前排从左至右：张英伯，林亚南，刘建亚，汤涛；后排从左至右：丁玖，朱斌，罗懋康，顾沛，蔡天新，贾朝华，庄歌

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

主　编　刘建亚（山东大学）
汤　涛（香港浸会大学）

编　委　邓明立（河北师范大学）　蔡天新（浙江大学）
丁　玖（南密西西比大学）　项武义（加州大学）
贾朝华（中国科学院）　罗懋康（四川大学）
张英伯（北京师范大学）　顾　沛（南开大学）
张智民（韦恩州立大学）　林亚南（厦门大学）
宗传明（北京大学）

美术编辑　庄　歌

文字编辑　付晓青

特约撰稿人　游志平　欧阳顺湘　王　桥　靳志辉
蒋　迅　卢昌海　陈关荣　柳形上

《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

《数学文化》欢迎投稿，来稿请寄：
Math.Cult@gmail.com

本刊网站：http://www.global-sci.org/mc/
本刊淘宝网：http://mysanco.taobao.com/
本期出版时间：2013年11月

本刊鸣谢国家自然科学基金数学天元基金的支持

Contents | 目录

渊沉而静 流深而远

——纪念中国解析数论先驱闵嗣鹤先生

张英伯 刘建亚

100 年前的 1913 年 3 月 8 日，一个婴儿降生在北京城南的奉新会馆。这个孩子从少儿时代起就显露出与众不同的数学才华，在大学读书时，受到恩师的栽培与提携。之后到西南联大任教，担任陈省身和华罗庚的助手，1945 年起赴欧、美深造，成为卓有建树的数学家。1948 年回到祖国，继续研究工作并着力培养学生。七、八年后，正值壮年的他不得不停下他视之为生命的纯数学研究，转入应用数学领域。他积忧积劳成疾，仍然一如既往地工作着、努力着。1973 年 10 月 10 日，前一天还在为数字地震勘探解决数学问题的他于清晨溘然长逝，享年六十岁。他是闵嗣鹤，字彦群；他为我国解析数论的发展做出了重大贡献。

100 年后的今天，已经很少有人听说过这个名字；他走得太早，甚至没能看到数学研究重新回归社会的那一天。他们那一代数学家，已经随着逝去的时代渐行渐远。

我们写下这篇文字，只是为了纪念那一些不应该被忘怀的人们，为了还原那一段不应该被忘记的历史。

一、书香世家

闵家世居江西奉新，那是一个文化底蕴深厚的地方。奉新地界内的书院多达五十余所，这些书院始于南唐，终于清末；奉新因而教育发达，人才兴盛。几百年间，这个约占江西全省面积百分之一的小县，涌现出160多名进士，几百名举人。宋徽宗曾经专门赋诗，称赞胡氏兴办的华林书院："一门三刺史，四代五尚书。他族未闻有，朕今只见胡。"这些官员在晚年回到故乡，故乡的人们世世代代延续着耕读传家的生活。

闵家的祖上亦颇有一些书生通过科举考试走上仕途，官至节度使、尚书、员外郎等职。闵嗣鹤的祖父闵荷生20岁时加入了求取功名的行列，经过乡试、会试、殿试的层层筛选，于光绪二年（1876）被录取为恩科三甲进士。几位考官对他试卷的批语是："吐属不凡，气清笔健，语义精琢，简洁名贵"，这位24岁年轻人的命运从此改变。只是未曾料到，他走进去的是一座大厦将倾的晚清京城。闵荷生官及四品，曾任大名府知府，为人慷慨好义。在十九世纪末年，他响应康有为等人发起的戊戌维新运动，作为江西的两名代表之一，在"国会代表请愿书"上签字，"冒死奏闻"朝廷颁布议院法和选举法，召集国会实行"立宪"。他在1909年被选为江西咨议局议员，后入选中央咨议院，为江西六名议员之首。1912年，严复、闵荷生等七人在陈宝琛起草的《中华帝国宪法草案》上签名，出台了中国的第一部、但是从来未曾实施过的宪法。为了抵制日本攫取江西的南浔铁路，闵荷生曾倾囊投资，不料卷进了股东会复杂的纷争，一箱股票顷刻成为废纸，家道从此中落。闵荷生晚景萧索，隐居于北京宣武门外果子巷羊肉胡同的江西奉新会馆北馆。

闵嗣鹤的父亲闵持正体弱多病，在京师警察厅任职员。母亲郑锦棠出身于江西上饶的一个进士之家，知书达理，对于子女的教育以至科学实业救国自有一番理解。虽然家境拮据，不免靠典当和亲友接济维持，但世代书香门第，对孩子的教育从来不敢有丝毫松懈。

在闵嗣鹤四、五岁时，祖父刚过七十，尚有精力教他读书识字。小孙子也不辜负祖父的辛苦，由此渐通古籍，打下了深厚的文学功底。这个孩子眉清目秀，聪颖好学，恭顺知礼，天性仁厚，深得祖父疼爱；以至祖父不让他进小学读书，只在家中自学。而对于孙子的谦和、退让，祖父甚为嘉许。

奉新会馆南馆的甘仲陶夫妇没有子女，但是特别喜欢孩子，会馆里东西南北中馆的儿童都是他家常客。民国初年，已经终止了以四书五经为内容、以科举考试为目的的私塾；欧美的新式教育随着西学东渐而日益兴盛，各类学校蓬蓬勃勃地开办起来。有一天，闵嗣鹤在甘先生家里和上小学的孩子们一起玩耍，为他们解答了一道算术难题。甘先生见后大为惊奇和赞赏，他是会馆的理事兼会计，长于计算，便断定这个孩子是闵家的希望。邻居当中的小学生们很快拜服了这位从未进过校门的小老师，常拿课本给闵嗣鹤看，所以他虽然身在校外，却能够了解学校的课程。有一位萧姓表兄在北京读书，见他自学勤奋，也时常相帮。就这样，他渐渐地爱上了数学。他每天一个人悄悄地来到甘先生家中，自己读课本，做习题。这一片小小的自学园地，既使他心无旁骛，又使他愉快自如。闵嗣鹤于1925年12岁时考入北京师范大学附属中学，进入了他的少年时代。

坐落在城南和平门外的北京师大附中是当年北京城里最出色的中学，能够考进这个学校的学生或多或少有些功底。因为家境清贫，闵嗣鹤生活十分简朴，一年四季穿着母亲手制的布鞋。他的言谈举止颇有几分书卷气，加上古籍知识丰富，这个眉清目秀的少年被同学们戏称为"老夫子"。他喜欢素描，轻妙的小手画出禽鱼虫草，栩栩如生。他也喜欢排球，课后常和同学去操场玩上两局。他每天总是天傍黑才回家，到家就匆匆吃饭，紧接着誊写笔记，赶做繁多的作业。这样的日子过得紧张，生活也充

满趣味。他是师长们称赞的好学生，学校的各门课程他都学得很好，语文和英语尤其突出。但是在这三年当中，他的兴趣却逐渐地转向了数学。祖父依照自己读书的观点，殷切地希望他读中国文学。故而 1928 年升高中时，他考入了师大附中的文科班。

闵嗣鹤虽然孝顺，但骨子里是一个执着的少年，心中的爱好和追求不曾动摇。由于学非所愿，他在高中一年级的暑假对祖父托称要上大学读书，同时考取了北京大学的文预科和北京师范大学的理预科。继而他以用度较少，离家较近为理由，选择了和平门外的北京师范大学。过了很久，当祖父发现他竟然专攻数学，十分不以为然，他对孙儿说：“你们也想懂数学，你看看中国的《周髀算经》是何等深奥！”

二、恩师挚友

闵嗣鹤在大学时代

傅种孙

1929 年，北师大预科生闵嗣鹤向他的数学老师傅种孙请教一个组合问题：“五对夫妇围坐一圆桌，要男女相间而夫妇不邻，问有多少种坐法？”因为问题不在老师的授课范围之内，傅先生过了几天才给他解答。但是通过这件事情，先生已经发觉闵嗣鹤用心精细。

傅种孙先生 1898 年生于江西高安。他身材瘦小，有几分文弱，而双目炯炯，语音洪亮，出口成章，气度不凡。其父为晚清秀才，教他不少古籍。12 岁时父亲去世，遗嘱万般困难也不能让傅种孙辍学。傅先生在南昌读中学时特别喜欢几何，写过一篇关于轨迹的论文。1916 年中学毕业，因家贫无力升入大学，刚好公费读书的北京高等师范学校（北京师范大学的前身）在南昌招生，傅先生考取进入数理学部。他在大学期间十分活跃，曾任学校数理学会的会长，并在《数理杂志》上发表过多篇文章。1920 年傅先生毕业，留在北京高等师范学校附属中学（后来的师大附中）任教。一年之后，高等师范学校聘请他担任数理学部讲师。1923 年高等师范学校改名北京师范大学。1928 年冬，北京师范大学校方采纳学生意见，请傅种孙回到母校，担任数学系教授。从预科到大学，傅种孙为闵嗣鹤所在的班级任课五年，深知他是一个不可多得的数学人才。

赵慈庚

正当闵嗣鹤锐意进取之际，1930 年祖母与父亲相继去世，家庭断了经济来源，到了难以为继的地步。八十三岁的祖父要赡养，三个妹妹要读书，眼看母亲以一介妇人之力，冒着风雨寒暑，奔走柴米油盐，尚未成年的闵嗣鹤心事沉重。仁孝之心不许他再像以往那样，毫不记挂家事。为了节省开支，他每天走读，即便是冰天雪地，也要回家吃午饭，往返学校两次。闵嗣鹤在 1931 年升入北师大本科。为了缓解家庭的窘境，他从本科三年级开始在市内私立中学和北师大学生主办的群化预备学校兼课，作为家中刚刚成年的男子汉，和母亲一起挑起了六口之家的生活重担。

在上世纪三十年代，民国的大学颇为活跃。凡国家大事，学校存亡，校长更迭，都会在血气方刚的大学生中引起轩然大波。尤其对校长人选，学生间好恶不一，结派互相攻击。身在这喧哗浮躁的局势之中，闵嗣鹤选择了认真读书，科学报国。

同班二十余人，闵嗣鹤年龄最小，个头最矮，且面庞清秀，是同学们喜爱的小弟弟。这个小弟弟学业出众，聪颖过人，加之天性谦和，平实温良，大家都与他谈笑无忌。学习中有了疑问，便不约而同地找他求解。若是他正在研究的问题，三言两语便能点出要害，不是他正在研究的问题，也能给出满意的答复，所以全班人人佩服。甚至他读过的数学课本上对较难问题的批注和证明，都成为班里同学的借鉴。闵嗣鹤不仅读书用心，对周围事物亦独立思考，从不麻烦别人。他不像一般学生那样过多地依赖老师，也从不议论老师的短长，对每位老师都很

北京师范大学数学系 1935 届毕业生合影
傅种孙（前排左二）、赵慈庚（后排左四）、闵嗣鹤（第三排左四）

尊重。他特别积极地参加系里的学术活动，那时北师大数学系发行《数学季刊》，他不仅努力撰稿，还主动组稿，直至排版校对、封面设计，他都格外用心。

闵嗣鹤读大二时，就在傅种孙、范会国老师的指导下撰写了《根式和代数数及代数函数》的论文，毕业前又完成了一篇 98 页的论文《函数方程式之解法和应用》，发表在《师大月刊》上，他在该文的致谢中写道：本篇之作，是由于傅先生“那个题目的刺激，所以首先当感谢傅先生”。同学们料定他是未来的教授，便给他取外号为“教授”。在大学的这几年里，他既要钻研自己酷爱的数学，又要兼顾工作赚钱养家，无暇料理生活。他常常凝神书案，或读书，或演算，直至深夜，致使家人不能理解。三个妹妹看到他这种样子，就借当时的一部电影片名戏称他为“科学怪人”。一次同学来家，指着满案狼藉的数学算草，开玩笑说：“有纸皆算草，无瓷不江西。”他最要好的同学，也是他终生的挚友赵慈庚写过一篇《数学系班史》，给每个同学做了一、两句话的评价，谈及闵嗣鹤时是这样说的：“超逸绝尘者，闵教授也，所识独多，名曰字典；见闻出众，号称博士。”

1935 年，闵嗣鹤毕业于北师大数学系。以他的家庭状况，无疑不能离京别去。但是在北京谋得一个合适的职位极其不易。这时，惜才如命、急公好义的傅先生挺身而出，为闵嗣鹤留京工作四处奔走。师大附中作为全国最好的中学之一，教师都从师大最优秀的毕业生中挑选。但年年遴选，未免人满为患，因而进入附中难而又难。傅先生亲自邀请师大教务长、数学系主任、附中教务主任一起去见校长，他动情地说：“从我教书以来，没见过闵嗣鹤这样的好学生。请求学校给他一条进修的道路，无论如何要把他留在附中。这也是鼓励学生读书，振作校风的机会。”傅先生还对校长说：“附中教务主任韩桂丛先生慨然让出四节课时，希望学校批准，请闵君担任。”傅先生的请求得到了认可，这四节课的教职，成为闵嗣鹤一生立业的基础。为了养家糊口，他有一年接替赵慈庚在傅先生家做些抄写工作，每月可得 20 元润笔费。他还担任附中《算学丛刊》的编辑，并到私立中学兼课，成为家庭的顶梁柱。

清华大学杨武之教授是我国第一位在解析数论领域获得博士学位的学者。他在清华任教的二十年，是清华数学系人才辈出的二十年。杨先生在识别人才方面有过人的眼力，选才、育才堪称大家。华罗庚、陈省身都曾得益于杨先生的相知、相助和举荐、提携。闵嗣鹤是杨先生在师大兼课时的学生，杨先生发现了他的才华，与傅先生一起鼎力推荐他去清华工作。在大学毕业两年之后的 1937 年夏天，闵嗣鹤接到了清华大学请他担任数学系助教的聘书，一时喜出望外。这一聘任成为他走上数学研究之路的起点。

闵嗣鹤在接到聘书前后还写了一篇《相合式解数之渐进公式及应用此理以讨论奇异级数》的应征论文，在高君伟女士纪念奖金评选中获得第一名。他用奖金购买了许多书籍，后来又不远千里将这些书籍带到了西南联大，在资料匮乏的年代，对学校的教学与研究颇有助力。

非常不幸的是，聘书到手未满一个月，震惊世界的卢沟桥事件爆发了。霎时间，偌大的北京变成了混沌世界，人们纷纷向日军尚未占领的后方逃离。赵慈庚与同班同学赵文敏决定在八月初启程，行前他们对闵嗣鹤放心不下：闵嗣鹤一人支撑着母亲和三个妹妹的五口之家，没有任何积蓄；前不久钟爱他的祖父去世，入殓后与祖母和父亲的灵柩一起停放在法源寺内，兵荒马乱之中，尚未营葬。当他们找到闵嗣鹤说明去向时，闵嗣鹤难过地说：“你们走吧！该走。我怎办呢？有家呀！刚刚接到清华的聘书，未曾一登校门，就来了这样大的变乱，清华将往何处去？……”话语间凄然欲泪。赵慈庚说：“清华大学无论走到哪里，聘约不能失效，向着清华奔过去，应该不会落空。还有那三口灵柩，自然是件大事，但是在这非常时期，也不能过于执旧理了。”赵慈庚保管着行知社的一个存折，折上有活期存款 220 元，这是当年住校的几位同学每月凑一些钱，准备毕业后在京置房以便同学聚会的公款。这时赵慈庚把存折交到闵嗣鹤手中，

诚恳地说:“这钱你尽管用，由我完全负责。”三位同窗便依依不舍地告别了。

同窗走后，闵嗣鹤将灵柩埋葬在北京城外的江西义地，与恩师傅种孙一起带着两家人返回故乡江西。然后，傅先生随北京师范大学撤往西北，闵嗣鹤偕全家历尽艰辛从长沙乘火车到广州，再到九龙，经香港乘船到越南，辗转来到昆明。

三、联大八年

1938 年，闵嗣鹤终于在西南联合大学开始工作了。这是在抗日战争的非常时期由清华、北大、南开三所学校合成的大学，聚集了那个年代知识阶层的精英，曾经在我国的教育史上谱写过惊天地、泣鬼神的不朽篇章。

闵嗣鹤以助教微薄的薪水供养母亲和三位妹妹。他一到昆明就托亲友从银行给赵慈庚汇去 220 元欠款；可叹的是又过了四、五年以后，这笔当时可以买到三、四头牛的款项只够买三、四个烧饼了。战时物价飞涨，生活艰难。

尽管如此，闵嗣鹤在这里却如鱼得水。西南联大数学系是藏龙卧虎之地，为我国现代数学研究做出过奠基性贡献的华罗庚、陈省身、许宝騄都在这里工作，号称数学系“三杰”；清华、北大、南开三个数学系的系主任杨武之、江泽涵、姜立夫也在这里，联大数学系则先由江泽涵，后由杨武之负责。闵嗣鹤置身于一个前沿、开放的学术氛围之中。他为陈省身讲授的黎曼几何担任助教，与陈先生结下了终生的友谊，陈先生晚年在给他的题词中写到：“1938 年在昆明西南联大，我们曾对几何学有过共研之雅。”他为华罗庚组织讨论班，当年的学生徐利治晚年回忆：“有闵先生做他的助教，给他帮了不少忙。”华罗庚的“堆垒素数论”开讲时，慕名而来的学生很多，以至满堂座无虚席。之后听众一天天减少，减到最后只剩下四人听讲。又过了一个礼拜，四人减为两人，教室中剩下了师生三人上课。在昆明天天有日本飞机空袭的日子，这两个学生索性搬到华家附近，租屋而居，以便就近到他家里上课。这两个人就是闵嗣鹤与钟开莱。他们认真阅读了华罗庚的手稿，并帮他做了一些修正与改进。华罗庚的名著《堆垒素数论》原拟 1941 年在前苏联出版，后因二战搁置，直到 1947 年俄文版才得以面世，其中收入了华先生为 1941 年版所作的原序，写有感谢这两位数学家“对于本文手稿和准备都曾给予了帮助”的语句。

