二进制，程序和数据均由二进制代码表示（虽然莱布尼兹早就发明了二进制，但并没有用到他发明的轮式计算机上）；程序由外插变成内存，当算题改变时，不必变换线路板而只需更换程序。由储存原理构造的电子计算机被称为冯·诺伊曼型机，或冯·诺伊曼结构，这一结构一直使用至今。冯·诺伊曼被誉为“电子计



冯•诺伊曼在普林斯顿高等研究所的计算机前



世界各国发行的冯•诺伊曼纪念邮票和雕塑

算机之父”，而另一位计算机领域的天才图灵的贡献主要在理想计算机和人工智能方面，后者因为性取向、英年早逝和图灵奖的颁发广为人知。在这两台机器中，冯•诺伊曼对 IAS 倾注了更多的精力，因为他本人担任普林斯顿高等研究院计算机技术研究所所长。1951 年，IAS 终于获得成功，其运行速度是 ENIAC 的数百倍。

虽然冯•诺伊曼的名字是与计算机设计家联系在一起的。然而，他本人对计算机的主要兴趣并不在于计算机的设计与制造，而在于如何利用这种新型工具，开创现代科学计算的新天地。1950年，冯•诺伊曼领导了一个天气预报研究小组，利用ENIAC完成了数值天气预报史上首次成功的计算。随着天气预报和其他科学、工程领域计算需要的增加，计算方法对于计算速度的提高可以说与计算机硬件同等重要，于是，在纯粹数学与应用数学之外，一门新的数学分支——计算数学应运而生。计算数学不仅设计、改进各种数值计算方法，同时还研究与之相关的误差分析、收敛性和稳定性等问题，冯•诺伊曼无疑也是这门学科的早期奠基人。

虽然冯·诺伊曼的名字是与计算机设计家联系在一起的。然而，他本人对计算机的主要兴趣并不在于计算机的设计与制造，而在于如何利用这种新型工具，开创现代科学计算的新天地。

在历史上，许多民族的数学家都创造了各种便捷的数值计算方法，可是，这些古典的方法对于计算机未必是最优的，而一些看起来在算法上极为复杂的方法，编制为程序后反而容易在计算机上实现。换句话说，计算机有其适合的计算方法和技巧。在这方面，冯•诺伊曼作出了许多重要贡献，他先后创造了矩阵特征值计算、求逆、多元函数值和随机数产生等十来种计算技巧，在工业部门和政府计划工作中得到广泛的应用。特别值得一提的是，他与奥地利出生的美国数学家乌拉姆合作创造了一种新型的计算方法——蒙特卡洛方法。这是一种通过人工抽样寻求问题近似解的方法，它将需要求解的数学

问题化为概率模型，在计算机上实现随机模拟获得近似解。举例来说，在总统选举以前，只需少量取样或随机取样，民意调查者就会对投票选举结果做出较准确的判断。

蒙特卡洛方法体现了计算机处理大量随机数据的能力，是计算机时代新型算法的先锋。它在解决实际问题时需要分两步：模拟产生各种概率分布的随机变量；用统计方法把模型的数字特征估计出来，从而得到实际问题的数值解。冯・诺伊曼用赌城蒙特卡洛命名，赋予其神秘的含义。这一方法在金融工程学领域也得到广泛的应用，比如金融衍生产品期权、期货、掉期等的定价及交易风险估算，变量的个数（维数）有时高达数百甚至上千，这就是所谓“维数的灾难”。蒙特卡洛方法的优点在于，它的计算复杂性不依赖于维数。值得一提的是，上个世纪七十年代中国数学家华罗庚和王元用确定性的超均匀分布序列代替随机数序列，提出了所谓的拟蒙特卡洛方法。对某些计算问题，华－王方法比蒙特卡洛方法快了数百倍，并可计算出精确度。

如果冯・诺伊曼活到今天，看到计算机数量激增和能力提高，无论公司、机关还是学校、家庭，无论上天还是入地都不可或缺，一定会倍感欣慰。引用冯・诺伊曼的女儿、经济学家玛丽娜・惠特曼博士的话说，“如果我的父亲被告知，我所在的通用汽车公司每年生产和使用数百万台电子计算机（该公司每年生产约八百万辆汽车，每一辆都包含计算机），我相信他一定会大吃一惊。虽然成年人因电子游戏带坏了青少年而指斥计算机，但这可能会使他感到有趣，甚至窃喜，因为他的个性中有童真、嬉戏的一面。”可是，我们也有理由猜测，冯・诺伊曼在惊诧于计算机造福全社会和全人类的同时，也会为它没能帮助在科学上取得更大的成就而沮丧。

冯•诺伊曼的墓碑

假如他的生命能够延长

“假如约翰尼的寿命像一般科学家那么长，活到现在，他会不会使我们的生活发生很大的变化呢？”1992 年，冯・诺伊曼的传记作者、英国经济学人诺曼・麦克雷曾这样发问。对此他自己的回答是肯定的。从冯・诺伊曼晚年未曾发表的笔记本来看，他对科学的未来有着自己的设想。事实上，在他生命的最后时刻，他还在探究一些其他科学家压根儿没有想过的问题，例如，从人类的神经系统可以学到那些技巧应用于计算机？这有点像小时候他在家庭午餐聚会上提出的问题。按照冯・诺伊曼在病榻上完成的遗著《计算机和大脑》中的设想，未来的计算机和机器人应根据环境的变化做出效率更高的反应，自我繁殖的下一代计算机应遵守适者生存法则和进化论法则。

二十世纪前半叶，冯•诺伊曼亲自参与了三项革命性的突破—对原子的科学认识、量子力学的数学化，以及随之而来的电子计算机的发展，并作出了卓越的贡献。而从他的讲座和留下的笔记本显示，他希望在未来可能的三项重大突破中扮演同样的角色，它们是：对大脑的科学认识、对细胞（基因）的科学认识、对自然环境的治理。最后一项是控制天气而不仅仅是预报天气，比如使冰天雪地的冰岛变成气候宜人的夏威夷。此外，他还期望能将模糊的经济学精确化。按照冯•诺伊曼的设想，计算机时代所有数的概念也应当重新确立。令人遗憾的是，在所有这些期望中，迄今为止只有对基因的理解取得了令人满意的长足进步，那还是基于他生前看到的一

个发现，即脱氧核糖核酸（DNA）的双螺旋分子结构。恰如冯•诺伊曼所预料的，人类基因是类似于计算机的简单信息储存器。

冯•诺伊曼女儿 Marina von Neumann Whitman
(左，曾任尼克松政府的经济顾问)和其女儿，外孙们

假如冯•诺伊曼的生命能够延长，“他会因为分子生物学而感到兴奋，就像当年因为量子力学而兴奋一样，他会非常期待将之数学化。”有意思的是，冯•诺伊曼唯一的孙辈现在是哈佛大学医学院的分子生物学家。至于其它科学领域的发展，显然不如冯•诺伊曼预计或期望的那么快、那么好，这可能是因为世界过早地失去他的缘故。公元前三世纪，古希腊的智者阿基米德用巨型弩炮发射每枚二百五十公斤的石弹，摧毁了罗马人的一支舰队。与阿基米德一样，冯•诺伊曼也曾用自己掌握的数学技能，帮助美国赢得第二次世界大战的最后胜利。1956年，冯•诺伊曼获得了首次颁发的爱因斯坦纪念奖和费米奖。后一个奖项授予那些对原子的科学认识贡献卓著的人，费米自己是第一个获奖者而冯•诺伊曼是第二个。

1957年，正当遥远的中国发动一场大规模的“反右运动”时，冯•诺伊曼的生命即将到达终点，核辐射带来的骨癌细胞已经在他的体内扩散（比邓稼先还早逝九年）。冯•诺伊曼很早就意识到了，最聪明能干的人往往不是犹太人就是中国人，晚年他在笔记本里称赞汉语是诗歌的语言。1937年，冯•诺伊曼从美国数学家、控制论的发明人维纳处了解到中国数学的现状，产生了到中国访问的愿望，曾在清华大学讲学一年的维纳遂致函清华校长梅贻琦和数学系主任熊庆来。遗憾的是，两个月以后发生了卢沟桥事变，日本侵华战争全面爆发，冯•诺伊曼的愿望落空了。想当年维纳和法国数学家哈达玛对中国的访问，引起了数学界的轰动，如果多才多艺的冯•诺伊曼能来中国，其推动力将难以估量，而他自己也可能从这一新奇的东方之旅中获取无穷的灵感。

弥留之际，美国国防部正副部长，陆海空三军总司令以及其他军政要员齐聚在病榻前，聆听他最后的建议和非凡的洞见。

1957年2月8日，冯•诺伊曼在华盛顿沃尔特•里德陆军医院去世，享年53岁。弥留之际，美国国防部正副部长，陆海空三军总司令以及其他军政要员齐聚在病榻前，聆听他最后的建议和非凡的洞见。时任美国原子能委员会主席的斯特劳斯上将亲眼目睹这一幕，他后来回忆道，“这是我见过的最富戏剧性的场景，也是对智者的最感人的致敬。”此前，艾森豪威尔总统亲自给坐在轮椅上的冯•诺伊曼颁发了一枚特别自由勋章。与此同时，乔装打扮的FBI特工不分昼夜地监视着病房，生怕昏迷中的冯•诺伊曼说出国家军事机密。斯特劳斯将军无法想象的是，半个世纪以后，这家医院成为主要收治阿富汗和伊拉克战争伤兵的场所。黄昏时分，夕阳的余辉洒落在波托马克河两岸，也透过了陆军医院的玻璃窗。这是日落前最后的辉煌，二十世纪最伟大、最活跃的大脑之一停止了思想。

2009年秋天，杭州

十位伟大的数学家

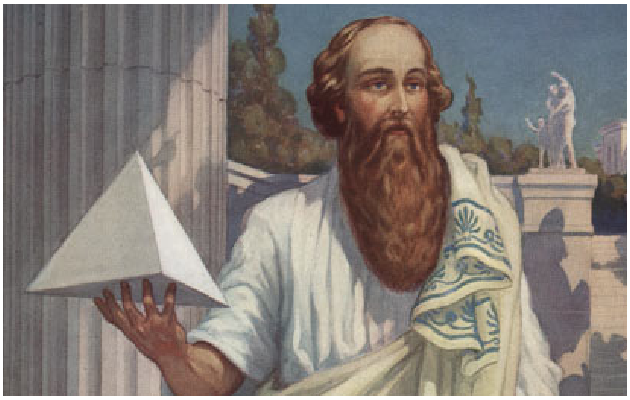
Alex Bellos 最近评选出十大数学天才，并认为他们划时代的研究成果改变了我们的世界。

Alex Bellos

编者按 2010 年 4 月 11 日，英国老牌报刊《卫报》(The Guardian) 邀请了专栏作家 Alex Bellos 评选了两千多年来十位伟大的数学家。《卫报》创刊于 1821 年，是英国第二大主流报刊，和《泰晤士报》及《每日电讯报》构成英国的三大主流报纸。作者 Alex Bellos 是英国畅销书作家，毕业于牛津大学，曾是《卫报》的驻外记者，专长于带数字分析的报道。他的《数字岛历险记》（Alex's Adventures in Numberland）是 2010 年英国的畅销书。关于这次《卫报》的数学家排名，Bellos 在他自己的博客中认为如果仅按数学家的能力这个唯一条件来选择，则这十位不一定是最合适的人选。但如果条件改成以下的更广泛的几条：即数学能力在不同年龄段的体现；在数学人群中的认知度；其事迹可用 200 字以下来描述；在文化层面上卓有贡献；且这十位中至少包含一个女性数学家，则以下人选将是比较合适的。

本文由香港浸会大学袁晓明博士翻译，在此谨致谢意。

毕达哥拉斯（Pythagoras，约公元前 570-495 年）



他是一个素食者、神秘主义的领袖，并对数字十分着迷。有关直角三角形的“毕达哥拉斯”定理（即“勾股定理”）的发现使得他成为数学史上最著名的人物之一，尽管现在看来这个定理并不是他首次发现的。在他生活的环境里，数字被认为是在精神世界里有着与在数学领域里一样重要的作用。毕达哥拉斯认为数字可以解释世界上的一切事物。他对数字的痴迷使得他成为古希腊数学的鼻祖，而古希腊数学实质上也是整个数学的起源。同时，他还因为从来不吃豆类食物而著名。

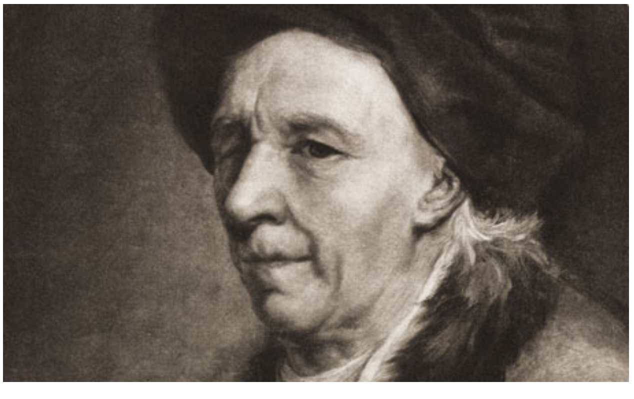
希帕提娅（Hypatia, 约公元 360-415 年），古希腊女数学家，哲学家

女性数学家相对比较少，但数学这个学科显然不只属于男性。希帕提娅是公元四世纪时期亚历山大图书馆的学者。她留下的最伟大的科学遗产是她编辑的欧几里得的《几何原本》。这本书是古希腊最重要的数学教科书，并且在希帕提娅去世后的好几个世纪一直是标准版本。希帕提娅的去世非常凄惨，狂热的基督徒把她赤身裸体地捆绑起来，用陶瓷碎片剜割她的身体并把她的四肢拉断。

卡尔达诺（Girolamo Cardano, 公元 1501-1576 年），意大利数学家，星象学家，内科医生

卡尔达诺是意大利文艺复兴时期的百科全书式的博学者。作为一个职业医生，他是 131 本书的作者。他同时也非常喜欢赌博，而正是赌博这个爱好使得他成为首个对概率论进行科学研究的学者。他意识到如果能用数字描述随机事件发生的似然度，那他在赌桌上获胜的机会将大大增加。这是一个划时代的思想，因为正是这一思想促进了概率论的形成，并随后产生了统计学、市场营销学、保险业以及天气预报。

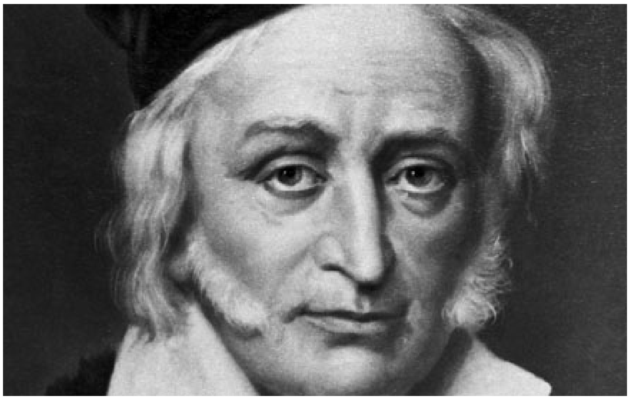
欧拉（Leonhard Euler, 公元 1707-1783 年）



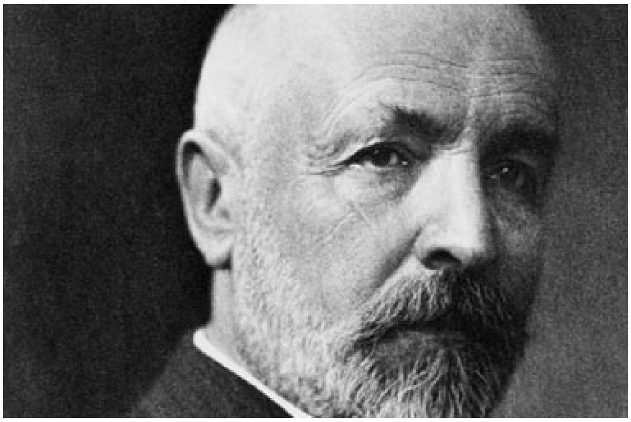
欧拉出版了近 900 本书，是有史以来最高产的数学家。他在 50 多岁的时候失明了，但之后他在诸多领域里的出版量反而增加了。他提出的著名公式 $e^{i\pi}+1=0$（其中e是一个数学常数，很多时候也被称为欧拉常数；i是-1的平方根），被很多人认为是数学上最美的公式。他后来对拉丁方阵产生了兴趣。拉丁方阵是指一个n维的方阵里，恰好有n种不同元素，使得每一个不同元素在同一行或同一列里只出现一次。没有欧拉在拉丁方阵方面的贡献，恐怕我们现在就没有“数独”这个游戏了。

高斯（Carl Friedrich Gauss, 公元 1777-1855 年）

高斯被誉为“数学王子”。他对 19 世纪数学的几乎所有领域都有十分重要的贡献。作为一个完美主义者，高斯很少出版他的研究成果，而是喜欢先对一些定理进行完善和提高。人们直到他去世以后，才在他留下的笔记里发现了非欧空间这一划时代的工作。他在分析天文学数据时，发现度量误差会导致一条钟形的曲线。这一形状的曲线现在已被命名为高斯分布曲线。



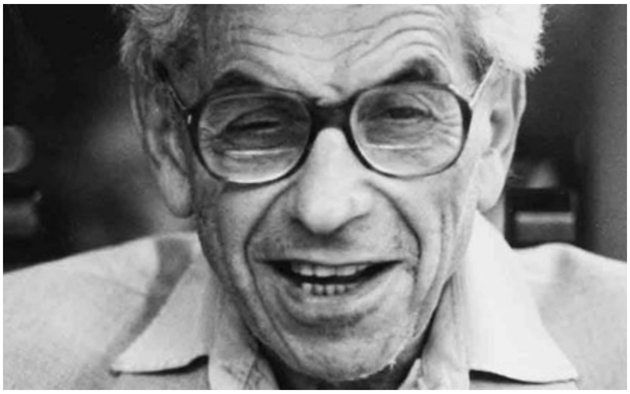
康托尔（Georg Cantor, 公元 1845-1918 年），德国数学家



好莱坞影片里总是喜欢把数学天才同时也塑造成一个精神疾病患者。在所有的伟大数学家里，康托尔大概最符合这个情节了。康托尔最深邃的天才思想在于他告诉了人们如何认识数学上的无穷这一概念。他的测度理论颠覆了人们的直观，告诉了人们无穷大的量也可以比较大小。这一成果令人震惊。不幸的是，康托尔深受神经疾病的困扰，时常需要在医院接受治疗。他后来兴趣发生了转移，想告诉世人莎士比亚的作品其实都是由培根（Francis Bacon）所撰写的。

埃尔德什（Paul Erdös, 公元 1913-1996 年）

埃尔德什一直过着居无定所的贫穷生活。他总是从一间大学搬到另一间大学，或者从同事的备用客房里搬到举办学术会议的酒店里。他甚少独自发表学术论文，因为他更喜欢与别人合作。他有 511 个合作者，发表了大概 1,500 篇论文，成为仅次于欧拉的产量第二高的数学家。作为对埃尔德什的致敬，人们现在用“埃尔德什数”来度量一个数学家与埃尔德什的合作距离。那些直接与埃尔德什合作的数学家的“埃尔德什数”是 1，那些与“埃尔德什数”为 1 的人合作的数学家的“埃尔德什数”就是 2，以此类推。

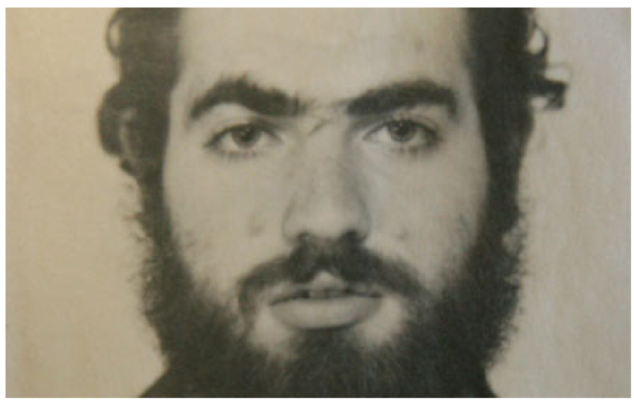


康威（John Horton Conway，公元 1937 至今）

这位在英国利物浦出生的数学家最广为人知的成就是他对游戏和拼字游戏的严格数学分析。1970 年，康威设计了“生命棋”游戏。在这个游戏里，人们可以在一个网格里看到细胞是如何进化的。早期的电脑科学家对这个游戏十分推崇，很多人都喜欢玩这个游戏。他在纯数学的很多领域都作出了十分重要的贡献，例如群论、数论和几何学。他还与合作者提出了一些听上去十分美妙的概念，例如超现实数、全反棱柱和魔幻月光猜想。

佩雷尔曼（Grigori Perelman，公元 1966 年至今），俄罗斯数学家

上个月，佩雷尔曼被授予一百万美金的奖金以奖励他解决了庞加莱猜想这一数学界最著名的数学难题之一。但是这位俄罗斯隐士拒绝接受这笔奖金。之前在 2006 年，他也拒绝接受数学界的最高奖项“菲尔兹奖”。据报道，他的理由是“如果数学证明是对的，那就不需要通过其它方式来获得认可”。庞加莱猜想是由数学家庞加莱（Henri Poincaré）于 1904 年首次提出关于三维球面的一个命题。佩雷尔曼现在没有工作，与他母亲在圣彼得堡过着俭朴的生活。



陶哲轩（Terry Tao，公元 1975 年至今）

华裔澳大利亚人，现居美国。他于 2006 年获得（并接受了）“菲尔兹奖”。陶哲轩与格林（Ben Green）合作证明了一个令人惊讶的有关素数的结论：存在任意长的素数等差数列。例如，数列 3,7,11 是含有 3 个素数的间距为 4 的素数等差数列；数列 11,17,23,29 是含有 4 个素数的间距为 6 的素数等差数列。尽管任意长的素数等差数列是存在的，目前能找到的最长的素数等差数列的长度仅是 25，其原因是那样的素数位数超过了 18 位。

数学聊斋连载

（连载二）

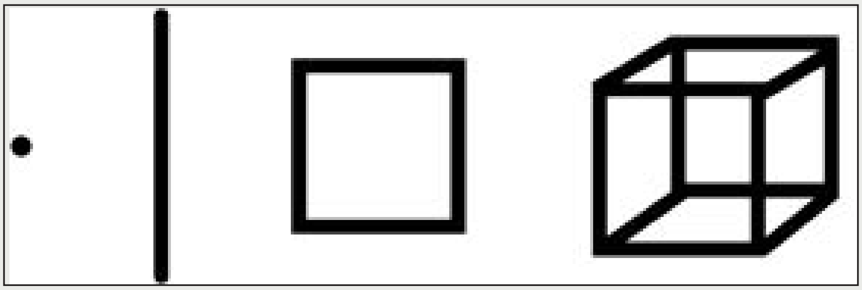
李尚志

人挤成照片之维数变化

有一次与几名中国学者和两名俄罗斯数学家一起吃饭。吃到后来照例问一个问题：吃什么主食？于是用英文问："Rice or noodle?"（米饭还是面条？）谁知这两位俄国人听不懂"noodle"(面条)这个词。几个中国人用手比划了好一会儿还是没能让他们搞懂。我急中生智地说："Rice is zero-dimensional, but noodle is one-dimensional."（米饭是零维的，面条是一维的。）不愧是数学家，两位马上就懂了。维数是数学上常用的概念，点的维数是 0，线的维数是 1，面的维数是 2，立体的维数是 3。说米饭是"零维的"，就是说它可以看成一个一个孤立的"点"组成的，说面条是"一维的"，就是说它是一条一条的线。依此类推，"飞饼"很薄，厚度可以忽略不计，可以认为是二维的；馒头自然就是三维的了。当然，严格说起来，米饭、面条、飞饼都是三维的。

说起维数，还有一件有趣的事：1969 年我第一次路过重庆，那时的公共汽车非常拥挤。有人形容这是"把人挤成照片了"。人是三维的物体，被挤成二维的照片，虽然太夸张了一些，但将拥挤的程度形容得活灵活现。

人是三维的物体，体积不为 0。挤成二维的照片，体积就变成了 0。行列式也是这样：三阶行列式表示平行六面体的有向体积，如果其中有某两行相等，就是说平行六面体的三条相邻的棱中有两条重合，平行六面体退化成平面图形，也就是被"挤成照片"了，体积变成 0。类似地，二阶行列式表示平行四边形的有向面积，如果两行相等，"平行四边形"的相邻两边重合，平行四边形退化为一条线段，面积为 0。一般地，n 阶行列式可以想象成一个 n 维立体的 n 维体积，如果它有某两行相等，"n 维立体"退化为 n-1 维或者更低维数的图形，"n 维体积"当然就等于 0。



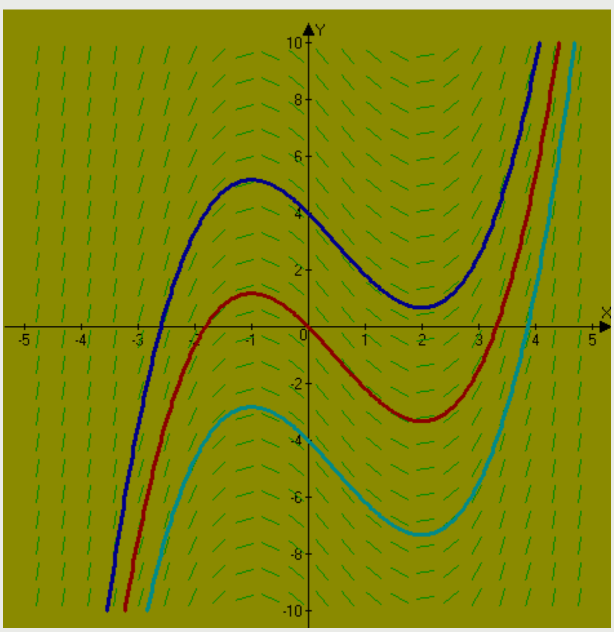
从左至右：0 维是一点，1 维是线，2 维是一个长和宽(或曲面)，3 维是 2 维加上高度形成体积面

飞檐走壁之电影实现

——微积分基本定理

小时候看电影，看见电影中的人物轻轻一跳就上了房顶，觉得演这些人物的演员真是了不起。世界跳高记录也只有 2 米多一点，还不如这些演员跳得高。于是就想：如果这些演员到国际上参加跳高比赛，不就可以打破世界跳高纪录并且拿到世界冠军了吗？

后来知道了这些演员并不能从地上跳到房顶上，电影镜头可以通过特技来实现。比如说可以让演员从房顶往下跳到地面，将往下跳的过程用电影胶片拍下来，将拍得的胶片颠倒顺序由后往前放映，看到的效果就是从地面往上跳到房顶了，甚至可以从水中往上跳到跳板上。数学中像这样“倒过来放映”的事情也不少。



函数 $F(x)=x^3/3-x^2/2+c$ 的梯度场。虽然三条曲线相差常数，但它们在同一个 x 处的导数是一样的。

比如，如果已知运动物体的路程对时间的函数关系 $S=S(t)$，求导数就可以得到速度函数 $V=S'(t)$，这比较容易。反过来，要由速度 $V=S'(t)$，求路程 $S=S(t)$，就要做定积分，也就是要将所经过的时间划分成许许多多很短的时间间隔，在每一小段时间内将物体的运动近似地看成匀速运动求得一小段路程，将各段路程相加得到总路程的近似值，再让各时间间隔长度趋于 0，求极限得到总路程的准确值。但是，这样太困难，就好像从地面跳到房顶那样困难。我们也可以化难为易，采用“从房顶往下跳”、再“倒过来放映”的方法，找到一个函数 $F(t)$ 使得由它（通过求导数）得到的速度函数 $V=F'(t)$ 正好等于预先已知的 $V=f(t)$，这样就可以比较容易得到所需的 $S=F(t)$。这样的 $F(t)$ 称为 $f(t)$ 的原函数。通过这样“倒过来放映”的方法求定积分，这就是微积分基本定理。

另一个例子是由数列的通项公式 $a(n)$ 求前 n 项之和 $S(n)$。比如，已知 $a(n)=n^2$ 求 $S(n)$，也就是求前 n 个正整数平方和公式。中学数学中将这个公式作为数学归纳法的证明的例子来讲。但这个公式很难想出来，就好像从地面跳到房顶上那么难。反过来，如果已知数列的前 n 项和的公式 $S(n)$ 反过来求通项公式 $a(n)$，就很容易：

$$a(1)=S(1),\ a(n)=S(n)-S(n-1),\ n=2,3,\cdots$$

比从房顶跳到地面还容易。能不能用“倒过来放映”的方法，设法找一个 $S(n)$ 使它求出的通项

$$a(n)=S(n)-S(n-1)$$

正好等于已知的 n^2？容易发现，当 $S(n)$ 是 K 次多项式时，$S(n)-S(n-1)$ 是 $K-1$ 次多项式。因此考虑三次多项式 $S(n)=an^3+bn^2+cn$ 很容易通过解方程求得待定系数 a,b,c，使得

$$S(n)-S(n-1)=n^2$$

问题就迎刃而解了。

算 24 之不可能问题与难题

算 24, 是很多人都知道的一种用扑克牌玩的游戏。每张牌代表一个的正整数。(为了简单起见，可以将大小王去掉，并约定 J, Q, K 代表 10，A 代表 1。) 参加游戏的 4 个人每人出一张牌，4 张牌就代表了 4 个正整数。四个人就开始竞争，看谁最先将这 4 个正整数通过加减乘除算出 24 来，而且每个整数恰好用一次。所用的数学知识虽然只是简单的算术，但要算得又快又正确也不容易。并且还有很多难题出现。

例如，如果 4 个数是 1, 1, 1, 1，你能算出 24 吗 ? 这个题目很难，所有的数学家都算不出来。你会不会因此而拼命地算这道题，希望有朝一日将这道题算出来，将所有的数学权威都打倒? 只要你具有一点算术常识，就能看出用四个 1 按上述规则算出 24 是不可能的。因此你也不会白费力气去算这道"难题"。这不是难题，而是不可能问题。其实，现在有很多"民间数学家"拼命想解决的问题，比如用尺规作图三等分任意角、找出 5 次以上的一般代数方程的求根公式等等，也和这个问题一样是不可能问题。只不过这些问题的不可能性不容易看出，而是前辈数学家用较高深的数学知识才证明出来的。不过，既然已经证明了，就不再是难题，而是已经解决了的问题。

又例如，4 个数是 5, 5, 5, 1，让你算 24，你能算出来吗? 还有，如果 4 个数是 3, 3, 7, 7，或者 4, 4, 7, 7，或者 3, 3, 8, 8，你能算出来吗? 也许，经过努力之后你仍然算不出来，于是你相信它们都是不可能算出的。不过，如果你看见这样的答案:

$$5\times(5-1\div5)=24$$

就知道用 5, 5, 5, 1 算 24 不是"不可能问题"，至多只能算是一个"难题"。其实，这个难题也不太难。只要你解除思想束缚，不要求中间每一步的计算结果都是整数，而允许出现分数，就能自己凑出答案来。不过，这样"凑出来"的答案让人感到是偶然的巧合。能不能有一个更自然的思考方法呢 ?

先用 5, 5, 1 算出 24：$5\times5-1=24$。还剩下一个 5 没有用上。我们 $5\times5-1$ 进行恒等变形，利用乘法对于加法的分配律将两项的公因子 5 提到括号外:

$$24=5\times5-1=5\times\left(5-\frac{1}{5}\right)$$

这样既保持了答数 24 不变，又将算式中两个 5 变成了右端的 3 个 5。

你不妨自己试一下，用类似的方法用4, 4, 7, 7 或3, 3, 7, 7 算 24。3, 3, 8, 8 稍微不同，但也可以用同样的思路解决。$24=(3\times8)\div(3\times3-8)$，分子分母同除以 3 得:

$$24=8\div(3-8\div3)$$

当然，这个游戏两个人也可以玩。

你能用上面两幅图中的四张扑克牌算出 24 吗?

乐谱速记法

——不可能问题的可能解

1970 年我从中国科大数学系毕业，被分配到川陕交界的大巴山区教公社小学附设初中班。除了教数学、物理、化学、外语，还负责组织和指导学生的文艺宣传队。搞文艺自然就需要乐曲，那时也不可能像现在这样有录音机甚至 MP3，更不可能到网上下载，只能从广播里听。听见一些好听的乐曲，就想把它们的曲谱记下来。好在我有一点起码的音乐素养，听见乐曲就能够写出谱。问题是乐曲进行得快，人写得慢，一边听一边记录是来不及的。还没有把前一句记录下来，后面又演奏了很多句了。

怎样提高记录速度？当然，可以加强训练，尽量写得快些。我用的是简谱，也就是用表示数字的 1234567 来作音符。这些数字虽然简单，但乐曲中每一拍中往往就有好几个音，要在乐曲进行的这么短的时间内将表示这几个音的数字写完，无论怎样练习也没有这样快。

于是我想到将这些数字简化，自己规定一些尽可能简单的符号来表示各个音。最简单的符号就是一个点。能不能将所有的音都用点来表示呢？如果将所有的音都用一个点来表示，那就没有区别了，不能表示不同的音。要表示各个不同的音，各个符号的形状总得有区别。这样，每个符号就不可能太简单，书写的时间就无论如何追赶不上乐曲的进行。

由此看来，要用不同形状的符号来表示不同的音，记录速度是无论如何达不到要求的。

出路何在？我想起了自己在小学音乐课学过的一点点五线谱的知识，想到五线谱的基本原理：将同一个符号放在不同的位置来表示不同高低的音（五线谱符号形状的不同只是为了区别音的长短而不是区别高低）。为了提高记录速度，我想到可以用同一个最简单的符号——点放在不同的位置来表示不同的音。可以预先将表示声音高低的五条线画在纸上作成五线谱纸，在乐曲进行时将表示各音的点画在纸上。为了表示各个音的长短（节拍），也为了进一步提高记录速度，还可以将表示不同音的点用适当的方式连接成折线段。

在那些年，我曾经用自己发明的这个速记法记录了一些自己喜欢的乐曲。后来有了录音机，有了 MP3，这个速记法似乎没有用处了。但我还是利用这个速记法从所录的歌曲中记录下了一些乐曲的乐谱，只不过条件更好了，可以多放几次，直到全部记录下来为止。

以上设计的乐谱速记法，看起来似乎没有用到数学知识，但是思维的方式却是数学的。其中关键的思考是 :“只要形状不同，符号就不可能太简单，就不可能写得很快。要写得很快，一个出路是所有的音都采用最简单的符号点来表示。点的形状没有区别，只能用位置来区别。”这里并没有讨论哪一种具体的符号，而是讨论所有这些符号的共同点 :“用形状的不同来区别音的高低”，然后一网打尽全盘否定了具有这个共同点的所有的符号方案。**考虑许多不同东西的共同点，这正是数学中典型的抽象思维方式。**这与证明“尺规作图不可能三等分任意角”类似，不论哪种具体的尺规作图方法，不论是以前的人想过的，或者是以后的人将要想出的，只要具有共同点“符合尺规作图的规则”，就都讨论过了并且被一网打尽全盘否定了。当然，利用形状区别来记谱也有另外的出路 : 假如你的音乐素养足够好，就不需要记下全部音，只要记下一些重要的部分就可以将其它部分补充出来。不过，我还没有这样好的素养，所以只好采用这个笨办法了。

数学与选举

万精油

每到大选，美国社会各界就全体总动员。政治家当然是到处拉选票，各大媒体更是评论加民意调查加八卦候选人，各种招数都使出来吸引眼球。连不食人间烟火的数学家也不例外。2008 年初的美国数学年会就有一个关于选举中的数学问题的报告，临近大选的那一期数学会刊又有一篇相关文章。文章中的一些例子很容易对大众讲清楚，我这里就把它们整理出来与大家分享。

主要结论是：在竞选者实力接近的时候（各方支持者数量差不多），选举结果只是对选举规则的反映，而不一定是对选民意见的反映。

什么叫对选举规则的反映？这结论听起来怎么有点违背常理。要说清楚这个问题，我们先来看一个例子。

假设有三个候选人 A，B，C。11 个人来投票，每个投票人列出他们对这三个人的支持程度，也就是给这三个人排一个从支持到不支持的序。结果如下：

3 人：A > B > C
2 人：A > C > B
2 人：B > C > A
4 人：C > B > A

如果选举规则是每人只选一个人，根据上面列出的表我们可以看出 A 会赢。只选一个人的结果是 A > C > B（得票依次是 5，4，2）。如果选举规则是每人可以选两人，然后再从前两名中挑出得票最多的（相当于初选加复选），我们可以看到其结果是 B > C > A（得票依次是 9，8，5）。这个例子说明，同样的选民，同样的意向，因为选举规则的不同可以得出完全相反的结论。还有一些地方（比如欧洲一些地方的选举）对意向采用 Borda 加权（起始于 1770 年）。对每个意向表，第一名得两分，第二名得一分。最后把每个人的得分加起来看谁的分多谁当选。如果对上面的意向表采用这个 Borda 加权，我们得出另一个不同的结果 C > B > A（依次得分是 12，11，10）。如果用另外的加权方法，我们还可以得出别的不同结果。

同样的意向表，不同的加权，到底会产生多少个不同的结果？有定理说：

对 N 个候选人，存在一个意向表使得不同的加权会产生 $(N-1)*(N-1)!$ 个不同的结果。

显然，对加权的限制是前面的权要大于等于后面的权。另外还要求最后一名的权是 0。在这种条件下，如果有 10 个候选人（比如美国的总统初选），同样的意向表可以产生超过三百万种不同的结果。

有人说数学上证明的存在例子都是人为造出来的特殊情况，实际选举出现这种特例的机会是不多的。对这些怀疑者正好有另一个定理等在那里回答。该定理说：

如果有三个候选人，他们的支持度差不多（没有人有特别大的优势），则有大于三分之二的可能性（实际数是 69%）选举规则会改变选举结果。

三分之二可不是一个小数，比一半大多了。也就是说当各方实力接近的时候，选举规则会改变选举结果的时候比不会改变结果的时候多一倍。

以 2008 年的大选为例，如果把全体美国人的意向列一个意向表，我们几乎可以肯定不同的规则会产生不同

的结果。也就是说对这个意向表不同的加权可以产生希拉里赢，或者奥巴马赢，或者麦凯恩赢。

这种现象并不只在选总统的时候出现，在日常生活中也会冒出来，甚至影响到你自己。比如你去面试一个工作，总共四个面试者，A，B，C，D。四个人每个人做一个报告。听报告的一共 30 个人。听完报告后这 30 个给出每人的意向表，结果如下：

3 人：A > C > D > B
6 人：A > D > C > B
3 人：B > C > D > A
5 人：B > D > C > A
2 人：C > B > D > A
5 人：C > D > B > A
2 人：D > B > C > A
4 人：D > C > B > A

假设你是 D，根据这个意向表，你就没有戏了。因为只有一个位置，所以只有一个人能得到。按第一票算，其次序是 A > B > C > D（得票依次是 9，8，7，6）。显然 A 胜。正当他们准备打电话通知 A 面试成功的时候，C 打电话来说他弃权，因为他已经接受了另一个工作。初看起来，C 排第三，他的弃权对只选一个人的结果不会有影响。其实不然，如果你把上面的意向表中的 C 都去掉，你会发现结果完全不同了。因为 C 的 7 票有 2 票给了 B，5 票给了你（D）。最后的结果是 D > B > A（得票依次是 11，10，9）。

如此的例子还有很多，单就上面的这个例子看，任何一个人弃权都会改变结果的次序。对这样的混乱现象有人用混沌来形容。

最后再回到开始的那句话：在竞选人实力差不多的情况下，选举结果是对选举规则的反映，而不一定是对选民意向的反映。

作家笔下的数学与数学家

万精油

有关物理学家或化学家的文学作品不少，因为物理或化学研究的东西有很多实用性，比较容易在生活中找到联系。与此相反，有关数学家的文学作品却非常少。一方面因为数学的东西太抽象，不太容易被大众接受。另一方面大众心目中的数学家都有怪癖，不好写。然而，正常的东西写多了就没有了新意，不正常的怪癖反倒变得更有吸引力。于是，被夸大了的怪僻数学家就有了市场。好莱坞有关数学家的两部大片都是走的这条怪僻路子。《美丽心灵》（A Beautiful Mind）干脆就是写一个精神病，虽然是写数学家，其实没有多少数学内容。另一部电影《Good Will Hunting》（中文译名《心灵捕手》），写数学家的，而且有不少数学内容，可以评一评。

电影《心灵捕手》的海报

《心灵捕手》讲的是一个具有超级数学天才的MIT（麻省理工学院）清洁工的离奇故事。清洁工小伙子没有受过什么高等教育，却可以在扫地之余，在黑板上随便画画就解决了第一流数学家几年都解决不了的问题。或者是在餐纸上胡乱涂两笔就得出了女朋友（哈佛大学学生）有机化学考试题的答案。故事编得很离奇，很讨观众的喜爱，票房结果还不错。但影片对数学的描述，以及对一个获过菲尔兹（Fields）奖的数学家的处理让我很不舒服。

菲尔兹奖相当于数学界的诺贝尔奖。据说诺贝尔的女朋友被一个大数学家拐走了，他恨透了那个数学家。牵连下来，祸及无辜，在他设奖的时候就没有设数学奖。菲尔兹奖弥补了这个空缺。但因为它每四年才颁发一次，而且只颁发给研究结果出在四十岁以下的年轻数学家，相对于每年都有的诺贝尔奖来说，获得的难度要大许多。

得菲尔兹奖的人都是当今数学界的领袖人物。而《心灵捕手》里这个清洁工把一个得了菲尔兹奖的麻省理工教授当垃圾一样，挥来呼去，

当小孩一样来教训。甚至有一个镜头是这个菲尔兹奖得主跪在地上去抢救一张被清洁工有意烧掉的写有数学证明的纸条。这也太过分了点，弄得我们这些搞数学的一点尊严都没有了。

电影《心灵捕手》用爱因斯坦、纳玛努贾（Ramanujam）来比喻这个清洁工，意思是说他与他们是一个数量级的，而且都有相同的背景。也就是说都是从默默无闻一下跳到科学前沿。但我们知道，从瑞士专利局出来的爱因斯坦，并没有对波尔、海森堡这些人不尊重。从印度来到英国的纳玛努贾对发现他的大数学家哈代（Hardy）也是尊敬有加，并没有象《心灵捕手》里的清洁工一样把一个第一流数学家当垃圾。

顺便扯点题外话。爱因斯坦大家都知道，但知道纳玛努贾的人也许不多。纳玛努贾是数学史上的奇才。他的数学可以说都是自学的。没有受过正规教育，却对现代数学有着惊人的洞察力。他解决了一系列超难度的数论问题，而且为后人开创了许多新的方向。我的印度朋友告诉我，纳玛努贾在印度是家喻户晓的英雄人物。最近读一篇关于老纳的传记，才知道他不是一般的呆。因为专注数学，他对其它课完全不重视，竟然到了多门不及格而毕不了业的地步。因为他是天才，别人又给他一次机会，他竟然还是毕不了业。没有学位，找不到工作，后来混到饭都吃不饱的地步。他给许多人写信，其中一封写给当时的大数论家哈代，里面列了一大堆等式和方程，都是他发现的“定理”。但信中没有证明。哈代回信让他补上证明。老纳回信说：“我如果在信里写下我的思路你肯定看不懂。我想要告诉你，请用你的传统证明方法验证我给你的这些公式。如果这些公式是对的，这说明我的方法是有根据的。我现在最需要的就是象你这样的知名学者承认我是有价值的。我现在几乎饿得半死。有了你的承认，我就可以在这里搞到一些钱……”。可见他还不是完全呆，知道给自己找路。

纳玛努贾对数字有特别的敏感。据说在他生病住院的时候，哈代去看他。进门就说，我今天来时坐的车，车牌号是 1729。这真是一个最乏味的数，找不到一个有趣的性质。谁知纳玛努贾却说，你完全说错了，我的朋友。1729 这个数真是太有意思了。它是第一个可以用两种不同方式写成两个数的立方和的数（12^3+1^3 或 9^3+10^3）。

再回头来接着谈这部电影。《心灵捕手》的问题不光表现在清洁工的行为方面。从技术上，也就是从数学上来说，这样的数学天才也是不可能存在的。电影里说，清洁工看见数学、化学问题就象莫扎特看见钢琴上的键盘，感觉自然就来了。这真是乱弹琴。需知道，音乐可以凭感觉，而以逻辑思维为依据的数学是不可以单凭感觉的。现代数学发展到今天，各种概念与理论都包含很深的思想，已经不可能仅凭一点感觉就走到第一线。也许有人会说，难到不可以突然冒出一个天才，摒弃一切现有概念，凭感觉创造出一套他自己的体系来解决现有问题吗？我说不可能。不管是什么体系，要解决现有问题，至少要看懂是什么问题。现代数学上的绝大多数前沿问题，单单是看懂题目就需要许多专业训练，而不可能凭感觉得到。比如现在数学界的第一大问题“黎曼猜想”，单是要把这个猜想讲清楚，就需要很多“感觉”不到的知识。当然，对好莱坞的东西也不能要求太高。他们关心的只是卖座。我只是觉得他们这样平庸化数学比较容易让公众对数学及数学家的认识更加扭曲。

电影或者小说要写数学家，当然是好事。但是他们常常为了讨好观众而人为地夸大或扭曲一些事实，以至于一般公众心目中的数学家形象都有一些扭曲。因为徐迟写的陈景润，这种扭曲在中国尤甚。大家认为数学家都是不食人间烟火、行为怪僻的人。似乎大学数学系的人都要修一门“怪癖课”。如果有谁表现正常，就会有人感到惊讶。常常有这种情况，新认识的朋友对我的最大恭维居然是：“你看起来简直不像学数学的。”听到这种恭维真是让人哭笑不得。学了一辈子数学，居然还没有学像。

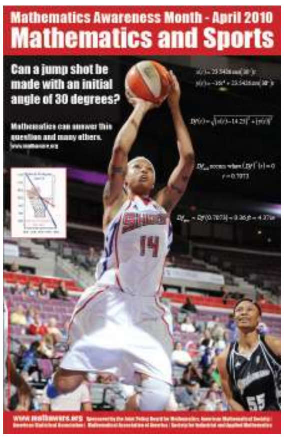
作者本科毕业于四川大学数学系，是中国科学院数学研究所硕士、美国马里兰大学数学博士。为本刊的特约撰稿人。

作者介绍：

蒋迅，本科和硕士毕业于北京师范大学，在美国马里兰大学获得博士学位。目前在美国从事科学计算工作。曾应北京师范大学张英伯教授邀请，开办了关于数学文化的个人博客；内容包括书评、随感和其他评论。

美国的数学推广月

蒋迅



四月份是美国数学宣传月(Math Awareness Month)，主办单位为美国数学会（AMS）、美国统计学会（ASA）、美国数学联合会（MAA）和工业和应用数学学会 (SIAM)。这四家都是美国大的数学机构，AMS 创建于 1888 年，主要面向高校和研究所，现有三万多个人会员和五百七十个社团会员；ASA 创建于 1839 年，主要面向统计研究者和使用者，现有会员一万八千名；MAA 创建于 1915 年，主要面向中学、大专和大学的老师和学生，侧重于教学和学习，现有会员两万人；SIAM 成立与 1951 年，侧重于实际应用中的数学问题，现有一万三千个人会员和五百个企业机构会员。美国的数学推广月已有二十五年的历史，今年的主题是数学和体育。

体育运动的科学研究中出现的数据、策略和机遇等问题都是很好的数学课题。除了最简单的给运动员打分以外，数学还被运用于诸如跑车轮胎的合成、高尔夫球表面模式的动力学模拟、比赛成绩预测、游泳池和游泳衣对速度的影响等等。松鼠会有一篇文章“世界杯的数学预测”，用的公式还挺复杂。数学也被运用到体育教育的研究中。

美国数学会为此发表了一篇名为“Mathematics and Sports, Some of the fascinating mathematics of sports scheduling...”的文章，讲的是图论在比赛时间表的安排上的应用。到四月底，已经有了数十篇论文发在网上，内容涉及到美式足球、棒球、田径、高尔夫球、足球、网球、篮球等。我想，这样的课题还有很多。这些课题正在等待数学家与体育工作者一起来研究。我们应该用科学的方法而不是投机取巧的方法来建成体育强国。

下面是历年来数学推广月的主题：

2010	数学和体育	Mathematics and Sports
2009	数学和气候	Mathematics and Climate
2008	数学与选举	Math and Voting
2007	数学和大脑	Mathematics and the Brain
2006	数学和因特网安全	Mathematics and Internet Security
2005	数学和宇宙	Mathematics and the Cosmos
2004	网络数学	Mathematics of Networks
2003	数学和艺术	Mathematics and Art
2002	数学和基因组	Mathematics and the Genome
2001	数学和海洋	Mathematics and the Ocean
2000	数学跨跃全时空	Math Spans all Dimensions
1999	数学和生物	Mathematics and Biology
1998	数学和成像	Mathematics and Imaging
1997	数学和因特网	Mathematics and the Internet
1996	数学和决策	Mathematics and Decision Making
1995	数学和对称	Mathematics and Symmetry
1994	数学和医药	Mathematics and Medicine
1993	数学和制造	Mathematics and Manufacturing
1992	数学和环境	Mathematics and the Environment
1991	数学是基础	Mathematics – IT'S Fundamental
1990	通讯数学	Communicating Mathematics
1989	发现模式	Discovering Patterns
1988	美国数学一百年	100 Years of American Mathematics
1987	数学美感和挑战	The Beauty and Challenge of Mathematics
1986	数学 – 基础训练	Mathematics – The Foundation Discipline

后面就是秘密！
——密码漫谈（续）

罗懋康

上期回顾：本文的前一部分刊登在本刊 2010 年 4 月创刊号的第 47 至 57 页。第一节介绍了密码的基本原理，特别是密码操作的五个基本要素。接下来，作者回顾了从远古时代至近代，密码学发展的起源和历史，特别是密码如何被军事家们不断地更新、发展和应用。在第三节，作者介绍了古代的密码，描述了密码的本质，以及让一项信息保持绝密的五种方法。作者还介绍了古代加密和解密常用的几类典型方法。

4. 生死之间，不见刀光剑影——密码的攻防

由于密码所关系的，经常都是一些生死攸关的事，因而围绕密码，历史上也就有着许许多多惊心动魄的事件展开。

图 22. 玛丽女王

（1） 玛丽女王：1578 年，因国内危机而逃亡英格兰的苏格兰玛丽女王被伊丽莎白女王软禁。1586 年 1 月 6 日，玛丽收到一批秘密信件，里面是她过去的侍从、当时在欧洲大陆的 24 岁的安东尼•贝宾顿（Anthony Babington）和她另外一些忠实追随者准备营救她的计划。

这些信件都是用密码写成、由贝宾顿交给一个对玛丽女王表现非常忠诚的天主教神甫吉法德带进监狱交给玛丽的。然而，贝宾顿怎么也没想到，这个吉法德却是伊丽莎白女王的间谍，执行英格兰大臣沃尔辛汉姆（Walsingham）爵士的命令。其结果，自然是所有这些信件都首先出现在沃尔辛汉姆的办公桌上。

图 23. 沃尔辛汉姆勋爵

这还不算贝宾顿和玛丽们最倒霉的事，更倒霉的是，沃尔辛汉姆不仅是负责君王安全的间谍首脑，而且还一直重视密码学的研究，在伦敦建立了一所密码学校，培养了一批专门人才。当他得到这批信件时，便让当时全欧洲最优秀的密码破译专家和笔迹摹仿专家托马斯•菲利普斯（Thomas Phelippes）将其破译了出来，汇报给了伊丽莎白。

此时的伊丽莎白，出于种种互相矛盾的利害考虑，对是否就此除掉玛丽女王举棋不定，沃尔辛汉姆猜透了伊丽莎白心里为难的原因，决定推动她杀掉玛丽女王，方式是设法构造玛丽图谋杀害伊丽莎白的证据。

他让间谍吉法德去告诉已经来到伦敦准备营救玛丽的贝宾顿们，现在要想武力营救玛丽是不可行的，因为玛丽

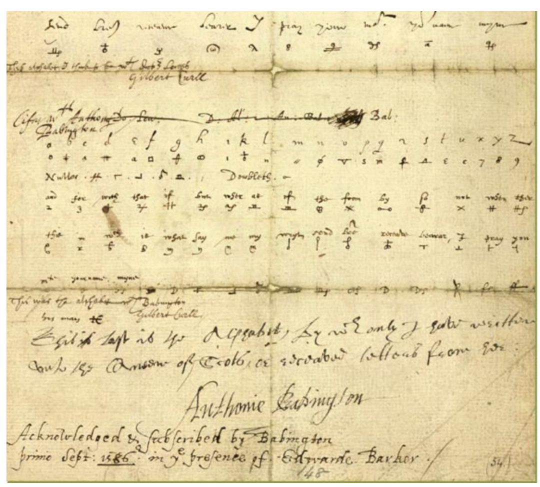


图 24. 玛丽女王解码密钥

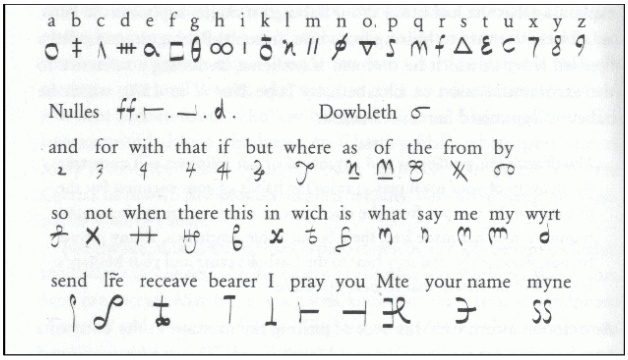


图 25. 贝宾顿与玛丽女王通信的密码表

被严密看守，并被指示稍有异动发生便立即处死。唯一可行的办法是暗杀伊丽莎白女王，然后便可利用玛丽是英格兰国王亨利八世的姐姐的孙女、伊丽莎白女王的表侄女这一王室血缘关系和名义让玛丽接掌英格兰王位，这样的话，所有问题就自然不复存在了。

贝宾顿们折服于吉法德的严密分析，立即重新拟定行动计划，并再次给玛丽女王写了一封信，说明他们将暗杀伊丽莎白女王，同时要求外国干涉、煽动英格兰天主教徒暴动（英国是新教的势力范围，天主教徒受压）。这封信还是由吉法德带给玛丽女王，并由玛丽女王签署了回信，表明她完全同意刺杀伊丽莎白女王的这一计划。

当然，这一切都在沃尔辛汉姆掌握之中；更可怕的是，他还让菲利普斯在玛丽女王的回信中，摹仿玛丽女王的口吻和笔迹加上附言，让贝宾顿列出重要成员的名字。于是，所有密谋者被一网打尽；最后，玛丽女王也在审判庭上，被自己那封由菲利普斯按沃尔辛汉姆的指示添加了私货，从而半真半假、自己也无从分辨的密谋信件推上了断头台。

（2）裴炎宰相： 与玛丽女王死于密码差相仿佛，中国古代也有一个类似的例子，这就是由于密码被武则天识破而丢命的宰相裴炎的故事。

公元 684 年，柳州司马徐敬业在扬州起兵，讨伐武则天。这事在历史上固然有名，但被后世流传更广的，却是骆宾王为此所起草的“古今第一檄文”《为徐敬业讨武曌檄》。骆宾王这篇檄文，端的是文辞华丽，音韵铿锵，磅礴豪迈，雄奇激越：

“海陵红粟，仓储之积靡穷；江浦黄旗，匡复之功何远？班声动而北风起，剑气冲而南斗平。喑呜则山岳崩颓，叱咤则风云变色。以此制敌，何敌不摧！以此图功，何功不克！”“或膺重寄于话言，或受顾命于宣室。言犹在耳，忠岂忘心！一抔之土未干，六尺之孤何托？”“请看今日之域中，竟是谁家之天下？”

据说，当《为徐敬业讨武曌檄》传至京都，武则天初读时微露讥笑，但读到“一抔之土未干，六尺之孤何托”一句时，不觉耸然一惊，问侍臣：“此语谁为之？”有人答曰：“骆宾王之辞也。”武则天叹道：“此乃宰相之过，安失此人？”

据唐人张鷟《朝野佥载》和《新唐书•裴炎传》所载，徐敬业此次起兵，当朝宰相裴炎亦曾与谋。《朝野佥载》称：徐敬业约裴炎为内应，裴炎书“青鵞”二字作答。事泄，无人可解“青鵞”二字含意；武则天沉思片刻，曰此乃“十二月（青），我自与（鵞）”之意，也就是说答应将于十二月在朝中发动政变，以为徐敬业响应。