闵嗣鹤于西南联大

有一天空袭警报响过之后，日本飞机许久未到，华罗庚对家人说：“我到闵嗣鹤的防空洞去一下，跟他谈个问题，一会儿就回来。”不料华罗庚刚到闵家的防空洞里，日本飞机就过来了，向山谷间倾泻了一串串炸弹，刹那间黄土飞溅，震耳轰鸣，大树被炸倒了一片。有一颗炸弹刚好在防空洞的洞口附近炸开，黄土向着洞里铺天盖地飞来，将洞口淹没。幸亏洞里有一个人听到爆炸巨响后伸手抱住了头，这样他的头和手才没有被黄土埋住。于是他将每个人的脑袋先扒拉出来，但黄土把几个人的下半身压得紧紧的。赶来救援的华罗庚家人怕伤着他们，用手慢慢地刨，花了两三个小时，才把他们从土里

刨出来了。闵嗣鹤被刨出来时，长袍变成了短衫，正襟全被撕掉；华罗庚的耳朵震出了血，大家挨了一次活埋，总算死里逃生了。

闵嗣鹤对解析数论表现出浓厚的兴趣，迅速地进入了现代科研领域。尽管战火连天，空袭不断；尽管与世隔绝，资料奇缺，他仍然发表了7篇论文，除了1940年的第一篇是组合问题之外，后面6篇皆为数论，其中1941-44年与华罗庚合作4篇，1944-45年独立完成两篇。华罗庚在 *On the number of solutions of certain congruences* 一文底稿的扉页上写道："闵君之工作，占异常重要之地位。"

华罗庚与闵嗣鹤年龄相仿，他们亦师亦友，相得益彰。但两人合作多年，难免有些摩擦。华罗庚是一位数学天才，他刚强果断，说一不二，有时不大顾及他人的感受。闵嗣鹤兢兢业业，凭着深厚的数学功底，着力于解决合作文章的关键证明。尽管闵嗣鹤温文尔雅，但是骨子里却不失倔强，有时隐忍不住，几次撂挑子不干了。每当二人失和，杨武之便赶来调解，工作于是重新开始。几十年下来，两人分分合合，竟结下了生死相依、患难与共的情谊。在闵嗣鹤的追悼会上，华罗庚悲伤垂泪。

1944年夏天，数学系主任杨武之致信西南联大理学院院长吴有训（字正之）："正之吾兄大鉴：敬启者，算学系教员闵嗣鹤先生到校迄今夏已过七年，服务忠勤，研究有得，先后著成论文十余篇（目录及稿件附呈）。弟意欲请兄向校长提出，自今夏起，聘闵先生为专任讲师，是否有意，更新裁酌，顺颂时绥。弟杨武之。"

由于美国空军对日军飞机的歼击，昆明的空袭有所缓解，迁往外地的昆明中学得以恢复。随着大批学生到昆明求学，自1942年以来，昆明新成立了公立和私立中学30余所。其中的龙渊中学是北师大毕业生创办的，学生在黄土坡的土坯房中上课，在黄尘漫卷中晨读。很多联大师生风尘仆仆前来助学，一时间龙渊中学名师济济。闵嗣鹤住处距此不远，便联络几位青年教师课余义务为学生上课，开设数学讲座。他讲得次数最多，颇受学生欢迎。一位学生在很多年后回忆："闵嗣鹤在龙渊教平面几何与高等代数，教学语言精练、准确、严密，概念讲解明白，推理层层分明。许多数学难点能一语点化，使学生思路豁然开朗。"正如好友赵慈庚所言，闵嗣鹤有"乐育为怀"的胸襟，他不大计较物质的报酬与别人的称赞，而是欣慰于少年的成长。不然的话，这种无名无利的义务劳动，大多数人是不会争先去做的。

在母亲和兄长的抚育下，闵嗣鹤的三个妹妹在西南联大长大了。四兄妹按照数理化生进行学科分布，闵嗣鹤在数学系任教，大妹闵嗣桂1938年入西南联大化学系学习，后任助教。二妹闵嗣云聪慧异常，1936年考入北京大学物理系，在人才济济的同班同学中成绩优秀，颇有巾帼不让须眉之势，1943年毕业后在联大担任助教。三妹闵嗣霓先在联大化学系就读，后考入清华大学生物系。当时有人开玩笑说："联大理学院让你们闵家包了"。四个儿女的不凡表现，成为含辛茹苦的母亲最大的安慰与自豪。

陈省身早在1934年赴德留学，1936年25岁时获德国理学博士学位后，到法国师从数学大师嘉当（E. Cartan）研究微分几何，再赴美于普林斯顿高等研究院从事数学研究，在欧美游学五年。在1938年抗日战争的烽火硝烟中，陈省身毅然归国，应聘清华大学教授，来到西南联大。1943至45年陈先生应韦伯伦（O. Veblen）之邀再访普林斯顿，完成了他关于示性类的巅峰之作，成为国际数学界的学术翘楚。陈先生为人宽厚大度，颇有长者风范。他鼓励闵嗣鹤出国留学以开阔眼界，求得学术上的发展，闵嗣鹤深以为然。

随着妹妹们长大成年，家庭生活的重担不再由闵嗣鹤一个人承担。他在1944年初参加了第八届庚款留英考试，成为被录取的30名留学生之一。1945年10月，闵嗣鹤乘船前往英国。上世纪四十年代中叶，二战的硝烟刚刚散去，海上行船仍然颇有风险。一群怀抱科技救国梦想的留学生们坐在三等舱内，途经印度洋、大西洋，在时有季风、惊涛骇浪的海上颠簸，耗时月余方才抵达。闵嗣鹤来到牛津大学，师从梯其马希（E. C. Titchmarsh）研究解析数论，进入了国际上这一方向的学术中心。

四、学术家谱

哈代（左）与李特尔伍德于剑桥

1930 年代，华罗庚曾在剑桥访问，研究工作受到哈代(G. H. Hardy)学派的影响，回国后培养出了王元、陈景润等新一代数学家。王元著《华罗庚传》对此有详尽的介绍。

如果编纂一个学术家谱，我国在解析数论领域师承哈代与梯其马希的一支可以这样排列：

—— 哈代
—— 梯其马希
—— 闵嗣鹤
—— 迟宗陶、尹文霖、邵品琮、潘承洞、潘承彪
—— 张益唐等等……

闵嗣鹤受哈代学派嫡传，学术猛进，回国后又努力提携后学，可谓“裕后光前”。为了讲清闵嗣鹤的学术渊源与学术贡献，我们选择了家谱式的叙述方法。

1. 第一代：哈代。在数论历史上，哈代堪称为一位领袖数学家。他与李特尔伍德（J. E. Littlewood）合作，在许多数论问题的研究中做出了开创性的贡献，而且二人的合作也被称为科学合作的典范。在此，仅举与本文内容相关的两个贡献。

哈代的第一个贡献事关黎曼 zeta 函数。众所周知，黎曼 zeta 函数是打开素数宝藏大门的钥匙，zeta 函数的零点分布对素数分布有着决定性的影响。黎曼已经知道，zeta 函数有无穷多个非显然零点，这些零点散布于临界带形之内；这里的临界带形是指复平面上实部介于 0 与 1 之间的竖直带形。著名的黎曼猜想是说，zeta 函数的所有非显然零点都应该落在临界直线上，即临界带形的中轴线上。黎曼手算了 3 个零点，其实部都等于 $\frac{1}{2}$. 哈代第一次证明了，黎曼 zeta 函数有无穷多个零点落在临界直线上。他又与李特尔伍德合作，推进了落在临界直线上的零点的密度。

哈代与本文有关的第二个贡献，是关于哥德巴赫猜想的研究，这是与李特尔伍德合作完成的。在他们系列文章的序言中，哈代与李特尔伍德自豪地宣称，这是历史上关于哥德巴赫猜想的第一次严肃研究；言下之意，此前虽然有很多名家致力于这个猜想，但都是不严肃的。在文章中，他们不但提出并发展了著名的圆法，还提出了许多著名的猜想。例如 k 生素数猜想：若非负整数 $a_1, a_2, \cdots, a_k$ 满足明显的必要条件，则多项式

$$x+a_1, x+a_2, \cdots, x+a_k$$

同时表示素数无穷多次。注意，若取 $k=2$，而 $a_1=0, a_2=2$，则这就是孪生素数猜想。

2. 第二代：梯其马希。梯其马希是哈代的入室弟子，致力于解析数论的研究。1931 年起，梯其马希任牛津大学 Savilian 讲席教授（Savilian Professor of Geometry）。能够担任这个职位的人尽皆英才；例如，梯其马希的前任是哈代，而继任者则是赫赫有名的阿提亚（M. Atiyah）。

梯其马希是黎曼 zeta 函数研究领域举足轻重的权威，他的专著《黎曼 zeta 函数论》(*The theory of the Riemann zeta-function*）初版刊印于 1951 年，后来几经再版，至今仍是本领域排名第一的重要著作。关于这本经典著作，

梯其马希

萨纳克（P. Sarnak）曾经评价说："如果我被流放到孤岛上，而且只允许我带一本关于 zeta 函数的书，那么无疑我会带梯其马希这本。"

3. 第三代：闵嗣鹤。 庚款考试后，闵嗣鹤被牛津大学艾克赛特学院（Exeter College）录取，师从梯其马希。闵嗣鹤于 1945 年底到达，1947 年获得博士学位，其博士论文将近 200 页，主要研究黎曼 zeta 函数，特别是 zeta 函数在临界直线上阶的增长，即所谓的林德洛夫（Lindelof）猜想。

1947 年，经梯其马希推荐，闵嗣鹤接受齐格尔（C. L. Siegel）邀请，赴美国普林斯顿高等研究院从事学术研究，为时一年。普林斯顿高等研究院始建于 1930 年，数学所是该院首个成立的研究所，以爱因斯坦（A. Einstein）的加入为标志，数学所满编制教授人数为 8 人。闵嗣鹤在高等研究院工作期间，数学所教授除爱因斯坦、齐格尔之外，还有外尔（H. Weyl）、哥德尔（K. Godel）、冯 • 诺依曼（J. von Neumann）；这几位全是领袖科学家。高等研究院尤其重视数论研究，其数学所一直是世界数论研究的中心；数学所的 8 位教授中，经常有两三位是数论家。当然，高等研究院的访问学者之中也不乏大家，下文将提到的塞尔伯格（A. Selberg）也是 1947 年到达数学所，而且也是受到齐格尔的邀请。

在普林斯顿，闵嗣鹤参加了外尔的讨论班，取得了丰富的研究成果。外尔真诚地挽留他继续在美工作，梯其马希则热情邀请他重返英国。但是，报效祖国、思念慈母的赤子之心促使他立即回国。1948 年秋，他回到清华大学数学系执教，初任副教授，翌年晋升为教授。1952 年院系调整，闵嗣

1947 年牛津大学毕业合影，第三排左一为闵嗣鹤

1947-1948 年，闵嗣鹤在普林斯顿高等研究院工作期间，摄于 Fuld Hall

鹤调任北京大学数学力学系教授。

3.1. 闵嗣鹤与林德洛夫猜想。林德洛夫猜想是说，对任意的 $\varepsilon>0$，估计式

$$\varsigma(\tfrac{1}{2}+it)=O(|t|^{\varepsilon})$$

对所有 $|t|>2$ 成立。这是一个极其困难的猜想，特别地，它是黎曼猜想的推论。利用函数论的一般方法可以证明，对任意的 $\varepsilon>0$，估计式

$$\varsigma(\tfrac{1}{2}+it)=O(|t|^{\frac{1}{4}+\varepsilon})$$

对所有 $|t|>2$ 成立。这里的 $\frac{1}{4}$ 被称为凸性上界，或者平凡上界。将 $\frac{1}{4}$ 用更小的常数替代，所得结果叫做亚凸性上界。亚凸性上界在数论中有众多重要的应用，因此一直是数论研究的热点。黎曼 zeta 函数的第一个亚凸性上界，由外尔于 1921 年得到。外尔所用的方法，在指数和理论中是一个比较自然的方法；因此超越外尔，将有重要意义，当然也需要有哲学上的新观察以及方法论上的创新。

闵嗣鹤在博士学位论文中，将 zeta 函数的凸性上界 $\frac{1}{4}$ 削减为亚凸性上界

$$\frac{15}{92}.$$

请注意，$\frac{1}{7}<\frac{15}{92}<\frac{1}{6}$. 这篇论文 1949 年刊于《美国数学会汇刊》(*Tran. Amer. Math. Soc.*)。这个亚凸性上界，源于闵嗣鹤在二维指数和

$$\sum_{m,n} e^{2\pi i f(m,n)}$$

估计方面的创新，而这个创新在别的场合也

高等研究院 Fuld Hall 雪景（刘建亚摄）

1950 年代，闵嗣鹤（左一）与华罗庚（左四）等合影

有深刻的应用。值得指出的是，经过众多数学家的努力，闵嗣鹤的亚凸性上界不断被改进，但是现在的世界纪录仍然大于 $\frac{1}{7}$.

3.2. 闵嗣鹤与黎曼猜想。二战期间，塞尔伯格蜷缩在挪威的一角，艰难从事着数学研究，并且得到了震惊世界的定理：黎曼 zeta 函数落在临界直线上的零点具有正密度。设 $N(T)$ 表示临界带形之内虚部不超过 T 的零点总数，而 $N_0(T)$ 表示落在临界直线上虚部不超过 T 的零点总数，则黎曼猜想就是说，对所有 T 都有

$$N_0(T) = N(T).$$

使用这些记号，塞尔伯格的定理可以更加精确地叙述为：存在一个正常数 c，使得对所有 T 都有

$$N_0(T) > cN(T).$$

这大大推进了哈代与李特尔伍德的前述结果。二战一结束，塞尔伯格的成果迅速传播开来，得到了国际同行的重视；这也是塞尔伯格获得菲尔兹奖的两个重要结果之一。但是，塞尔伯格并没有给出这个常数 c 的具体数值。

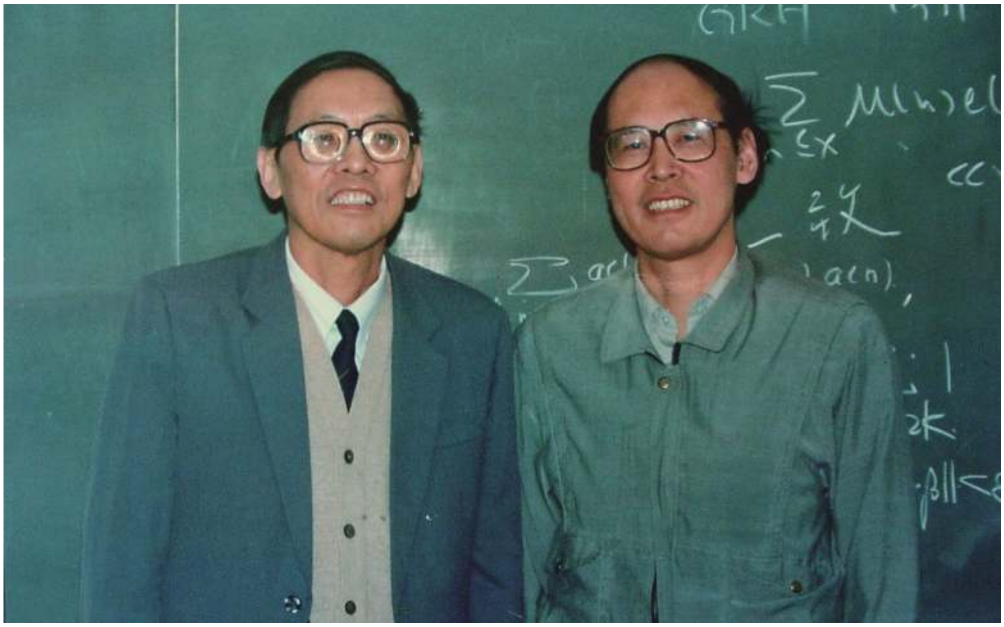
闵嗣鹤第一个定出了塞尔伯格定理中 c 的可允许数值。闵嗣鹤证明了

$$c = \frac{1}{60000}$$

是可以允许的。不要小看这个常数；从闵嗣鹤的这个常数开始，人类开始准确地知道，我们距离黎曼猜想到底有多远。这项工作，是闵嗣鹤在普林斯顿时期就开始研究的，最后在国内完成，论文刊于《北京大学学报》。

1980 年代，康瑞（B. Conrey）证明了 $c > 0.4$, 从而 zeta 函数 40% 以上的零点落在临界直线上。现在最好的纪录是冯绍继的 $c > 0.41$. 参见本期《数学文化》读者来信栏目。

1970 年代以来轰轰烈烈发展的朗兰兹纲领，其研究基石是各种各样推广了的 zeta 函数，即自守 L 函数。对这些丰富多彩的 L 函数来说，都有广义黎曼猜想与广义林德洛夫猜想。遗憾的是，关于黎曼 zeta 函数的塞尔伯格定理，只被成功推广到了一些相对简单的 $GL(2)$ 自守 L 函数；而对绝大多数自守 L 函数而言，根本就没能证明相应的哈代定理，即无限多个零点落在临界直线之上。关于自守 L 函数的林德洛夫猜想，结果也是寥若晨星；到目前为止，只得到了某些 $GL(2)$，$GL(3)$ 以及 $GL(4)$ 的自守 L 函数的外尔型亚凸性上界。闵嗣鹤形式的精确上界，则是完全没有得到。



1995 年潘承洞（左）与潘承彪合影（展涛摄）

4. 第四代以及第五代：闵嗣鹤的弟子与再传弟子。在清华大学，闵嗣鹤指导迟宗陶研究解析数论。利用闵嗣鹤关于 zeta 函数亚凸性上界的思想，迟宗陶改进了经典的狄利克雷除数问题的余项，所得到的新指数小于 $\frac{1}{3}$. 在北京大学，闵嗣鹤的研究生有尹文霖、邵品琮、潘承洞。潘承洞的胞弟潘承彪，年级稍低，但也得到了闵嗣鹤的指导。

张益唐（叶扬波摄）

尹文霖、邵品琮从北京大学毕业后，分别到四川大学、曲阜师范大学任教。潘承洞从北京大学研究生毕业以后，到山东大学任教；而潘承彪则从北京大学到北京农机学院（现中国农业大学）任教，文化大革命结束以后，开始在北京大学指导数论方向的研究生。

在闵嗣鹤指导下，潘承洞本科时期就研究了著名难题——算术级数中的最小素数。经典的狄利克雷（P. G. L. Dirichlet）定理是说，若 $(a, q) = 1$，则在算术级数

$$a + q,\ a + 2q, a + 3q, \cdots$$

中有无穷多的素数。一个自然的问题是：这个级数中的第一个素数 $P(a, q)$ 出现在什么位置？前苏联的领袖数学家林尼克（Yu. V. Linnik）证明了，存在一个常数 L，使得

$$P(a, q) = O(q^L).$$

这个常数 L 被成为林尼克常数。林尼克并没有给出这个常数的具体数值；确定林尼克常数 L 具体数值，是一件困难的工作，因为 L 依赖于推广了的 zeta 函数的零点分布结果。在闵嗣鹤指导下，潘承洞得到了林尼克常数的第一个可允许的数值 $L = 5448$. 经过许多数学家承前启后的工作，1992 年英

国数学家希斯 - 布朗（D. R. Heath-Brown）得到了 $L = 5.5$；到本世纪，这个结果又稍有改进，现在最好的纪录是 $L = 5.18$. 从这个工作中，以及从潘承洞后来关于哥德巴赫猜想（1 + 5）的工作中，都不难看到闵嗣鹤的哲学与精神。这就是传统的力量。

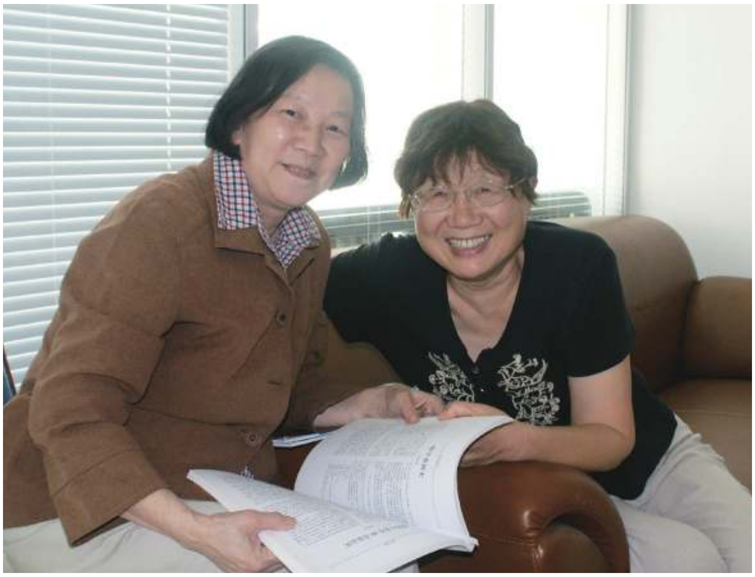
闵嗣鹤的再传弟子，大多出自潘氏兄弟门墙。潘氏兄弟倾其心力，培养的硕士、博士计有 30 余人，其中的大多数仍在从事数论及其应用领域的研究。

张益唐早年师从潘承彪，是闵嗣鹤再传弟子的杰出代表。最近他证明了，存在无穷多对相邻素数，其间隔不超过 7 千万。关于张益唐生平与工作的全面介绍，请参看汤涛《张益唐与北大数学 78 级》，刊于《数学文化》2013 年第 3 期。把张益唐定理中的 7 千万换成 2，就得到孪生素数猜想的证明。7 千万这个数字，貌似巨大，但是它只是一个固定的常数，因此与 2 并无哲学上的差别；况且，张益唐的论文公布之后，这个数字不断被削减。

克隆尼克（L. Kronecker）说：“自然数是上帝给的，而其他全是人造的。”如此说来，孪生素数猜想无疑是“上帝的猜想”。张益唐的结果，是对孪生素数猜想的决定性贡献。闵嗣鹤乃至哈代，若于仙界有知，必大感欣慰！为人师者，有一二徒子徒孙如此，夫复何求？

待续

本文作者采访闵乐泉（中）



本文作者采访赵藉丰（左）

作者简介：

张英伯，北京师范大学教授，《数学文化》编委。

刘建亚，山东大学教授，闵嗣鹤的再传弟子，《数学文化》联合主编。

致谢：本文写作素材取自作者对赵藉丰、闵惠泉、闵乐泉、潘承彪、严士健、李忠、王元诸位老师的依次采访，以及闵惠泉、赵慈庚关于闵嗣鹤先生的文章，和王元著述的相关情节。此外，本刊编委罗懋康、贾朝华对本文的命题及部分细节均提出了中肯的建议，在此一并致谢。

中国古代最伟大的数学家刘徽

——为纪念刘徽注《九章筭术》1750周年而作

郭书春

中国古代最伟大的数学家不是祖冲之吗？怎么会是刘徽呢？祖冲之（429-500）确实是伟大的数学家，应该说，他的数学水平不会低于刘徽。但是他的数学著作《缀术》(一作《缀述》)由于隋唐最高数学学府算学馆的学官“莫能究其深奥”，因而失传。因此其全部数学贡献人们至今无法了解。我们现在仅知道他的两项确切成就：将圆周率精确到8位有效数字以及与他的儿子祖暅之完成的球体的体积公式的推导。这两项成就都是刘徽为其提出方法或建立理论基础的。从数学的角度而言，这当然比祖冲之的贡献更重要。

中国科学院系统科学研究所于1985年10月举办了现代数学讨论班，要以一位伟大的数学家冠名。许多学者主张称为祖冲之讨论班，吴文俊院士力排众议，主张以刘徽命名。吴先生认为，刘徽无可争议地是我国传统数学中唯一的代表人物。

刘徽以演绎逻辑为主要方法全面证明了《九章筭术》的算法，建立了中国传统数学的理论体系。最值得称道的是他在世界数学史上第一次将无穷小分割方法和极限思想用于数学证明。刘徽逻辑之严谨，所达到的高度，在中国古代也无居其右者。可是，在上世纪70年代末以前，中国数学史界对刘徽没有给予应有的重视。其原因主要是刘徽注十分难读，其最重要成就，中国人或者以为弄通了，实际上搞错了，比如割圆术；或者根本没有搞懂，比如刘徽原理；或者没有涉及，比如刘徽关于“率”的理论和刘徽的逻辑思想。加之，它以为《九章筭术》作注的形式出现，很容易被误以为依附于《九章筭术》，因而导致把刘徽看成是一位二流的数学家。

上世纪70年代末至90年代出现了研究《九章筭术》及其刘徽注的高潮，对《九章筭术》的编纂和体例，刘徽的主要成就，刘徽的思想，产生刘徽注这样划时代著作的社会背景，以及《九章筭术》的版本基本上弄清楚了，对《九章筭术》的校勘也有重大进展。

《九章筭术》——中国传统数学框架的确立

刘徽是为《九章筭术》作注而名垂青史的。我们平日所说的《九章筭术》有狭义与广义两种涵义。狭义地说，仅指《九章筭术》本文。谈成就、编纂、体例等，常用这种涵义。广义地说，还包括魏刘徽注、唐李淳风等注释。谈版本、校勘等常用这种涵义。

《九章筭术》的体例和编纂

学术界一种流行的看法是把《九章筭术》说成一部“一题、一答、一术的应用问题集”，甚至说“概莫能外”。但这是一种似是而非的说法，而且会引起许多误解，往往成为中国古代数学没有理论的根据。但是，只要打开《九章筭术》，就会发现这并不符合《九章筭术》的实际情况。实际上，《九章筭术》的题、答、术的关系相当复杂。下面简要叙述。

《九章筭术》大部分内容采用算法统率例题的形式，往往是多题一术或一题一术，甚或多题多术。这里又有不同的情形：(i) 给出一个或几个例题，然后给出一条或几条抽象性术文，而例题中只有题目、答案，没有具体演算的术文。整个方田章、商功章的大部分内容以及粟米、少广、均输、盈不足、勾股章的部分内容，都属于这类情形，共有 73 术，106 道例题。(ii) 先给出抽象的术文，再列出几个例题；而例题只有题目、答案，亦没有演算细草。商功章的堑等、刍童等 2 条术及其 10 道例题便是如此。(iii) 先给出抽象性的总术，再给出若干例题；而例题包含了题目、答案、术文三项，其术文是总术的应用。方程章及粟米、衰分、少广、盈不足章的部分共 7 术 80 个例题是如此。

以上三种情形共 82 术，196 问，约占《九章筭术》全书的 80%。我们将之称为算法（术）统率例题的形式。尽管其间的表达方式有差异，却有几个共同特点：术文都非常抽象、严谨，具有普适性，换成现代符号就是公式或运算程序；在这里抽象性术文是中心，是主体，题目是作为它的例题出现的，是依附于术文的，而不是相反；这些术文具有构造性、机械化。

另外还有一少部分内容采取应用问题集的形式，往往是一题、一答、一术，共有 50 个题目，都是以题目为中心。尽管计算程序是正确的，但都是应用问题的演算细草。

值得注意的是，《九章筭术》的这些体例，在近年发现的秦简《数》、秦简《筭书》、汉简《筭数书》等秦汉数学简牍中全都有。《九章筭术》和秦汉数学简牍的内容大多数都是完成于秦和先秦的。因此，这反映了秦和先秦数学的共同特点。

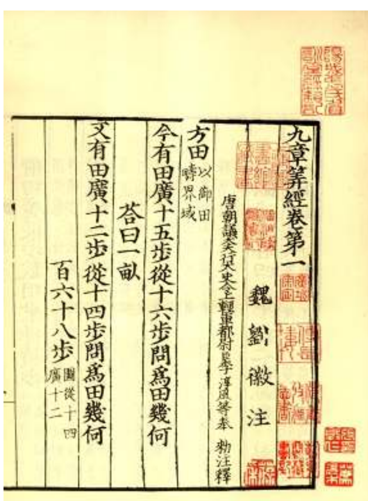

九章筭經卷第一
魏劉徽注
唐朝議大夫行太史令上輕車都尉臣李淳風等奉勑注釋
方田以御田疇界域
今有田廣十五步從十六步問爲田幾何
荅曰一畝
又有田廣十二步從十四步問爲田幾何
百六十八步

图 1《九章筭术》书影（南宋本）

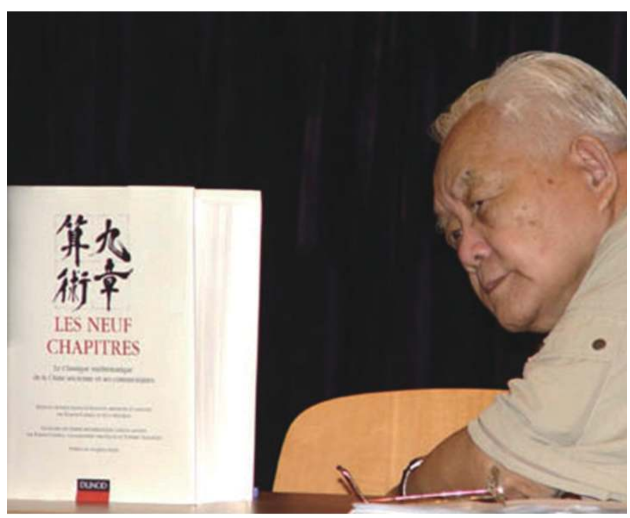


图 2 吴文俊院士在中法对照本《九章筭术》的新闻发布会上

很显然，笼统地将《九章筭术》称为“一题、一答、一术的应用问题集”是不合适的。笔者认为，数学史上起码存在三种不同体例的著作，一是像欧几里得《几何原本》那样的公理化体系，一是像希腊的丢番图的《算术》、中国的《孙子筭经》、《五曹筭经》等那样的应用问题集，一是以《九章筭术》的主体部分为代表的以算法为中心，算法统率例题的形式。

《九章筭术》的体例多种多样，表明它肯定不是一人一时编写的，而是经过许多世代，若干人的劳动积累而成的，这是学术界的共识。然而，到底是什么时候编纂的，却存在不同的看法。现存资料中最早谈到《九章筭术》编纂的就是本文所要谈到的刘徽。他说：

周公制礼而有九数，九数之流则《九章》是矣。往者暴秦焚书，经术散坏。自始厥后，汉北平侯张苍、大司农中丞耿寿昌皆以善算命世。苍等因旧文之遗残，各称删补。故校其目则与古或异，而所论者多近语也。

事实证明，刘徽关于《九章筭术》编纂的论述是最准确的。也就是说，在先秦已经存在某种形式的《九章筭术》，它在战乱中遭到破坏。西汉张苍（？- 前 152 年）、耿寿昌（公元前 1 世纪）搜集遗残，加以删补，编定了《九章筭术》。

《九章筭术》的内容和成就

《九章筭术》分九章。第一章方田，刘徽说“以御田畴界域”，解决田地面积问题，给出若干直线形、曲线形的面积的抽象公式。更重要的，提出世界上最早的系统、完整、抽象的分数四则运算法则。第二章粟米，刘徽说“以御交质变易”，解决粟米互换问题。提出十分抽象的“今有术”，即比例算法。此法在后来的印度和西方称为三率法。第三章衰分，刘徽说“以御贵贱禀税”，用“衰分术”、“返衰术”解决比例分配问题。后半章不是衰分问题，而是贸易、取保、贷钱等应用题，应该用今有术求解。第四章少广，刘徽说“以御积幂方圆”，解决面积、体积的逆运算问题。提出了世界上最早的开平方、开立方的抽象程序。第五章商功，刘徽说“以御功程积实”。此章的本义是解决土方工程中工作量的分配问题，但现今人们更重视其中的若干多面体、圆体的抽象的体积公式。第六章均输，刘徽说“以御远近劳费”，解决赋税中的合理负担问题，是更为复杂的衰分问题。后半章是各种算术难题。第七章盈不足，刘徽说“以御隐杂互见”，解决盈亏类问题，并用盈不足术，通过两次假设解决了若干一般数学问题，在世界数学史上影响巨大。第八章方程，刘徽说“以御错糅正负”。“方程”即现今线性方程组。此章提出了世界上最早的线性方程组解法，“正负术”即正负数加减法则，以及列“方程”的方法“损益”法。第九章勾股，刘徽说“以御高深广远”，提出了抽象的“勾股术”即勾股定理，给出了解勾股形的各种方法和世界上最早的勾股数组通解公式，以及勾股容圆和简单测望等问题。

以上许多成就超前其他文化传统几个世纪甚至上千年。

《九章筭术》历来被尊为算经之首，明中叶至清中叶的数学家已经看不到《九章筭术》，许多数学著作的标题却都有“九章”或“九数”二字，或以“九数”分类。甚至在西方数学传入之后，还有人将以西方数学为主体的内容按“九数”分类，著书立说。

另一方面，为《九章筭术》作注是中国传统数学著作的重要形式，成为中国传统数学成就的重要载体。其中成就最大的是魏刘徽的《九章筭术注》，北宋贾宪的《黄帝九章算经细草》。它们分别奠定了魏晋南北朝与宋元两个数学高潮的基础。《九章筭术》还传到朝鲜、日本和东南亚，成为这些地区数学知识的源泉。《九章筭术》在东方数学中的地位，大体相当于欧几里得《几何原本》在西方数学中的地位。《九章筭术》与《几何原本》像两颗璀璨的明珠，在古代东西晖映。

《九章筭术》的成书之时，正值古希腊数学越过其高峰，走向衰替之际。《九章筭术》的问世标志着中国及后来的印度、阿拉伯地区取代古希腊成为世界数学研究的重心，也标志着世界数学从研究空间形式为主，转变为以研究数量关系为主，标志着数学机械化算法体系取代数学公理化演绎体系成为世界数学发展中的主流。

我们在表彰《九章筭术》的成就的同时，不能忽视它的缺点。首先就是《九章筭术》没有任何数学定义，也没有任何推导和证明。当然，这并不是说《九章筭术》在提出这些算法时没有某种形式的推导。其次，受儒家传统思想的束缚，《九章筭术》没有突破“九数”的限制。这一方面使九章的分类不尽合理，有的按应用分类，有的按数学方法分类，标准不同一。另一方面，对当时提出的许多新问题，编纂者未能与时俱进，打破“九数”的格局，设置新的类别，而是将一些题目硬塞入衰分章和均输章，不伦不类。

刘徽及其《九章筭术注》《海岛算经》

刘徽生平不详。笔者根据《宋史•算学祀典》及有关史料断定，刘徽的籍贯是淄乡，属今山东邹平县。他自述“徽幼习《九章》，长再详览”。根据《晋书•律历志》、《隋书•律历志》记载，刘徽于魏景元四年（公元 263 年）撰《九章筭术注》，今年恰好是 1750 周年。国内外的学者在邹平成功举行了国际学术研讨会。