这里，“青鵞”相当于同时使用了替代法和移位法的密码，只可惜还是被破解了。

不过，此事不见于《旧唐书》，《通鉴考异》也认为这些记述“皆当时构陷炎者所言耳，非其实也”，这就是史家的事了。

（3）生死攸关的六天，由密码决定： 1918 年，一战后期，同盟国中为首的德国，与协约国中的英、法、俄作战已近 3 年，双方伤亡已达 284 万 8 千人。此时的德国，虽然由于俄国在十月革命后宣布退出战争而似得转机，但此前 1917 年 4 月 2 日，由于德国“齐默尔曼电报”密码被秘密破译而导致的美国对德国的宣战（*呵呵，另一个密码影响历史走向的事例，来龙去脉太长，还是暂付想象吧*），却使德国的压力有增无减。不过，协约国方面的情况更为严重：德军当时停在距离索姆省的省会亚眠（Amiens）仅仅 16 公里的地方，距离巴黎也就百把公里。

双方都在紧张集聚力量，准备着决定双方各自命运的最后一战。

图 26. 武则天《升仙太子碑》拓片

1918年3月5日，一战后期的德国，启用了由纳贝尔（Fritz Nebel）上校发明的全新的战地密码，也就是密码史上著名的ADFGX战地密码体制。这套密码仅用ADFGX这5个字母表达全部的密文。但直至4月1日，26天中，协约国方面对这些德文密电一筹莫展。

4月1日，是西方传统上的愚人节；就像上帝真要愚弄这帮法国佬一样，这一天，法国截收了18封这种用ADFGX战地密码加密的电报，却只能干瞪眼。

事实上，后来知道，这些ADFGX密码是通过"方表替代"和"密钥移位"两个过程的加密而得的。对比于当初破译这种密码时在黑暗中万千艰难的摸索，我们现在可以比较轻松地来看看它是怎么加密的了：

[1] 替代

首先构造一张由行、列都由ADFGX这5个字母作为标号、空格中随意填有a到z各个字母的用于替代的方表。

	A	D	F	G	X
A	q	w	e	r	t
D	u	i	o	p	a
F	s	d	f	g	h
G	j	k	l	z	x
X	c	v	b	n	m

图27. ADFGX密码的替代方表

由于这是一个5×5的方表，只有25个空格，又由于y在德语中使用较少，所以y在表中略去。

假定要加密的明文是"Let us go"。首先全部改为小写、删除空格，将明文变为"letusgo"。然后，对第1个字母l，在上面的方表中找到其对应的行、列编号分别为G、F，因此l就以GF替代。照此办理，直到完成全部7个字母的替代编码：

l	e	t	u	s	g	o
GF	AF	AX	DA	FA	GF	DF

[2] 移位

将这些编码连起来，变成GFAFAXDAFAGFDF。

现在假设要求密钥的长度为n（从安全的角度考虑，这个n当然越大越好；事实上，在ADFGX当年的使用中，这个密钥序列的长度一般要取到20左右），将1到n这n个自然数的顺序打乱，重新排列；比如，取密钥长度为8，将12345678打乱成63482517。

6	3	4	8	2	5	1	7
G	F	A	F	A	X	D	A
F	A	G	F	D	F		

图28. ADFGX的移位表

将重新排列后的长度为8的序列63482517分开写成一行，作为8个纵列的编号，然后将刚才连起来的编码中的字母顺序逐一填到这8个纵列中去，由左至右，到头再返回左边继续。

然后，将每个纵列的字母，不再管63482517的顺序，而是按12345678的自然顺序，逐一取出排序：

1	2	3	4	5	6	7	8
D	AD	FA	AG	XF	GF	A	FF

连起来，就得到了明文"letusgo"的最终加密结果：DADFAAGXFGFAFF。

因此，ADFGX密码通过自己才掌握的方表替代和密钥移位，将每个字母加密成ADFGX这5个字母中的2个。

其实，发明ADFGX密码的纳贝尔上校是很谨慎的，他曾经提出：替换-换位之后形成的密文，应该再作一次移位，才能作为最后的密文。

但德国无线电和密码机关人员认为先前的替代和移位已经够结实了，除非上帝本人来，是没人破得了的，何况，作为战地密码，再往复杂里搞不仅容易出错，也白白增加加密和解密的时间；而在战场上，什么比时间更重要呢？于是，这个给敌军找麻烦的主意被否决了。

现在回到1918年4月1日这个ADFGX密码让法军郁闷的愚人节。

前面提到，这一天，法军一共截获了德军用ADFGX战地密码加密的18份密电；面对这些不知所云的密电，法军密码分析员乔治•潘万（Georges Painvin）似乎已经绞尽脑汁。可他却丝毫不敢懈怠：面对着正在疯狂攻击的德军，事实上他已身系正在苦苦支撑着的法军的生死存亡，早已完全是在超负荷工作，根本没有休息时间，玩儿命了！

好在，潘万的冥思苦索已经得出以下3个判断：

（i）德军所用的是复合加密，即先用替代方表加密，

再用密钥移位表加密；

(ii) 经过频率分析得知，该方表每天一换，也就是说，图 27 中那种方表，虽然每天都还是 5 × 5 的，但是填写顺序每天就完全不同；

(iii) 经过频率分析得知，该换位表的密钥每天一换，也就是说，图 28 中那种移位表，每列字母头顶上的数字排成的序列，不仅它们的长度每天要变，而且它们之间的排列顺序也每天要变。

现在，盯着已经越来越相信突破口就在它们身上的两份密电 CHI-110 和 CHI-104，潘万首先要解决的问题是：这么一连串全无间隔的字符，而且，CHI-104 电文中遗失了一个字母，以问号替代，怎么分组？换句话说，怎么断句？

CHI-110：

ADXDAXGFXGDAXXGXGDADFFGXDAGA
GFFFDXGDDGADFADGAAFFGXDDDXDDGXAX
ADXFFDDXFAGXGGAGAGFGFFAGXXDDAGGF
DAADXFXADFGXDAAXAG

CHI-104：

ADXDDXGFFDDAXAGDGDGXDGXDFGAG
AAXGGXG?DDFADGAAFFFDDDFFDGDGFDXX
XADXFDAXGGAGFGFGXXAGXXAAGGAAAAD
AFFADFFGAAFFA

由于潘万已经判断它们的最后一步是用一个移位表加密的，因此现在的问题具体来说就是，怎么把这两串字符按它们原来在图 28 那样的移位表中的纵向排列方式分割开来？要知道，对于潘万，这个移位表有多少列、多少行、有哪些列并没有排满，这些可都是不知道的！

潘万注意到，这两份密电都是同一天截收的，因此它们用的方表、密钥和移位表都应该是相同的，他决定就从这一点插进去！

无穷无尽的思索、尝试、失败和从头再来，潘万终于走出了第一步，对这两份密电完成了分组：

CHI-110:	① ADXDA	② XGFXG	③ DAXXGX	④ GDADFF	⑤ GXDAG	⑥ AGFFFD	⑦ XGDDGA
CHI-110:	⑧ DFADG	⑨ AAFFGX	⑩ DDDXD	⑪ DGXAXA	⑫ DXFFD	⑬ DXFAG	⑭ XGGAGA
CHI-110:	⑮ GFGFF	⑯ AGXXDD	⑰ AGGFD	⑱ AADXFX	⑲ ADFGXD	⑳ AAXAG	
CHI-104:	① ADXDD	② XGFFD	③ DAXAGD	④ GDGXD	⑤ GXDFG	⑥ AGAAXG	⑦ GXG?D
CHI-104:	⑧ DFADG	⑨ AAFFF	⑩ DDDFF	⑪ DGDGF	⑫ DXXXA	⑬ DXFDA	⑭ XGGAGF
CHI-104:	⑮ GFGXX	⑯ AGXXA	⑰ AGGAA	⑱ AADAFF	⑲ ADFFG	⑳ AAFFA	

潘万大受鼓舞，继续不眠不休地进攻。两天两夜过去了，4 月 3 日，突然，仿佛就在一瞬间，ADFGX 的壁垒终于在潘万中尉顽强无比却又精妙无比的攻击下轰然倒塌，他终于成功地破译了 4 月 1 日这两份德军电文！接着，余下的 16 份电文的保护层，也就都在一鼓作气之下全部击碎了！

从这时开始，法军对于对面的德军，已经能够做到“知敌先机”了；但由于战场态势对于法军过于严峻，要对强大的德军做到“制敌先机”，法军还心有余而力不足，还得等待时机。

这个时机终于来了。1918 年 6 月 1 日，德军启用了 ADFGX 战地密码的升级版——ADFGVX 密码。

其实德军此时并不知道 ADFGX 密码已被法军破译，他们仍然认为这个密码牢固得足以抗御除了上帝本人外的天下一切攻击；他们之所以对这个密码升级，原因是 ADFGX 密码不能直接对阿拉伯数字编码、加密。

从图 27 的替代方表可以看出，25 格的表中，连 26 个拉丁字母都没法装完，更没有 0 ～ 9 这 10 个阿拉伯数字的空余位置。然而，战场信息显然又不可能离开大量的数字，这样一来，就必须将所有数字都以德文来表达；这种用某一种民族语言来表达数字的麻烦，在瞬息万变的战场上，特别是在战场上操作本来就非常复杂的加密、解密（脱密）过程中，有时足以令人疯掉。例如，365872，用中文表示是“三十六万五千八百七十二”，用英文表示就得是“three and sixty-five thousand and eight hundred and seventy-two”。

为此，发明 ADFGX 密码的纳贝尔上校在 ADFGX 中增加了一个字母 V，变成 ADFGVX，这样，图 27 的替代方表就变成了 6 × 6 = 36 个空格了，不仅可以将先前略去的 y 放入，而且还余下 10 个空格，刚好可以放置 0 ～ 9 这 10 个数字。

图 29. 法军密码分析员乔治·潘万中尉

而且，由于增加了方表格数，也就增加了方表中字符排列顺序的变化种类，同时也就增加了破译难度。

更而且，现在包含 0 ～ 9 这 10 个数字的方表将这些数字与字母一视同仁都编码为 ADFGVX 中的两个字母，再通过移位表移位，那么，有着诸如“the”、“any”、“back”之类固定搭配的语言单词，就和没有这类固定搭配的数字一起，被混合打乱、搅成一锅浆糊了，让敌人更加难以从词频、字频的角度发现蛛丝马迹。

至于为什么增加的字母是 V 而不是另外什么字母，原因是字母 V 的摩尔斯电码为“. . . –”，易于拍发也易于分辨和抄收。

在战场上，选用一些无论在拍发还是在抄收时都不容易出错的字母作为密码字符，这一点非常重要：枪林弹雨中，密码操作员精神高度紧张，如果事先设计密码时对此考虑不周，这时出错的概率必然大大增加。

很完美，是不是？可惜，他们遇上的是一个天才级的对手，乔治 • 潘万！

在法国这边，结合战场形势，已经基本可以肯定德国人即将发动一场对于双方都是决定性的强大攻势；再从德国人并不知道 ADFGX 密码已被破译的情况下，却“悍然”启用强度更高的 ADFGVX 密码来看，德国人对这一攻势的期望之高可见一斑！因此，这一攻势之于法国命运的重要性，可想而知。

而且，关键是德国人要的只是协约国这边在战役结束之前不能破译即可，而协约国特别是法国这边，却必须在德国发起攻势之前——还不能是已经临近敌人进攻开始的“之前”，还必须得让自己有起码的反应、调动、准备的时间——破译这个密码，否则在此之后，败局已定，无论多么完美的破译也都没用了。这一点，德国人很清楚，法国人很清楚，潘万中尉也很清楚。

图 30. 联军统帅福煦元帅

在对截获的密电进行仔细端详以后，潘万的注意力很快集中到其中三份电文上。这三份电文有个共同特点：都是 GCI 电台发出的，电文的时间组都是 00 : 05。

基于此前他对 ADFGX 密码的成功破译，终于，他在第二天下午七时前，也就是 6 月 2 日 19 时前，完全还原了德军 6 月 1 日使用的 ADFGVX 的移位表和方表！

图 31. 贡比涅森林：福煦与德国签订停战协定后在福煦车厢前留影

剩下的事情就没什么可说的了，他很快得出了这两份密电的明文：

“第 14 步兵师：司令部要求电告前线（情况）。第 7（军）司令部。”“第 216 步兵师：司令部要求电告前线（情况）。第 7（军）司令部。”

但这对于法国来说，还没解决问题的全部，他们还必须尽早知道，德国将在何时、何地发起这场对于法国生死攸关的战役？

要知道，此时不仅德军前锋距巴黎已不足 70 公里，德军还占据了巴黎以北亚眠和蒂耶里堡两大突出部，对巴黎已形成了钳形进攻的态势！

这样的情况下，作为协约国联军统帅的法国福煦元帅，怎能不为猜测对面的德军统帅鲁登道夫元帅的想法而犯愁呢：他手里没有那么多预备队兵力，能让他布置到所有可能的德军进攻方向上，他必须知道鲁登道夫到底想在哪里动手。

好在，上帝此时对法国的心情似乎不错，让法国人的好运气再一次延续：6 月 2 日了，德军居然还在使用 6 月 1 日的替代方表和移位表！这已经够出奇的了，可到了 6 月 3 日，这种情况居然还在延续！真能让人晕倒！

这可犯的是密码学的大忌：“一次一密”做不到也就算了，但若连“一天一密”都不做到，这个战地密码最最起码的底线也就丢掉了！

6 月 3 日清晨，潘万的下级吉塔尔，面对着新截获的德军密电，不知德军今天的密钥又会把密文的分组搞成什么样；抱着死马当作活马医的态度，先用前天的分组方式试试，居然成功了！再用前天的替代表和移位表一试，让他都不敢相信自己的眼睛：居然都对了！这不是见鬼了么？

看看电文：“赶运弹药，不被发现（的话）白天也运。

就这么简单的十二个字，成为了协约国军队战场态势的一道分水岭！由此，赶紧辅以其他来源的情报和分析，法国

图 32. 贡比涅森林：德国凯特尔元帅与法国亨其格尔将军在福煦车厢中签署停战协定

人终于笑了：德国这次的进攻主力是第 18 集团军，进攻方向就是距离它在雷马奇的司令部 26 公里的贡比涅！

密码破译和无线电侦察，给协约国军队在这次致命的进攻之前，争取到了整整六天！

6 天之后的 6 月 9 日 04 时 20 分，德军准时发动了西线的第四次战役，一切都如法军判断的一样：

主攻部队：第 18 集团军；

战役目的：消除驻守在苏瓦松一带第 7 集团军右翼的威胁，并拉直亚眠、蒂耶里堡两个突出部之间的战线。

攻击方向：贡比涅。

战役的最后结果，是 1918 年 11 月 11 日，福煦代表协约国，与德国代表在贡比涅森林雷道车站的一节火车车厢里，接受了德国的投降，签订了停战协定；11 时，各战胜国鸣放礼炮 101 响，宣告第一次世界大战结束。此后，这节从此以福煦命名的车厢被放入了博物馆。

也正因如此，始终对德国在一战中的失败耿耿于怀的希特勒，在二战中击溃法国的抵抗、占领巴黎后，特别指定，谈判地点不设在巴黎，而是设在这片一战时令他心摧欲裂的贡比涅森林，而且，按照希特勒为了羞辱法国人而作出的指示，6 月 22 日下午 3 时 30 分，法国代表进场时才发现，要签订停战协定的场所，居然就是 1918 年德国在这里签订停战协定的那节福煦车厢，而且，在这节从博物馆中拉出来的车厢里，所有的摆设还都刻意恢复成了当年的模样。

这……太伤自尊了，法国人弱弱地表示难以接受。可在这种场合下，哪里还有他们表示不满的余地？希特勒、戈林、里宾特洛甫等人起身离去，在凯特尔元帅以典型容克贵族风格的冷漠有礼宣布完对法国的要求后，身为法国代表团团长的查尔斯·亨其格尔蒋军，代表法国在停战协定上签字。

此后，福煦车厢作为战利品，被德军运到柏林。后来，为了免于德国再次战败时的再次羞辱，希特勒下令炸毁了福煦车厢。

（4） 恩尼格玛密码： 一战结束后，人们开始感觉“一张纸一支笔”的密码编写、拍发、抄收的方式效率实在不能再满足要求，开始研究各种各样的机械式和机电式密码机。这些密码机大都是将带有特别设计的导电触点的机械转轮以导线进行可变电气连接，来完成密码替代。

这些转轮机通常有一个键盘和一系列转轮，每个转轮是字母的任意组合，有 26 个位置，并且完成一种简单代替。例如：一个转轮可能被用线连起来使得可以用 F 代替 A，用 U 代替 B，等等，一个转轮的电气信号输出往往作为另一个转轮的输入。而且，设计者还往往给转轮装上各种各样的进位传动齿轮。这样，动态改变多个转轮之间的连接关系和传动关系，便可以对替代关系产生复杂的动态改变，使得一个明文字母在不同时候被替代成不同的密文字母，用以对抗字频攻击。

由德国发明家亚瑟 • 谢尔比乌斯（Arthur Scherbius）发明的电气编码机械“恩尼格玛”（ENIGMA，意为哑谜），就是这些密码机中最出色、最著名的代表。恩尼格玛在二战期间由德国人使用，而且，为了战时的需要，还大大地加强了它的基本设计。

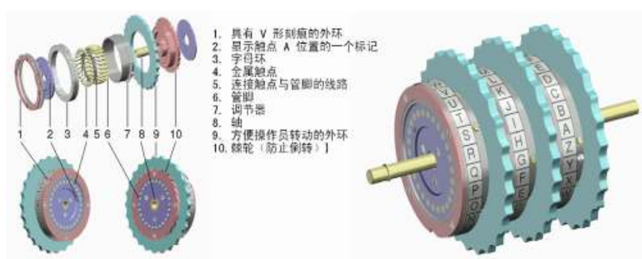


图 35. 恩尼格玛机的转轮结构和排列方式

恩尼格玛有 5 个转轮，每个转轮都有按不同位置和连接关系排列的 26 个字母，每次使用从这 5 个转轮中选择 3 个。机器中还有一块能将 6 对字母两两交换的连接板。恩尼格玛的密钥，就是由“3 个转轮相互之间的不同排列位置、3 个转轮各自的不同初始位置和连接板对 6 对字母的不同交换方式”构成；再考虑到从 5 个不同转轮中选择 3 个使用的可能性，这样的密钥数目有多大呢？这是一个令人头晕目眩的数字：

10×17576×6×100391791500

=105,869,167,644,240,000,

十亿亿零五千八百六十九万一千六百七十六亿

四千四百二十四万！

这个数字有多大呢？如果一秒钟尝试一个密钥，那么尝试完所有这些密钥需要 335,708,928 年！如果从过去算到现在，三亿多年前，那可还是石炭纪，连恐龙都还要再等一亿多年后才会在三叠纪出现。

如此复杂而强固的密码，可是却由于使用它的德国加密员在传送决定密钥使用方式的 3 个字母时为了避免错漏，而将这 3 个字母作了两次加密发送，导致两组（每组 3 个字母）不同的密文对应了相同的一组明文，给波兰总参二局密码处的密码专家马里安 • 雷杰夫斯基（Marian Rejewski）、杰尔兹 • 罗佐基（Jerzy Rozycki）和亨里克 • 佐加尔斯基（Henryk Zygalski）造成了后来终于撕裂恩尼格玛密码坚固外壳的细如发丝的隐蔽裂纹，最后在一系列卷入波、英、法、美多国情报人员和数学家、密码学家、工程师的充满阴谋陷阱、利益收买、暗夺明抢和卓绝思维、令人惊心动魄的行动后，被盟军破译和掌握。

在这个过程中，不仅有原为波兰波兹南大学数学教师的雷杰夫斯基最初的杰出贡献，而且，还有英国剑桥后来以天才计算机科学家、天才逻辑学家闻名于世的图灵（Alan M. Turing，1912—1954）和同事们设计的恩尼格玛专用解密机的强大推动。

所有德军恩尼格玛密码中，唯有海军的密码由于始终不惮其烦地严格遵守“尽可能保持最高强度”的使用原则，在盟军的密码攻击下基本上得以保全。

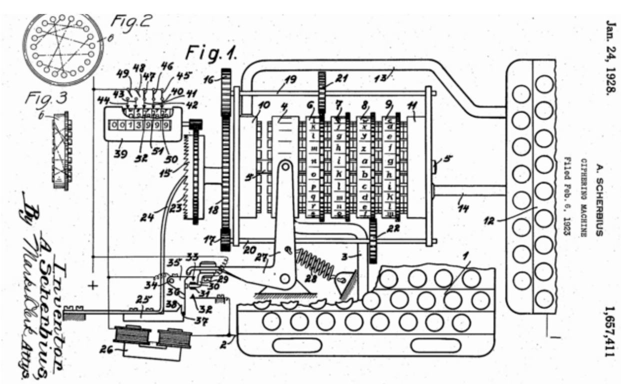


图 33. 谢尔比乌斯设计的密码机 1928 年取得的美国专利 1,657,411

盟军的情报部门将破译出来的恩尼格玛密码称为“超级密码”（ULTRA）。虽然“超级密码”对二战到底有多大贡献还在争论中，但是人们都普遍认为，盟军在西欧的胜利能够提前两年，完全是因为恩尼格玛密码机被成功破译。

图 34. 二战德军恩尼格玛机

5. 当人力终于不能承受——现代密码

二战后，密码的需求日益增长，越来越难以像以往一样靠人力来完成；另一方面，电子学与计算机逐渐以越来越高的速度发展，加上信息的 2 进制表示在计算机中已成为基本信息形式，也促成了日益复杂的密码理论和技术。结果是，手工的加、解密运算越来越被计算机所取代，而且，计算机还可以加密任何 2 进制形式的资料，密码理论和技术的应用对象不再仅仅限于书写的文字。

这样一来，以语言学为基础的破译方法基本失效。不过，另一方面，计算机的强大计算能力却也同时促进了破译方法（密码分析）的发展，使得很多情况下的攻击尝试变得简单。

加密法的设计应该使得信息的安全性由密钥的安全性充分保证，而不应依赖加密法本身的安全性。这一由荷兰语言学家奥古斯特 • 柯克霍夫（Auguste Kerckhoffs）于 1883 年在《军事密码学》一书中提出并被称为柯克霍夫原则的加密法设计准则，已经得到普遍的采用。事实上，二战中德军的恩尼格玛密码机的设计，已经遵循了这一准则，而由美国国家安全局（NSA）和 IBM 为了抗御密码分析中新发展起来的差分分析法而制定、由美国国家标准局于 1977 年 1 月 15 日颁布为国家标准的数据加密标准（DES，Data Encryption Standard），更是典型地体现了这一准则。在计算机的计算能力以摩尔定律高速发展的二十年中，公开了算法的 DES 一直都在保护着银行、公司甚至核武器密钥的安全。直到 20 世纪 90 年代后期，DES 的加强版本 AES、3-DES 等加密法的应用才开始被提上日程。

不过，美国国家标准局公布的 DES 算法中，可没包括

$$S_1=\begin{pmatrix} 14 & 4 & 13 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\ 15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \end{pmatrix}$$

$$\vdots \qquad\qquad\qquad \vdots$$

$$S_8=\begin{pmatrix} 13 & 2 & 8 & 4 & 6 & 15 & 11 & 1 & 10 & 9 & 3 & 14 & 5 & 0 & 12 & 7 \\ 1 & 15 & 13 & 8 & 10 & 3 & 7 & 4 & 12 & 5 & 6 & 11 & 0 & 14 & 9 & 2 \\ 7 & 11 & 4 & 1 & 9 & 12 & 14 & 2 & 0 & 6 & 10 & 13 & 15 & 3 & 5 & 8 \\ 2 & 1 & 14 & 7 & 4 & 10 & 8 & 13 & 15 & 12 & 9 & 0 & 3 & 5 & 6 & 11 \end{pmatrix}$$

算法中要用到的 8 个被称为 S 盒（S-box）的 4×16 数字矩阵的设计由来，这一点长期受到质疑和非议，被认为是政府秘密保留的窥探私人秘密的暗门。

由于加密方法越来越脱离语言学的具体理论，而更多地向二进制数字信息处理的方向发展，包括信息论、计算复杂性理论、统计学、组合学、抽象代数以及数论等等数学分支的理论越来越多、越来越深地被用于密码学。

自古以来，直到 1976 年以前，密码的加密和解密使用的都是同一个密钥，正如锁上房门和打开房门的都是同一把钥匙一样；这已经成为天经地义的认识。这种用同一个密钥加密和解密的体制称为“对称密钥体制”，也因其必需的密钥必须全部严格保密的私密性而被称作“私钥体制”。但是，对称密钥体制或私钥体制从来就隐含严重的问题：

[1] 由于加密和解密使用的是同样的密钥，因此在分发加密密钥时，事实上也就是在分发解密密钥，也就必须严格保证分发途径和分发过程不能出错，即使分发顺利完成了，此后密钥的安全性也还只能寄希望于掌握加密密钥的人的可靠性；

[2] 由于加密和解密使用的是同样的密钥，因此在分发加密密钥时，如果需要分发的处所不止一个，就都得分别分发；这在分发数量增多时，将会使密钥分发或传送的过程变得严重困难；

[3] 如果需要分发密钥的人不止一个，而又须得保证他们之间不能以自己的密钥互相解密，便须为不同的人配置不同密钥，而作为对应措施，自己这边也就必须分别配置多个不同密钥；这在配发数量增多时，将会使密钥管理变得严重困难。

这些问题一直就存在着，但很少有人去尝试改变，因为难以想像一个公开了的密钥还怎么能发挥它原有的作用。

革命性的突破发生在 1976 年，这一年，美国斯坦福大学教授马丁 • 赫尔曼（Martin Hellman）和他的研究助理怀特菲尔德 • 迪菲（Whitfield Diffie）以及博士生默克勒（R.C. Merkle），提出了被称作“公钥密码体制”的概念：

加密、解密用两个不同的密钥，加密用公钥（public key），即可以公开，不必保密，任何人都可以用；解密只能用私钥（private key），此钥必须严加管理，不能泄漏。

而且，他们还发明了防止篡改和抵赖的数字签名（digital signatures）技术，即用私钥签名，再用公钥验证。

概括地说，公开密钥由一个密钥对组成，只适用于下列两个串连的行为：

[I] 一个人对某些人的“密钥发布”

[II] 这些人对这个人的“密文集中”

我们可以用一把专门设计的“公钥机械锁”来平行说明这个体制的原理。

如下是一把有两个锁孔和两把钥匙 A、B 的“公钥机械锁”的立体图和俯视透视图。为显示清楚起见，略掉了锁的外壳和一些辅助的作动机构。其中，

[i] 钥匙 B 是可以公开派发、随意复制的公钥，用它插入右边的锁孔向右扭转，便可使得钥匙 B 的锁闭定位销在弹簧拉动下滑入钥匙 B 的锁闭滑槽；此时，锁舌 B 插入锁杆上的锁槽 B，使得锁杆不能再被拉起，达到了用公钥进行锁闭的效果。

[ii] 一旦用钥匙 B 锁闭，由于钥匙 B 的锁闭滑槽的阻挡，钥匙 B 已无法再左右扭动，这就达到了再用公钥无法开锁的效果。

[iii] 钥匙 A 是由自己私密保管、不能公开的私钥。当自己要开锁时，将钥匙 A 插入左边的锁孔向左扭动，则钥匙 A 的开锁滑槽带动钥匙 B 的开锁定位销向左边移动，最后将锁舌 B 从锁槽 B 中拉出，解脱锁舌 B 对锁杆的卡阻，使锁杆恢复可以向上拉起的状态，达到了用私钥开锁的效果。

[iv] 用钥匙 A 作锁闭用的公钥的情况与此对称。

这把“公钥机械锁”的锁闭、开启的机制，便是公钥密码体制的一个具体演示。

不过，后来有人提出真正最早发明公钥体制的并非迪菲和贺尔曼二人，认为 1997 年的公开文件中表明早在 1970 年，英国的情报部门“政府通信总部”GCHQ 的数学家 James H. Ellis 便已发明非对称钥匙密码，只是由于保密的原因，把这 “密码革命”的巨大荣誉让迪菲和赫尔曼得了。但这一