刘徽的思想受何晏（？ -249）、嵇康（223-262）、王弼（226-249）等玄学名士的影响较大，甚至有许多语句相类。由此，我们可以推断，刘徽的生年大约与嵇康、王弼相近，或稍晚一些，就是说，刘徽应该生于公元 3 世纪 20 年代后期至公元 240 年之间。换言之，公元 263 年他完成《九章筭术注》时，年仅 30 岁上下，或更小一点。有的画家将正在注《九章筭术》的刘徽画成一位满脸皱纹的耄耋老人，有悖于魏晋的时代精神和特点。

《九章筭术注》原十卷，第十卷“重差”系自撰自注，后来以《海岛算经》为名单行，因第 1 问是测望一海岛高、远，故名。其宋刻本已亡佚，今传本是清戴震从《永乐大典》辑录出来的，只有 9 问，且无刘徽自注。刘徽还有《九章重差图》一卷，已佚。

《海岛算经》将以重差术为主的中国测望技术发展得相当完善，在西方测望技术于明末传入中国之前，再无大的突破。图 4 是测望海岛示意图。刘徽测望海岛的原型可能是泰山。

尽管对刘徽的生平我们知之甚少，但是由于他的《九章筭术注》比较完整地保存下来了，因此对他的思想品格，却是明末之前的数学家中我们了解最多的一位。刘徽博览群书，精心研究了墨家、儒家、道家等先

图 3 纪念刘徽注《九章筭术》1750 周年国际学术研讨会主席台

图 4 刘徽测望海岛示意图

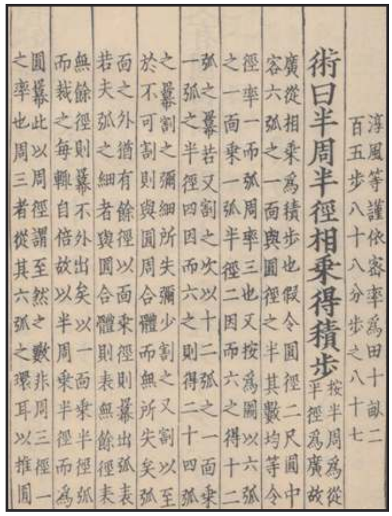

淳風等謹依密率爲田十畝二百五步八十八分步之八十七
術曰半周半徑相乘得積步 按半周爲從半徑爲廣故
廣從相乘爲積步也假令圓徑二尺圓中容六弧之一面與圓徑之半其數均等令
徑一率三也又按爲圖以六弧之一面乘一弧半徑二因而六之得十二
弧之冪若又割之次以十二弧之一面乘一弧之半徑四因而六之則得二十四弧
之冪割之彌細所失彌少割之又割以至於不可割則與圓周合體而無所失矣弧
面之外猶有餘徑以面乘徑則冪出弧表若夫弧之細者與圓合體則表無餘徑表
無餘徑則冪不外出矣以一面乘半徑弧而裁之每輒自倍故以半周乘半徑而爲
圓冪此以周徑謂至然之數非周三徑一之率也周三者從其六弧之環耳以推圓

图 5 刘徽割圆术书影（南宋本）

秦诸子的著述，以及司马迁、王充、郑玄等两汉学者的著作。他受思想界的正始之音（240-248）和此后的辩难之风的深刻影响，善于从其中及在辩难中泛起的先秦诸子、两汉典籍中汲取大量的思想资料，或者以某些命题作外壳，加以改造，融会贯通，赋予数学内容，得出正确或比较正确的结论，或者撷取其正确部分指导自己的数学研究。他的深邃的思想方法和数学理论蕴含着对传统文化的深刻理解。

坚持实事求是，一切从实际出发，是刘徽治学的重大特点。整个刘徽注言必有据，不讲空话。历来有“隶首作数”的说法，刘徽说“其详未之闻也”。汉代盛行谶纬迷信，出现数字神秘主义，大科学家张衡也未能免俗，刘徽批评他是“欲协其阴阳奇耦之说而不顾疏密矣”。刘徽把自己的数学知识和创造完全建立在必然性基础之上，没有任何猜测或神秘的成分。

刘徽认为人们的数学知识是不断进步的，他不迷信古人。《九章筭术》最迟在东汉已被官方奉为经典，刘徽为之作注，自然对之很推崇。但他并不妄从，指出了它若干不准确之处甚或错误。刘徽是在中国数学史上批评《九章筭术》最多的数学家。

敢于创新，是刘徽治学的突出特点，这是他实事求是精神的升华。刘徽《九章筭术注》的创新非常多。在一部著作中，新的思想、新的方法、新的成就这么多，在中国数学史上是少见的。

刘徽还具有知之为知之，不知为不知，不图虚名，敢于承认自己的不足，寄希望于后学的高尚品格。他对自己设计的牟合方盖，功亏一篑，没能求出其体积，便老老实实地承认：“欲陋形措意，惧失正理，敢不阙疑，以俟能言者。”反映了一位真正的科学家的光辉本色。

刘徽还善于灵活运用数学方法，指出不弄通数学原理，“徒按本术”，是“胶柱调瑟”，就像把琴瑟的弦的转柱胶住而要调节弦的音律。他常常在《九章筭术》的术文之外，提出另外的方法，或者对《九章筭术》的同一条术文，记下不同的思路。有时候他明知自己提出的新方法不如原来的方法简便，为什么还要提出呢？他说：“广异法也。”要广开思路。

《九章筭术注》的结构和成就

刘徽的《九章筭术注》是不是全都反映了刘徽的思想呢？学术界实际上存在着不同意见。刘徽自述注《九章筭术》的过程时说：

> 徽幼习《九章》，长再详览。观阴阳之割裂，总筭术之根源，探赜之暇，遂悟其意。是以敢竭顽鲁，采其所见，为之作注。

这说明，《九章筭术注》中含有两种内容：一

是他自己的数学创造，即“悟其意”者；二是前人的研究成果，即“采其所见”者。两者的分野在许多术文和问题的注解中十分清楚。比如刘徽几次严厉地批评前人使用周三径一的错误，但又有大量的段落使用周三径一；他指出使用棊验法对证明长、宽、高不等的阳马和鳖腝体积公式“则难为之矣”，但在许多多面体体积公式的注的第一段中往往使用棊验法。这些段落显然不是刘徽的思想，而是前人的，刘徽“采其所见”，写入注中。

认识刘徽注中有“采其所见”者，对《九章筭术》及其刘徽注的研究有重要意义。首先，刘徽注中的“采其所见”者透露出《九章筭术》成书时代的某些信息，比如，棊验法就是《九章筭术》成书时代推导多面体体积公式的一种方法。

其次，可以使我们更加清晰地认识刘徽。如果将刘徽注都看成是刘徽的思想，那么刘徽是一个成就极大，但思想混乱的数学家。如果在刘徽注中剔除了“采其所见”者，那么，一位成就极大、逻辑清晰、思想深邃的刘徽，便跃然纸上。

还有，对《九章筭术》的校勘特别重要。戴震等人由于不懂刘徽注有“采其所见”者，发现其中有不同思路时，便将后面一种思路改为李淳风等注释，造成极大混乱。

刘徽的数学成就大致有下面几方面：发展了传统的率概念和齐同原理，拓展了其应用，指出它们是“算之纲纪”。继承发展了传统的出入相补原理。首创极限思想和无穷小分割方法并严格证明了《九章筭术》提出的圆面积公式和他自己提出的刘徽原理。前者今称为割圆术，后者将多面体的体积理论建立在无穷小分割基础之上。刘徽明确认识了截面积原理，是为中国人完全认识祖暅之原理的关键一步。将极限思想应用于近似计算，在开方不尽时提出求其“微数”，以十进分数逼近无理根的思想。他在中国首创求圆周率的科学方法，奠定了中国的圆周率近似值的计算领先世界千余年的基础。修正了《九章筭术》的若干错误和不精确之处，提出了许多新的公式和解法，大大改善并丰富了《九章筭术》的内容。改变了《九章筭术》对数学概念的涵义约定俗成的做法，给出了若干明确的数学定义。以演绎逻辑为主全面论证了《九章筭术》的算法。他的论证常常是真正的数学证明。分析了各种数学概念、数学方法和命题之间的关系，梳理了各个分支乃至整个数学的逻辑系统。他认为数学像一株发自一端、枝繁叶茂、条缕分明而具有同一本干的大树，并基于此认识完成了中国传统数学的理论体系。

下面仅简要介绍刘徽的割圆术、刘徽原理、逻辑思想和数学体系。

割圆术

刘徽的圆田术注即割圆术分两部分。第一部分是证明《九章筭术》的圆面积公式。第二部分是求圆周率。《九章筭术》提出了圆面积公式：

术曰：半周半径相乘得积步。

以 S，L，r 分别记圆面积，圆周长和半径，那么术文用现代符号写出，就是：

$$S=\frac{1}{2}Lr. \qquad (1)$$

据刘徽记载，他之前使用出入相补原理推导这个公式。他认为，这是基于周三径一，以圆内接正六边形的周长作为圆周长，以圆内接正十二边形的面积作为圆面积，实际上并没有严格证明圆面积公式（1），遂提出了使用极限思想和无穷小分割方法的证明方法。他说：

又按：为图。以六觚之一面乘一弧半径，三之，得十二觚之幂。若又割之，次以十二觚之一面乘一弧之半径，六之，则得二十四觚之幂。割之弥细，所失弥少。割之又割，以至于不可割，则与圆周合体而无所失矣。觚面之外，犹有余径。以面乘余径，则幂出弧表。若夫觚之细者，与圆合体，则表无余径。表无余径，则幂不外出矣。以一面乘半径，觚而裁之，每辄自倍。故以半周乘半径而为圆幂。

如图 6，刘徽从圆内接正 6 边形开始割圆。设第 n 次分割得到正 6×2^n 边形的面积为 S_n，刘徽认为 $S_{n+1}<S<S_n+2(S_{n+1}-S_n)$。而

$$\lim_{n\to\infty}S_n=S,\ \lim_{n\to\infty}\left[S_n+2(S_{n+1}-S_n)\right]=S.$$

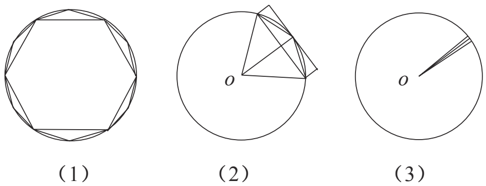


图 6 刘徽对圆面积公式的证明（采自《古代世界数学泰斗刘徽》）

刘徽将极限状态即与圆合体的正无穷多边形分割成以圆心为顶点，以每边为底的无穷多个小等腰三角形，每个的高 r，设每个的底边长 l_i，面积为 A_i。显然 $l_ir = 2A_i$。所有这些小等腰三角形的底边之和为圆周长 $\sum_{i=1}^{\infty} l_i = L$，它们的面积之和为圆面积 $\sum_{i=1}^{\infty} A_i = S$。因此，

$$\sum_{i=1}^{\infty} l_i r = \sum_{i=1}^{\infty} 2A_i = 2S.$$

由此式反求出 S，就得到（1）式。

这是一个论点明确，论据充分，逻辑清晰的完整证明。可是在上世纪 70 年代末以前，所有涉及刘徽割圆术的著述都有意无意地忽略了其中“以一面乘半径，觚而裁之，每辄自倍。故以半周乘半径而为圆幂”这几句画龙点睛之语——甚至一篇逐字逐句翻译刘徽割圆术的文章对这几句话竟略而不译，因此都没有认识到刘徽在证明《九章筭术》的圆面积公式（1）。

在证明了《九章筭术》的圆面积公式（1）之后，刘徽接着说：

此以周、径，谓至然之数，非周三径一之率也。

因此需要求周、径的“至然之数”，即圆周率。他在批评了“学者踵古，习其谬失”，沿用“周三径一之率”的错误之后，提出了求圆周率近似值的程序。他从直径为 2 尺的圆的内接正 6 边形开始割圆，得到圆内接各正多边形的边长以及正 96 边形的面积 $S_4=313\frac{584}{625}$ 平方寸，正 192 边形的面积 $S_5=314\frac{64}{625}$ 平方寸。刘徽求出 $S_5-S_4=\frac{105}{625}$ 平方寸。而 $314\frac{64}{625}$ 平方寸 $<S<314\frac{169}{625}$ 平方寸，因此取 314 平方寸作为圆面积的近似值。然后刘徽说：

以半径一尺除圆幂，倍所得，六尺二寸八分，即周数。……令径二尺与周六尺二寸八分相约，周得一百五十七，径得五十，则其相与之率也。周率犹为微少也。

即将这个近似值与半径 1 尺代入公式（1），求出圆周长的近似值 6 尺 2 寸 8 分。将圆的直径与周长相约，便得到圆周率 $\frac{157}{50}$，相当于 $\pi=3.14$。数学史上一般将它称为徽率或徽术。

显然，刘徽求圆周率的方法是以被他刚刚证明了的圆面积公式（1）为前提的，其中并未用到极限思想，只是极限思想在近似计算中的应用，没有任何费解之处。可是，在上世纪 70 年代末之前的所有著述都说刘徽此注中的几个极限过程是为了求圆周率，并且，在求出圆面积近似值 314 平方寸之后，利用 $S=\pi r^2$，由 $r^2=100$ 平方寸求出 $\pi=\frac{157}{50}$，无疑背离了刘徽注，并且还会将刘徽置于他从未犯过的循环推理错误之中。原来，刘徽在求出徽率之后，用它将《九章筭术》提出的与上述公式相当的圆面积公式 $S=\frac{3}{4}r^2$，修正为 $S=\frac{157}{200}r^2$。

刘徽原理

近代数学大师高斯曾提出一个猜想：多面体体积的解决不借助于无穷小分割是不是不可能的？这一猜想构成了希尔伯特《数学问题》（1900 年）第三问题的基础。不久，他的学生德恩作了肯定的回答。实际上，早在高斯前 1500 多年，刘徽在证明《九章筭术》提出的阳马和鳖臑的体积公式时，就涉及到了高斯猜想和希尔伯特第三问题。

中国古代在多面体分割中，一个长方体沿相对两棱剖开，得到两个楔形体，叫做堑堵，如图 7（1）。一个堑堵从一个顶点到底面一边剖开，得到一个锥体，其高的垂足在

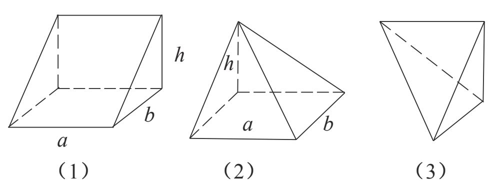


图 7 堑堵、阳马、鳖臑

底面的一角上，叫做阳马，如图 7（2）；剩下的是四面皆为勾股形的四面体，叫做鳖腝，如图 7（3）。《九章筭术》给出了阳马的体积公式：

$$V=\frac{1}{3}abh, \qquad (2)$$

其中 a，b，h 分别是阳马的广、袤和高。又给出鳖腝的体积公式

$$V=\frac{1}{6}abh, \qquad (3)$$

其中 a，b，h 分别是鳖腝的下广、上袤和高。

在 $a=b=h$ 的情况下，由于一个正方体可以分解为 3 个全等的阳马，或 6 个三三全等、两两对称的鳖腝，“验之以棊，其形露矣”，（2），（3）无疑是正确的。但是，在 $a\neq b\neq h$ 的情况下，一个正方体分解成的三个阳马不全等，6 个鳖腝尽管两两对称，却不三三全等，所谓“鳖腝殊形，阳马异体”。刘徽指出：“阳马异体，则不可纯合，不纯合，则难为之矣。”换言之，用棊验法即传统的出入相补方法是无法严格证明（2），（3）两式的。他只好另辟蹊径。刘徽提出了一个重要原理：

邪解堑堵，其一为阳马，一为鳖腝。阳马居二，鳖腝居一，不易之率也。

即在一个堑堵中，恒有

$$V_{阳马}:V_{鳖腝}=2:1 \qquad (4)$$

吴文俊把它称为刘徽原理。显然，只要证明了刘徽原理，由于堑堵的体积公式为 $V=\frac{1}{2}abh$，则（2），（3）两式是不言而喻的。

刘徽使用极限思想和无穷小分割方法证明了这个原理。他说：

设为阳马为分内，鳖腝为分外。棊虽或随脩短广狭，犹有此分常率知，殊形异体，亦同也者，以此而已。其使鳖腝广、袤、高各二尺，用堑堵、鳖腝之棊各二，皆用赤棊。又使阳马之广、袤、高各二尺，用立方之棊一，堑堵、阳马之棊各二，皆用黑棊。棊之赤、黑，接为堑堵，广、袤、高各二尺。于是中攽其广、袤，又中分其高。令赤、黑堑堵各自适当一方，高一尺、方一尺，每二分鳖腝，则一阳马也。其

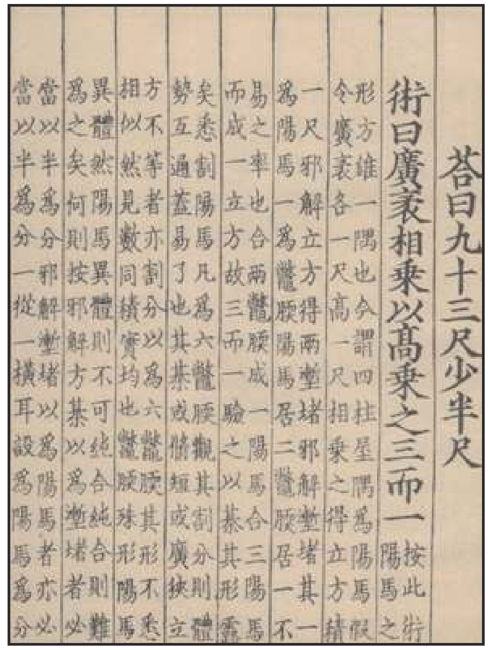

荅曰九十三尺少半尺
術曰廣袤相乘以高乘之三而一

图 8 刘徽原理书影（南宋本）

余两端各积本体，合成一方焉。是为别种而方者率居三，通其体而方者率居一。虽方随棊改，而固有常然之势也。按：余数具而可知者有一、二分之别，即一、二之为率定矣。其于理也岂虚矣？若为数而穷之，置余广、袤、高之数各半之，则四分之三又可知也。半之弥少，其余弥细。至细曰微，微则无形。由是言之，安取余哉？

刘徽将由两个小堑堵Ⅱ′、Ⅲ′，两个小鳖腝Ⅳ′、Ⅴ′ 合成的鳖腝（图 9（1））与由一个小长方体Ⅰ，两个小堑堵Ⅱ、Ⅲ，两个小阳马Ⅳ、Ⅴ合成的阳马（图 9（2））拼合成一个堑堵，如图 9（3），则相当于堑堵被三个互相垂直的平面平分。显然，小堑堵Ⅱ与Ⅱ′、Ⅲ与Ⅲ′ 可以分别拼合成与Ⅰ全等的小长方体，如图 9（5）和（6）所示。小阳马Ⅳ与小鳖腝Ⅳ′，小阳马Ⅴ与小鳖腝Ⅴ′ 可以分别拼合成两个与小堑堵Ⅱ、Ⅲ、Ⅱ′、Ⅲ′ 全等的小堑堵，它们又可以拼合成与Ⅰ全等的第 4 个小长方体，如图 9（7）所示。显然，在前三个小长方体Ⅰ、Ⅱ-Ⅱ′、Ⅲ-Ⅲ′ 中，属于阳马的和属于鳖腝的体积的比是 2:1，即在原堑堵的 $\frac{3}{4}$ 中（4）式成立，所谓“别种而方者率居三”。刘徽

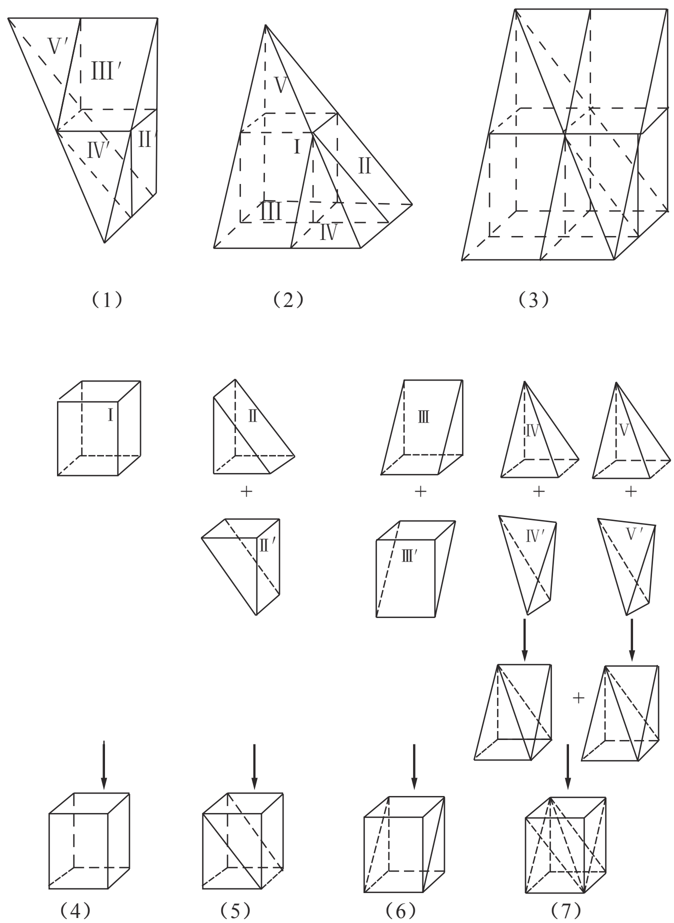


图 9 刘徽原理之证明

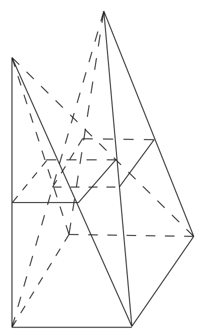


图 10 方锥与阳马同实

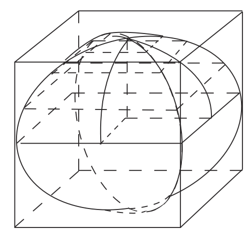


图 11 牟合方盖

认为，如果能证明（4）式在第 4 个小长方体中成立，则（4）式便在整个堑堵中成立。而第 4 个小长方体中的两个小堑堵与原堑堵完全相似，所谓“通其体而方者率居一”。因此，上述分割过程完全可以继续在剩余的两个小堑堵中施行，那么又可以证明在其中的$\frac{3}{4}$中（4）式成立，在其中的$\frac{1}{4}$中尚未知。换言之，已经证明了原堑堵中的$\frac{3}{4}+\frac{1}{4}\cdot\frac{3}{4}$中（4）式成立，而在$\frac{1}{4}\times\frac{1}{4}$中尚未知。这个过程可以无限继续下去，第 n 次分割后只剩原堑堵的 $1/4^n$ 中（4）式是否成立尚未知。显然，$\lim\limits_{n\to\infty} 1/4^n = 0$。这就在整个堑堵中证明了（4）式，即刘徽原理成立。

刘徽原理是其多面体体积理论的基础。刘徽说：

不有鳖臑，无以审阳马之数，不有阳马，无以知锥亭之类，功实之主也。

刘徽认为，鳖臑是其解决多面体体积问题的关键。刘徽为求方锥、方亭、刍甍、刍童、羡除等多面体的体积，都要通过有限次分割，将其分割成长方体、堑堵、阳马、鳖臑等已被证明了体积公式的立体，然后求其体积之和解决之。刘徽原理把多面体体积理论建立在无穷小分割基础上的思想，与现代数学的体积理论惊人地一致。

截面积原理

《九章算术》是通过比较其底面积由体积已知方体推知圆体体积的。刘徽则更进了一步，他说：“上连无成不方，故方锥与阳马同实。”如图 10。可见，刘徽实际上已经认识了祖暅之原理：“缘幂势既同，则积不容异。”此即后来西方的卡瓦列里原理。正因为如此，刘徽认识到，《九章算术》时代由圆柱体与其内切球的体积之比是 4:π 推导球体积，从而得出的开立圆术是错误的。他设计了牟合方盖，如图 11。刘徽指出：牟合方盖与内切球的体积之比才是 4:π，只要求出牟合方盖的体积，便可以解决球体积问题，从而指出了解决球体积的正确途径。200 年后的祖冲之父子在刘徽基础上求出了牟合方盖的体积。

刘徽的逻辑思想和数学理论体系

中国古代数学没有理论，似成为学术界的主流看法。不仅鄙视中国的西方中心论者和民族虚无主义者如是说，即使是对中国古代数学成就评价甚高的学者如英国的李约瑟等亦持这种看法。众所周知，要证明数学命题为真，必须靠演绎推理。说中国传统数学没有理论，主要是说没有演绎推理。事实上，认真考察刘徽注就会发现，刘徽在数学命题的证明中主要使用了演绎推理，其中有三段论、关系推理、假言推理、选言推理、联言推理、二难推理等演绎逻辑的最重要的推理形式，还有数学归纳法的雏形。说中国传统数学没有逻辑的学者，或者是没有读刘徽的《九章筭术注》，或者是读了但没有读懂。

刘徽的演绎逻辑

三段论是演绎推理的性质判断推理中极其重要的一种。三段论不是个别民族或学派的专利，刘徽注的许多推理是典型的三段论。例如盈不足术刘徽注曰：

> 注云若两设有分者，齐其子，同其母。此问两设俱见零分，故齐其子，同其母。

其推理形式是：若两设有分者（M），须齐其子，同其母（P）。此问（S）两设俱有分（M），故此问（S）须齐其子，同其母（P）。其中含有三个概念：两设俱有分（中项 M），齐其子，同其母（大项 P），此问（小项 S）。中项在大前提中周延，结论中的概念的外延与它们在前提中的外延相同，还有，大前提是全称肯定判断，小前提是单称肯定判断，结论是单称肯定判断。可见，这个推理完全符合三段论的规则，是其第一格的 AAA 式。

关系推理实际上是三段论的一种。初等数学是关于客观世界的空间形式和数量关系的科学，关系推理在刘徽的推理中所占的比重自然特别大。而在关系推理所使用的关系判断中，又以等量关系为最多。例如方田章圆田术刘徽注对圆田又术“周、径相乘，四而一”的证明是：

> 周、径相乘各当以半，而今周、径两全，故两母相乘为四，以报除之。

其推理形式就是：

已知

$S=\frac{1}{2}Lr$（等量关系判断，刘徽已经证明），

及

$r=\frac{1}{2}d$（等量关系判断），

故

$S=\frac{1}{2}Lr=\frac{1}{2}L\times\frac{1}{2}d=\frac{1}{4}Ld$（等量关系判断）。

刘徽有时使用不等量关系推理。例如在推断圆囷（圆柱体）与所容之丸（内切球）的体积之比不是 $4:\pi$ 时说：

> 按：合盖者，方率也，丸居其中，即圆率也。推此言之，谓夫圆囷为方率，岂不阙哉？

其推理形式是：已知 $V_{hg}:V_w=4:\pi$（等量关系判断），及 $V_{yq}:V_w\neq V_{hg}:V_w$，（不等量关系判断），故 $V_{yq}:V_w\neq 4:\pi$（不等量关系判断）。其中 V_{hg}，V_w，V_{yq} 分别是牟合方盖、丸、圆囷的体积。

假言推理是数学推理中常用的一种形式，包括充分条件假言推理和必要条件假言推理。充分条件假言推理的推理形式是：若 p，则 q，今 p，故 q。上面提到的“上连无成不方，故方锥与阳马同实”，文字很简括，其完备形式是：

> 若两立体每一层都是相等的方形（p），
> 则其体积相等（q），
> 今方锥与阳马每一层都是相等的方形（p），
> 故方锥与阳马体积相等（q）。

在**充分条件假言推理**中，若 p，则 q。若非 p，则 q 真假不定。刘徽对此有深刻的认识。例如刘徽在记述用棊验法推证阳马、鳖臑体积公式时指出，将一正方棊分割为三个阳马，或六个鳖臑。“观其割分，则体势互通，盖易了也”。“体势互通”即全等或对称。然而在长、宽、高不等的情况下，“则难为之矣”。其推理形式是：

> 若诸立体体势互通（p），则其体积相等（q）。
> 今诸立体体势不互通（非 p），
> 故难为之矣（q 真假不定）。

这是刘徽认识到棊验法不能在数学上真正证明多面体体积公式的逻辑基础。

选言推理有两个前提。第一个前提是含有两个选言支的选言判断，第二个前提是某一选言支的否定，那么其结论是另一选言支的肯定。其推理形式是：或 p，或 q。今非 q，故 p。刘徽在许多地方使用了选言推理。例如在四则运算中，根据需要，可以先乘后除，也可以先除后乘。刘徽在商功章负土术注中指出："乘除之或先后，意各有所在而同归耳。"刘徽通常主张先乘后除，因为先除后乘，有时会出现分数。这是一个选言推理，其形式为：

> 或先乘后除（p），或先除后乘（q）。
> 今非先除后乘（q），
> 故先乘后除（p）。

联言推理的前提是一个联言判断，其结论是一个联言支。刘徽在羡除术注中用截面积原理推导椭方锥（即长方锥）的体积时说："阳马之棊两邪，棊底方。当其方也，不问旁角而割之，相半可知也。……角而割之者相半之势。"这是一个分解式联言推理，其推理形式是：

> 前提：对方锥平行于底的截面，用一平面切割其对边的中点，则将其体积平分（p），用一平面切割其对角，也将其体积平分（q）。
>
> 结论：用一平面切割其对角，将其体积平分（q）。

由此证明了将半个椭方锥角而割之得到的大鳖臑，其体积是椭方锥的一半，亦即与《九章筭术》的鳖臑体积公式取同样的形式。

二难推理是将假言推理与选言推理结合起来的一种推理，又称为假言选言推理。其大前提是两个假言判断，小前提是选言判断。刘徽证明《九章筭术》圆田又术 $S=\frac{1}{12}L^2$ 不准确时说：

> 六觚之周，其于圆径，三与一也。故六觚之周自相乘幂，若圆径自乘者九方，九方凡为十二觚者十有二，故曰十二而一，即十二觚之幂也。今此令周自乘，非但若为圆径自乘者九方而已。然则十二而一，所得又非十二觚之类也。若欲以为圆幂，失之于多矣。

它有两个假言前提：一个是：若以圆内接正六边形的周长作为圆周长自乘，其十二分之一，是圆内接正十二边形的面积（p），小于圆面积（r）；另一个是：若令圆周自乘，其十二分之一（q），则大于圆面积（S）。还有一个选言前提：或者以正六边形周长自乘，十二而一，或者以圆周长自乘，十二而一（或 p 或 q）。结论是：或失之于少，或失之于多（或 r 或 S），都证明了《九章筭术》该公式不准确。

数学归纳法是演绎推理的一种。刘徽继承的《九章筭术》的开方术，他创造的割圆术和用无穷小分割方法证明刘徽原理的方法，等等，都是递推方法。在后二者中更是无限递推。无限递推是数学归纳法的核心。仅以刘徽原理的证明中的递推方法说明数学归纳法的雏形。

刘徽首先通过第一次分割证明了在整个堑堵的 $\frac{3}{4}$ 中阳马与鳖臑的体积之比为 2:1，而在其 $\frac{1}{4}$ 中尚未知，这相当于在 $n=1$ 时候，刘徽原理在堑堵的 $\frac{3}{4}$ 中成立。刘徽认为第一次分割可以无限递推，"置余广、袤、高之数各半之，则四分之三又可知也"。然后，刘徽说："按余数具而可知者有一、二分之别，即一、二之为率定矣。其于理也岂虚矣。若为数而穷之，置余广、袤、高之数各半之，则四分之三又可知也。半之弥少，其余弥细。至细曰微，微则无形。由是言之，安取余哉？"这相当于设 $n=k$ 时，刘徽原理在堑堵的 $\frac{1}{4^{k-1}}\times\frac{3}{4}$ 中成立，则刘徽原理在堑堵的 $\frac{1}{4^k}\times\frac{3}{4}$ 中成立。刘徽当然无法严格地表达出数学归纳法，但是他说"数而求穷之者，谓以情推，不用筹算"。"情推"具备了数学归纳法的基本要素。

总之，刘徽在论证《九章筭术》和他自己提出的公式、解法、原理时，主要使用了演绎推理，并且，现代逻辑学教科书中的演绎推理的几种最主要的形式，刘徽都使用了。这不仅在数学著作中是空前的，就严谨和抽象程度上，恐怕也是中国古代的最高水平。

数学证明

一般说来，推理形式的正确只能保证其前提和结论之间的或然的或者必然的联系，因此，推理形式的正确不能保证其前提正确，也就不能保证其结论是正确的。只有当前提是正确的时候，运用正确的推理形式，才能

获得正确的结论。这就是论证。论证是由推理组成的，推理是为论证服务的。像推理一样，只有演绎论证才能得到必然性的正确结论。由于数学具有严谨、精确、抽象的特点，因此论证数学公式、定理、解法的正确性时，只能采用演绎推理，并且前提应该是正确的，这种过程通常称为数学证明。前面所举的例子，由于其前提都是正确的，并且都是演绎推理，因而都是数学证明。特别应该指出，刘徽数学证明的依据都是已知其正确性的公理或自己已经证明过的命题。

数学证明根据其思路的方向不同，或者从予到求，或者从求到予，通常分为分析法和综合法两种。刘徽的数学证明以综合法居多，而对难度较大的命题，则往往采取综合法和分析法相结合的方法。

综合法是根据已知条件，援引公理及已经证明过的公式、解法，通过一系列推理，最终引导到论题。刘徽对《九章筭术》圆面积公式（1）的证明是一个典型的综合法证明。再以刘徽对已知勾股差与弦求勾、股的公式

$$a=\frac{1}{2}\left[\sqrt{2c^2-(b-a)^2}-(b-a)\right],$$

$$b=\frac{1}{2}\left[\sqrt{2c^2-(b-a)^2}+(b-a)\right]$$

的证明为例。刘徽说：

> 按图为位，弦幂适满万寸。倍之，减勾股差幂，开方除之。其所得即高广并数。以差减并而半之，即户广；加相多之数，即户高也。

其中有的推理，刘徽行文时省去了，将其补足便是：

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

$$2c^2-(b-a)^2=2a^2+2b^2-(b-a)^2=(a+b)^2,$$

故

$$\sqrt{2c^2-(b-a)^2}=(a+b),$$

而

$$a=\frac{1}{2}[(a+b)-(b-a)],$$

$$b=\frac{1}{2}[(a+b)+(b-a)],$$

将（$a+b$）代入即完成证明。

显然，这是一个由已知的勾股定理及题设，逐步运用关系推理，以证明公式的综合法。其中的“弦幂适满万寸”是不必要的，还保留了归纳推理的某些痕迹。

分析法是从论题回溯论据的过程。对非常复杂的证明，刘徽往往采取综合法和分析法相结合的方式。比如关于《九章筭术》的鳖臑与阳马体积公式（2），（3）的证明，刘徽提出了刘徽原理（4）。他认为，为了证明这两个公式，只要证明刘徽原理（4）就够了。这是从论题回溯论据的分析法。为了证明刘徽原理，刘徽首先对由阳马和鳖臑合成的堑堵进行分割，证明在堑堵的$\frac{3}{4}$中，刘徽原理所指出的阳马与鳖臑的体积之比为 2:1 成立。这是综合法。接着，刘徽认为，如果能证明在堑堵剩余的$\frac{1}{4}$中可以知道其体积的部分中阳马与鳖臑的体积之比仍为 2:1，则就在整个堑堵中证明了刘徽原理。这又是分析法。随后，刘徽用无穷小分割方法和极限思想证明了这一点。这又是综合法。这种分析法与综合法相结合的方式对难度较大的复杂证明，常常可以起到画龙点睛的作用，使整个证明思路清晰，文字不冗长，不枯燥，又使读者容易抓住证明过程的关键所在。