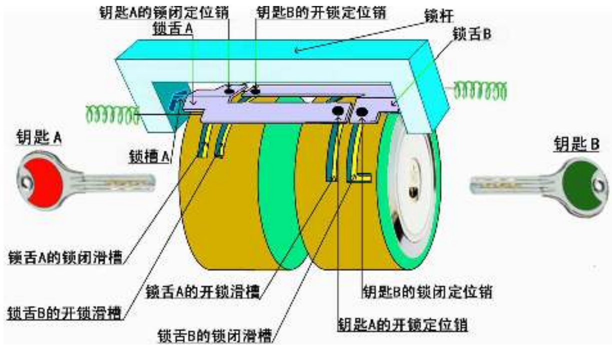


图 37. “公钥机械锁”的内部构造立体图

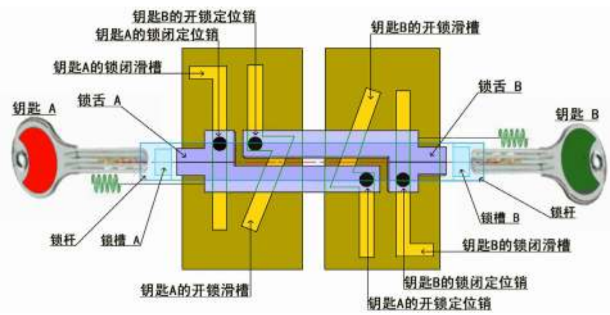


图 38. “公钥机械锁”的内部构造俯视图

点有争议。美国国家安全局也有过类似的宣称，不过就没多少人附和了。

公钥体制的概念提出后，人们立即开始投入其实现研究。比较典型的首先是美国斯坦福大学的默克勒（Ralph Merkle）和赫尔曼（Martin Hellman）在 1978 年提出的陷门背包公钥密码方法，以二人姓名首字母简称为 MH 法。

“背包问题”是组合数学中的一个经典问题，说的是：假如有一堆物品，所有重量都不同，问能否从中选择几件放入一个背包中使得总重量等于一个预先给定的值？用形式化一些的语言来描述: 设有 n 个正整数 $x_1, x_2, \cdots, x_n$（称为“重量序列”）和另一个正整数 S，问能否找到一个长度为 n 的由 0、1 构成的序列 $\{a_1, \cdots, a_n\}$，使得

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = S \ ?$$

例如，假设这些物品的重量序列为 1，5，6，11，14，20，则可以用 5、6 和 11 组成一个重为 22 的背包，但却不可能组成一个重为 24 的背包。

背包问题的求解复杂度随着物品个数（即重量序列的长度）的增长而呈指数增长；也就是说，当物品个数比较大时，要对一个指定的背包重量用穷举的办法找出物品搭配的方式，将会变得非常困难。

例如，实际上使用的背包算法中的重量序列长度至少为 250 个数字，每个数字一般在 200 到 400 位之间。现在世界上速度最快的超级计算机是每秒千万亿次，中国 2009 年 10 月公布的巨型机“天河一号”的速度是 1206 万亿次，也是这个最高级别。就算用这样的计算机来对这样的背包问题进行穷举搜索求解，要试完所有可能的值也要10^{36}年，在太阳毁灭之前也没法算完。

默克勒和赫尔曼的想法是: 选定一个由互不相同的正整数排成的序列作为重量序列；将明文用二进制编码，再将其按重量序列长度分段；然后将这些二进制的明文段分别与重量序列作乘积和（也就是按照一个二进制明文段中的 0、1 排列对那一堆物品作取舍，将取出来的物品重量求和）；所得的各个乘积和（背包重量）就作为密文：

明文:	1 1 1 0 0 1	0 1 0 1 1 0	0 0 0 0 0	0 1 1 0 0 0
重量序列:	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14	1 5 6 11 14 20
密文:	1 + 5 + 6 + 0 + 0 + 20 = 32	0 + 5 + 0 + 11 + 14 + 0 = 30	0 + 0 + 0 + 0 + 0 = 0	0 + 5 + 6 + 0 + 0 + 0 = 11

如上面这个例子，明文的二进制编码结果是 111001010110000000011000，重量序列取为 1，5，6，11，14，20；将明文的二进制序列按密钥长度 6 分为 4 段: 111001，010110，000000，011000；将各段明文分别与重量序列作乘积和，分别得到 32，30，0，11，这就是明文的二进制序列 111001010110000000011000 加密后的结果—密文。

注意这里加密时是将先行取定的二进制明文序列作为背包问题的解，由此求出对应的背包重量，将其作为密文，这与背包问题的顺序刚好是倒着的：背包问题是先给出背包重量，然后问包中物品的重量是哪些。因此，解密时的运算才和背包问题同步：都是根据背包重量来求对重量序列中各项的选取方式。

数学上证明背包问题是著名的 NP 完全类困难问题，至今没有统一的好解法；而要通过硬搜索来解这个问题，正如前面所述，一般而言在实际上是不可能的。

既然如此，这种方法可就还不能作为一种加密方法；道理很简单: 别人固然没法从密文找出你的明文了，可你自己也没法重新找出来，知道重量序列也没用！

好在默克勒和赫尔曼在这个基础上进一步研究出了一种自己作解密运算很简单、但让别人解密却继续令他崩溃的方法；而且，他们这个方法还对两年前由赫尔曼、迪菲和默克勒提出的“公钥体制”思想，首先给出了一个具体的实现。

我们不妨来看看这是如何实现的：

> 背包问题一般而言非常难解，但是，对于一种特殊的重量序列，所谓“超递增序列”（superincreasing sequence），它却又有非常简单方便的解法。

超递增序列是这样一种序列，其中每一项都大于它前面所有项之和。例如 1，3，6，13，27，52 是超递增序列，而 1，3，4，9，15，25 则不是。

也就是说，当一个背包问题的重量序列是超递增序列时，对于任意给定的背包重量，要从重量序列中找出相应的重量组合非常容易；而当重量序列不是超递增序列时，要做到这一点就变得非常困难，难度之大，正如上述。

默克勒和赫尔曼找到一种方法，可以将一个超递增序列按照给定的参数，以统一的方式转换为一个非超递增序列，而且，使得从非超递增序列按某一种重量选取方式产生出来的背包重量，用这个超递增序列去求出这种重量选取方式是轻而易举的事。也就是说，一个超递增序列与由它转换而得的非超递增序列，面对同样的背包重量时，在各自的序列中决定了同样的重量选取方式，比如，都是第 2 项、第 5 项、第 11 项、……，等等。

因此，如果以一个超递增序列作为私钥，将其转换而得的非超递增序列作为公钥，那么，他人用公钥按上面的方式加密后，再用这公钥却几乎完全没法重新求出明文来；而对于掌握私钥的人，则可从超递增序列轻易求出。就这样，默克勒和赫尔曼用背包算法成功地实现了“公钥密码体制”的思想。

不幸的是，幸福实在太过短暂，好景也实在太不长，就在他们提出这个称为 MH 方法的密码体制后的两年，1980 年，MH 方法便被以色列的密码学家、图灵奖获得者 Adi Shamir 和美国密码学家 Richard Zippel 破译（Shamir，A. and Zipple, R. E. (1980), On the security of the Merkle-Hellman cryptographic scheme. IEEE Transaction on Information Theory, 26, 339-340）！他们找出了一种从 MH 密码系统所给出的公钥（非超递增序列）重构出其对应的私钥（原来的超递增序列）的算法，宣告了这种加密算法的夭折。

后来至今，还有一些人想方设法改进 MH 方法，希望重新恢复其安全性，但都已经没有多大意义了。特别地，当另一种基于完全不同的原理（素数分解复杂性）的公钥密码——RSA 密码的地位越来越巩固时，事实上基于背包算法的加密方法已经基本走到了尽头。

1978 年，美国麻省理工学院（MIT）的 Ron Rivest、Adi Shamir 和 Len Adleman 公布了另一个公开钥匙系统 RSA。RSA 公钥密码算法是目前网络上进行保密通信和数字签名的最有效的安全算法之一，其安全性完全基于数论中大素数分解的困难性，所以，RSA 需采用足够大的整数。因子分解越困难，密码就越难以破译，加密强度就越高。

围绕这个 RSA 算法，在 1990 年代还发生了几起挑战美国出口规范的事件。其中一件是 Phillip Zimmermann 著名的 PGP（Pretty Good Privacy，良好隐私）加密程序事件。

1991 年 6 月，基于 RSA 算法的网络加密程序 PGP 的作者 Zimmermann 在美国将 PGP 连同其源代码一并公开在互联网上。在以 RSA 为其根本的 RSA Security 公司提出抗议后，商务部和联邦调查局对 Zimmermann 进行了长达数年的调查、询问。

事实上，PGP 的出现是美国国务院和国家安全局所最不愿意看到的事情。美国政府的 Clipper 计划和托管加密标准，就是企图保证当局能够随时窃听任何私人的电话和拆看任何私人的文件。Zimmermann 之所以把 PGP 在网上公开，就是为了在美国国会开始考虑限制计算机自由并制订严酷的法律之前，让大家有一个保护电子通信隐私的程序。PGP 也因此和 Linux 一样，被并列为最伟大的自由软件。

由于美国政府按照“美国国际贸易和武器管制条例”，把加密系统列入军火范畴，把加密软件的出口视同于武器走私，同时美国政府又规定源代码只能以书面形式而不能以电子形式出口，因此 Zimmermann 在他的 1995 年出版的《PGP Source Code and Internals》书中尽数列出 PGP 的源代码，让美国政府十分恼火。

当然，政府也不是白吃饭的，立即就此向法院提出对 Zimmermann 的诉讼。但是，紧接着就被柏克莱加州大学的研究生 Daniel Bernstein 以言论自由的理由发起对美国政府的反诉讼。最终，法院在 1999 年判决，印出密码算法的源代码属美国宪法言论自由保障范围。Zimmermann 的自由最终得以保全。

图 40. PGP 作者 Zimmermann

不过，虽然已经确定 RSA 的安全性完全依赖于大数分解的困难性，但却至今没能证明大数分解就必定困难，只证明了它的难度与数

学中一类著名的困难问题——NP 完全类问题相当；但 NP 问题到底有多难，也至今没能有一个确切的答案。

正因如此，加上此后大素数分解的新纪录不时被打破，例如，2007 年 3 月 6 日波恩大学等 3 个机构的计算机集群在 11 个月的计算后的结果便颇有演示意义：这个结果把一个 307 位的数字分解成了两个素数因子：

$2^{1039}-1=$
1159420574 0725730643698071 48876894640753899791 70201772498686835353882248385
9966756608 0006095408005179 47205399326123020487 44028604353028619141014409345
7970787973 8061870084377771 86828680889844712822 00293520180607475545154137071
1023817

因子：

5585366661 9936291260 7492046583 1594496864
6527018488 6376480100 5234631985 3288374753
×
2075818194 6442382764 5704813703 5946951629
3970800739 5209881208 3870379272 9090324679
3823431438 8414483488 2534053344 7691122230
2815832769 6525376091 4101891052 4199389933
4109711624 3589620659 7216748116 1749004803
6597355734 0925320542 5523689

现在，人们对 RSA 安全性的信心已经开始有所动摇，目前建议其密钥（由数字组成）长度最好取到 1024 位或以上。

目前国际上公认比较安全实用的公钥密码体制是所谓的椭圆曲线密码体制，但也只是“公认”，并没能证明这一点。椭圆曲线密码的原理对于非专业人士来说已经过于专业，这里就不介绍了。

此外，还有正在热烈研究之中的量子密码，由物理学基本原理决定了被不露痕迹地中途截收是不可能的，这里也不介绍了。

6. 吁一口气，回到现实——几点建议

经过了如此漫长（但仍然挂一漏万，密码学的内容和历史实在太丰富了）走马观花式的浏览，作为非密码专业人士却又没法离开密码的我们，可以得出几个有用的结论：当我们不得不使用密码（实际上是前面叙述中所说的“密钥”）时，

(1) 尽可能不要采用别人站在你的角度容易设想到的密码，例如自己的或家人的姓名或姓名缩写、生日、电话号码、身份证号码、门牌号码之类的字符；要让自己想到：如果这样设置密码，固然带来很大的便利，但由此同时带来的巨大风险是否值得？

(2) 以无线电波或红外光波之类无线传输用作通过口令类型的密码（如汽车门钥、车库门钥等），只要密码不是可变的，其安全性都值得怀疑：试想，当你发送密码时别人也可以不露痕迹地接收，而且还不必非得破译其中的密码，直接记录下来便相当于复制了你的钥匙，在你离开后便可大摇大摆地打开车门、房门了。

(3) 在网上，没什么信息是绝对安全的，切记，凡是要跟网络连接的计算机，上面任何没有足够强度加密的信息，在有心人面前都如自己囊中之物一般。

(4) 绝大多数公开发售或网上下载的商业性加密方法，在专业人士特别是以国家力量支撑、配备了巨大计算能力的专业人士面前，都如篱笆墙一样，对破译只具有象征性的防御意义。例如，现在广泛使用的 RAR 压缩软件自带的加密功能，从算法设计看貌似够强固了，采用了数据加密标准的加强版 AES，但其密码验证机制的设计却有重大缺陷，难不住专业人员。因此，如果认为自己的秘密事关重大，建议使用在专业密码界有很好口碑的加密算法，特别是其中那些公开了源代码的加密算法，例如，前面介绍的 PGP 就是一个不错的选择。虽然这样做也仍然不能绝对保证安全，但毕竟是相对最为稳妥的选择了。

(5) 又要密码安全可靠，又要密码使用方便，这不是难为人吗？但还是有办法的：用一句自己熟悉却并不普遍、长度足够的句子（起码 16 个字以上），以其单字首字母的排列甚至就是单字本身的排列来作密码，尽量把其中的标点符号也包括进去，这就能比较好地兼顾这两个互相冲突的要求。

最后，祝长久好运！

全文完

注：本文中，除图 18、图 37、图 38 和各个表格为自绘外，其余图片取自网上公开资源，这里不及一一列明，谨一并致谢。另外，本文属于科普文章，参考了大量公开文献，但均只按本文体例需要取其含义、另予表述。

布拉格天文钟的数学原理

The Mathematics Behind Prague's Horologe

M. Krizek （捷克）
A. Solcova (捷克)
L. Somer （美国）

一、引言

欢迎来到捷克共和国的首都——布拉格。这个中欧城市不但拥有“千塔之城”的美誉，而且更被联合国教科文组织列入世界文化遗产。不少举世闻名的数学家、物理学家和天文学家都在这片土地上度过光辉的岁月，留下许许多多永不磨灭的历史印记。其中的代表人物包括文艺复兴时期的意大利哲学家乔尔达诺•布鲁诺(Giordano Bruno)、丹麦天文学家第谷•布拉赫 (Tycho Brahe)、其助手德国天文学家约翰尼斯•开普勒 (Johannes Kepler)、波希米亚数学家伯纳德•波尔查诺 (Bernard Bolzano)、法国数学家奥古斯汀•柯西 (August Cauchy)、挪威数学家尼尔斯•亨利克•阿贝尔 (Niels Henrik Abel)、奥地利数学及物理学家克里斯提昂•多普勒 (Christian Doppler)、奥地利物理学及哲学家恩斯特•马赫 (Ernst Mach)、相对论创立人德国理论物理学家阿尔伯特•爱因

1. Introduction

Welcome to Prague — the capital of the Czech Republic, called the “City of a Hundred Towers”, located in central Europe, and designated as a World Heritage site by UNESCO. Many famous mathematicians, physicists and astronomers have spent here very fruitful and creative years, and left unforgettable traces in Prague, in particular, Giordano Bruno, Tycho Brahe, Johannes Kepler, Bernard Bolzano, August Cauchy, Niels Henrik Abel, Christian Doppler, Ernst Mach, Albert Einstein and his mathematical colleague Georg Pick who was one of the people who taught him the tensor calculus. During their stays in Prague the above-mentioned scientists developed several fundamental mathematical and physical theories and engaged in related activities. For instance, in the beginning of the 17th century Kepler formulated the first two of his three laws of planetary motion based on Tycho Brahe's observations. In the first half of the 19th century Bolzano constructed a nondifferentiable continuous function (of a fractal character) and wrote a treatise on infinite sets entitled Paradoxes of infinity (1851). In 1842 Doppler, professor of mathematics at the Prague Technical University, first lectured about his

斯坦 (Albert Einstein) 和他的大学同僚乔治•皮克 (Georg Pick)，而皮克是教授爱因斯坦张量微积分的数学家之一。上述科学家在布拉格生活期间，建立了几个对后世影响深远的数学和物理学理论，并且从事相关之研究工作。十七世纪初，开普勒根据第谷•布拉赫的观测结果，提出行星运动三大定律之第一、第二定律。十九世纪上半叶，波尔查诺给出了一个既有分形特征，又不可微分的连续函数，并且以无限数集 (infinite sets) 为题撰写了《无穷的诡论》(Paradoxes of Infinity, 1851)。1842年，布拉格理工大学数学教授多普勒在布拉格Ovocný trh(图1)的查理大学，首次就其创立的效应 (后来称为“多普勒效应”) 发表公开演讲。1911年至1912年，爱因斯坦在布拉格德国大学 (Prague German University) 担任理论物理学教授，醉心于广义相对论的研究工作。甚至著名捷克作家卡雷尔• 恰佩克 (Karel Capek) 也是在布拉格发明“robot”这个字 (捷克语Robota，意谓劳役、苦工)。本文后面会简单介绍这些与布拉格息息相关的伟人纪念碑和雕塑。接下来，本文集中讨论布拉格旧城广场中心的一个著名建筑物，分析其中有趣的数学问题。

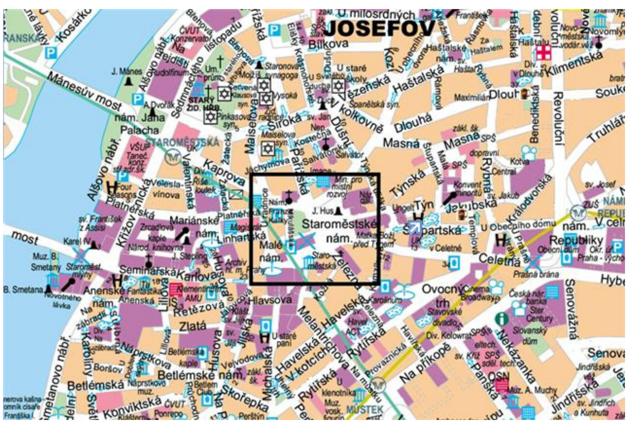


Fig.1 布拉格旧城区中心地图

Map of the Old Town in the center of Prague

布拉格旧城区中心(图1-2)有一个古色古香的天文钟 (捷克语orloj，英语horologe)。无论是一般游客，或是热爱数学的人，都会慕名而来一睹这个举世稀有的珍品。本文将揭示天文钟与三角形数之间鲜为人知的关系，探讨三角形数的特性，以及这些特性如何提升大钟的准确度。

布拉格天文钟的数学模型设计来自简•安卓亚 (Joannes Andreae，捷克语Jan Ondrejuv，生于1375年，

effect (later called the Doppler effect) at Charles University at Ovocný trh (see Figure 1). Einstein, while a professor of theoretical physics at the Prague German University, worked on his theory of general relativity in 1911–1912. The famous Czech writer Karel Čapek invented the term “robot” in Prague. Before briefly detailing plaques, statues, and other memorials to these personalities of Prague at the end of this paper, we discuss some unexpected mathematics associated with a prominent building at the heart of the Old Town Square of Prague.

In the center of Old Town in Prague (see Figures 1 and 2), there is an astronomical clock (called “orloj” in the Czech language and horologe in English) — an interesting rarity often visited by many tourists, not only mathematical tourists. We found that there is a surprising connection between this clock and triangular numbers. In this article we take notice of special properties of these numbers that make the regulation of the bellworks more precise.

Fig 2. 旧城广场天文钟的位置

Location of the astronomical clock at the Old Town Square (Staroměstské náměstí)

The mathematical model of the astronomical clock of Prague was invented by Jan Ondřejův, called Šindel (Joannes Andreae, cca 1375–1456), a professor at Prague University founded in 1348 by the Emperor Charles IV. In 1410, Šindel was the rector there. The astronomical clock was realized by the skilled clockmaker Mikuláš (Nicholas) from Kadaň in 1410, i.e., exactly 600 years ago.

The astronomical clock of Prague is placed inside an almost 60 m high tower of the Old Town City Hall. The clock has two large dial-plates on the south wall of the tower (see Figure 3). Over the centuries the construction of the clock has been renovated several times, for example, by the clockmaker Jan from Růže (called Master Hanuš) around 1490. A memorial plaque devoted to the creators of the clock is on the left of the lower dial-plate.

The upper dial-plate of the astronomical clock is an astrolabe controlled by a clockwork mechanism. It represents a stereographic

卒于1456年)。安卓亚又名辛蒂尔 (Šindel)，在国王查理四世于1348年所创办的布拉格大学任教。1410年，辛蒂尔当上大学院长，天文钟的设计意念终于通过卡丹市 (Kadaň) 的钟匠密库拉斯 (捷克语Mikulás，即英语Nicholas) 得以实现。

布拉格天文钟设于旧城市政厅一座约六十米高的钟楼内，而两个大钟盘 (图3) 则镶嵌在钟楼南面的外墙上。六百年来，天文钟经历过几次大型翻新，其中一次约在1490年，由克伦洛夫城 (Ruze) 的钟表工匠简恩 (Jan，又名哈劳斯大师Master Hanus) 带领进行。天文钟下钟盘的左方特别设置一面纪念碑，用来表彰这些钟匠们的付出和贡献。

Fig. 4 天文钟的上钟盘
The upper dial-plate of the astronomical clock

Fig 3. 布拉格天文钟的两个钟盘
The dial-plates of the astronomical clock of Prague

projection of the celestial sphere from its North Pole onto the tangent plane passing through the South Pole. The center of the dial-plate thus corresponds to the South Pole of the celestial sphere. The smallest interior circle around the South Pole illustrates the Tropic of Capricorn, whereas the exterior circle illustrates the Tropic of Cancer. The concentric circle between them corresponds to the equator of the celestial sphere (see Fig 4).

An important property (known already to Ptolemy) of the stereographic projection is:

Any circle on the sphere which does not pass through the North Pole is mapped onto a circle as well.

Therefore, the ecliptic on the celestial sphere is projected on a circle, which is represented by the gilded ring with zodiac signs along the ecliptic. However, its center is not the South Pole, but the ring eccentrically rotates around this pole (see Figure 4). The astronomical clock also shows the approximate position of the Sun on the ecliptic, the motion of the Moon and its phases, and the rising, culmination and setting of the Sun, the Moon and zodiac signs.

The gilded solar hand indicates the Central-European time (CET) in the ring of Roman numerals. Note that the difference between CET and the original Prague local time is only 138 seconds. The clock-hand with a small gilded asterisk shows the sidereal time (see Figure 4). Twenty four golden Arabic

天文钟的上钟盘是一个靠发条机制控制而运作的星盘，象征天球 (celestial sphere) 由其北极通过南极落在切平面上的球极平面投影 (stereographic projection)。钟盘的中心点相当于天球的南极，南极四周的最小内圆代表南回归线，而外圆则代表北回归线，两者之间的同心圆相当于天球赤道 (图4)。

球极平面投影有一基本性质 (由古希腊天文学家托勒密Ptolemy提出)：

球体上所有异于北极的圆，经过球极平面投影法，在平面上的投影也是一个圆。

因此，天球黄道的投影也是圆形，用刻有十二星座图案的镀金钟圈表示。虽然天球黄道的中心点并不是南极点，但是镀金钟圈却神奇地绕着南极点转动(如图4所示)。此外，天文钟也指出了太阳在黄道上的大概位置、月球的运动和月相，以及日、月和十二星座各自的出、落和中天时间。

镀金太阳指针在罗马数字钟圈上转动，显示的是中欧时间 (Central European Time，简称CET)，值得留意的是，中欧时间和原来的布拉格当地时间相差只有138秒。旁边那枝镀金星星指针所显示的是恒星时(sidereal time)。最外那个钟圈上有金制的阿拉伯数字1至24，标示从日落起计算的古捷克时间；而下方黑色的阿拉伯数字1至12，是用来标示早在巴比伦时代已经开始使用的行星时间 (planetary hours)。行星时间则由日出开始算起，与古捷克时间的计算方法相反。

钟盘下方的黑色圆形部分代表天文曙暮光 (astronomical night)，即太阳处于地平线下18度的时段；外围的棕色部分象征黎明和黄昏(AVRORA和CREPVSCVLV标志着白昼和夜晚)，而ORTVS和OCCASVS则代表日出和日落。

天文钟的主装置有三个同心大齿轮，每个直径为116厘米，最初由三个各有24齿的小齿轮驱动。第一个大齿轮有365齿，每个恒星日（即23小时56分4秒）推动星座钟圈转一周。第二个大齿轮有366齿，每一平太阳日 (mean sun day) 推动太阳指针转动一圈。由于地球环绕太阳的的公转轨道是椭圆形而非圆形，因此太阳在天球上的运动速度不均一。现时，星座钟圈的位置每年要经人手调校两次。第三个大齿轮有379齿，推动月

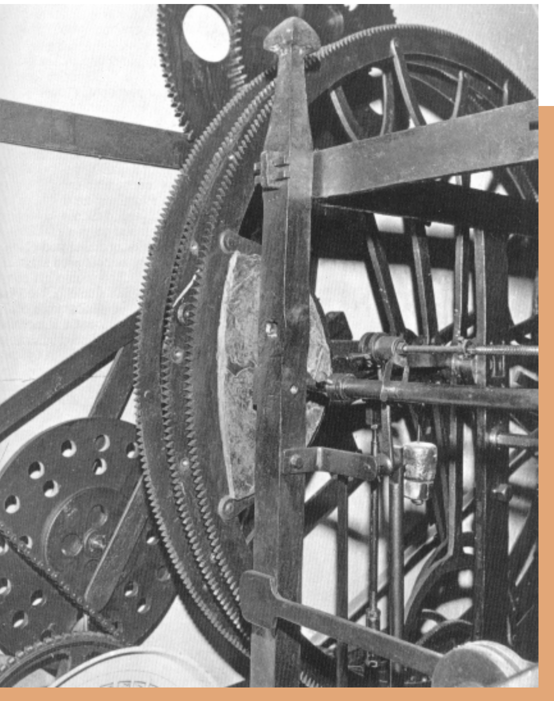


Fig. 5 主钟的详图(后面那三个同心大齿轮十五世纪初开始运作)
A detail of the main clock. The three large concentric gears behind are from the beginning of the 15th century

numerals are used for the ancient Czech time measured from sunset. Twelve black Arabic numerals denote planetary hours of the Babylonian time measured from sunrise.

The black circular area at the bottom of the dial-plate corresponds to the astronomical night, when the Sun is lower than 18° below horizon. The brown area stands for twilight (AVRORA in the morning and CREPVSCVLVM in the evening). Sunrise is denoted by ORTVS and sunset by OCCASVS.

In the main clockwork, there are three large original concentric gears of the same diameter 116 cm (see Figure 5) which were originally driven on one axis by three pinions, each with 24 teeth. The first gear has 365 teeth and turns round the zodiac ring once per sidereal day (23 hr 56 min 4 s). The second gear, which has 366 teeth, drives the solar pointer and turns round once per mean solar day. Since the true orbit of the Earth is elliptic, the Sun does not move uniformly on the celestial sphere. Therefore, the position of the zodiac ring is at present slightly corrected manually twice per year. The third gear, which has 379 teeth, drives the Moon's hand and rotates according to the mean apparent motion of the Moon. The lunar pointer is also at present manually corrected due to the elliptic orbit of the Moon. The lunar pointer (see Figure 4) is a hollow sphere with a hidden mechanism inside that displays the phases of the Moon. It was developed in the 17th century

亮指针根据月球的视运动 (mean apparent motion) 而转动。因为月球轨道同样是椭圆形，所以月亮指针也需要不时以人手校准。月亮指针（图 4）其实是个空心球体，内藏机关，可展示月相。这个指针设计于十七世纪，转动的动力来自椭圆环圈的运动。

下面的钟盘是个月历钟，上面有十二幅由马内斯 (Josef Mánes) 绘画的饼图画，每一年转一周，最上的钟针标示一年中的某一日，同时亦提供取名日 (namedays) 等信息。

二、布拉格天文钟隐藏着怎样的数学原理？

下述例子诠释了十五世纪钟表工匠的精湛技术。天文钟的机械组件里，有一个大齿轮，它的圆周上有24道齿槽，齿槽间的距离随圆周逐渐递增（图6-7）。这个装置使大钟每天重复地按时敲打一至二十四下。与大齿轮连着一个辅助齿轮有六道齿槽，齿轮圆周按照“1，2，3，4，3，2”的比例分成六段。这几个数字合起来构成了一个循环周期，令齿轮不断地重复转动。这六个数字的和是15。

每到整点，扣子便会升起，大小齿轮便会运转。耶稣十二门徒的小木偶会通过钟面两侧的小窗口列队绕行

and draws energy from the movement of the Moon hand.

The lower dial-plate with 12 round pictures by Josef Mánes (see Fig 3) is a calendar. It turns round only once per year. The clock-hand on the top shows the particular day of the year. It also provides information about namedays and other items.