刘徽的数学理论体系

中国数学史界有一个耳熟能详的提法，说《九章筭术》建立了中国古代的数学体系。这种提法似是而非。说“数学体系”，应该指数学理论体系。而一个理论体系，应该包含概念，由这些概念联结起来的命题，以及使用逻辑方法对这些命题的论证。对数学而言，这种论证，必须主要使用演绎逻辑。《九章筭术》只有概念和命题，没有留下逻辑论证。前已指出，从刘徽注可以探知，《九章筭术》时代实际上是存在着某些推导和论证的，但是，这些推导和论证是以归纳逻辑为主的。因此，我们认为，《九章筭术》没有建立中国古代数学的理论体系，只是构筑了中国传统数学的基本框架。在这个框架中，各章的方法之间，甚至同一章不同方法之间，除了均输术是衰分术的子术之外，几乎看不出它们的逻辑关系。

刘徽以演绎逻辑为主要方法全面证明了《九章筭术》的公式、解法，因此，到刘徽完成《九章筭术注》，中国传统数学才形成了数

学理论体系。逻辑方法的改变，必然导致一个学科内部结构的相应改变。事实上，刘徽的数学理论体系不是《九章筭术》数学框架的简单继承和补充，也不仅是为这个框架注入了血肉和灵魂，而且包括了对这个框架的根本改造。

近代人们常把数学形象地画作一株大树，通常是一株大栎树。树根上画着代数、平面几何、三角、解析几何和无理数。在这些根上长出强大的树干，即微积分。树干的顶端发出许多大的枝条，并再分成较小的枝条，即复变函数、实变函数、变分法、概率论等等高等数学的各个分支。实际上，早在 1700 多年前，刘徽通过深入研究《九章筭术》，“观阴阳之割裂，总算术之根源”，提出了数学之树的思想：

> 事类相推，各有攸归，故枝条虽分而同本知，发其一端而已。又所析理以辞，解体用图，庶亦约而能周，通而不黩，览之者思过半矣。

刘徽的数学之树“发其一端”，“端”就是数学之树的根。这个“端”是什么呢？刘徽说：

> 虽曰九数，其能穷纤入微，探测无方。至于以法相传，亦犹规矩度量可得而共，非特难为也。

规矩在这里指几何图形，即我们通常所说的客观世界的空间形式；度量是度量衡，在这里指客观世界的数量关系。因此，规矩、度量可以看成刘徽数学之树的根，数学方法由之产生出来。刘徽的话很形象地概括了中国传统数学中数与形相结合，几何问题与算术、代数问题相统一这个重要特点。根据刘徽的《九章筭术注序》及其为九章写的注中形诸文字者，我们大体可以将刘徽的数学之树的面貌勾勒于下：

数学之树从规矩、度量这两条根生长出来，统一于数，形成以率为纲纪的数学运算这一本干。刘徽以《九章筭术》的长方形面积公式、长方体体积公式（刘徽没有试图证明，可视为定义）及他自己提出的率和正负数的定义为前提，以今有术为都术，以比例问题、盈不足问题、开方问题、方程问题、面积问题、体积问题、勾股测望问题等作为主要枝条。又分出经率术，其率术和返其率术，衰分术和返衰术，重今有术，均输术，盈不足术和两盈两不足术、盈适足不足适足术，多边形面积，圆田术、圆周率和曲边形面积，刘徽原理和多面体体积公式，截面积原理和圆体体积公式，勾股术和解勾股形诸术，勾股容方和勾股容圆术，一次测望问题和重差问题，开方术和开立方术，正负术，方程术和损益术、方程新术，不定方程等等方法作为更细的枝条，形成了一株枝叶繁茂、硕果累累的大树，形成了一个完整的数学体系。如图 12 所示。

在这个体系中，刘徽尽管也使用类比和归纳逻辑，但主要地是使用演绎逻辑，从而将数学知识建立在必然性的基础之上。

在这个体系中，齐同原理、出入相补原理、极限思想和无穷小分割方法及截面积原理是刘徽所使用的主要原理。齐同原理用于计算问题，出入相补原理用于解决多边形和多面体体积，极限思想、无穷小分割方法和截面积原理用于解决曲边形面积、多面体体积和圆体体积。

这个体系“约而能周，通而不黩”，全面反映了当时中国人所掌握的数学知识，略知

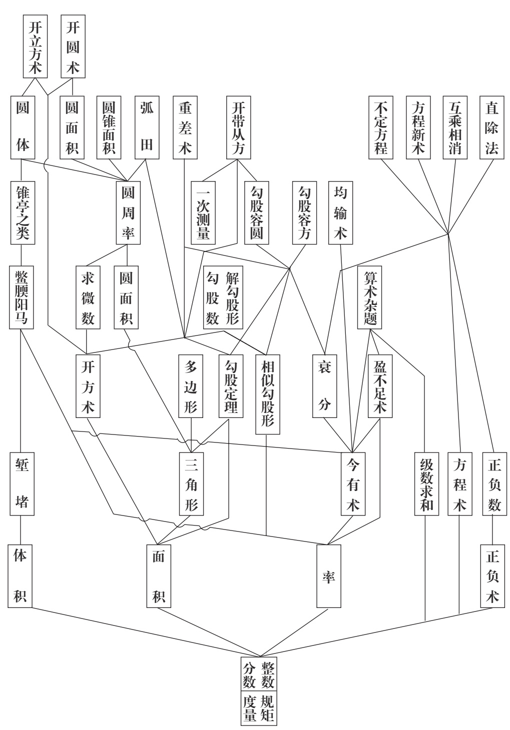


图 12 刘徽的数学之树

《九章筭术》的人即可看出九章的分布。在这里，数学概念和各个公式、解法不再是简单的堆砌，而是以演绎推理和数学证明为纽带，按照数学内部的实际联系和转化关系，形成了有机的知识体系。而刘徽数学理论体系与《九章筭术》框架的结构有着根本的不同，因此，它不是《九章筭术》框架的添补，而是对《九章筭术》的改造。

需要指出的是，说刘徽对《九章筭术》框架的改造，不是说在形式上，而是在实际上，在刘徽的头脑中。在形式上，刘徽没有改变《九章筭术》的术文和题目的顺序。在这种情况下，刘徽《九章筭术注》中没有任何循环推理，说明刘徽逻辑水平之高超。在文献注疏中以互训为重要方法的中国古代，这更是难能可贵的。可以说，刘徽的《九章筭术注》在内容上是革命的，而在形式上是保守的。然而，正是这种保守的形式，而不是撰著一部自成系统的高深著作，使刘徽的数学创造避免了《缀术》的厄运。

结论

通过上面的分析，我们可以得出以下几个结论：首先，刘徽是中国古代最伟大的数学家。祖冲之的数学水平不会低于刘徽，但《缀术》已不存，残存的几项成就都是刘徽为其奠定基础。宋元数学高潮的代表人物贾宪、李冶、秦九韶、朱世杰等，他们在高次方程数值解法和多元高次方程组解法等方面，水平当然超过刘徽，在其创造性上与刘徽也不分轩轾。但他们对极限思想和无穷小分割方法却一无所知，在演绎逻辑和数学证明上更是远逊于刘徽。考虑到刘徽比他们早七八百年至千年左右，因此刘徽是中国古代当之无愧的最伟大的数学家。

其次，刘徽《九章筭术注》奠定了中国传统数学的理论基础，建立了中国传统数学的理论体系。近年有"《九章筭术》与刘徽的数学体系"的提法。笔者认为这似是而非。刘徽《九章筭术注》无论从数学的研究方向，还是理论高度、逻辑方法，都与《九章筭术》时代有明显的不同，它的体系与《九章筭术》的框架根本不同，在数学上应该属于另一个阶段。

第三，以刘徽《九章筭术注》为代表的魏晋南北朝也是中国传统数学的一个高潮。学术界常有宋元是中国传统数学的高潮的说法。实际上，这是一个筹算高潮。笔者认为，中国传统数学的繁荣时期产生过三个高潮：第一个发生在春秋战国秦汉，是以《九章筭术》为代表的数学框架的确立；第二个发生在魏晋南北朝，是以刘徽《九章筭术注》（或许还有祖冲之）为代表的数学理论的奠基；第三个发生在唐中叶至元中叶，是筹算高潮。

作者简介：

郭书春，山东大学数学系毕业。中国科学院自然科学史研究所研究员，曾任研究所学术委员会副主任、全国数学史学会理事长。现任《中华大典》常务编委，《中华大典·数学典》主编。长期从事中国数学史研究，发表论文100余篇，著有汇校《九章算术》及其增补版、《中国古代数学》、《古代世界数学泰斗刘徽》、中法对照《九章算术》（合作）、《九章算术译注》、汉英对照《九章算术》（合作）等，主持编纂了《中国科学技术典籍通汇·数学卷》、《中国科学技术史·数学卷》等学术著作。

人心不足蛇吞象

金 磊

海盗问题

8 个海盗得到了 100 枚金币，他们要分配这些金币（金币的最小单位为 1）。海盗按实力排序依次为老大、老二……老八，他们的分配方式很“民主”：由老大提出一种分配方案，然后所有人（包括老大）投票表决，如果赞成率（即赞成人数与总人数之比）$p>0.5$，则方案通过，按此方案分配；反之，即若 $p\leq 0.5$，则老大将受到“惩罚”，强盗的唯一惩罚方式就是扔进海里喂鲨鱼。把老大扔进海里喂鲨鱼后，由老二继续提方案、大家表决……，以此类推。假设所有的海盗都足够聪明（傻瓜不适合从事海盗这种高风险的“职业”），海盗也都极度贪婪自私，各自为政，不群不党，也就是说他们在保护性命的同时会想方设法占有尽可能多的金币，在不损害自己利益的情况下尽量害死别人，当然，“盗亦有道”，他们都是“死理性派”，还是严格遵守规则的。那么这些金币最终会如何分配呢？

此类问题最早见于 1999 年《科学美国人》刊登过的趣题“海盗分金”，国内也有不少研究，本问题为“变种”版。

思路分析

乍一看此题无从入手，按常识来猜测，要么老大必死、要么平均分配、要么按实力强弱等差分配等。而事实上，对于陌生的、条件繁多的难题，最常用也是最重要的方法就是——探索法，从简单情况做起！正如《老子》所说：道生一，一生二，二生三，三生万物。因此我们可以从最简单的情形去列举以帮助我们理解题意，找到突破口。我们按强盗人数 n 从少到多考虑（其实这正是数学归纳法的精髓：有序思考），不妨设 n 个强盗按实力强弱顺序为 1 号，2 号，3 号……n 号，则

若 $n=1$，无需分配。

若 $n=2$，则无论 1 号提什么方案，2 号都会反对，这样通过率 $p\leq 0.5$，则 1 号被喂鲨鱼，2 号获得所有金币。

若 $n=3$，由上面的分析，1 号知道：若自己死掉，则 2 号必死；从而 2 号为保命，必然赞成自己的任何方案。因此他可以放心地把金币全部据为己有。分配方案为(100, 0, 0)，投票结果为 1 号、2 号赞成，通过。

这样我们就找到了这个问题的解决思路，以此类推，应该即能解决多个海盗的问题。

若 $n=4$，同理，1 号知道：若自己死掉，则分配方案如上，从而当前的 3 号，4 号将一无所获，因此他只要给 3 号、4 号各一个金币，即可收买他们，分配方案为（98, 0, 1, 1），投票结果为得钱者赞同，通过！

若 $n=5$，1 号需用 1 个金币收买 3 号，用 2 个金币收买 4 号、5 号中的某一个即可。故有两种方案：(97, 0, 1, 2, 0）或者（97, 0, 1, 0, 2）。

若 $n=6$，若 1 号死掉，则对最后两人 5 号、6 号而言，他可能得不到，也可能得 2 个金币，

平均值（即数学期望）为 1。因此 1 号只需各用 1 枚金币即可收买到他们（俗话说“隔夜的金不如到手的铜”，在收益相同的情况下，理性的人总是尽量避免冒险）。然后 1 号再用 1 枚金币收买 3 号即可。最佳分配方案只有一种为（97, 0, 1, 0, 1, 1）。

若 $n=7$，类似的，1 号除了各用 1 枚金币收买 3、5 号外，还需要用 2 个金币收买 4、6、7 中的任一个。故有 3 种分配方案，分别为：

（96, 0, 1, 2, 1, 0, 0）或（96, 0, 1, 0, 1, 2, 0）或（96, 0, 1, 0, 1, 0, 2）。

若 $n=8$，同理 1 号只要各用 1 枚金币收买 3, 5, 7, 8 号即可，故只有一种方案（96, 0, 1, 0, 1, 0, 1, 1）。

上述结果列表如下，其中 $n>3$ 投票时分得金币者都会赞同方案。

n	分配方案	备注
1	（100）	
2	（0, 100）	1 号死掉
3	（100, 0, 0）	
4	（98,0, 1, 1）	
5	（97, 0, 1, 2, 0）或（97, 0, 1, 0, 2）	
6	（97, 0, 1, 0, 1, 1）	
7	（96, 0, 1, 2, 1, 0, 0）或（96, 0, 1, 0, 1, 2, 0）或（96, 0, 1, 0, 1, 0, 2）	
8	（96, 0, 1, 0, 1, 0, 1, 1）	

意外结局

至此，8 个海盗分赃完毕，但分配结果却让人大跌眼镜！尽管规则看起来很公平，甚至还有些对老大不利，可是老大在充分利用规则和每个个体都是“死理性派”的情况下，各个击破，不但有惊无险，而且攫取了几乎全部金币（96%）。但是我们仔细想来，这也基本符合现实。比如某些垄断企业在平等竞争的招牌下占据着行业的绝大多数利润；再比如一些人宁为鸡头、不为牛后，宁愿在一个小地方做“土皇帝”也不愿意到一个大地方受人管制，原因可能就在于山高皇帝远，当个“老大”还是非常“有利可图”的。

其次，在此种极其绝对的假设下，老二永远得不到任何利益，因为他一直觊觎老大的位置，而老大知道无法收买他，因此选择将其隔离开来，退而收买其余的海盗。故老二得到的利益还不如后面实力比他弱很多的海盗。现实中确也有类似的事情，一个组织的二把手往往被一把手隔离，处于一个“上不着天、下不着地”的尴尬境地。

最后，此道数学题也从另一个方面展示了“囚徒困境”：每个个体利益的最大化并不是集体利益的最大化！在一个集体中每个人都“绝对理性”的情况下，如果我们人人抱着“人不为己，天诛地灭”的自私自利心态，一些人往往可以利用我们的“理性”，利用规则，对我们各个击破，使得最后我们感觉自己得到了便宜而实际却吃了大亏，最终每个个体都利益最大化，集体利益却远远没有达到最大化。

问题延伸

当然，本题还有很多问题值得思考，例如若海盗人数 n 继续增加呢？类似于以上的分析，我们可以得到，$2<n<201$ 时

当 n 为偶数时，设 $n=2k$，只有一种分配方案：$(100-k, 0, 1, 0, 1\cdots, 0, 1, 0, 1, 1)$（其中 $100-k$ 后面有（$k-1$）个交错排列的 0，k 个 1）；

当 n 为奇数时，设 $n=2k+1$，1 号只需将上述中的 0 全换成 1，再用 2 枚金币收买某一个 1，剩下的留给自己即可，有 k 种分配方案，例如（$99-k, 1, 2, 1, 0, 1, 0\cdots, 1, 0, 1, 0, 0$）（其中除 $99-k$ 外，有 k 个 0，（$k-1$）个交错的 1，1 个 2）等。

例如当 $n=200$ 时，只有一种分配方案:（$0, 0, 1, 0, 1\cdots, 0, 1, 0, 1, 1$）（其中有 100 个 0，100 个 1）

如果海盗的队伍继续发展壮大，超过了 200 人，只抢到 100 枚金币的话，僧多粥少，海盗船长要收买超过半数的人似乎不太可能，他是否就死定了呢？下面我们接着往下分析：

当 $n=201$ 时，1 号需各用 1 枚金币收买上述 $n=200$ 中的 100 个 0，再加自己的一票，1 号险险保命，一文不名。

当 $n=202$ 时，1 号要买通 $n=201$ 时的 101 个 0，不可能，故老大必被投入大海喂鲨鱼，变成 $n=201$ 时的情况。

当 $n=203$ 时，2 号为保命，必然赞成，加上 1 号自己的一票，需要再买通 100 人，故只要买通上述 $n=201$ 时 101 个 0 中的 100 个 0，共有 101 种方案。

同理，当 $n=204, 205, 206$ 时，前面的必被投入大海喂鲨鱼，直到 $n=203$ 时的情形。

当 $n=207$ 时，1、2、3、4 号为保命，必然赞成，故需要买通 $n=203$ 时的 103 个 0 中 100 个，故共有 C_{103}^{100} 种选择。

当 $n=208$ 到 214 时，同理，前面的必被投入大海喂鲨鱼，直到 $n=207$ 时的情形。

当 $n=215$ 时，1 到 8 号为保命，必然赞成，故需要买通 $n=207$ 时的 107 个 0 中 100 个，故共有 C_{107}^{100} 种选择。

以此类推，可以得到，当 $n>200$ 后：

若 $n=199+2^m(m>0)$，则 1 到 2^{m-1} 号为保命，必然赞成，只需从 $199+2^{m-1}$ 情形时的 $99+2^{m-1}$ 个 0 中选出 100 个 0 即可，故共有 $C_{99+2^{m-1}}^{100}$ 种选择；