2. What mathematics is hidden behind the astronomical clock of Prague?

The ingenuity and skill of clockmakers of the 15th century can be demonstrated by the following example. The bellworks of the astronomical clock contains a large gear with 24 slots (the first two are connected) at increasing distances along its circumference (see Figs 6 and 7). This arrangement allows for a periodic repetition of 1–24 strokes of the bell each day. There is also a small auxiliary gear whose circumference is divided by 6 slots into segments of arc lengths 1, 2, 3, 4, 3, 2 (see Figs 6 and 7). These numbers constitute a period which repeats after each revolution and their sum is s = 15.

At the beginning of every hour a catch rises, both gears start to revolve, the 12 apostles appear and transit through two windows in sequence, and finally the bell chimes. The gears stop when the catch simultaneously falls back into the slots on both gears. The bell strikes

$$1 + 2 + \cdots + 24 = 300$$

times every day. Since this number is divisible by s = 15, the small gear is always at the same position at the beginning of each day.

The large gear has 120 interior teeth which drop into a pin gear

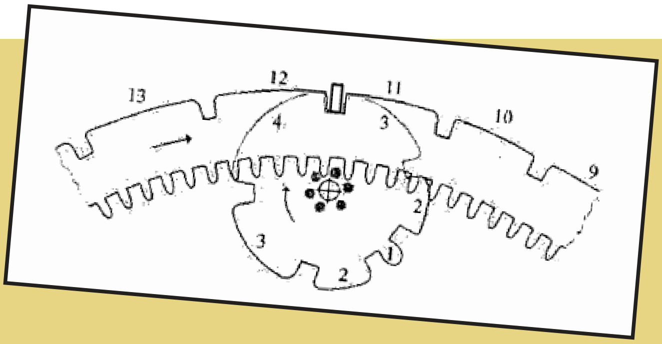


Fig.6 大齿轮外显示的数字表示大钟在整点时敲打的次数——“9，10，11，12，13……”。后面小齿轮的弧长比例为 1，2，3，4，3，2。上面的小长方形代表卡在两个齿轮之间的扣子。小齿轮转动时，通过其齿槽产生一个循环序列，其总和相等于整点时大钟敲打的次数——1，2，3，4，5=3+2，6=1+2+3，7=4+3，8=2+1+2+3，9=4+3+2，10=1+2+3+4，11=3+2+1+2+3，12=4+3+2+1+2，13=3+4+3+2+1，14=2+3+4+3+2，15=1+2+3+4+3+2……。

The number of bell strokes is denoted by the numbers ⋯ , 9, 10, 11, 12, 13, ⋯ along the large gear. The small gear placed behind it is divided by slots into segments of arc lengths 1, 2, 3, 4, 3, 2. The catch is indicated by a small rectangle on the top. When the small gear revolves it generates by means of its slots a periodic sequence whose particular sums correspond to the number of strokes of the bell at each hour:1, 2, 3, 4, 5 = 3 + 2, 6 = 1 + 2 + 3, 7 = 4 + 3, 8 = 2 + 1 + 2 + 3, 9 = 4 + 3 + 2, 10 = 1 + 2 + 3 + 4, 11 = 3 + 2 + 1 + 2 + 3, 12 = 4 + 3 + 2 + 1 + 2, 13 = 3 + 4 + 3 + 2 + 1, 14 = 2 + 3 + 4 + 3 + 2, 15 = 1 + 2 + 3 + 4 + 3 + 2 ⋯

一圈，然后钟声徐徐响起。待扣子回落在齿槽时，两个齿轮就会停止转动。大钟每天敲打的次数是1 + 2 + ⋯ + 24 = 300下。由于300能被15整除，所以小齿轮每天同一时间的位置都是不变的。

Fig. 7 天文钟详图中小齿轮的位置。图中的扣子卡在大齿轮的十八时与十九时之间的齿距上。

The location of the small gear. The catch is in the slot between the segments corresponding to 18 and 19 hours on the large gear. (Photo: Lukas Kalista)

大齿轮有120个内齿，啮合在一个针齿轮之中，针齿轮有六支围住小齿轮轴心的水平小横杆。大齿轮一天转一圈，而小齿轮则以高四倍左右的圆周速度一天转二十圈。这么一来，就算大齿轮出现磨损的情况，小齿轮都可以保持天文钟按刻报时的准确度。与此同时，小齿轮能够有效地使大钟在每天凌晨一时，只敲打一次。从(图7)所见，大齿轮的第一、二个齿槽之间并没有轮齿，即便有，也会因为太小而容易断开，所以，扣子只能够接触到小齿轮弧长为一的轮齿。

从文献 [2] 得知，上述的数列能够不断被建构出来，直至无限大。可是，并不是所有周期数列都拥有如此巧妙的总和特性。例如，我们可以很快便知道 1，2，3，4，5，

with 6 little horizontal bars that surround the center of the small gear (see Figures 6 and 7). The large gear revolves one time per day and therefore, the small gear revolves 20 times per day with approximately 4 times greater circumferential speed. Thus, the small gear makes the regulation of strokes sufficiently precise despite the wearing out of the slots on the large gear. Moreover, one stroke of the bell at one a.m. is due only to the movement of the small gear. In Figure 7 we observe that there is no tooth between the first and second slot of the large gear, since such a tooth would be extremely thin and thus, it could break. Therefore, in this case the catch is in contact only with the tooth of arc length 1 of the small gear, which makes the use of the small gear essential.

In [2] we show that we could continue in this way until infinity. However, not all periodic sequences have such a nice summation property. For instance, we immediately find that the period 1, 2, 3, 4, 5, 4, 3, 2 could not be used for such a purpose, since $6 < 4 + 3$. Also the period 1, 2, 3, 2 could not be used, since $2 + 1 < 4 < 2 + 1 + 2$.

The astronomical clock of Prague is probably the oldest [1, p. 76] still functioning clock that contains such an apparatus illustrated in Figure 6. Due to the beautiful summation property discussed above, Sloane in [3] and [4, A028355, A028356] calls the sequence 1, 2, 3, 4, 3, 2, 1, 2, 3, 4, … the clock sequence.

3. Connections with triangular numbers and periodic sequences

In this section we briefly mention how the triangular numbers

$$T_k = 1 + 2 + \cdots + k, \quad k = 0,\ 1,\ 2,\ \cdots$$

are related to the astronomical clock. We shall look for all periodic sequences that have a similar property as the clock sequence 1, 2, 3, 4, 3, 2, i.e., that could be used in the construction of the small gear. Put $N = \{1, 2, \cdots\}$.

The periodic sequence $\{a_i\}$ is said to be a Šindel sequence if for any positive integer k there exists a positive integer n such that

$$T_k = a_1 + \cdots + a_n, \tag{1}$$

where the triangular number T_k on the left-hand side is equal to the sum $1 + \cdots + k$ of hours on the large gear, whereas the sum on the right-hand side expresses the corresponding rotation of the small gear (see Figure 8). In [2] we show that the above condition can be replaced by a much weaker condition based on only a finite number of k's: namely, the sequence $a_1, a_2, \cdots, a_p, a_1, a_2, \cdots$ with period length p is a Šindel sequence if there exists a positive integer n such that equation (1) holds for $k = 1, 2, \cdots, a_1 + a_2 + \cdots + a_p - 1$. This enables us to perform only a finite number of arithmetic operations to check whether a given period $a_1, \cdots, a_p$ yields a Šindel sequence. In [2] we also give an explicit algorithm for finding Šindel sequences.

4，3，2 不可用，因为 6 < 4 + 3；而 1，2，3，2 也不可用，因为 2 + 1 < 4 < 2 + 1 + 2。

布拉格天文钟很可能是世上现存少数装有（图 6）零件的大钟当中最古老的一个（文献 [1]，76 页）。正因上述完美的总和特性，美国数学家斯洛恩（Sloane，参考书目 [3] 及 [4，A028355，A028356] 的作者）把 1，2，3，4，3，2，1，2，3，4……称为时钟数列（clock sequence）。

$$1\ 2\ 3\ 4\quad \underbrace{3\ 2}_{5}\quad \underbrace{1\ 2\ 3}_{6}\quad \underbrace{4\ 3}_{7}$$

$$\underbrace{2\ 1\ 2\ 3}_{8}\quad \underbrace{4\ 3\ 2}_{9}\quad \underbrace{1\ 2\ 3\ 4}_{10}\quad \underbrace{3\ 2\ 1\ 2\ 3}_{11}\quad \underbrace{4\ 3\ 2\ 1\ 2}_{12}$$

$$\underbrace{3\ 4\ 3\ 2\ 1}_{13}\quad \underbrace{2\ 3\ 4\ 3\ 2}_{14}\quad \underbrace{1\ 2\ 3\ 4\ 3\ 2}_{15}\quad \cdots$$

Fig. 8：每行上面的数代表了小齿轮的小节的长度；而下面的数表示第 k 个小时大钟敲打的次数。

The upper numbers denote lengths of segments on the small gear, whereas the lower numbers indicate the number of strokes at the k-th hour.

三、三角形数与周期数列的关系

本节简洁地论述三角形数

$$T_k = 1+2+\cdots+k, \quad k = 0,\ 1,\ 2,\ \cdots$$

与天文钟的关系，并找出所有跟时钟数列1，2，3，4，3，2拥有相同特性的周期数列，亦即可应用在小齿轮构造的周期数列。设 $N = \{1, 2, \cdots\}$。

若对任意正整数 k，存在一个正整数 n 使得

$$T_k = a_1 + \cdots + a_n \qquad (1)$$

成立，那么该周期数列 $\{a_i\}$ 会被称为辛蒂尔（Šindel）数列，其中等号左边的三角形数 T_k 等于大齿轮所有时刻的总和 $1+\cdots+k$，而右边数字的总和则表示小齿轮相应的转动圈数（图 8）。我们在参考资料 [2] 证明了，上述条件可被一个弱得多的条件所取代，只需要有限个 k，那就是，序列 $a_1, a_2, \cdots, a_p, a_1, a_2, \cdots$ 的周期长为 p，若存在正整数 n，使等式（1）对 $k = 1, 2, \cdots, a_1 + a_2 + \cdots + a_p - 1$ 成立，那么该数列就是辛蒂尔数列。这样便可在有限的运算次数中，检查某一周期 $a_1, \cdots, a_p$ 能否得出辛蒂尔数列。文献 [2] 也提供了查找辛蒂尔数列的显式算法。

四、其它具有数学及科学意义的名胜

离天文钟几米远的地方，竖立着一个爱因斯坦纪念牌，纪念他在1911年至1912年间，在旧城广场十七号暂住的岁月（见图9）。纪念牌旁边的哥德式教堂泰恩（Týn），安放了建于1601年的第谷·布拉赫的墓冢，供游人参观。沿旧城广场向前走，一直到契里特纳大街

4. Further mathematical and scientific sights

Within a few meters from the horologe there is a memorial plaque devoted to Albert Einstein (see Fig 9) who often visited the house at Old Town Square no. 17 during 1911–1912. In the nearby gothic church called Týn we can find the tomb of Tycho Brahe from 1601. In Celetná street no. 25, which leads from the Old Town Square, there is a memorial plaque to Bernard Bolzano (see Fig 10). We also recommend visiting other plaques and busts of Albert Einstein (Viničná no. 7 and Lesnická no. 7), of Christian Doppler (Charles Square no. 20 and U Obecního dvora no. 7 – see Fig 11), of Johannes Kepler (Karlova street no. 4 and Ovocný trh no. 12/573), a large statue of Kepler and Brahe in Parléřova street no. 2 (see Fig 12), etc.

Prague is very popular among tourists and is celebrated as

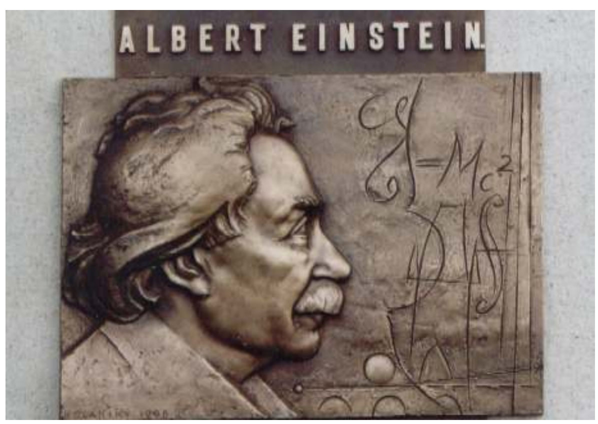


Fig .9 爱因斯坦纪念牌

Memorial plaque of Albert Einstein

(Celetná Street)25号，就会看见波尔查诺纪念碑(图10)。旧城广场附近还有其它科学家的纪念碑及半身塑像，同样也值得参观。这些人物包括爱因斯坦（Vinicná 7号、Lesnická 7号)、多普勒(查理广场20号、Obecniho dvora 7号；图11)、开普勒(查理大街 4号、Ovocny trh 12/573号)，以及位于Parlerova街2号的开普勒和布拉赫的大型雕像(图12)等。

作为旅游热点，布拉格拥有不同历史风格的建筑物，罗马式、哥德式、文艺复兴、巴洛克等建筑在市内比比皆是，因此被誉为最美、最浪漫的中欧城市之一。宏伟的布拉格城堡、艺术家和巴洛克雕塑处处可见的查理大桥(Charles Bridge)，还有泥巴妖怪勾勒姆(Golem) 传说的发源地——犹太区 (Jewish Town)。相传勾勒姆是由德高望重的犹太教师罗乌 (Rabbi Loew) 在十六世纪末左右制造，用来帮助当时居住在布拉格的犹太人对抗迫害。此外，布拉格也是欧洲的文化重镇，拥有浓厚的音乐传统，历史上曾有多部著名作品在此公演。1787年10月29日，享负盛名的莫扎特歌剧《唐璜》在查理大学附近的艾斯特歌剧院 (Estate Theatre) 首度公演。总括来说，不管你对数学是否感兴趣，布拉格都会给你带来无穷乐趣。

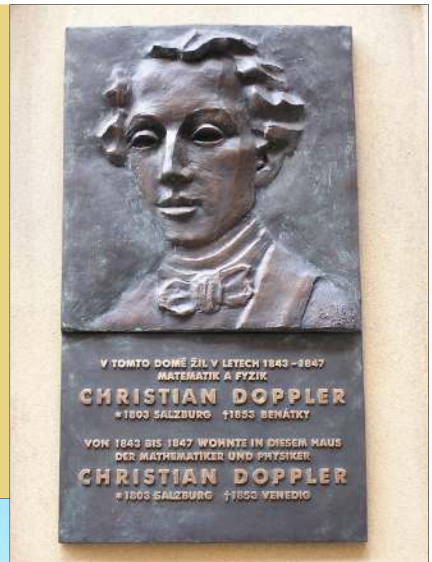


Fig. 11 多普勒纪念碑
Christian Doppler

Fig. 12 开普勒与布拉赫的大型雕塑
Johannes Kepler and Tycho Brahe

Fig. 10 波尔查诺纪念碑
Bernard Bolzano

one of the most beautiful and romantic cities in central Europe due to its varied architectural styles from many periods (Romanesque, Gothic, Renaissance, Baroque, …), the impressive Prague Castle, Charles Bridge with its many artists and Baroque statues, and the Jewish Town with its legend of the Golem, which was said to be created in the late 16th Century or early 17th Century by Rabbi Loew, the Maharal of Prague, to protect the Jews. Prague also has a rich musical tradition. For example, Mozart's opera Don Giovanni had its world premiere on October 29, 1787 at the Estates Theatre, which is adjacent to Charles University, where Jan Šindel taught about mathematics and astronomy. In addition, as demonstrated above, Prague also has much to offer to mathematical tourists.

鸣谢

本论文由捷克科学院的院校研究计划（编号 AV0Z 10190503）及研究基金（编号 IAA 100190803）资助。感谢 Jakub Šolc 先生提供图像技术支持。

This paper was supported by Institutional Research Plan nr. AV0Z 10190503 and Grant nr. IAA 100190803 of the Academy of Sciences of the Czech Republic. The authors wish to thank Jakub Šolc for his technical help with the figures.

References

[1] Z. Horský: The astronomical clock of Prague, Panorama, Prague, 1988.

[2] M. Křížek, A. Šolcová, L. Somer: Construction of Šindel sequences, Comment. Math. Univ. Carolin. 48 (2007), 373–388.

[3] N. J. A. Sloane: My favorite integer sequences, arXiv:math.C0/0207175v1, 2002, 1–28.

[4] N. J. A. Sloane: The on-line encyclopedia of integer sequences, 2007, published electronically at http://www.research.att.com/~njas/sequences/

作者简介

Michal Krizek，捷克科学院数学研究所高级研究员，布拉格查理大学数学及物理学院教授。曾经多次访问中国，包括北京、天津、香港、湘潭等地。研究兴趣广泛，包括纯数学、计算数学和数学史。

Michal Křížek is a Senior Researcher at the Mathematical Institute of the Academy of Sciences of the Czech Republic and Professor at the Faculty of Mathematics and Physics of Charles University in Prague.

Alena Solcova，捷克理工大学信息技术学院计算机科学系助理教授，十七年前开始定期举办数学历史研讨会。

Alena Šolcová is an Associate Professor at the Department of Computer Science of the Faculty of Information Technology of the Czech Technical University in Prague. For more than 17 years she has held a regular seminar on the history of mathematics.

Lawrence Somer，华盛顿美国天主教大学数学教授，曾发表以数论为题材的论文。

Lawrence Somer is a Professor of mathematics at the Catholic University of America in Washington, D.C. He has published a number of papers on number theory.

谈数学职业

张恭庆

一、前言

上个世纪50年代，数学通报 [1] 刊登了苏联数学家柯尔莫哥洛夫的“论数学职业”的译文。我上大学时，这是我们“专业教育”的材料。对于我们这代学数学的人产生了很大的影响。然而半个多世纪过去了，数学的面貌发生了很大的变化，数学的职业也多样化了。2009年的《华尔街日报》上，发表了一篇文章 [2]，其中附有一张由CareerCast.com制作的，以工作环境、收入、就业前景、体力要求、体力强度为指标的职业排行榜。在这排行榜中，数学家荣登榜首，保险精算师和统计学家分列第二和第三，后面是生物学家、软件工程师、计算机系统分析员等等。从这5个指标来看，数学家的收入不算很高，但综合起来还排在第一，可见在其它方面占有优势。

The Best and Worst Jobs

Of 200 Jobs studied, these came

The Best

1. Mathematician
2. Actuary
3. Statistician
4. Biologist
5. Software Engineer
6. Computer Systems Analyst
7. Historian

2009年《华尔街日报》列出的职业排名表的部分内容

二、数学和它的基本特征

什么是数学？

从中学起，我们就知道数学是研究“空间形式”和“数量关系”的学科。数量关系，简称为“数”，空间形式简称为“形”；“数”的对象比如说自然数、复数、向量、矩阵、函数、概率等，“形”的对象比如说曲线、图、空间、流形等。

数学实际上是一门形式科学，它研究的是抽象元素之间的“关系”和“运算法则”。这些“相互关系”和“运算法则”构成了数学“结构”。判断数学结论的真伪，主要看其逻辑演绎是否正确，被实践检验的只是构成这些“相互关系”与“运算法则”的“结构”是否与实际相符。

2009年的华尔街日报上，发表了以工作环境、收入、就业前景、体力要求、体力强度为指标的职业排行榜。在这排行榜中，数学家荣登榜首，保险精算师和统计学家分列第二和第三。

我们举一个例子来说明。大家都知道平面几何中的“平行公设”：在平面上过直线外一点，有且仅有一条直线平行于该直线。这是公设，是假定，可以由此推出平面几何的很多定理。但为什么在平面上过直线外一点有且只有一条直线平行于该直线呢？可不可以没有？可不可以不止一条？就几何学来说，假定只有一条，可以推出一大堆几何命题，例如：三角形三内角之和为180°，这是欧氏几何；假定有不止一条也可以推出另外一大堆命题，例如：三角形三内角之和小于180°，这是双曲几何；假定一条也没有照样还可以推出一大堆命题，这是椭圆几何。双曲几何与椭圆几何都是非欧几何。那么到底哪一种几何的结论是正确的？这要看你把这些几何结论应用在什么范围内，应用到什么问题上去。在以地球为尺度的空间范围内，欧氏几何是适用的，实际上它与非欧几何中

的双曲几何的差异不大。当把宇宙作为一个整体来描述时，就要用双曲几何了。这有点像牛顿力学与相对论力学的关系。由此可见，决不能认为凡是数学上证明了的定理就是真理。只能认为这些结论是在它的"结构"中在逻辑上被正确地证明了。至于其是否与实际相符，还要检查它的前提。从这个意义上说，数学只是一个形式体系。

如果把数学的研究对象只用"数"和"形"来概括，那么有些东西还无法概括进去，比如数学语言学。各种计算机的语言都是根据数学原理制做出来的，可语言是"形"还是"数"呢？看来都不是。又比如在"选举"办法上，一个非常有名的结论——阿罗不可能性定理[3]。阿罗(K. Arrow)是个经济学家，诺贝尔奖获得者，学数学出身。他证明了一条定理：对于不少于3个候选人的选举按"排序"投票，不存在任何同时遵循以下四个原则的群体决策：

肯尼斯•阿罗(Kenneth Arrow)
1972年诺贝尔经济学奖得主

1. 无限制原则。(任何人可对所有候选人任意排序)。
2. 一致性原则。(如果每个人的态度都是"A 优于 B"，那么群体决策结果也应"A 优于 B")。
3. 独立性原则。(添加或减少候选人，"排序"不变)。
4. 非独裁原则。(不能一个人说了算)

这也是一条经济学上的定理：没有同时遵从以上四条原则的"社会福利函数"。这是数学在其他领域——政治学、经济学——的一个重要的应用。在这条定理中，哪里有"数"？哪里有"形"？可见"数"和"形"已经不能完全概括数学的研究对象了。现代人们不再限定研究对象是不是"数"和"形"，只要能对其建立数学模型，就能通过模拟计算来研究其中的规律，例如对于社会心理、动物行为等方面的数学分析。所以，数学研究的范围扩大了，现在人们说数学的对象是："模式"(pattern)、"秩序"(order)、"结构"(structure)。

纯数学与应用数学

数学又划分为纯数学和应用数学，纯数学在我国又称基础数学。研究数学自身提出的问题，划归纯数学；研究数学之外（特别是现实世界中）提出来的问题划归应用数学。应该说，这种划分只是大致的，并没有严格的界限。一方面，纯数学中的许多对象，追根溯源还是来自解决其它方面的问题，如天文学、力学、物理学等。比如几何来源于测量：天文测量、大地测量。就在数学已经高度发展了的今天，从外部提出来的数学问题照样可以转化为非常有意义的纯数学的问题，刺激出深刻的数学理论。比如说，Navier-Stokes方程是流体力学中的重要的方程，NP 问题是从计算理论中提出来的问题，到现在都还没有被解决，成为"千年七大难题"中的两个。另一方面，纯数学的理论在适当条件下也能在其它科学中放出异彩：群论和几何对物理的贡献是众所周知的。大家都认为数论是很"纯"的数学，但数论在现代密码学中起重要作用，此外如傅里叶 (Fourier) 分析与通讯，随机过程与金融，几何分析与图像处理等等都是这方面的例子。特别是，许多在应用数学中行之有效的方法都有深刻的纯数学背景，如快速傅里叶变换，有限元方法等。

纯数学大致有：数理逻辑、数论、代数、拓扑、几何、分析、组合与图论等分支，它们之间的融合与渗透又产生出许许多多的交叉分支，如代数几何、代数数论、微分几何、代数拓扑、表示理论、动力系统、泛函分析等，以及更多的子分支。

微分方程与概率论是介于纯数学与应用数学之间的分支，它们的理论部分属于纯数学，其余部分则是应用数学。计算数学与数理统计是应用数学最重要的两个分支。

纯数学对于问题的解答往往只停留在研究解的存在性以及个数上，未必讨论解的具体算法（如代数方程求根）。但实际问题的解答一般总要求具体的数据，单有纯数学的结论不能满足要求，因此还要研究

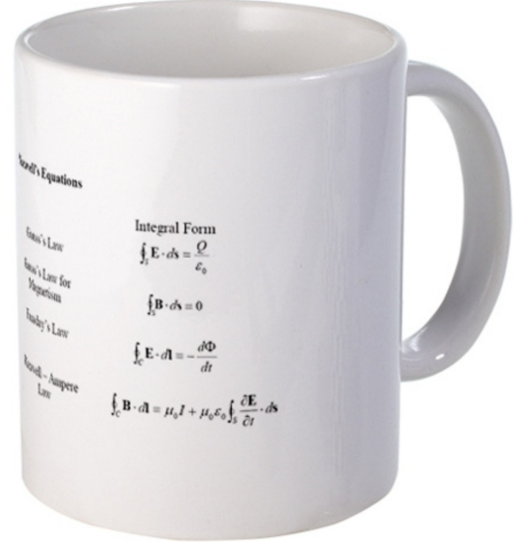
正如 Borel 说的："纯数学和应用数学就像是一座冰山 —— 水面上的是应用数学，因为它有用，大家都看得见；水底下的是纯数学。"没有水底下纯数学的深厚积累，上面的应用数学是建立不起来的。

算法，以及如何对待巨大的计算量、存储量、复杂性、精确性、速度、稳定性等等问题。这些就是计算数学要解决的问题。

以概率论为基础的统计学称为数理统计。日常生活、社会调查、科学实验都积累了大量的数据，如何从这些数据中科学地得到有用的信息？数理统计研究如何通过有效的收集、整理和分析带有随机性的数据，对所考察的问题做出推断、预测乃至决策的方法。

当代的数学已被应用到很多领域。自然科学：物理、化学、生物、天文、地质、气象等，人文科学：经济、金融、精算、语言、考古等。很多管理科学问题也要用到数学。

这么多有用处的数学，表面上看都属于应用数学。然而，正如 Borel 说的：“纯数学和应用数学就像是一座冰山—水面上的是应用数学，因为它有用，大家都看得见；水底下的是纯数学。”[4] 没有水底下纯数学的深厚积累，上面的应用数学是建立不起来的。



印在茶杯上的麦克斯韦尔方程组

数学的基本特征

因为数学研究的是抽象的对象，所以应用范围必然广泛；又因为它的研究手段不是实验，而是逻辑推理。这就决定了它必须是严密的和精确的。因此数学明显地有如下基本特征：

(1) 高度的抽象性与严密的逻辑性

(2) 应用的广泛性与描述的精确性

数学应用的广泛性不仅表现在：它是各门科学和技术的语言和工具，数学的概念、公式和理论早已渗透到其它学科的教科书和研究文献中去了；而且还表现在：许许多多数学方法都已被写成软件，有的还被制成芯片装置在几亿台电脑以及各种电器设备之中，成为产品高科技含量的核心，还有些数学软件则是作为商品在出售。

在这些应用中，我想特别指出：数学是探求知识的重要手段。举一个例子，历史上许多重要的发现，没有数学光靠实验是不够的。现在大家人人用手机，不论多远几秒钟就能通上话，为什么信息能传输得这么快？靠的是电磁波。电磁波是怎样发现的？

英国理论物理学家、数学家麦克斯韦尔 (Maxwell) 运用电流的法拉第定律、安培定律、电荷的高斯定律和磁场的高斯定律，推出一组偏微分方程。在推写过程中，他注意到原来的安培定律和时间无关，而且与其他几个定律不相容。为了解决这个问题，麦克斯韦尔提出加上一“位移电流”到原先的安培定律中去，写出了今天通用的麦克斯韦尔方程组，这个修正后的方程组导出波动方程，由此预见了电磁波。麦克斯韦尔以液体流动，热传导及弹性力学作为模型，认为“以太”是传导电磁波的媒介 [5]，尽管这种解释在物理上是不对的，也讲不清楚，但它的数学形式——麦克斯韦尔方程组却是正确的，它奠定了电磁学的基础。后来赫兹 (Hertz) 在实验上证实了电磁波的存在。

同样地，在量子力学电脑、相对论的理论建立过程中，数学也起了极为重要的作用。

在当今时代，科学计算更是在一定程度上取代实验。一旦研究对象的机理已经清楚，准确的数学模型已经建立，就可以用模拟计算替代部分试验，如核试验等。

数学的基本特征除以上两条外，还有

(3) 数学研究对象的多样性和内部的统一性

随着数学研究对象的扩充，数学分支不断增加，方向繁多，内容丰富。同时数学分支之间的内在联系也不断被发现，数学内部的千丝万缕的联系被愈理愈清。希尔伯特－诺特－布尔巴基 (Hilbert-Noether-Bourbaki) 利用数学分支间的这些被清理过的联系和公理化方法，从规定的几条“公理”及其相关的一套演算规则中提炼出数学“结构”，如代数结构、拓扑结构、序结构等。数学的不同分支是由这些不同的“结构”组成的，而这些结构之间的错综复杂、盘根错节的联系又把