若 $n \neq 199+2^m(m>0)$，设 $199+2^m< n < 199+2^{m+1}(m>0)$，则前面连续 $n-199+2^m$ 个强盗都要被喂鲨鱼，然后退成 $199+2^m(m>0)$ 的情形。

当然，对于本问题，还可以思考当金币的数量变化时的情况，结果基本类似。还有当赞成率改变时，例如变成 $p>2/3, p \geq 1/2$ 等，可以发现 p 的变化对结果还是影响蛮大的，请有兴趣的读者自行研究。

数学之外

上面我们解决了任意多个海盗的问题。从这个结果，我们也可以发一些感慨：在资源稀缺、数量透明且规则得以贯彻的情况下，做老大不但没有便宜，而且还很有风险（正所谓：枪打出头鸟也），韩非子都说过："是以人之于让也，轻辞古之天子，难去今之县令者，薄厚之实异也！"上古尧舜禹等实行禅让制，有可能是因为在当时当头领风险很大，又没有收益，只能禅让，还会有叔齐、伯夷、许由等人主动逃避呢。当资源相对极大丰富的时候，做首领就能"垄断"绝大多数的物质了，这就是后来封建社会大家为当帝王将相争得头破血流的原因啦。

最后要说明的是，虽然本题在大家都是严格理性的基础上，有些结果比较"奇怪"，但这并不是"理性"的问题，而是分配规则不合理。因此我们不能因为这个结果而反对理性，恰恰相反，就是因为理性，我们才能发现这些"理性"的问题，用更理性、更科学的方法加以修正，而如果用其他非理性的方法更是无能为力，可证伪性、可修正性正是科学理性的重要标志！

当然，这一切的前提还是规则和财务的"公开化"，没有"潜规则"，而且所有人都严格按这个规则办事！

作者简介：金磊，2008 年毕业于西安交通大学。现任教于西安交大附中，除常规教学外，一直致力于特色教学的实践与研究。近年来在《数学通讯》等多个杂志上发表文章近 10 篇。

是非成败转头空 *异或运算的应用*

万精油

上期趣味数学专栏的题目是棋盘定位。为方便解答，我们把上期题目再列一遍。

上期题目：

棋盘定位：教授把你叫到他的办公室，给你一个国际象棋棋盘（8×8 方格），棋盘上有些格子里有棋子，有些格子里没有棋子。棋子都是翻过来的，也就是说每个棋子都一样。教授在棋盘上随便指了一格。你现在需要做下面两件事中的一个：

1. 选一个有棋子的格子，把棋子从格子中拿走。

   或者

2. 选一个没有棋子的格子，放一个棋子到格子中。

教授再把你的朋友叫进来，把你改变过的棋盘给他看。他的任务是从棋盘中看出教授所指的那个格子。

注意，棋盘的初始状态是随机的，教授所指的格子也是随机的。两个动作你只能选一样来做。你可以事先与你的朋友商量好一套利用棋盘上的棋子位置的信息传递系统，使得你的朋友总可以确定教授所指的格子。

解答：将棋盘上的位置按 0, 1,⋯, 63 标号。对任何一个格局 A，设 $F(A) = x_1\text{^}x_2\text{^}\cdots\text{^}x_k$，其中 $x_1,\cdots x_k$ 为其位置上有棋子的点的标号。符号 ^ 为对应于每一个比特的异或运算。对于教授指定的任何一点 p，只要变动 $F(A)\text{^}p$ 位置上的棋盘即可。如果该点没有子则加子，有子则把它拿掉。

你的朋友看到格局 B 时，只需算出 $F(B)$, $F(B)$ 所对应的点即为教授所指定的点 p。

对于熟悉异或运算的人来说，这个解法一目了然，非常漂亮。对于不熟悉异或运算的人来说，可能看不懂。我们现在就来介绍一下这个异或运算。

异或运算是一个逻辑运算。当两个输入量不同时，输出 1，反之输出 0。这个运算英文叫 ExclusiveOR，计算机语言里常用 XOR 表示对每一个比特的异或运算。比如，12 与 9，表示成 2 进制就是 1100, 1001，12^9 = 1100^1001 = 0101 = 5。显然，在有多个数做异或运算时，运算结果由每一个比特上的 1 的奇偶性决定。奇数个 1 结果就是 1，偶数个 1 结果就是 0。

异或运算表

输入		输出
A	B	
0	0	0
0	1	1
1	0	1
1	1	0

考虑一下模 2 的加法运算。$0+0=0$; $0+1=1$; $1+0=1$; $1+1\equiv 0(\mathrm{mod}2)$。可以看出，异或运算与模 2 的加法等价。它满足交换律、结合律。

从这个模 2 等价可以得出异或运算的一个重要性能，我把它称为还原功能。具体说起来就是，对任意 x, y : x^$(x$^$y)=y$。因为任何比特自己与自己相加总是偶数，模 2 就是 0。所以，别的数不受影响。

当 y 与 x 进行异或运算后，表面上看起来，y 的信息消失了。但是，如果我们把这个结果再与 x 进行异或运算，消失的 y 又出现了。

有了这个还原性，我们可以来解释一下本文的标题。第一次运算，是是非非都成了 0(是与是，非与非都变成了 0)，正好对应了“是非成败转头空”。第二次运算，“转头空”的东西又出现了，正好对应那句诗的后一句，“青山依旧在”。

有了这些准备工作，我们可以来解释前面的解答了。

假设原来的棋盘格局是 A，教授指定点 p，我们变动的是 $F(A)$^p 点，其中 $F(A)$ 是对 A 中所有有棋子的点的标号做的连续异或运算。$F(A)=x_1$^x_2^$\cdots$^x_k，其中 $x_1,\cdots x_k$ 为其位置上有棋子的点的标号。

如果 $F(A)$^p 点没有棋子，我们在那里加一个子。设变动后的格局为 B。格局 B 就是格局 A 加上 $F(A)$^p，所以，

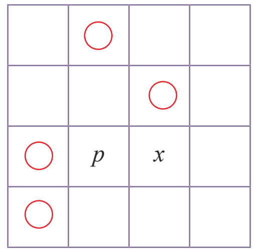
$F(B)=x_1$^x_2^$\cdots$^x_k^$(F(A)$^$p)=F(A)$^$(F(A)$^$p)$。利用异或运算的还原性，两个 $F(A)$ 消掉了，结果正好是教授指定的点 p。

如果 $F(A)$^p 点有棋子，设该点为 x_i, 我们把 x_i 点的棋子去掉，相当于对 x_i 异或运算两次（两次就把该点化为 0）。所以，

$F(B)=x_1$^x_2^$\cdots x_{i-1}$^$x_{i+1}\ldots$^$x_k=x_1$^x_2^$\cdots x_{i-1}$^$x_{i+1}\cdots$^x_k^$(x_i$^$x_i)=x_1$^x_2^$\cdots x_{i-1}$^x_i^$x_{i+1}\cdots$^x_k^x_i $=F(A)$^$x_i=F(A)$^$(F(A)$^$p)$，结果还是教授指定的点 p。

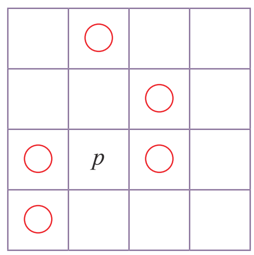
前面的解释或许太抽象，不好懂。我们来看一个具体例子：

假设棋盘是 4×4 的大小。初始格局如下图（有圆圈的格子表示有棋子）。



初始的格局 A

我们把棋盘从左到右，从上到下标为 0, 1, 2, ⋯, 15。有棋子的点的标号是 1, 6, 8, 12。在 2 进制下用比特表示这些数就是 0001, 0110, 1000, 1100。对这些标号做异或运算，我们有：$F(A)$ = 0001^0110^1000^1100 = 0011（只需数每个比特上的 1 是奇数还是偶数）；假设教授指定的点是 p（图中有 p 的点），这点的标号是 9，那么我们有：$F(A)$^9 = 0011^1001 = 1010。这是标号为 10 的点（图中有 x 的点）。根据我们的解答方法，由于这个点没有棋子，我们要在这个点加一个棋子。加完后我门得到格局 B 如下图



变换后的格局 B

你的朋友进来后看到格局 B，对格局 B 做异或运算 F(B) = 0001^0110^1000^1010^1100 = 1001，这是标号为 9 的点，正好是教授指定的点。解答完毕。

简单的异或运算漂亮地解决了这个初看起来似乎不可能的题目，异或运算大显神通。

这个题目实际上可以推广到大小为 $2^N \times 2^N$ 的任意棋盘。其证明不难。稍难一点的是证明只有这种大小的棋盘才可行。不是 $2^N \times 2^N$ 大小的棋盘就没有解。这个证明留给读者做练习。

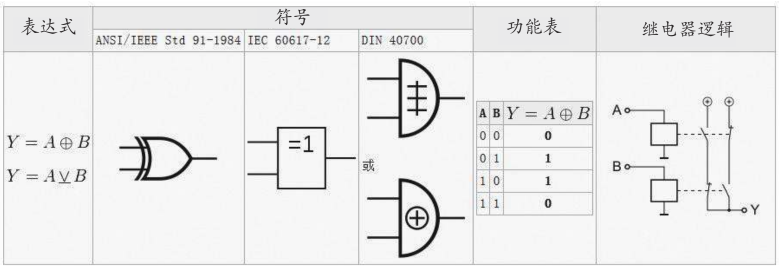
我们再回头来说异或运算。

学计算机编程语言的人基本上都会遇到一个经典题目，要求不用第三个变量，把两个变量的值互换。显然，如果用第三个变量，很容易互换两个变量的值。比如我们要把 X 与 Y 互换，只需引入一个临时变量 Z。$Z = X$; $X = Y$; $Y = Z$；X 与 Y 的值就互换了。如果没有第三个变量，一个变量赋予了一个值，那么它原来的值就丢失了，不能再传给另一个变量。初看起来这是一个几乎不可能完成的任务。这个时候异或运算的还原性就派上了用场。X = X^Y; Y = Y^X; X = Y^X。X 与 Y 巧妙的得到了互换。

说到不用第三个变量互换两个变量的值，想起一道小学时候的趣味题目。说是两个人在路上相遇，他们想交换各自大布袋里的货物（比如一个装的是小米，一个装的是大米），但又想把自己的袋子带回家。没有第三个袋子来倒腾，路面很脏，也不可能倒在路上。问他们怎样完成这个任务。（注：假设布袋很大，货物不到一半）。

这个题比较有趣，但与异或运算没有太大关系。我们还是回头来说异或运算。

异或运算的引入当然不是为了来解决这些趣味题目。它在逻辑、数字电路、计算机里有很广泛的应用。数字电路里的异或门就是异或运算的直接对应。若两个输入的电平相异，则输出为高电平（1）；若两个输入的电平相同，则输出为低电平（0）。



异或运算还可以应用在密码、储存、校码等等诸多方面。其基本原理都是依赖于前面提到的还原功能。

利用异或运算的简单密码：一个信息 X，与钥匙码 K 做异或运算后得 Y，传给另一方。另一方再用钥匙码 K 对 Y 做异或运算，恢复 X。

比如 X 为字符串 math，钥匙码为 12，$Y=$ math^12 $=$ amxd, 另一方得到字符串 amxd 后，与钥匙码 12 异或，amxd^12 $=$ (math^12)^12 $=$ math。原来的字符串得到恢复。不同的钥匙码会对原始码进行不同的加密。当然，这种加密法实在是太过于简单，很容易破。我们这里只是展现它的一个功能。

异或运算在储存与校码上的应用就比较实际了。假设有码 A，B 需要传递。我们传递 A, B 的同时也传递 A^B。对方收到 A, B 后可以用 A^B 来验证。用这种方法来做储存，如果其中任意一个有损坏，都可通过其它两个来恢复。A^(A^B) $= B$, B^(A^B) $= A$。

异或运算还有很多其它应用，我们不可能全部介绍完，有兴趣的读者可以自己去找相关资料来看。

本期趣味题目：

本期题目是被公认为最有趣的含数学原理的一个扑克牌游戏。

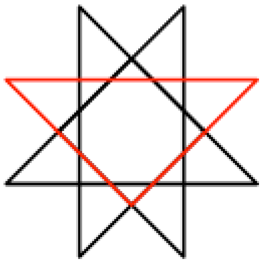
扑克传信：一副牌 52 张，没有大小王。一个观众从中随机抽出五张。你从其中选出一张藏起来，把剩下的四张放在桌上，让你的朋友根据桌上这四张牌的面值及顺序来推出藏起来的那张牌是什么。也就是说请你和你的朋友设计一套信号系统，使得不管抽出的是哪五张牌，你都可以用其中的四张牌来表示另一张牌。注意，你的朋友可以利用的信息只能是四张牌的面值与顺序。诸如把某张牌翻过来或是放斜一点，高一点，角上折一下之类的旁门左道都不能用。

上面的题做出来以后，请再考虑一下更进一步的情况——不是一副牌，而是一副麻将。筒、条、万各 36 张，中、发、白各四张，再加上春、夏、秋、冬，总共 124 张牌。能不能设计一套信号系统，使得不管抽出的是哪五张牌，你都可以用其中的四张牌来表示另一张牌？注：我们假设每张牌都是不同的。比如四个八万，应该可以像春夏秋冬一样区分。八万春，八万夏，八万秋，八万冬，诸如此类。也就是说我们有 124 张不同的牌。

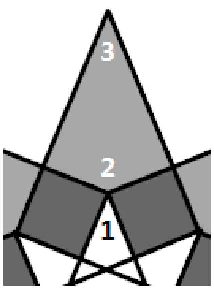
《数学文化》2013 年第 3 期数学趣题答案

1

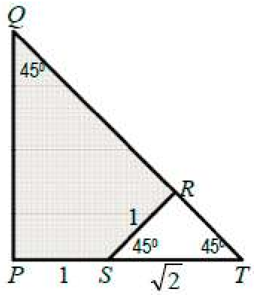
由题图易知，白色正八角星是由 4 个等腰三角形构成的。



题中已指明，深灰色部分为正方形；因此，上图中红色边框三角形为等腰直角三角形。故正八角星的每个角均为 45°。



所以，∠ 2 ＝ 360° − 90° ×2 −∠ 1 ＝ 135° ；
∠ 3 ＝ 360° − 90° ×2 −∠ 2 ＝ 45°。
对每个“风筝形”$QPSR$，延长 PS，QR 交于点 T，可作出如下图形：



$$S_{\Delta QPT}=\frac{1}{2}(1+\sqrt{2})^2=\frac{3+2\sqrt{2}}{2};$$

$$S_{\Delta RST}=\frac{1}{2}\times 1\times 1=\frac{1}{2}$$

所以“风筝形”的面积 $S_{\Delta QPSR}=S_{\Delta QPT}-S_{\Delta RST}=1+\sqrt{2}$

2

选一对方格填黄色，其余的填绿色，共有 C(49,2) ＝ 1176 种选法。

① 如果这一对方格关于棋盘中心对称，那么旋转 90° (或 270°) 后将与另一对方格重合；
旋转 180° 后与自身重合。
这种方格共 (49 − 1)/2 ＝ 24 对，因此不同的“对称涂色法”有 24/2 ＝ 12 种。
② 如果这对方格不关于棋盘中心对称，那么绕中心旋转 90°，180°，270° 后，将分别与另外 3 对方格重合。故不同的“不对称涂色法”有 (1176 − 24)/4 ＝ 288 种。
综上所述，不同填色法的数量为为 12 ＋ 288 ＝ 300。

3

设第 i 对男女栓对的概率为 $P(A_i)$，则一对都没拴中的概率为 $1-P(A_1\cup A_2\cdots\cup A_5)$。由容斥原理的基本公式，得

$$\begin{aligned}&P(A_1\cup A_2\cdots A_5)\\&=\sum_{i=1}^{5}P(A_i)-\sum_{1\le j\le i\le 5}P(A_i\cap A_j)+\cdots\\&\quad+(-1)^{5+1}P(A_1\cap A_2\cdots\cap A_5)\\&=C_5^1\frac{A_4^4}{A_5^5}-C_5^2\frac{A_3^3}{A_5^5}+\cdots+(-1)^{5+1}\frac{1}{A_5^5}\\&=\frac{1}{1!}-\frac{1}{2!}+\frac{1}{3!}-\frac{1}{4!}+\frac{1}{5!}.\end{aligned}$$

因此

$$\begin{aligned}&P(\overline{A_1\cup A_2\cdots A_5})\\&=1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\frac{1}{5!}\\&=\frac{11}{30}.\end{aligned}$$

补充：由以上计算可知，n 对男女都没栓中的概率，等于

$$1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}\cdots+(-1)^n\frac{1}{n!},$$

即 $1/e$ 的泰勒展开式的前 n 项和。当 n 趋向于无穷，该概率趋向于 $1/e$。

4

总共有 100 种分数，200 个人，所以每个分数至少重复两次（抽屉原理）。如果每个分数重复两次，总分 ＝（1 ＋ 100）×100 ＝ 10100（高斯求和）。10101－10100＝1，还余下 1 分，把这 1 分分配给任何一人，就会造成 3 个人同分。故至少有三个人的分数相同。

5

不考虑特殊因素 (例如闰年，双胞胎)，并假设一年 365 天的出生概率是平均分布的。若班上只有两个学生，很显然，这两个学生生日不同的概率是 1 × 364/365。再加入第三个学生，若要满足三人生日各不相同，则只剩下 363 种选择，此刻的概率是 1 ×364/365 × 363/365。

以此类推，n 个学生生日各不相同的概率

$$Q(n)=\frac{365}{365}\times\frac{364}{365}\times\frac{363}{365}\times\cdots\times\frac{365-n+1}{365}=\frac{365!}{365^n(365-n)!}$$