所有的分支联成一个整体。在这方面反映了数学的统一性。

对统一性追求的意义在于：对于同一个对象可以从不同角度去认识，不同分支的问题可以相互转化，理论和方法可以相互渗透，从而发展出许多新的强有力的工具，解决许多单个分支方法难于解决的重大问题。

回顾以下历史是颇有裨益的。历史上有三大几何难题：倍立方问题，化圆为方问题，三等分角问题，都是“圆规直尺”的作图题。两千多年了，光用几何方法研究，不知有多少人费了多少心血，可就是解决不了！在那些时代，代数学主要研究解方程。后来笛卡尔用解析几何统一了几何与代数。18 世纪末到 19 世纪初，多项式方程可解性的研究继高斯 (Gauss) 代数基本定理证明之后应运而生。高斯研究正多边形的圆规直尺作图就换了一个角度，把它看成一个多项式方程的可解性问题，从几何问题转化到了代数问题。后来阿贝尔 (Abel)、伽罗华 (Galois) 在代数上把方程的可解性研究推向了高峰。

许多困难的问题都需要很多学科的知识综合起来才能解决。例如，庞加莱猜想的提法本来纯粹是拓扑学的，后来转化为几何问题，最后是综合使用偏微分方程、拓扑、几何的思想、理论和方法才把这一个复杂问题解决了的。

什么样的“数”能被圆规直尺作出来？对于事先给定了的一组实数 Q，能从它们“尺规作图”出来的数 x，就是从它们出发，作加减乘除以及开平方所能得到的数。也就是说：尺规作图问题可解等价于存在正整数 m，使得 x 属于 F_m，其中

$$F_{i+1}=\left\{a_i+b_i\sqrt{c_i}\,\middle|\,a_i,\ b_i,\ c_i^2\in F_i\right\},\quad F_1=Q。$$

三等分角问题是：对任意给定的角 θ，作出一个大小为其三分之一的角 $\theta/3$。令 $\alpha=\cos\theta$，要作出数 $x=\cos(\theta/3)$。x 是多项式

$$4x^3-3x-\alpha=0$$

的根。只要证明对于任意的正整数 m，它的根 x 都是不属于 F_m 的，就证明了三等分一个任意角只用圆规与直尺是不可能的！

1837 年法国数学家 Wantzel 证明了以上方程连同倍立方问题对应的方程在 $\{F_m\mid m=1,2,\cdots\}$ 都是不可解的。后来，1882 年林德曼（von Lindemann，希尔伯特的导师）证明了 π 的超越性从而确立了尺规作图化圆为方也是不可能的。两千年前的三大几何难题就是这样用代数和数论的方法以否定的形式解决了！

现在数学已经发展成为一个庞大的、内部和谐与统一的、充满活力的有机的整体，它是人类文化宝库中一座既宏伟又精致的创造物。

三、当代社会对数学家的要求

当今世界，数学已被应用到几乎一切领域。然而现实情况一方面是，许许多多新的领域要求人们用数学的眼光，数学的理论和方法去探讨；另一方面，科学的发展使人们的分工愈来愈细。18 世纪以前的数学家中有不少人同时也是天文学家、力学家、物理学家；在 19 世纪，许多数学家还可以在数学的几个不同分支上工作；但自庞加莱 (Poincare) 和希尔伯特 (Hilbert) 之后，已经没有一个人能够像他们当年那样通晓数学全貌了。大多数的数学家只能在狭窄的领域内从事研究。这种过于专门化的趋势对于数学学科的发展是十分有害的！ 这确实是个矛盾的现象。如果我们不能对当今数学的发展与趋势有一个大致的了解，我们就不知道如何应对，也不知道应该怎样培养学生。

当代数学发展的趋势

当代数学发展的趋势大致有如下几个特点：

1、数学内部的联系进一步加强 在指数增涨的研究文献中，尽管数学的各个分支的前沿都在不断推进，数学在深度与广度两方面都得到快速发展，然而不同分支之间的融合与相互渗透则是一个重要的特征。这表现为：原来长期处于纯数学边缘的分支，比如偏微分方程和概率论，现在已经进入了纯数学的核心。相隔很远的分支间的内在联系不断发现，如 de Rham-Hodge 定理、阿蒂亚－辛格 (Atiyah-Singer) 指标定理等。许多困难的问题都需要很多学科的知识综合起来才能解决，例如，庞加莱猜想的提法本来纯粹是拓扑学的，后来转化为几何问题，光从几何也解决不了，最后是综合使用偏微分方程、拓扑、几何的思想、理论和方法才把这一个复杂问题解决了的。

2、数学与其它科学的交叉形成了许多交叉学科群 比如，科学计算就是数学与物理、化学、材料、生物、力学等很多学科的交叉。数学与控制论、运筹学交叉形成了系统科学。数学与物理交叉，形成数学物理。此外还有计算机科学、信息科学、数量经济学、金融数学、生物数学、数学化学、数学地质学、数学心理学、数学语言学等等很多的交叉学科。

3、数学应用的领域空前扩张，成为开发高新技术的主要工具 信息安全、信息传输、图像处理、语音识别、医疗诊断、网络、海量数据处理、网页搜索、商业广告、反恐侦破、遥测遥感，包括当代制造业、成衣业等等都大量应用数学。

数学家的职业

长期以来人们心目中的数学职业只是限于学术界和教育界：大学、中学教师和科研机构的研究人员。这种现象如今逐渐有所改变，有些公司也开始雇用学数学的人了。在一些发达国家，过去工业界（计算机）和商业界（比如统计、保险）雇用一些数学硕士、学士从事计算、统计、程序编制和数据处理工作。随着工业中有趣的应用数学问题愈来愈多，近年来吸引了一定比例的数学博士和优秀的数学家，像弗里德曼（M. Freedman，1986 年菲尔兹奖获得者），现就职于微软公司。许多发达国家现在都有专门的机构支持工业应用数学的发展，这标志着数学在这些国家的应用已相当广泛。我查了美国最近几期的《美国数学会通讯》(Notices of the American Mathematical Society)， 从 2003 年到 2008 年，美国大概每年有 800 多名数学博士毕业后在美国求职。这 800 多个人中大约有 200 人，约占四分之一，到工商业界去；其他的人都就职于各种类型的学校，有研究型的，也有教学型的。不过，从读数学研究生到拿到数学博士学位其人数比大约是四比一，除去其中有些人转到别的学科攻读博士学位外，其余大多数或是直接，或是再读一个其它学位，如统计、精算等之后，都到工商业界和政府部门去工作了，这个数字可是惊人的。

然而在有些数学家中流行一种看法，认为应用数学是搞不了纯数学的人才去搞的。这是极为错误的。20 世纪不仅有许多极有才华的应用数学家开创了许多应用数学分支，而且还有些在纯数学领域中有卓越成就的数学家后来都又在应用数学领域做出了极富开创性的贡献。

学术界和工商界对数学的要求很不一样。在学术界，要求发表论文，证明定理，推进数学的进展；工商界的要求则是解决问题，尽快给出结果。

对学术界来说，研究结果深刻、精确、有新思想的是好工作；工商界则要求有针对性和可用性，如果得到的公式虽然很广泛、很精确，但计算起来太费时费钱，就不一定会被采用。对于学术界的人，做研究可以自由选题，不受限制；但是在工商界，数学家的工作是被指定的，开发的项目也是被指定的。大家在选择自己的出路时要注意这些差别。

对数学家的要求

主修数学的人在学习过程中提高了抽象能力和逻辑推理能力，思考问题比较严密，学习那些属于符号分析方面的新知识比较容易入门，这是学数学的人的优势。他们当然也有劣势，比如不擅长做实验等。

(1) 到工商界工作的数学家主要从事符号分析、数据处理、建模、编程等方面的工作。然而数学的宝库是非常丰富的，如何采用更有效的理论和方法来解决问题，则要求更多地懂得该工作领域以及数学两方面的知识。要想工作有成绩，就不能只掌握几套现成的方法，而是要拓宽数学的知识面。

(2) 在交叉学科从事应用数学研究的数学家，更要深入到这个新领域中去，了解研究问题的来龙去脉。这些数学家并不以证明定理为成果的主要表现方式，而是创建好的模型。创建好的模型正如证明深刻定理一样有意义，它是利用数学工具寻找客观规律的重要手段。实际问题很复杂，如何抓主要因素，使之既能反映出主要现象，又能在数学上有办法处理。这种抽象、简化以及解决问题的方法是一种数学艺术。

然而在有些数学家中流行一种看法，认为应用数学是搞不了纯数学的人才去搞的。这是极为错误的，也是有害的观点！20 世纪不仅有许多极有才华的应用数学家开创了许多应用数学分支，把数学的疆界空前地扩大了，如图灵（Turing）、山龙（Shannon）；而且还有些在纯数学领域中有卓越成就的数学家后来都又在应用数学领域做出了极富开创性的贡献，如冯·诺依曼（von Neumann）、维纳（Wiener）、托姆（Thom，拓扑学家，1958 年费尔兹奖得主）、斯梅尔（Smale，1966 年费尔兹奖得主），以及 2007 年获得邵逸夫奖的芒福德（Mumford，1974 年费尔兹奖得主）和吴文俊等。

(3) 纯数学的研究是非功利的。这个意义上有点像文学和艺术，也没有统一的评价标准。研究的成果贵在创新。然而这种创新并不是数学家们没有目标的随心所欲的创造。正如柯朗（R. Courant）说过，“只有在以达到有机整体为目标的前提，只有在内在需要的引导下，自由的思维才能做出有科学价值的成果”。[6] 整个数学是一个有机整体，学科之间是相互牵连在一起，互相补充，互相促进的。一项工作如果很孤立，和主流上的问题都没有联系，也没有多少新的思想，那么就很难说意义有多大了。

数学分支间的融合与渗透是当代数学发展趋势的一个特征，要想在有意义的问题上做出贡献，知识面一定不能太窄。然而当代大多数数学家工作面过于专门化却是一种普遍现象。这有其内在的原因：数学的体系太庞大，内容又极为丰富，要想在前人工作的基础上有所拓广就很难有精力去了

解其它分支；同时也有其外在原因，数量剧增的研究人员产生了大量的研究论文，发表的论文多就逼迫研究人员多读，而且“发表论文的压力”又逼迫他们多写，如此互为因果，也就无暇他顾了。这是当今国际学术界普遍存在的严重问题。然而研究贵在创新！真正的“原创”思想往往来自那些能“精通”看来相距遥远的几个领域，而且能“洞察”到把一个领域的结果用于解决另一个领域问题的途径。那是建立在全面了解、长期思考、过人功力基础之上的。

(4) 有人说，我不想做研究，只想当老师教书。不错，本来教书就是学数学的一个重要出路。作为大学，甚至中学的数学老师，对他们所教的学科也不能只掌握教科书上所写的那一点内容，如果那样的话，或者会把书教得枯燥无味，或者不得要领。反之，如果教师的知识渊博，再肯学习新东西教给学生，学生对学习一定会产生很大的兴趣。事实上，只有那些热爱数学，并能把数学看成活生生的、不断发展着的人才能激励起学生的好奇心和求知欲。很多数学家回忆自己走过的道路时，怀念当年的数学老师，正是这些老师把他们引进了数学的殿堂。我们现在正处于数学理论和应用空前大发展的时代，怎么改革数学教育？怎样的师资才能适应大发展的需求？这些都是需要我们认真思考的问题。

四、数学教育的重要性

作为一种“思想的体操”，数学一直是中、小学义务教育的重要组成部分。现在大学理、工、文、法、农、医等科都有数学课，说明了人们认识到数学的重要性。不过，在许多学校，这些数学课的收效并不理想。原因可能是多种多样的，要具体分析。比如某系课程表上规定要上数学课，任课老师未必知道为什么这个系的学生需要开这门课。是作为“语言”的需要？专业课的需要？看书看文献的需要？还是做研究的需要？这是不同层次的要求。不按需要教，就是无的放矢，学生自然没有兴趣，效果也不会好。所以我建议教非数学专业学生的教师首先要了解一下这个专业的需求。

改善数学教育

几千年数学发展的丰富积累是人类的知识宝库。在知识社会，这个知识宝库是一种重要的资源。怎样能让这些资源共享，就要靠老师们传承给各行各业的人。

如何改善我国现行的数学教育，我认为要综合考虑以下几方面：

(1) **知识**。既重视基础，也照顾前沿，特别要考虑受教育对象的需要和基础。

(2) **能力**。“数学是一种普遍适用的，并赋予人以能力的技术”。在教学过程中，不能只灌输知识，更重要的是培养能力，包括计算能力（包括使用计算机进行计算的能力）、几何直观能力、逻辑推理能力、抽象能力、把实际问题转化为数学问题的能力。而具体通过哪些内容培养哪些能力，或者培养哪几方面的能力，教师要做到心里有数。

如果教师的知识渊博，再肯学习新东西教给学生，学生对学习一定会产生很大的兴趣。事实上，只有那些热爱数学，并能把数学看成活生生的、不断发展着的人才能激励起学生的好奇心和求知欲。

(3) **修养**。数学是一种文化。数学不是一门自然科学，它有文化的层面。受过良好数学教育的人看问题的角度和一般的人不完全一样，数学能开阔人的视野，增添人的智慧。一个人是否受过这种文化熏陶，在观察世界、思考问题时会有很大差别。会不会欣赏数学，怎样欣赏数学，与数学修养有关，就如同欣赏音乐一样，不是人人都能欣赏贝多芬的交响乐的。

然而数学修养不但对数学工作者很重要，对于一般科学工作者也重要。具备数学修养的经营者、决策者在面临市场有多种可能的结果，技术路线有多种不同选择的时候，会借助数学的思想和方法，甚至通过计算来做判断，以避免或减少失误。詹姆斯·西蒙斯（James Simons）就是一个最好的例证。在进入华尔街之前，西蒙斯是个优秀的数学家。他和巴菲特的“价值投资”不同，西蒙斯依靠数学模型和电脑管理自己旗下的巨额基金，用数学模型捕捉市场机会，由电脑做出交易决策。他称自己为“模型先生”，认为建立好的模型可以有效地降低风险。在西蒙斯的公司里雇用了大量的数学、统计和自然科学的博士。

发达国家在大型公共设施建设，管道、网线铺设以及航班时刻表的编排等方面早已普遍应用运筹学的理论和方法，既省钱、省力又提高效率。可惜，运筹学的应用在我国还不普遍。

其实我们不能要求决策者本人一定要懂很多数学，但至少他们要经常想想工作中有没有数学问题需要咨询数学家。

数学修养对于国民素质的影响，正如美国国家研究委员会发表的“人人关心数学教育的未来”一书中所说：“除了经济以外，对数学无知的社会和政治后果给每个民主政治的生存提出了惊恐的信号。因为数学掌握着我们的基于信息的社会的领导能力的关键。”[8]

对于教学改革的几点意见

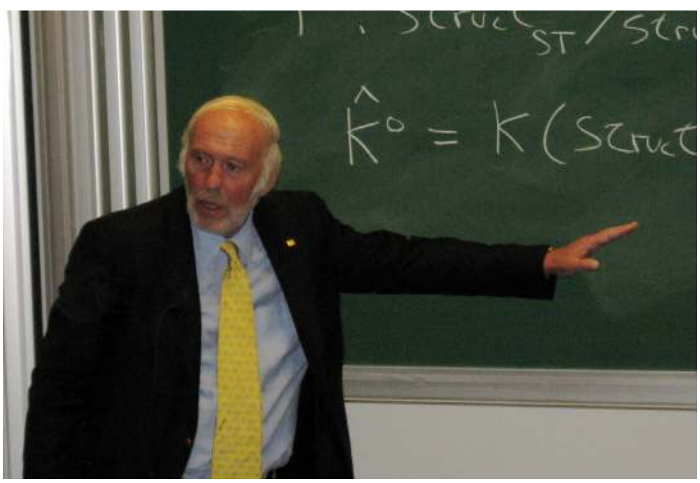
“十年树木，百年树人”说明教育的成果需要经过相当长的时间才能收获。因此教学改革的效果也不可能立竿见影。这就决定了教学改革只能“渐进”不能“革命”。20 世纪中期美国的“新数学运动”以及 1958-1960 年中国的“教育大革命”的历史教训必须记取！

要“改革”就可能有成功也可能有失败，而且成败未必就那么容易察觉，有时很可能所得之处就含有所失，所以做改革实验之前必须考虑到可能出现的问题与补救方法。

我们应当鼓励实验的多样化。事实上每个教师都可以通过自己的教学实践对具体教学内容进行改革，这是应当受到鼓励的。所以教学改革的关键在教师，特别是教师的学术水平和知识视野。

我对于数学教学改革的具体意见是正确处理好：一般与特殊、抽象与具体、形式与实质的关系。特别在讲述中，要避免过分形式化。大多数人学习数学并不是为了从事专门的纯数学研究，形式化的教学会使人或如堕云雾，或如隔靴搔痒，甚至令人望而生畏。即使是培养专门的纯数学研究人才，形式化方法有时虽有其直截了当、逻辑清晰的优点，但过于形式化也不利于更深刻的理解。

我们不仅要关注主修数学学科学生的教学改革，也要关心其它学科的数学课程改革。事实上，数学在其它学科中应用的新的生长点往往首先是由该学科的研究者开始的，而且要使数学家能够进入这个领域工作，也必须有该学科的研究者的帮助与支持。在这个意义上说其它学科数学课程的改革和数学学科的课程改革一样重要。



詹姆斯•西蒙斯 (James Simons) 是世界级的数学家，曾和陈省身作出了以他们的名字命名的定理。他也是最伟大的对冲基金经理之一。2010年，他以85亿美元跻身福布斯世界富人榜的第80位。

人人学好数学

我们不必过分夸大数学需要特殊的才能。数学特别难的印象往往是由于数学的书和文献在表达中过于形式化的缘故。如果课堂教学是干巴巴地“定义——定理——推理”形式地讲，自学时也是亦步亦趋地跟着复习，那么必然会感到枯燥乏味。但如果喜爱数学，而且“教”与“学”都得法，普通中等才能的人照样可以学好数学，顺利地完成大学数学的学业。然而学习方法很重要，每个人要根据学习的不同阶段，来调整自己的学习方法。不断认识自己，明确目标，不断改进学习方法。

五、中国青年数学家的使命

“中国要成为数学大国”

中国没有理由不能成为数学大国。

第一，中国有辉煌的古代数学——祖冲之、刘徽等都遥遥领先于他们的同辈西方学者。只是由于我国的封建社会太长，有很长一段时间不鼓励科学发展，才落后于西方。

第二，老一辈数学家在 20 世纪初才从西方引进近代数学的“火种”。在不到 100 年这段期间，还经历过八年抗战和十年“文化革命”的灾难，几代数学家艰苦奋斗，承上启下，终于以 2002 年世界数学家大会（ICM2002）在北京召开为标志，登上了世界数学舞台。

然而怎样才算“数学大国”呢？我认为：第一，在基础研究方面能在有重大意义的问题上，做原创性的、有自己特色的工作。或者是对数学的有机整体作出贡献，或者是在交叉学科中独辟蹊径。我们要逐渐改变跟在别人后面走的状态，争取引领潮流，逐渐形成中国自己的学派。第二，在应用研究方面，中国数学家要为自己的国家，包括科学技术、国防建设、经济建设等各个方面做贡献，使数学真正扎根在我国自己的土地上。

我们在这方面确实还有相当长的路要走。过去我国自主创新的产品与我国的经济状况很不适应。许多在发达国家工商业界早已应用成熟的数学理论和方法在我国还没有需求，也应用不上。因此我国和世界强国在研究基金和数学毕业生就业方面差别很大。以美国为例，美国数学研究基金除美国国家科学基金（NSF）外，还来自海军、空军、陆军、国

过去我国自主创新的产品与我国的经济状况很不适应。许多在发达国家工商业界早已应用成熟的数学理论和方法在我国还没有需求，也应用不上。因此我国和世界强国在研究基金和数学毕业生就业方面差别很大。

家安全局、高技术局、宇航局、能源部、健康医疗（NIH）等很多方面。除此之外，在美国，不仅传统的科技领域，而且金融、保险、医药、信息、交通运输、材料等等行业也大量应用数学。所以学数学的学生出路很广，除了大学和研究机构外，还有许许多多大大小小的公司雇用数学家。不管经济好坏，不大会有拿了数学博士学位而没有职业的情况。这是因为：数学已经成为他们社会发展的需要。

现在我国经济的发展已经到了提高 GDP 中科技含量的阶段，对于我国青年数学家来说这是一个空前的机会，也一定是大有作为的！真正用数学来提高我国的科技、国防、经济、管理各方面的水平是我们大家共同努力的方向。

抗拒“诱惑”，“锲而不舍”

青年人要有充分的自信。“数学是年青人的学问”。大家都知道天才的阿贝尔、伽罗华在很年轻的时候就做出了划时代的贡献。如今尽管数学的内容已经如此丰富，体系如此庞大，研究人员如此众多，然而真正有能力的青年数学家照样可以脱颖而出！每四年一次的费尔兹奖就是奖给 40 岁以下青年数学家的。从历届菲尔兹奖得主的成就来看，“数学是年青人的学问”这句话至今依然未变。

我国当今青年一代数学家享有中国历史上最好的学习条件和工作条件。包括图书资料、网络信息和学术交流等方面都与发达国家相差无几了。因此没有理由说在中国不能做出第一流的成果。问题在于当今我们的学术环境不理想：急功近利，虚夸浮躁，正在腐蚀人们的思想，败坏我们的学风。中国有志气的青年数学家要自觉抗拒各种“诱惑”、抵制学术不端行为；要继承优良学术传统，要脚踏实地，不畏艰难，锲而不舍，团结奋斗；这样就一定能够实现中国的数学大国和强国之梦。

编者后记 >>

本文的主要内容曾在《数学通报》上发表。承蒙《数学通报》允许，作者根据本刊的风格进行了修改，使本文能够在本栏目和读者见面。在此对《数学通报》和作者表示感谢。

参考文献 >>

[1] 柯尔莫果洛夫，论数学职业，数学通报，1953（中译）。
[2] Doing the Math to Find the Good Jobs, Wall Street Journal, Jan. 6th 2009, www.CareerCast.com
[3] Arrow, K. J. Social Choice and Individual Values, John Wiley and Sons,1951（中译本：社会选择与个人价值，成都，四川大学出版社，1957）。
[4] Dreifuss, R., Speech at ICM’94, Proc. of ICM’94, Zurich, Birkhauser,1995, pp.24-27.
[5] Kline, M., Mathematics and the search for knowledge, Oxford University Press, 1986（中译本：数学与知识的探求，上海复旦大学出版社，2005）。
[6] Courant, R., Robbins, H., What is Mathematics, （中译本：什么是数学－对思想和方法的基本研究，上海复旦大学出版社，2005）。
[7] 胡作玄，邓明立，大有可为的数学，河北教育出版社，2006。
[8] 人人关心数学教育的未来，美国国家研究委员会，世界图书出版公司，1993。

作者介绍：

张恭庆，著名数学家，北京大学教授，中国科学院院士，第三世界科学院院士，曾任中国数学会理事长。

聊聊数学家的故事（连载一）

ukim／文

写给那些，喜欢数学和不喜欢数学的人们
写给那些，了解数学家和不了解数学家的人们

序 多年以前，我有一个很宏伟的计划，打算写一本厚厚的书。这本书有三部，第一部写那些数学牛人们的传奇动人荒诞不经的轶事，第二部充满着历史上最最经典的定理最最美妙的证明，第三部去真实地记录北大数学的这群烂人，写他们那脏乱的宿舍和芜杂的生活。这一直是一个理想，直到我动手写这些文字的时候，我知道，这将永远是一个美好的梦。所以，这里只是那个计划的一小部分，讲述的是那些虔诚的人做过的虔诚的事。

第一次因为数学感动，是听到大人们讲华罗庚先生的故事，不知道那时候多大，隐约记得他们说华先生去苏联算一个卫星的东西，怕他们把自己的算法偷去，于是所有的东西都是心算。故事的真实性自然不可信，不过这很让小孩子神往。我要讲述的也是这么一些事情，很多都是高中和大一大二读过的，那是一段美妙的时光。美妙的东西希望大家一起分享，与人乐乐。

故事一：贝努利家族

约翰·贝努利 (John Bernoulli) 于 1696 年在一个叫做《教师学报》的杂志上公开提出了最速降线问题，挑战的矛头主要针对他的哥哥加可比·贝努利 (Jacobi Bernoulli)。这两个人在学术上一直相互不忿，据说当年约翰求悬链线的方程，熬了一夜就搞定了，加可比做了一年还认为悬链线应该是抛物线，实在是很没面子。那个杂志好像是莱布尼兹（Leibniz）办的，很牛，欧洲的牛人们都来做这个东西。到最后，约翰收到了 5 份答案，有他自己的，莱布尼兹的，还有一个洛比塔（L.Hospital）侯爵的（我们比较喜欢的那个洛比塔法则好像是他雇人做的，是个有钱人），然后是他哥哥加可比的，最后一份是盖着英国邮戳的，必然是牛顿（Newton）的。约翰自己说“我从它的利爪上认出了这头狮子。”据说当年牛顿从造币厂回去，看到了贝努利的题，感觉浑身不爽，熬夜到凌晨 4 点，就搞定了。这么多解答当中，约翰的应该是最漂亮的，类比了费马（Fermat）原理，用光学一下做了出来。但是从影响来说，加可比的做法真正体现了变分思想。

约翰·贝努利 (1667-1748)， 瑞士数学家

贝努利一家在欧洲享有盛誉。有一个传说，讲的是丹尼尔·贝努利（Daniel Bernoulli，他是约翰·贝努利的儿子）有一次正在做穿越欧洲的旅行，他与一个陌生人聊天，很谦虚地自我介绍：“我是丹尼尔·贝努利。”那个人当时就怒了，说：“那我还是艾萨克·牛顿呢。”丹尼尔此后在很多场合深情地回忆起这一次经历，把它当作他曾经听过的最衷心的赞扬。

约翰和加可比这两个贝努利家族的人，都算不出自然倒数的平方和这个级数，欧拉（Euler）从他老师约翰那里知道了这个问题，并且给出了 $\pi^2/6$ 这个正确的答案。欧拉是他那个时代最伟大的数学家。

法国有一个很著名的哲学家，叫做狄德罗（Denis Diderot），是个无神论者，这个让叶卡捷琳娜女皇不爽，于是她请欧拉来教育一下狄德罗。其

实欧拉本来是弄神学的，他老爸就是，后来是好几个叫贝努利的来劝他父亲，他父亲才让欧拉做数学了。欧拉邀请狄德罗来了皇宫，他这次的工作是证明上帝的存在性，为此，他在众人面前说：“先生，(a-bn)/n=x，因此上帝存在;请回答！”狄德罗自然不懂代数，于是被羞辱，显然他面对的是欧洲最伟大的数学家。他不得不离开圣彼得堡，回到了巴黎……

故事二：四色定理

一次拓扑课上，哥廷根大学数学教授闵可夫斯基（Minkowski）向学生们自负地宣称：“这个定理没有证明的主要原因是至今只有一些三流的数学家在这上面花过时间。下面我就来证明它。”于是闵可夫斯基开始拿起粉笔。这节课结束的时候，没有证完，到下一次课的时候，闵可夫斯基继续证明，一直几个星期过去了……。一个阴霾的早上，闵可夫斯基跨入教室，那时候，恰好一道闪电划过长空，雷声震耳，闵可夫斯基很严肃地说：“上天被我的骄傲激怒了，我的证明是不完全的。”

1942年的时候，数学家莱夫谢茨（Lefschetz）去哈佛大学做了个报告，伯克霍夫（Birkhoff）是他的好朋友，讲座结束之后，就问他最近在普林斯顿大学有没有什么有意思的东西。莱夫谢茨说有一个人刚刚证明了四色猜想。伯克霍夫严重地不相信，说要是这是真的，就用手和膝盖，直接爬到普林斯顿大学的 Fine Hall 去。Fine Hall 是普林斯顿大学的数学楼。

闵可夫斯基 (1864-1909), 德国数学家

故事三：做数论的人

由于费尔马（Fermat）大定理的名声，在纽约的地铁车站出现了乱涂在墙上的话：$x^n+y^n=z^n$ 没有解，对此我已经发现了一种真正美妙的证明，可惜我现在没时间写出来，因我的火车正在开来。

希尔伯特（Hilbert）曾有一个学生，给了他一篇论文来证明黎曼（Riemann）猜想，尽管其中有个无法挽回的错误，希尔伯特还是被深深地吸引了。第二年，这个学生不知道怎么回事就死了，希尔伯特要求在葬礼上做一个演说。那天，风雨瑟瑟，这个学生的家属们哀不自胜。希尔伯特开始致词，首先指出，这样的天才这么早离开我们实在是痛惜呀，众人同感，哭得越来越凶。接下来，希尔伯特说，尽管这个人的证明有错，但是如果按照这条路走，应该有可能证明黎曼猜想，再接下来，希尔伯特继续热烈地冒雨讲道：“事实上，让我们考虑一个单变量的复函数……”众人皆倒。

有一个人叫做沃尔夫凯勒（Paul Wolfskehl），大学读过数学，痴狂地迷恋一个漂亮的女孩子，令他沮丧的是他无数次被拒绝，感到无所依靠，于是定下了自杀的日子，决定在午夜钟

费尔马（? -1665），法国数学家、法学家

声响起的时候，告别这个世界，再也不理会尘世间的事。沃尔夫凯勒在剩下的日子里依然努力地工作，当然不是数学，而是一些商业的东西，最后一天，他写了遗嘱，并且给他所有的朋友亲戚写了信。由于他的效率比较高的缘故，在午夜之前，他就搞定了所有的事情，剩下的几个小时，他就跑到了图书馆，随便翻起了数学书。很快，他被 Kummer 的一篇解释哥西（Cauchy）等前辈做费尔马大定理为什么不行的论文吸引住了。那是一篇伟大的论文，适合要自杀的数学家最后的时刻阅读。沃尔夫凯勒竟然发现了 Kummer 的一个错，一直到黎明的时候，他做出了这个证明。他自己狂骄傲不止，于是一切皆成烟云……，这样他重新立了遗嘱，把他财产的一大部分设为一个奖，奖给第一个证明费尔马大定理的人10万马克……，这就是沃尔夫凯勒奖的来历。

故事四：哥廷根的传说

1854年，黎曼（Riemann）为了在

哥廷根（这是二战之前数学和物理的中心，德国著名的学府）获得一个讲师的席位，发表了他划时代的关于几何学的演说。由于当时听这个演说的人很多是学校里的行政官员，对于数学根本就不懂，黎曼在演说中仅仅用了一个数学公式。韦伯（Weber）回忆说，当演说结束后，高斯（Gauss）带着少见的表情激动地称赞黎曼的想法。如果读读黎曼的讲稿，就会发现那几乎就是哲学。当时的观众中只有一个人可以理解黎曼，那就是高斯。而整个数学界，为了完善消化黎曼的这些想法，花费了将近 100 年的时间。

有人说，黎曼的著作更接近于哲学而不是数学。甚至在一开始，欧洲的很多数学家认为黎曼的东西是一种家庭出版物，更接近物理学家的看法，与数学家没有关系。一次，赫姆霍尔兹（Helmholz）和魏尔斯特拉斯（Weiestrass）一起外出度假，魏尔斯特拉斯随身带了一篇黎曼的博士论文，以便能在一个山清水秀的环境里静静地研究这篇他认为是复杂又宏伟的作品。但是赫姆霍尔兹大惑不解，他认为，黎曼的文章再明白不过了，为什么魏尔斯特拉斯作为数学家要这么花功夫呢？

克莱茵（Klein）上了年纪之后，在哥廷根的地位几乎就和神一般，大家对他敬畏有加。那里流行一个关于克莱茵的笑话。说哥廷根有两种数学家，一种数学家做他们自己要做但不是克莱茵要他们做的事；另一类数家做克莱茵要做但不是他们自己要做的事。这样克莱茵不属于第一类，也不属于第二类，于是克莱茵不是数学家。

维纳（Wiener）去哥廷根拜访这位老人家，他在门口见到女管家时，询

黎曼（1826-1866），德国数学家

问教授先生是否在家。女管家训斥道："枢密官先生在家。"一个枢密官在德国科学界的地位就相当于一个被封爵的数学家在英国科学界的地位，譬如说牛顿（Newton）。维纳见到克莱茵的时候，感觉就像去拜佛，后者高高在上。维纳的描述是"对他而言时间已经变得不再有任何意义"。

故事五：希尔伯特的故事

大卫 • 希尔伯特（David Hilbert）并不是哥廷根毕业的。19 世纪 80 年代，柏林大学的博士论文答辩，需要 2 名学生作为对手（他们向你不停地发问）。希尔伯特的一个对手叫埃米尔 • 魏恰特（Emil Wiechert），后来是最著名的地震学家。那时候，德国（也许叫做普鲁士）的大学教授特别少。柏林只有 3 名数学教授，一般的大学至多 2 个。

在希尔伯特的博士宣誓仪式上，校长主持说："我庄严地要你回答，宣誓是否能使你用真诚的良心承担如下的许诺和保证：你将勇敢地去捍卫真正的科学，将其开拓，为之添彩；既不为厚禄所驱，也不为虚名所赶……"很想知道现在中国的授予博士仪式是不是也有类似的话。

有一次，上了年纪的希尔伯特见到一群年轻人正在谈论一个他知道的数学家。那时候，像闵可夫斯基这些他很熟悉的人，有很多都已经故去，所以他特别关心正在被谈论的这个人。当大家说完这个人有几个孩子之类的事情之后，他就问道："他还'存在'么……"。

一次在希尔伯特的讨论班上，一个年轻人在报告中用了一个很漂亮的定理，希尔伯特说："这可真是一个妙不可言（wunderbaschon）的定理呀，是谁发现的？"那个年轻人茫然地站了很久，对希尔伯特说："是您……"。

哥廷根广为流传着一个关于闵可夫斯基的故事。说是他在街上散步时，发现一个年轻人正在默默地想着某个很重要的问题，于是闵可夫斯基轻轻地拍拍他的肩膀，告诉他"收敛是肯定的"，年轻人感激而笑。

希尔伯特（1862-1943），德国数学家

作者毕业于北京大学数学系，2010 年获得普林斯顿大学数学博士学位。为本刊特约撰稿人。

卢丁和他的《数学分析原理》

—— 谨以本文纪念赵慈庚教授百年诞辰

蒋迅

卢丁(Walter Rudin)1921年5月2日出生在维也纳的一个犹太家庭里。早年的卢丁有些不幸。1938年德奥合并时全家逃到法国，1940年法国投降时，卢丁又逃到了英国。在英国，他加入了皇家海军，直到二战结束。战后，他到了美国。1945年秋季到杜克大学攻读博士学位，1949年6月获得了博士学位(本书背面的介绍说1953年是不对的)。然后他在麻省理工学院、罗切斯特大学任教数年，这本《数学分析原理》就是他在麻省理工学院教书时写的。当时他获得博士学位才两年。以后他转到威斯康辛大学的迈迪森分校任教授，直至退休。在杜克，他与另一位数学家玛丽•艾伦(Mary Ellen Estill)相遇，1953年结婚，晚年一起居住在威斯康星州的迈迪森。卢丁于2010年5月20日去世。

卢丁(Walter Rudin)，著名数学教育家

卢丁一共写过七本书：著名的分析学三部曲《数学分析原理》、《实分析与复分析》、《泛函分析》以及《群上的傅里叶分析》、《多圆盘上函数论》、《单位球 C^n 上的函数论》和自传《我记忆中的路》(The Way I Remember It)。其中,《数学分析原理》和《实分析和复分析》常常分别被数学学生们称作“小卢丁”(Baby Rudin)和“大卢丁”(Big Rudin)。而被称为“小卢丁”的那本就是我要介绍的《数学分析原理》(Principles of Mathematical Analysis)。

卢丁的《数学分析原理》是古典分析的经典教科书，在美国很受欢迎。即使象陶哲轩(Terence Tao)那样的著名教授，已经写了自己的《陶哲轩实分析》，也仍然使用这本书作为教材。它恐怕是数学教材中被引用最多的教材了。美国的数学系教程设计与中国有些不同。美国的理工科大学生在入学后不管是哪个系的都统统学微积分课。这样做对数学系学生的好处是：第一，数学系学生可以更多地接触到应该得到的感性认识和大量的广泛的应用；第二,万一发现自己不适合留在数学系的话，可以立即转系而不会有什么不适应(同样，其他系的学生转到数学系也相对容易)。当一个数学系学生决定自己要学这门课时，他应该已经学完了基本的微积分课，也通过线性代数、离散数学等课程得到了严格推理的基本训练。卢丁的书正是基于这个背景写的。因此，它的起点比较高，特别是字里行间有些有意识的“遗漏”。这对学生也许是一个挑战，但如果你真的喜爱数学的话，不正是因为数学富有挑战吗？所以，当你读这本书的时候，一定不能跳跃，而是要扎扎实实地读懂每一行，每一段,补上证明中“遗漏”的步子。笔者看到有些人表示对此书的失望，很可能就是因为他们没有真正地做好了准备就匆忙开始阅读了。

本书由实数和复数的简单讨论开始(第一章)，但这一章的最大亮点是在它的附录里：戴德金分割。它告诉你如何通过有理数来构造无理数。第二章是基本的拓扑知识，这些都是后面要用的。所以它们看似简单，但不能忽略。注意作者在这里讲的仅仅是拓扑空间的一个特例：距离空间。更广义的拓扑学需要专门的课程。这样的处理与中国不同。其原因还是因为它已经假定了微积分的基础了。第三章中的数列和极限也是后面要用到的基本知识，这些对于中国的学生也许是不太难的。作者把极限的正式引入推迟到数列的收敛之后(第四章)显然符合循序渐进的原则，也是国内大多数教材的思路。注意作者这时候已经不是在普通的实数空间里，而是一

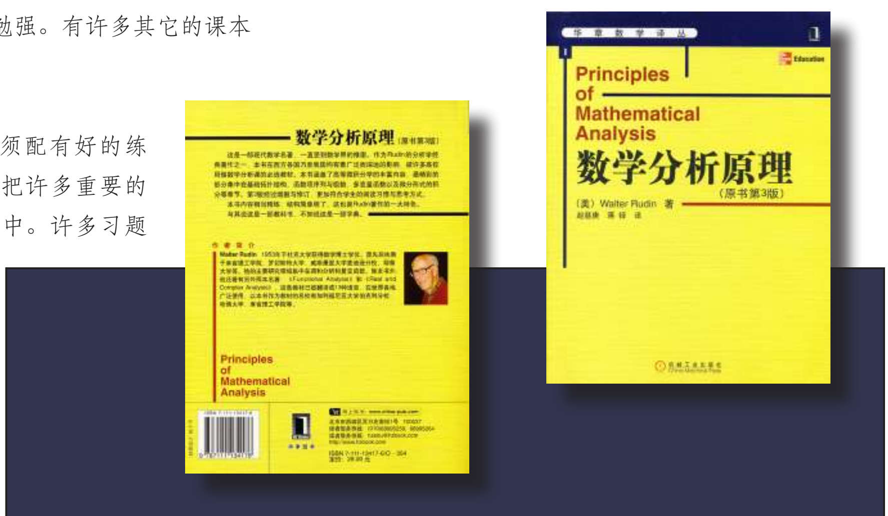
般的距离空间讨论了。这样的高起点将在后面发挥作用。假如你已经学过初等微积分的话，第五章讲微分可能没有太多的挑战，读者应该注意罗毕塔法则的重要性。(其实这个法则本应属于贝努利兄弟的，见本刊第一期万精油的文章。) 积分部分 (第六章) 关于黎曼-斯蒂尔吉斯积分的一章是作者在第三版花了较大工夫的部分。这是在初等微积分的基础上对 (实值、复值和向量值) 积分概念的严格化。注意有些定理是基于黎曼积分进行讨论的。其中的微积分基本定理、分部积分是极为重要的。函数序列与函数项级数 (第七章) 是第三章中数列与级数的讨论的延伸。这可以说是本书最重要的部分了。本章要解决的是两个极限交换的问题，魏尔斯特拉斯一致逼近定理起了关键作用。有了第七章的准备，作者在下面的一章里讨论了一些特殊函数。指数函数是作为一个特殊的幂函数定义的，对数函数和三角函数则从指数函数导出。傅立叶 (Fourier) 级数的内容很重要。注意正如作者指出的，对傅立叶级数的许多讨论需要后面第十一章里的勒贝格积分。关于 Γ 函数的一段可能不太重要，不过，如果你将来想往概率统计方向发展，还是不应该放过的。第九章转到多元函数。作者首先介绍了线性代数的基本性质。但是线性代数不能仅仅被看成是学习多元微积分的工具。本章里的线性算子就是泛函分析中的更为抽象的巴拿赫 (Banach) 空间中的重要概念。反函数定理是另一个重要的内容。第十章是微分几何导引。主要是斯托克斯 (Stokes) 定理。笔者所在学校当年是单独作为一门课"流形上的微积分"来讲授的。坦率地说，它有一定的难度。不过，对于想向微分几何或偏微分方程的同学们是不能放弃的一章。第十一章讲的是勒贝格积分，这一章对于本书来说似乎有些超出了范围。笔者认为读者不必过于勉强。有许多其它的课本是专门讲这个课题的。

不用说，一本好的教材必须配有好的练习题，这本书也不例外。作者把许多重要的结果和重要的反例放在了习题中。许多习题有提示。读者应该认真地尝试本书中的所有练习题 (注意，习题的难易不一定是从易到难的)。除非你是象陶哲轩那样聪明，很有可能有些题会难倒你。但是，你会发现受益匪浅。

如果你有更多的精力，或者你的老师推荐的话，不妨将本书和王昆扬教授翻译的《陶哲轩实分析》一起阅读。笔者还建议同学们可以结合西尔维亚 (Evelyn M. Silvia) 教授写的辅助材料一起阅读，这样可能会相对容易一些。当然这要求读者有一定的英文阅读能力。笔者曾经与西尔维亚教授在加州大学戴维斯分校共事。她是一位极其敬业又充满精力的好老师，长期致力于中小学数学教育。可惜她在 2006 年 1 月因癌症去世，终年才 57 岁。

作者在前言中提到，本书"说到了美国数学月刊或数学杂志上出现的作品，以期学生逐步养成阅读期刊文献的习惯"。笔者认为这是一个很好的尝试。原书最后有一个"重要符号表"，在译本中放在了最前面。这样做很有意义。否则放在最后的话，同学们可能在读了许多章之后都不知道有这个表的存在。原书还有一个索引，可惜在译本里没有收入进去，在重新印刷时最好能补上。作者在一些叙述上有一点小的错误，比如实数和广义实数、实数和复数的陈述上缺乏一点精确性，读者可能需要留心一点。

《数学分析原理》(原书第 3 版) 由北京师范大学的赵慈庚教授和蒋铎教授翻译，先由人民教育出版社出版，后由机械工业出版社重新出版。两位先生都已经作古，所以本书是他们献给同学们的最后礼物。今年是译者赵慈庚教授诞辰一百周年。我们介绍他和蒋铎教授的译著作为对他们的纪念。这本书的中英文版本在网上有电子版，但是作为一本数学分析的经典书，它是所有数学工作者的必备图书之一，很难想象会有人不舍得花二十几元人民币而让书架上缺少它。我相信，读过本书的人都会同意的。

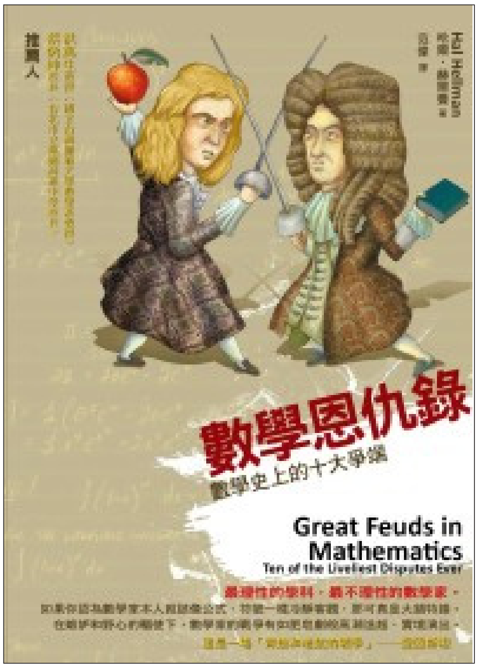


我读《数学恩仇录》

深刻领略了数学理性与感性的丰富乐章

蔡炳坤

我从小就喜欢数学。并不是对数学特别有天分，也不是碰到特别好的数学老师，而是因为只要上课听懂了(这句话很重要，数学的学习重在理解)，就可以在大大小小的考试中得高分，不必像其他科目必须背诵许多东西，记得当年参加高中联考的时候，几乎考满分。印象中，从小学到国中，每次作文题目“我最喜欢的科目”，我都毫不犹豫地写“数学”。后来进了师专以后，注意力转移到了音乐方面，也就慢慢与数学疏远了。直到四年前，我的孩子高中毕业选择“数学系”当第一志愿，我才又开始接触与数学相关的议题或书籍。我的学校——建中，又是台湾高中数学学科中心学校，有机会经常与杰出的大学数学教授、优秀的高中数学老师们讨论相关课题，多少也熏染了一些数学的专业氛围。



日前接到五南图书编辑部门邀我撰写《数学恩仇录》导读的讯息，的确有所犹豫，我主修的领域是教育，并非数学，如何能够胜任这项专业的工作？但当开始试着阅读时，竟然流畅地停不下来，爱不释手于每个事件的情节中。总的来说，从本书颇具吸引力的译名开始，就注定了她的“成功”。主标题《数学恩仇录》(Great Feuds in mathematics) 使人不由得联想到著名作家大仲马所著的《基度山恩仇记》(Le Comte De Monte-Cristo，一部脍炙人口，描写善有善报、正义伸张的小说)；副标题《数学史上的十大争端》(Ten of the Liveliest Disputes Ever) 则点名了本书描述的其实就是十个深富哲理与人情世故的有趣故事(篇篇读来淋漓痛快，让人废寝忘食)，虽然当中有诸多难解的数学公式、深奥的解题方法和艰涩的专有名词，但并不影响故事情节高潮迭起的巧妙铺陈。书中内容更多的是对人性好恶的探索、对学术伦理与价值观冲突的描述以及激情过后的深刻省思等等，趣味中带着泪水，科学中蕴含人文哲理。我虽自不量力，但非常乐意地带领年轻的莘莘学子们，一起领略这篇充满数学理性与感性的华彩乐章。

作者哈尔·赫尔曼选择十六年世纪中叶作为本书选材的起点，首先登场的便是赫尔塔利亚 (Niccolo Tartaglia) 和吉罗拉莫·卡尔达诺 (Gerolamo Cardano)，这两位意大利数学家谁才是求解三次和四次代数方程序的原创者？又究竟卡尔达诺曾经对赫尔塔利亚做出什么样的承诺，自此一再遭受“背信弃义”的严重指控？凡此种种都在1545年《大技术》一书出版后引爆开来，这本书，直到现在，仍被众多学者认为是文艺复兴时期的科学杰作之一，可与维萨里的《人体构造》、哥白尼的《天体运行论》相提并论。

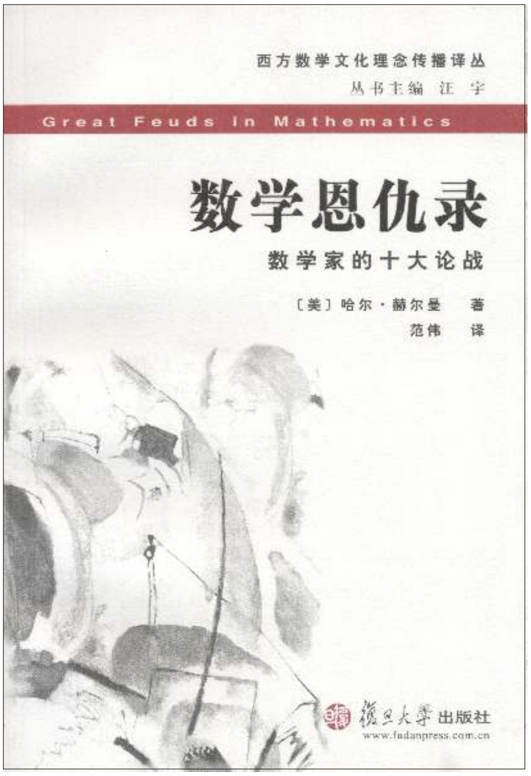
令人惊讶的是，直到1576年，两人相继去世后的三十余年间，"授权"与"剽窃"之争从未间断，公说公有理，婆说婆有理，虽未对簿公堂，但在数学界所掀起的轩然大波，果真是"罄竹难书"，对这两位数学家而言，或有"既生瑜，何生亮"的遗憾情结，但就整个数学界的发展来说，也未必全然的负面，作者写下了这样的脚注："当赫尔塔利亚和卡尔达诺两人鹬蚌相争时，毫无疑问地，数学是那个得利的渔翁。"读过精采的原创之争，想必您心有戚戚，在知识产权尚未充分彰显的那个年代，数学家不得不对自己的创见有所保留，在展现某些问题的解法时，却对所用的方法保密，以免被他人据为己有。有人可以终其一生为捍卫原创而战斗，姑且不论真相如何（似已成为罗生门），但其维护自身权益，不计毁誉、奋战到底的意志，倒是值得仍多少存在抄袭现象的今之学界，引以为鉴。

接下来的这个故事更精采了（第二章）。众所周知"我思，故我在"出自法国哲学家勒内•笛卡儿的名言，他在1637年所发表的《方法论》中以"一种系统化的怀疑"的哲学思考方式写道："不能确知是对的事，不要接受。这就是说，在判断时谨慎地避免仓促和偏见，只接受那些截然清晰地印在脑中不容置疑的东西。"这本书是好几个学科领域的里程碑论著，涉及哲学、科学史以及数学思想。有人把她与牛顿的《原理》一书相媲美，并认为她为十七世纪数学的伟大复兴做出了卓越贡献。人们多半因为这本书，普遍地把统一代数和几何，甚至是创立解析几何的荣誉归于笛卡儿。的确，"笛卡儿坐标系统"就是以他的名字命名的。然而，笛卡儿在《方法论》三篇文章中的两篇（折射光学与几何），却成了与同是法国人的业余数学家皮埃尔•费马争论的焦点。说到"费马最后定理"(Format's Last Theorem)，也是无人不知、无人不晓的重大发现。著名的数学史学家贝尔 (E.T. Bell) 在二十世纪初所撰写的著作中，称费马为"业余数学家之王"（他具有法官和议员的全职工作）。贝尔深信，费马比他同时代的大多数专业数学家更有成就。十七世纪是杰出数学家活跃的世纪，而贝尔认为费马是十七世纪数学家中最多产的明星。在近二十年的数学争端中，贝尔如此形容："让脾气有些暴躁的笛卡儿和沉稳内敛的'Gascon'费马并驾齐驱，看来极不自然。在关于费马切线理论的争议中，这个好战的家伙（笛卡儿）经常烦躁易怒，出语刻薄，而这位不动声色的法官却表现得真诚、谦恭。"读过笛卡儿和费马在数学理论上的争辩，颇令人有文人相轻之慨，但话说回来，所谓的"真理"愈辩愈明，未到最后关头，胜负难分，亦随着时间的变化而被凸显出来，作者对此写下令人玩味的脚注："一场旷日持久的争斗诞生了一个明显的胜利者和失败者。但具讽刺意味的是，胜利者（指笛卡儿）从争斗中受益微薄，而失败者（指费马）却被争斗激发，提出了科学上一个重要的原理，为微积分的发展打下了重要的基础。"的确是如此，笛卡儿渐渐远离了数学，专注在哲学和形而上学的研究，在尊敬和赞誉声中结束了荣耀的一生。而费马则继续钻研数学，默默耕耘，并做出好几项重大贡献。

笛卡儿渐渐远离了数学，专注在哲学和形而上学的研究，在尊敬和赞誉声中结束了荣耀的一生。而费马则继续钻研数学，默默耕耘，并做出好几项重大贡献。

相较于前述两位意大利数学家"原创"之争、两位法国数学家"理论"之争，接下来要登场的是英德"微积分发明"之争，主角分别是伊萨克•牛顿与威尔海姆•莱布尼兹（第三章），两人从未谋面，但因为这两人的追随者富有侵略性的行为，使得这场争端狂热地持续了一个多世纪，难怪科学史家丹尼尔•布尔斯丁将他们的争端命名为"世纪景观"。牛顿的主要兴趣在于用数学方法解决自然科学问题，"万有引力理论"的提出就是明证，但莱布尼兹则像笛卡儿一样，希望在哲学上有重大创建，认为数学可以为他开路。前者在英国被奉为偶像，并受封为爵士，1703年被推举为皇家学会的主席，并连年当选，直到1727年去世为止，且被授予国葬尊荣；后者的声望在欧陆也是快速增长，1699年法国科学院制作的外籍院士名单中，牛顿排名第七位，而莱布尼兹则排在第一位，他在符号逻辑和微积分，还有其他诸多领域，特别是宇宙论和地质学，都做了很重要的早期研究，只是到了晚年，微积分的争议事件给他蒙上了巨大的阴影，凡事皆不顺利，1716年在汉诺威去世时，只有生前的一位助手参加葬礼，令人不胜唏嘘！究竟这两位杰出的天才，谁才是微积分的首创者呢？总的来说，在微积分发展上，牛顿约在1665-1666年，而莱布尼兹则在1673年以后，是由牛顿领先；至于微积分的发表上，莱布尼兹在1684-1686年，而牛顿则在1704年以后，却是由莱布尼兹领先。简单地说，牛顿先发展了微积分，但没有公诸于世，莱布尼兹先发表了微积分，而且他的方法更好用，也确实先投入运用。这项首创的荣誉应该归谁呢？他们各自的国家都诉说着完全不同的故事。这场争论并没有因为两人的去世而停歇，

并导致了两个重要的结果：一是两派数学家之间的关系破裂了，一直持续到十九世纪；二是在莱布尼兹微积分的基础上，欧陆的数学家在十八世纪取得了飞速的进步，大大超越英国的数学家。是以，作者写下了如此简短而有力的脚注：莱布尼兹输了那场战役，却赢得了整场战争。您说，不是吗？



哇！连着三大争端读下来，过瘾极了！在接下来的故事中，有兄弟阋墙者(第四章)、有观点不同者(第五章)，前者便是瑞士的伯努利兄弟，哥哥雅各布透过自学钻研数学，33岁已经成为巴塞尔大学的教授，莱布尼兹对他有相当高的评价。弟弟约翰原本学医，但与雅各布一样，心在数学，所以私底下跟着哥哥学习数学。他们两位是首先认识到微积分的重要性，并将其投入运用、向世界宣传它的意义的数学家。然而，他们之间却也为了谁的地位更崇高而发生了激烈的论争，最后爆发成一场彼此之间公开的数学挑战。而后者便是英国的托马斯·赫胥黎和詹姆斯·西尔维斯特，赫胥黎是一位有着崇高威望的科学家，在动物学、地质学和人类学领域都作出了重要的贡献，他对当时新提出并广为人所憎恨的“进化论”的捍卫，为他赢得了“达尔文的斗牛犬”的称号，他喜爱科学，在他的脑中，科学是生命的一部分，对于数学，他却敬而远之，他把数学看成一种游戏，但与科学无关，所以他说“数学对观察、实验、归纳和因果律一无所知”做工作。简言之，“它对实现科学的目的无用”。这话可把西尔维斯特给惹恼了，他是犹太人，是个桀骜不驯、饱经磨难的人，是一位才华洋溢的数学家，也是一位斗士、一位出色的演说家。1869年，时为英国协会(也称英国科学促进协会)数学和物理学分会主席的西尔维斯特，在主席讲话中，回应指出“数学分析不断地援引新原则、新观念和新方法，它不能用任何言语来定义，但它促使我们大脑里内在的能量和活力爆发出来，透过持续地审视内心世界，不断地激发我们观察和比较的能力。它最主要的手段是归纳，它需要经常求助于试验和确认，它给我们最大程度地发挥想象力和创造力，提供了无尽广阔的空间。”当斗牛犬遇上斗士，各自迥异的观点令人窒息，“但对于英国教育和美国教育系统来说，他们能够并肩作战，实是我们的幸运。”作者如是说。

一个欧几里得广为人知的“普遍观念”是：整体大于它的部分。这个观念在1870年代早期，被一位不知名的数学家质疑，主张：就对数和数论来说，整体不一定大于它的部分。他就是创造了集合论，并将集合论和无穷这两个观念结合起来，提出了无穷集，为数学世界开创了一个广阔新领域的格奥尔格·康托尔。他大胆寻求突破的行动，对利奥波德·克罗内克这位保守的知名数学教授、曾经友好地支持过他的老师来说，就像是“数学的疯狂”，克罗内克毫不客气地批评康托尔是一个科学骗子、叛徒、青年的败坏者。对于这场长达数十年的康托尔与克罗内克争端(第六章)，两位社会学家柯林斯和瑞斯提沃提出了一个有趣的观点：“克罗内克和康托尔之间的斗争，不是传统和创新的数学形式之间的冲突，而是新典范的竞争。克罗内克不是数学上的传统主义者，为了反对当时的无穷和无理数、超越数和超限数等观念，他被迫在一个激进的新基础上重建一门新数学，他的成果预示着二十世纪直觉学派的诞生；正如康托尔成为形式主义运动的先驱一样。两个派别都希望数学变得更严密，但在如何达到这个要求上，他们有很深的分歧。”

延续上一章的话题，竭力想创建新数学理论的康托尔，其理论相继受到严峻的挑战，1900年第二届国际数学家大会在巴黎召开，著名的德国数学家戴维·希尔伯特指出：康托尔的连续统假设还没有找到证据。1904年

第三届国际数学家大会在海德堡举行，来自布达佩斯的著名数学家朱尔斯·柯尼希宣称：康托尔连续统的势不是任何阿列夫数。对此，来自哥廷根大学的年轻数学家恩斯特·策梅洛跳出来维护了康托尔，策梅洛不仅指出了柯尼希的错误，并认为证明康托尔的良序原理是完善集合论的首要工作，且进一步提供了证明良序原理所需要的关键步骤，此步骤的假定被称为“声名远播的公理”(因为在很多国家、很多数学家之间激起回响)，有赞成的，当然，也有反对的。最主要的反对者是法国的数学家埃米尔·波莱尔，根本上来说，波莱尔在直接挑战策梅洛“从每一个非空子集中，可以挑出或指定一个元素作为特殊元素，这样，我们就可以创建一个良序集合”的主张，也反对选择所谓的“公理”，因为它需要无穷次操作，这是难以想象的。波莱尔和策梅洛的“公理”之争(第七章)，一直没有完全地解决，《数学中的现实主义》一书作者佩尼洛普·马迪倒是作出这样的诠释：“这整段历史插曲中最具讽刺意味的是：对这个公理最强烈的反对正是来自法国分析家小组——贝尔、波莱尔和勒贝格，而他们却在无意中非常频繁地用到它，他们的工作部分地说明了数学中不可缺少它。”

但我可以期待，或至少可以希望，每一次危机之后，数学界将会从以前所发生的事中学到某些东西，从而变得更强大、更聪明。

一九〇一年的春天，数学家们都面临着伯特兰·罗素“悖论”的挑战(第八章)。这位由哲学家转变而成的英国著名数学家，提出了一个乍看之下很简单的问题“他假定一个由所有不是自身元素的集合所组成的集合，称这个集合为R。然后他问：集合R是它自身的一个元素吗？如果是，那么它不符合这个集合元素的定义；如果不是，那么它是这个集合的一个元素。”这个悖论有着深刻的寓意，早期的集合论考虑过包容一切事物的泛集合的可能性，现在看来，这是不可能的，不是每种事物都能形成集合。它居然动摇了集合论和它所支撑的广阔数学领域的基础。由于它没有答案，所以是一个悖论，或者说是个矛盾。当罗素提出他的悖论时，也已经开始致力于他在逻辑主义上的努力，他坚信纯粹数学可以建立在少数基本的、合乎逻辑的观念基础上，所有的命题都可以从一小部分基本的、合乎逻辑的原理推导出来，他也希望能够解决这个悖论，《数学原理》便是在这样的努力下问世。对此，备受推崇的法国数学家莱尔斯·庞加莱对罗素的逻辑主义发起了一个全面的批判。这位在数论、拓朴学、机率论和数学物理等诸多领域都有建树的数学科学家，和罗素之间的一系列争论和反击从一九〇六年持续到一九一〇年，虽然两人彼此非常尊重，但攻击起对方来毫不犹豫。

就在罗素“逻辑主义”方兴未艾之际，数学界已经同时领会了戴维·希尔伯特的代表作《几何基础》，在他的观点中，有一个想让公理化体系更普遍的愿望，他想建立首尾一致的算术公理体系和从它们开始推导的步骤。他还认为，给罗素等人带来问题的悖论是由所用语言的语意内容造成的，也就是说，是由语句的模糊造成的。就这样，以希尔伯特为代表的形式主义学派诞生了。但是，就在这时，荷兰数学家伊兹·布劳威尔持有一个针锋相对的立场，他相信人类存在着根深蒂固的关于数学基础的思考模式，大部分以数学方式提出来的东西只不过是装饰而已，他成为了后来称之为直觉主义数学学派的旗手。在希尔伯特与布劳威尔的论战中(第九章)，所有的分歧——包括参与者的国籍，都派上了用场。当论战扩大到欲拉拢彼此的支持者时，选择保持中立的爱因斯坦形容它就像是一场“青蛙和老鼠的战争”。

最后，作者回顾了一个很多年来令数学家们苦恼并着迷的问题：数学的进步是发明还是发现？虽然它本身相当有趣，但也引发了一场论战(第十章)。绝对主义或柏拉图主义的拥护者们，把数学看作是客观和精确的，他们运用数学非凡的能力来描述自然和技术中的运动和形态，并主张：真正的数学知识是完美和永恒的(所以说：数学的进步是发现)。持相反意见的是易误论者与建构主义者，他们把数学看成是一个不断进步的活动，甚至主张：某些数学进展被接受是建立在数学家们的权威基础上(所以说：数学的进步是发明)。您认为呢？全书到这里告一段落，您是否也有意犹未尽的感觉？作者留下了这样一段话“但我可以期待，或至少可以希望，每一次危机之后，数学界将会从以前所发生的事中学到某些东西，从而变得更强大、更聪明”。作者是否为下一部著作预留了伏笔？值得进一步期待。

本文作者为台北市立建国高级中学校长

报刊链接

《数学恩仇录》数学“江湖”的恩怨情仇

“有人群的地方就有江湖，有江湖就有是非恩怨”，武侠大师古龙这句名言可以作为《数学恩仇录》一书最精彩的注脚。在本应纯净的数学界，我们看到了同行相争、师生反目、兄弟阋墙、父子成仇这些肥皂剧一般的情节，而且出场的主角都是牛顿、笛卡尔、费马这样的大牌人物。

数学中的刀光剑影

《数学恩仇录：数学家的十大论战》（Great Feuds in Mathematics）出自美国自由科普作家哈尔•赫尔曼之手。著述颇丰的他近些年以大争论为主题撰写了系列图书，最早写过 Great Feuds in Science（中文书名《真实地带》），接着又涉足医学、技术等领域的争论。当出版公司建议赫尔曼再写一本关于数学史上大争端的书时，他差点回绝了，因为赫尔曼认为，“比起政治和宗教，甚至自然科学，数学很少有人类情感的参与”，数学不太可能有争端。然而当他查找一些资料后，渐渐发现“数学家和政治家、牧师们一样，也是人，都容易犯嫉妒、偏见、野心、骄傲、手足相残、急于求成的毛病。显然，数学界里发生了很多有意思的事情”，以至于后来赫尔曼都觉得很麻烦，因为要从太多的论争中选取一些重要和有意思的事件。

赫尔曼选择 16 世纪中叶作为起点，在《数学恩仇录》中首先登场的是赫尔塔利亚和卡尔达诺，这两位意大利数学家谁才是求解三次和四次代数方程式的原创者？又究竟卡尔达诺曾经对赫尔塔利亚作出什么样的承诺，自此一再遭受“背信弃义”的严重指控？当赫尔塔利亚利用卡尔达诺的儿子做告密者，将卡尔达诺交给了西班牙宗教裁判所，他们之间的阴谋和对抗才宣告结束。接下来几个世纪的故事一个比一个精彩，在解析几何和光学的问题上，笛卡尔和费马争论不休；在微积分的首创权上，牛顿和莱布尼兹之间产生了激烈的争端；在微积分问题上，伯努利兄弟针锋相对；在数学的逻辑基础问题上，庞加莱和罗素战斗不休。在 20 世纪一场令人瞩目的数学冲突中，希尔伯特和布劳威尔卷了进来，爱因斯坦却采取中立的立场，形容他们之间的论战是青蛙和老鼠的战争。

很多人喜爱武侠小说，沉浸在江湖的波澜和刀光剑影中，体验着情感的跌宕起伏、世事的变幻无常，其实数学史上的历史真实事件，其精彩与残酷不亚于甚至是更甚于虚构的武侠小说。“通览全书，仿佛看到天才们在智力的巅峰上，以笔为剑，捉对厮杀，直到双方凄凉离世，一生一世也较量不出胜负。其情其景惊心动魄，多么壮观多么悲凉，着实让人动容。”在跋中汪宇这样写到。

数学是得利的渔翁

《数学恩仇录》一书的书名足以让读者产生无限的联想，相信不少读者选择这本书也是奔着八卦、猎奇的心理来的，《数学恩仇录》算是一本严肃的著作吗？该书责编、复旦大学出版社编辑梁玲说：“书中描述的十大论战，不是从猎奇的角度选取的，实际上，这十大论战所涉都是数学史上最基础、最关键、最根本的问题，是紧绕数学根基的动摇和新数学的建立而展开的。数学丧失了确定性后，如何夯实数学基础，如何建立‘基础而统一的’数学理论，可以视作本书的主线。很多人知道的沃利斯与霍布斯的‘化圆为方’之争，对垒了四分之一个世纪，詈骂不逊于泼妇，热闹得很，但由于没有太高的‘数学含量’，该书并未收录。在作者看来，无论是正方还是反方，无论是出于纯粹的数学目的还是挟带个人私怨，数学家们的所作所为实际上都是在捍卫数学、拯救数学，也是在拯救科学、拯救人类文明。”

《数学恩仇录》所选取的十大论战其实是十个深富哲理与人情世故的有趣故事，虽然当中有诸多难解的数学公式、深奥的解题方法或艰涩的专有名词，没有专业背景的读者未必都懂，但并不影响故事情节高潮迭起的巧妙铺陈，因为书中更多的是人性好恶的探索、学术伦理与价值观的冲突、激情过后的深刻省思等等，趣味中带着泪水，科学中又蕴含人文哲理。

因而《数学恩仇录》是一本“由猎奇入，从正史出”的数学史著作，这本书也是在从另一个角度向我们展示巨大的争端是如何推动数学的伟大进步的。正如第一章赫尔塔利亚和卡尔达诺的论争，对这两位数学家而言，或有“既生瑜，何生亮”的遗憾情结，但就整个数学界的发展来说，

报刊链接

也未必全然是负面的，赫尔曼在这章的最后写下了这句话："当赫尔塔利亚和卡尔达诺两人鹬蚌相争时，毫无疑问地，数学是那个得利的渔翁。"

并非纯粹的数学

读罢《数学恩仇录》，读者尤其是那些对数学、数学家怀有莫名崇敬的年轻学子的某些观念必定会有颠覆性的冲击——纯粹的数学和数学家并不存在。首先，数学并非纯粹的。数学史上的争论，多为意气之争，但意气之外，也让我们看到了数学知识本身的不确定性，尽管数学的确是所有科学中最接近确定性的一门学问。其次，数学家们也并非纯粹的。数学家也是人，也有感情，也有好恶，而且他们都摆脱不了人性的弱点——自私、贪婪、偏执、虚荣、嫉妒等等。这些人性弱点，渗透于科学研究之中，某些时候甚至直接影响他们的学术研究成果。

数学家在人们眼里一直是一个比较特殊的群体：他们聪明绝顶，却不食人间烟火，成天想些常人无法理解的东西。其实，数学家的脑瓜儿再神，但是他们也是人；即使有点古怪，那也是人的生活方式。梁玲说："赫尔曼从数学家为维护自身学术利益或名誉等角度，阐述了他们作为人的一面，但这丝毫没有贬低、歪曲数学大师卓绝的智慧和贡献（即使提到了他们的一点瑕疵），而是能够更加准确地呈现数学家的工作与个性。"

梁玲认为，引进《数学恩仇录》除了让读者了解科学中的人性因素外，还希望这本书能引起读者的一些哲学思考："今天的社会，对科学技术的崇拜形成一股潮流，这本身没有错，但崇拜过度，就容易偏颇。比如当前社会上各种'科星'的塑造。塑造的结果是权威的出现，再肆意发展的恶果是压制不同声音、唯我独尊、搞小圈子，进而抑制创新，僵化机制，不利于科学的进一步发展。而对于科学圈内人而言，通过本书，应该认识到正常的学术之争与个人恩怨的意气之争，需要辨析清楚。不要把个人的意气过多掺进科学研究的过程，科学需要论争，需要正常的、公开化的和民主化的争论。这有助于学术的规范和健康发展。"

（摘自《科学时报》2009 年 09 月 03 日　文 / 李芸）

《数学恩仇录》数学天才捉对厮杀

我想，第一个发现无理数的那个古希腊人是人类献给数学的第一个生命。他是毕达哥拉斯 (中国人称之为"勾股定理"的"毕达哥拉斯定理"就是以他命名) 的弟子，他发现当两条直角边的长度为 1 时，斜边的长度 (今天我们都知道那是 2 的平方根) 不能用两个整数的比来表示。这违反了毕达哥拉斯学派的信念，于是他被他的同学们淹死在海里。

我们经常会忘记，数学史是以如此血腥的故事作为开端的。我们总是像英国数学家伯特兰·罗素那样认为，"公正地看，数学里不仅有很多真理，而且有着极致的美。这种美冷峻如雕塑，它不迎合我们天性中的任何弱点，也没有绘画和音乐那样的华丽外表；但它极纯净，能够向我们展示只有最伟大的艺术才具有的完美"。这样的数学，难道会有勾心斗角、欺压迫害？《数学恩仇录》的作者、美国作家哈尔·赫尔曼就曾经这样说过："比起政治和宗教，甚至自然科学，数学很少有人类情感的参与。在数学里，怎会有争端？"

错了。大错特错了。在这里，我们需要复习一遍一句与毕达哥拉斯定理同样正确的名言：有人的地方就有江湖。数学家们无疑是天才，但是天才也不能免俗啊。当一个天才与另一个天才冤家路窄狭路相逢头碰头地站在对立两端的时候，一场闪现着智慧之美与人性之暗的恶斗就不可避免了。

《数学恩仇录》(这个典型的汉语词组来自译者的手笔，原文题目直译过来的话是"数学的大争论") 以"数学家的十大论战"为副标题。这十场厮杀里，既有不分胜负打个平手，也有明里败了一着，暗里功力更深，不过最令人浩叹的，却是两败俱伤，连数学本身也没有得到一丝好处。

套用武侠小说的说法，"牛顿 vs 莱布尼茨"就是类似于东邪西毒华山论剑这样的顶尖高手之间的过招。这是代表了人类最高智慧水平的两个头脑：《天才引导的历程》的作者、美国数学史学家威廉·邓纳姆说，"不论牛顿住

报刊链接

在哪里，哪里就是世界的数学中心”；同样的，也只有莱布尼茨这样的人物才配得上做牛顿的对手，“数学王子”高斯认为莱布尼茨在数学上拥有最高的才智。他们差不多同时发现了微积分这件对日后数学发展至关重要的武器，他们各自的追随者为了独占这一荣誉而掀起了旷日持久的争论。

作为当事人，牛顿和莱布尼茨一开始并没有掺合进去。美国著名数学史学家 E•T•贝尔说，在这场“数学史上关于优先权的最可耻的纠纷”的最初阶段，“两个人都从未怀疑过对方会从自己这里偷去关于微积分的哪怕一丁点儿的想法”。只是微积分的发明权与民族主义扯上关系之后，双方的拥趸都在叫嚣对方是个贼和说谎者，牛顿和莱布尼茨终于也不得不卷入了其中。他们默许甚至鼓励了那些不正当的攻击。

对于此事的真相，哈尔•赫尔曼说，后来研究者的基本共识是“尽管两个人都被指控有无礼和肮脏的行为，但他们都没有任何形式的剽窃”，也就是说，“他们在没有任何直接借用对方成果的情况下，独立地提出了各自的微积分”。我们只能说，这是一个伟大的巧合。牛顿和莱布尼茨仍然那么伟大，但是受到伤害的是数学，在牛顿死后的一个世纪中，顽固的英国人在数学上衰败了。

就牛顿和莱布尼茨个人来说，争端没有让他们受伤，这是令人感到安慰的。但是另一场论战却直接夺去了当事人的理智与健康。那就是可怜的康托尔。简单来说，这位创建了集合论的天才的工作之一是证明了有的无穷是可数的，有的无穷是不可数的，也就是说，同样是无穷，有的无穷 (比如说实数集) 比其他的无穷 (比如说有理数集) 在数量上更多。

这颠覆了我们的直觉！因此不难想象康托尔的革命性思想在 19 世纪 70 年代横空出世那会儿是何等的惊世骇俗，简直与众人初见错练《九阴真经》的欧阳锋一般，心中涌起的都是同一个想法：此人定是疯了。对数学持传统观点的数学家无法接受康托尔的发现，其中他以前的良师益友克罗内克尤其如此。克罗内克的信条是：“最深奥的数学研究的全部结果，最终都一定可以表示成整数性质的简单形式。”康托尔的无穷世界当然极大地冒犯了他的理念。这是错误而疯狂的，他必须捍卫正确的那一方。E•T•贝尔在《数学大师》里描述说，“他们吵翻了天，弃矜持而不顾，就差没把对方的喉咙切断了”。

于是康托尔被排挤在德国主流数学界之外，因为克罗内克在那里很有势力。可悲的是，长期的怀才不遇感与受迫害感使康托尔表现出妄想狂的倾向。他在四十岁时经历他的第一次精神崩溃，往后这种崩溃反复发作。1918 年，他因精神病发作再次住院期间死去了。这真是一个令人悲痛的结局。

在我看来，让人不那么难过的唯一一点是，人们在这个悲剧里是凭着“数学的良心”行事的。克罗内克不是专门对康托尔使坏，他只是认为康托尔的数学观念误入歧途了，就像我们今天对伪科学捋起袖子一样。但是在另一方面，这反倒更可悲了——请时刻记住，你奉行的真理没准是错的呢，你眼里的那个顽固分子没准是个殉道者呢；请勿以真理之名施行罪恶。

还是说点痛快的吧。1696 年，瑞士数学家约翰•伯努利 (他和他的哥哥雅各布•伯努利也是此书的一对较劲主角) 向欧洲的数学家们提出挑战。他的题目是“最速降线”问题 (具体内容就不讲了)。当时已经远离数学研究多年、正担任造币局局长的牛顿也接到了伯努利寄来的问题，54 岁的他在造币局工作一整天后筋疲力尽地回到家，但是他吃完晚饭就解决了这个问题。整个欧洲只有五个人给出了正确答案，约翰•伯努利在其中一封匿名回信上看到了英国的邮戳。据说他敬畏地说了一句话：“我从他的利爪认出了这头狮子。”

你看，这就是“整个数学史中最引人入胜的一则故事”(威廉•邓纳姆语)。它多像来自金庸小说的情节啊：少年凌厉的招数，宗师谈笑间就化解了。快意如此，一泯恩仇也罢。

（摘自《南方都市报》2009 年 09 月 22 日　文 / 费小马）

读者来信

Dear Editors,

I finished reading the whole first issue. Overall, I think it is a very good journal, and I believe it should have good market among scientific oriented people, from high school to college.

Surprised to see many familiar faces. Li Shangzhi was a Ph.D. student when I was a master student in the math institute of science academy. I thought he should be very old by now :) , didn't know he's still active. Really surprised to see Luo MaoKang there. He and I went to the same high school , and I knew him since then.

I find a typo in other people's article. Normally, I would not point it out, since it is not my article, and it is already out. However, this is important for a math related journal, and this may happen again and again if you don't watch out. On page 45, the third line from bottom, we see 210 = 1024. We all know this is 2^10 = 1024. The power charactor ^ dissappear. This is very common in HTML text and many other text format. You should really watch out for that. 210=1024 is easy to correct in our head, if it is ab = c instead of a^b = c, then, readers will be completely lost.

Thanks for the efforts.

Zhiping You

美国马里兰州

2010 年 6 月 7 日

尊敬的刘建亚、汤涛主编：

您们好！收到贵刊惠赠的《数学文化》创刊号，深感荣幸，深表谢意！

拜读赠刊，在《罗庚与省身》一文，再现了两位数学大师的生平事迹，展示了他们为人类数学事业作出的不朽功绩，以及大师之间纯洁而深厚的友谊，深深地让我感动；读《坐地日行八万里》，感受了近代数学在航天飞行中的应用，体现了数学知识的价值；《发达国家数学英才教育的启示》给了我有益的启迪，将在我的数学教学活动中发挥重要的指导作用……

在此，对贵刊表示衷心的祝福！祝《数学文化》越办越好！下面短诗，是我献给贵刊的一份心意，请笑纳！

读《数学文化》创刊号有感

数理天地奥秘多，
学问精深勤探索。
文以载道传真谛，
化作甘霖润新禾。

读者：王远征

于 2010 年 6 月 16 日端午节

读者来信

汤教授：

非常喜欢你写的关于冯康先生的文章，他是我敬重的人之一。也是我心怀感激的人之一。

可以想象他是如何在黑夜中一步步地走到计算中心去参加我们的婚礼，作我们的证婚人……

据说他大学时门门功课优秀， 就是体育不及格。为了毕业，有次曾请弟弟冯端代他考体育。

89 年夏天他到马里兰附近开会，应邀来我们在研究生宿舍的家。他非常随和，任凭我女儿在他身边窜来跳去。我们提出第二天带他到华盛顿地区去玩儿，他说你们忙，把我放到那里，四点半来接我就行了。差五分四点半我们来到华盛顿纪念碑旁早上把他放下的地点，不一会儿 , 就见冯先生斜挎个书包，从马路对面的人行道走过来。

二十多年过去了，这一幕仍深刻地印在我的脑海里。相比现在动用公款大吃大喝的旅游团，冯先生弱小弯曲的身躯显得多么伟大 !

Julie Zhu (美国韦恩大学)

2010 年 5 月 13 日

尊敬的 Global Science Press 的负责同志：

您好！数学杂志免费赠阅的样刊我已经收到，非常感谢，虽然订阅的原版期刊在这之前已经邮寄给我了! 很高兴能成为数学文化杂志创刊号的订阅者，我会成为贵刊的一名忠实的订阅者的，因为我对数学非常感兴趣，而且还是一名数学老师! 数学杂志的内容非常好，涉及面很广，有些给我很大的寓意。

另外, 我在阅读创刊号的时候，在45页下方有这样一句 “……总共可能组成210=1024种不同的序列……”， 似乎应该是“2的10次方=1024”， 也可能是我理解错误。

总之我会长期订阅《数学文化》的！最后祝《数学文化》杂志越办越好 !

辽宁建筑技术技术学院
基础部　数学教研室　冯大雨
2010 年 6 月 22 日

征订信息 >>

中国大陆

每期: 30元 (包含邮费)
全年: 100元 (包含邮费; 按期邮寄)
学生价 (学校集体订购; 20本以上) 价格如下:
每期: 16元 (包含邮费)
全年: 50元 (包含邮费; 按期邮寄)
联络人: 北京中科进出口有限责任公司
电邮: periodical@bjzhongke.com.cn
开户银行: 中国银行北京金宝街支行
银行帐户: 810907911408091001

中国大陆之外

每期: US$9 (包含邮费)
全年: US$30 (包含邮费)
电邮: info@global-sci.org
帐户信息: Bank name: DBS Bank (Hong Kong) Limited
Account number: 7881097250
Bank Code: 016
Branch Code: 478
Swift Code: DHBKHKHH
Account Name: Global Science Press Limited

樱花掩映的普林斯顿高等研究院的 Fuld Hall
刘建亚 摄

加入SIAM[工业与应用数学学会]
理由众多

工业与应用数学学会有超过13,000名学者分别来自数学，计算机，工程，物理和多个其他学科。SIAM会员由超过95个国家，工作在工业界，实验室，政府部分和研究机构的研究学者，教育工作者，实际工作者，学生组成。

SIAM热诚欢迎您的加入，欢迎您成为我们国际性、多学科社区的一员。

处于前沿
- 您可以定期收到SIAM Review期刊并且拥有权限进入从1997年以来此期刊的电子版本。SIAM Review每年出版 4 期，提供应用数学学科的整体概览。
- 您可以收到我们应用数学社区的新闻期刊SIAM News。
- 您可以收到SIAM的电子新闻通讯Unwrapped。
- 您可以注册收到任何SIAM期刊的内容提要。

参与帮助建设更强的应用数学和计算科学社区
- SIAM一直致力于提高对应用和工业数学及计算科学重要性的认知和鼓励青年学者加入本行业研究。您的加入将是对此事业的强力支持。
- SIAM是国际工业与应用数学会议(ICIAM)的创始会员并且是将于加拿大不列颠哥伦比亚省温哥华市召开的ICIAM 2011 会议的组织者之一。

在专业化的发展和认可中提升您的事业发展
- 在会议上，在SIAM职业信息网站，在SIAM职位发布公告栏，通过SIAM News新闻稿，您可以找到您需要的职业信息。
- 通过获得SIAM奖，得到SIAM资助，成为SIAM院士您可以得到同事和同行的认可。

充分利用网络的机会
- SIAM, AMS, MAA, AWM, AMATYC和MPS有超过53,000个会员。您可以使用这些协会的联合会员信息。
- 您可以网上加入17个SIAM活动小组(SIAGS)中的和您有共同研究兴趣的一个小组。
- 您可以网上参加您所在区域同行组织的活动。

购买SIAM 期刊和书籍的优惠
- 会员在购买SIAM书籍，期刊，电子期刊，SIAM Locus和其他SIAM产品时享受30%到95%的特殊折扣。

为您的学生找到更多资源
- 您可以推荐两个学生免费成为会员。
- 您可以告知您的学生SIAM提供免费和折扣入会资格，学生旅行资助，本科生网络出版物和学生分会。

现在加入
仅需70元人民币

立即加入：
www.siam.org/membership/individual/china.php
www.siam.org/joinsiam

中国大陆申请人可以通过SIAM在北京的联络人付人民币申请入会。
申请人需要填写完整的会员申请表格，用人民币支付会费给
林群院士
北京中关村东大街55号
中国科学院数学与系统科学学院　100190
电子信箱：siamchina@siam.org
办公电话：0086-10-62624806

There are lots of reasons to JOIN SIAM
The Society for Industrial and Applied Mathematics

Over 13,000 mathematicians, computer scientists, engineers, physicists, and a variety of other scientists belong to the Society for Industrial and Applied Mathematics. SIAM members are researchers, educators, practitioners, and students from over 95 countries working in industry, laboratories, government, and academia.

You are invited to join SIAM and be a part of our international and interdisciplinary community.

Stay Current
- Receive SIAM Review, a quarterly publication providing an overview of the entire field of applied mathematics including electronic access back to 1997.
- Receive SIAM News, the newsjournal of the applied mathematics community.
- Attend any of the many SIAM conferences each year at reduced member rates.
- Receive Unwrapped , SIAM's monthly electronic e-newsletter.
- Sign up for email Table-of-Contents alerts for any SIAM journal.

Help Create a Stronger Applied Math and Computing Community
- Support SIAM's efforts to increase awareness of the importance of applied and industrial mathematics and computational science and to encourage young scientists to pursue careers in the field.
- SIAM is a founding member of the International Council for Industrial and Applied Mathematics (ICIAM) and co-organizer of the ICIAM 2011 meeting in Vancouver, British Columbia, Canada.

Advance Your Career Through Professional Development and Recognition
- Get access to career information at meetings, on the SIAM career website, on the SIAM Job Board, and through SIAM News.
- Be recognized by colleagues and peers through SIAM Prizes, awards, and the SIAM Fellows Program.

Take Advantage of Networking Opportunities
- Use the online Combined Membership List, which includes over 53,000 members of SIAM, AMS, MAA, AWM, AMATYC, and MPS
- Join one of 17 SIAM Activity Groups (SIAGS) to network with professionals who share your research interests.
- Participate in section activities to network with peers in your geographic region.

Get Discounted Rates on SIAM Journals and Books
- Get special members-only rates—from 30% to 95% off list price—on SIAM books, journals, e-journals, Locus, and more.

Find Resources for Your Students
- Nominate two students for free membership.
- Tell your students about free and discounted memberships, student travel awards,SIURO, and student chapters.

Join for
as little as
70 RMB yuan

JOIN NOW:
www.siam.org/membership/individual/china.php
www.siam.org/joinsiam

Residents of China now have the option of joining SIAM through a liaison in Beijing so that they may pay in local currency. Send a completed membership application with payment in RMB yuan to:
Qun Lin
Zhongguancun East Road, **No.55**
Academy of Mathematics and Systems Science Chinese Academy of Sciences Beijing
P. R.China 100190
Email: *siamchina@siam.org* · Telephone: **0086-10-62624806** (office)