当 n ＝ 50 时，$Q(n)\approx3\%$。班主任的胜率低得可怜！这种与常识相悖的计算结果，被称为生日“悖论”。理解生日悖论的关键在于，任意两个人的搭配方式可以有很多。譬如 50 个人，就有高达 $C(50,2)$ ＝ 1225 种搭配方式。

本期数学趣题

1

一列长 200m 的火车沿长直轨道匀速前进。火车外面，一只闲的发慌的蜜蜂自车尾起飞，飞向车头，抵达后立即飞回车尾（全程匀速）。当蜜蜂回到车尾时，火车恰好行驶了等同于自身长度的距离。问这只蜜蜂总共的飞行路程是多少？

2

很多整数都能用由三个 2 组成的算式表达，譬如 4 等于 2 的 2 ＋ 2 次方的平方根，231 等于 $C(22, 2)$……那么，最小的不能用三个 2 表达的正整数是什么？为明确起见，本题可用的运算仅限加、减、乘、除、乘方、开根、阶乘、对数、排列数和组合数。

3

“若 x, y 均为无理数，则 x 的 y 次方一定为无理数”是真命题吗？请作出证明。

4

2012 是否可以写成两个整数的平方差？2014 呢？只要找准方法，解答或许会出乎意料地简单。

5

已知正方形 ABCD，只用一根直尺，能否作出面积为 ABCD 两倍的正方形？

注：直尺只能用来作连结两点的直线，尺上面没有刻度，也不能做标记。

数学与互联网安全

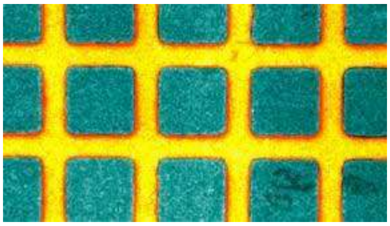
Joe Malkevitch ／文　袁晓明／译

2005 年 12 月离新年假期只有几天的时候，纽约的公交系统员工在纽约市区举行了大罢工。市民如果试图到商店去购物，可能会在路上堵上好几个小时、再走上很久的路、并且也很难拦到出租车。因此很多纽约市民选择了在网上进行购物。不过还是有很多人因为担心交易的安全性而对网上购物退避三舍。

大家心里的疑问包括：

- 网上金融交易是否安全？
- 通过互联网发送电子邮件是否受到第三方的监控从而导致邮件内容泄露？
- 网络病毒以及“流氓软件”正越来越猖狂，我们如何对付这些问题？

数学正在尽力解决上述这些问题，从而使得网络交易百分之百的安全，以及让电子邮件系统成为人们值得信赖的一种生活方式。实现这些目标的工具恰恰是一些以前被认为是毫无实用价值的数学知识！人们一直在发明新兴技术从而制造出更快更小的电脑芯片。一部分人正在致力于创造一个安全的互联网环境，而另一部分同时也在不停地试图通过互联网“提取”他人的财富（而不是在银行里排队取款！）。这是一场猫和老鼠的游戏，而这个游戏也受到电脑芯片技术的影响。



由美国国家标准与技术研究所（NIST, National Institute of Standards and Technology）开发的一项新的光刻技术，用于制造质量更好、速度更快的芯片

互联网技术涉及的数学知识十分广泛，从数据压缩和误差压缩技术，到信息传递的方法和安全设计都需要大量的数学知识。本文将着重讨论与互联网安全的几个数学问题。

密码学

一个战争指挥官总是希望他发给前线军官的命令不会落到敌方手中。因此，如果命令是通过书面来传递，那是十分不安全的。因为一旦命令书被敌方拦截，自己的计划就彻底暴露了。（当然要通讯员把命令背下来再进行传递也不现实，大家看看电视里的谍战片或反恐片就知道这种方式是多么不安全了。）尤利乌斯 • 凯撒（Julius Caesar）被认为是最早使用数学知识来对信息进行加密的人之一。据说他的加密方法是把一段文

字（也就是原始信息）的每一个英文字母都用字母表里其对应的后一个字母来代替，而字母表的最后一个字母就用其第一个字母来代替。按照这种方法，Caesar Cipher 这个短语就由 Dbftbs Djqifs 来代替。其实我们有很多种类似的加密方式来产生这样一段信息。因此，这样的加密方式足以迷惑“敌人”一段时间了。前面这个例子我们是把一段文字按照字母表往后移动 1 个位置。更一般的，我们可以按照字母表往后移动 r 个位置。比如 $r=5$ 的话，Caesar Cipher 这个短语经过加密以后就变成了 hfjxfw hnumjw。今天我们把这种加密方式都叫做凯撒密码。

但是，如果解密员碰巧想到一段文字的加密方式是把每一个英文字母按照字母表顺移同样的位置，那就算把每种可能的方式都试一遍来解密，其工作量都不大，因为毕竟只有 26 个英文字母。这个简单的例子已经说明了无论是互联网密码学还是军事密码学，“复杂度”和安全性两者之间都存在着有趣的联系。有时候，我们的目的仅仅是拖延对手的行动。比如，我们可以把一段毫无意义的信息加密，然后让对手花上整整一个小时去解密。不过，一旦一条信息被对方成功解密，下次我们再有一条类似的信息被对方拦截的话，解密时间可能就会从一小时急剧减少为 3 分钟了。所以我们必须想办法永远比“敌人”快一步。接下来的讨论里，我有时候混用“代码”和“密码”，以及“解码”和“解密”。不过，“密码”一般是指把一段文字的每一个符号都用同一字母表或其它字母表里的另一个符号来代替。相反，“代码”是指把一段文字的每一组符号用另一组符号来代替。

自从凯撒密码提出后，密码学得到了极大的发展。其中一个很简单的想法是加密的信息不一定要与原始信息有相同的字数。如果字母“*I*”或者“*a*”作为一个单词单独出现在一段加密字符串里，那这段加密字符串就很容易被破解了。通常的做法是，把一段信息的每 5 个字母分成一组（不记字间的空格和标点符号），然后每组都用另外 5 个字母代替。这样加密的字符显得更难破解。如果原始信息的字符数不是 5 的倍数，那我们可以额外地将一些符号定义为这个“转换”里的空集，然后用这些符号来补齐缺少的字符数。

另外一个简单的想法是用多字码密码，也就是说给原始信息加密的字母表按照某个密钥随字母逐字变化。由于原始信息的每一个字母都对应到密钥里的一个字母，用以加密的字母表也会不断变化。这个想法的代表人物是利昂 • 阿尔伯蒂（Leone Alberti），他也是射影几何的先驱。最初人们都相信这样一个“复杂”的加密系统是不可攻破的。不过，如果密钥含有的字符数不多，并且由同一加密系统得到的密文样本足够多的话，我们可以用一些统计的方法来破解这样的密码。如果一个钥匙是随机产生并只使用过一次，也即一次性密钥，那这样的密码是无法破解的。如今当我们试图对一些信息进行安全保护时，面临的一个很重要的问题是如何交换密钥，特别是随机产生的大量钥匙。

利昂 • 阿尔伯蒂（1404-1472）

在现代生活里，人们更是意识到数学在安全事物中的重要性，其中不得不提的人物是阿兰 • 图灵（Alan Turing）。

阿兰 • 图灵（1912-1954）

希特勒在攻占荷兰、法国等国家后，试图进一步攻占英国。当时，英国全力以赴试图通过使用通讯和信号智能技术以及解密信息技术来阻止德军侵占不列颠群岛。英军在布莱切利公园成立了一个由语言学家和数学家组成的特别行动组，尽量从拦截到的敌军信息里获得有用的信息。包括马里安•雷耶夫斯基（Marian Rejewski）在内的波兰数学家首先获得了成功，他们将破解的德军代码交给英军。

马里安•雷耶夫斯基（1905-1980）

图灵及团队根据波兰提供的信息，成功地破解了德军“恩尼格玛机”（Enigma machine）以及其它密码系统发出的密码。毫无疑问，图灵等人的成功改变了这场战争的结果，也改变了历史。

二战时德军的恩尼格玛机

图灵与数学家戈登•威尔士曼（Gordon Welchman）还发明了一种特殊的“计算机”来破解德军恩尼格玛机产生的密码。

图灵与威尔士曼共同发明的“炸弹机”（Bombe）

在美国，包括语言学家和数学家在内的男男女女们同样在战争中发挥了作用。其中最著名的可能是威廉•弗里德曼（William Friedman）（他是业余数学家）以及他的妻子、语言学家伊丽莎白。二战期间，美军破获了日本军队大量的密码，也因此成功取得了战争的胜利。

伊丽莎白•弗里德曼与威廉•弗里德曼

如今，密码学不再仅仅是为军事与外交服务了，它越来越多地用在资本财富的建设上，例如通讯与互联网。对于电子转账、电子邮件或者网上购物等系统的用户而言，他们总是担心自己的交易是否按照计划进行而没有被“劫持”。当然，这涉及到的问题也是十分地复杂多样。当我们给别人发送一条信息时，我们自然要考虑这些问题：第一，对方收到的信息是否就是我们发出的原始信息，而不是被人更改过的；第二，现在发出的信息是否会危害到将来发出的信息的安全；第三，别人会不会通过我们发送信息的方式而盗用我们的资料，然后以我们的名义再给别人发送邮件。

“阴谋”这个人们常常与间谍或者间谍行为联系在一起的词，一样会在互联网安全领域里大肆横行。

散列法

散列法即按照某种方法，用一串短很多的字符替代一串长字符。例如，我们可以仅仅用一首诗包含的字母个数来表示这首诗。乍看上去，散列法似乎是关乎数据压缩，而不是数据安全的。显然在散列系统里我们可以设法隐藏原始字符，使之很难破解。因此很容易理解为什么一串被打散的字符可以起到加密的作用。使用散列法需要注意的是避免两组不同的字符串最后被散列成同一字符串。这种情况叫做冲突。在这样定义的散列系统里，如果两首诗歌有相同的字符个数，那么就会产生冲突。因此，我们在设计散列系统时，必须要说明怎么处理冲突情况。散列法的另外一个好处就是，两列相似的字符串经过散列后，可能会大不一样。因此，即使有人试图对一个加密过的文档进行微小的修改，也会很容易地被发现。因为原始的和伪造过的两个文档的散列字符串大相径庭。同样我们可以理解为什么散列法与用户登录密码和数字签名密切相关。数字签名是一个电子确认系统，其功能与我们书信或支票中常用的手写签名类似。我们当然希望一个数字签名系统可以尽可能地降低伪造的风险。在 1990 年代中期，麻省理工学院的罗纳德 • 李维斯特（Ronald Rivest）设计的 MD-5（Message-Digest Algorithm 5）散列系统被广泛的使用。不过，数学家和计算机学家于 1996 年在这方面做出了一系列的研究，使得人们意识到 MD-5 有着安全性能方面的缺陷。于是 MD-5 被 SHA-1 取代。

散列法在用户密码管理系统里十分常用，因此它与互联网安全也早已密不可分。除了登录电子邮件账户，人们还常常需要使用用户密码来登录一些互联网提供的商业服务（例如报纸或金融网站的账户）。你可以很快根据一些简单的规则来改进自己的用户密码，从而使得自己的密码比大多数人的更安全。不幸地是，只要计算设备足够好，好几个有关散列系统的标准都被证明是有安全性能隐患的。最近，被认为是有关散列系统安全性能通用标准的 SHA-1 也被证实是不安全的。这是由中国数学家王小云和她的团队发现的。当然，人们对王小云的成果短期内是否会影响业界意见并不一致。尽管我们暂时还没有可破解 SHA-1 的计算设备，但王小云取得的成果足以让我们相信她的尖端成果有可能攻击现有的安全系统。比 SHA-1 更安全的散列系统确实已经出现了，不过这方面的进展并不快。

王小云（1966-）

有这么多的加密办法，好像要从一段加密信息恢复出原始信息实在是太困难了。一般有两种破解办法。第一种方法是用统计技术。如果我们拿到大量的加密数据，那么我们可以试图寻找其中的一些特定模式（例如分析一些符号的出现频率的分布情况）来进行破解。另一种方法是注意到加密的人经常会有些特定的语言习惯，而我们可以利用这一点作为解密的切入点。比如有些人在一段信息的开始总是用同样的问候语。再比如有些信息都是以天气报告为开头，这也使得解密者可以试图猜测一些相同的字符是如何编码的。还有一点就是，一个被广泛使用的系统通常都有不少人参与管理与维护。这时候，很难确保该系统的信息不被流传出来。因此，用来解决替代密码的方法与基于母体技术的方法不同。从现实角度来看，很多人都接受以下观点，即只有在假设攻击安全系统的人已经完全知道该系统的设计方案的前提之下，才能真正解决安全问题。因此，“敌人”或许已经知道你正在使用 RSA（下面会解释）还是 Hill 密码（基于矩阵的系统）。

公钥系统

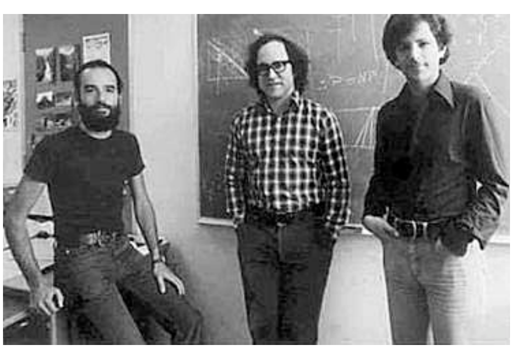
1970 年代中期，人们发现了一种全新的编码方式（也有人认为其实早就有人发现了），这是密码学的一个里程碑式的发展。传统的密码学里，需要共享一段加密信息的双方会设置一个系统，并需要完成一把钥匙的交换。直观上我们可以理解为这把钥匙将一段秘密发送的信息锁起来。当接收信息的人有一把一模一样的钥匙时，

自左至右依次为惠特菲尔德•迪菲（1944-）、马丁•赫尔曼（1945-）、拉尔夫•梅克尔（1952-）

他就可以解开这段被锁起来的信息。因此，在单钥系统里，加密和解密的双方有一把同样的钥匙。

公钥系统的出现改变了这一切。有关公钥系统的发展三言两语无法说清楚，不过人们普遍认为拉尔夫•梅克尔（Ralph Merkle）、惠特菲尔德•迪菲（Whitfield Diffie）和马丁•赫尔曼（Martin Hellman）三人在这个领域做出了非常重要的贡献。

公钥系统有两把钥匙。一把用于给某人 X 发送一段密码信息。正如电话簿上的电话号码，这把钥匙是公开的。另一把则不公开，它与公钥一起由 X 保留。公钥加密学与现代私钥系统还允许陌生人之间随意交换钥匙。这样的系统是由迪菲和赫尔曼在梅克尔的想法基础之上发明的，并用于不加密的通讯系统。这个系统已经申请了专利，不过现在专利保护的时间已经到期了。下面我们略微讨论一下最为人们所熟知的公钥系统，即以罗纳德•李维斯特、阿迪•萨莫尔（Adi Shamir）和伦纳德•阿德曼（Leonard Adleman）这三位发明者命名的 RSA 系统。



自左至右依次为阿迪•萨莫尔（1952-）、罗纳德•李维斯特（1947-）、伦纳德•阿德曼（1945-）

还有一个很常用的公钥系统是由塔西尔•埃尔格莫尔（Taher Elgamal）在 1984 年提出来的。这套系统主要用群论和复杂性的知识来保证安全。

塔西尔•埃尔格莫尔（1955-）

对 RSA 和 ElGamal（也包括其它系统）而言，一个很有用的概念就是同余。如果两个整数 a 和 b 被一个大于或等于 2 的正整数 m 除以后，得到相同的余数，那么我们就说 a 和 b 同余，记为

$$a \equiv b \text{ modulo } m.$$

此时，$b-a$ 被 m 除的余数是 0。以下是一些例子

$$12 \equiv 2 \text{ modulo } 5.$$

$$-3 \equiv 2 \text{ modulo } 5.$$

$$-3 \equiv 23 \text{ modulo } 13.$$

对于模 m，我们总共可以将一对同余数右边的那个数替换成介于 0 与 $m-1$ 之间的一个整数。比如，上述最后一对同余数，我们可以将 23 替换成 10。在以下表达式里，我们可以很容易确定“？”的值：

$$5^{72} \equiv ? \text{ modulo } 19,$$

办法是计算 $5, 5^2, 5^4, 5^8$ 等数取 19 的模，然后利用指数的二元表示法表示出 72 这个指数，并把答案找出来。不过，要找到整数 k 使得同余表达式：

$$5^k \equiv 13 \text{ modulo } 19$$

成立就不那么简单了。类似于这样的寻找 k 的问题被称为离散对数问题。当模非常大的时候，人们还不知道有什么方法比穷举法快很多。而对于解决离散对数问题和一些在设计公钥系统中用到的算法的复杂度，人们还知之甚少。一些基于 NP-complete 问题而建的系统崩溃了，而一些基于复杂度并没有完全搞清楚的问题而建的系统反而运行良好。下面我们将简单讨论一下被广泛用以衡量互联网安全性能的 RSA 系统。

小测试

许多公钥加密系统人员都受到“单向函数”的启发。有些任务很容易完成，但他们的反向任务则很难，除非有特殊的附加信息。

如果你想感受一下有关复杂度的数学知识是什么以及它是如何与安全性能联系在一起的话，试试下面的例子，用一个带秒钟的表测试一下你需要花多少时间求解这些例子。

问题 1：123457 乘以 372451 等于多少？

问题 2：374251 的因子？（我确定除了 1 和它本身，还有别的因子）

你也许会发现，问题 1 虽然很繁琐，但是得到它的答案并不难。然而，即使你能解决问题 2，你花的时间可能要比问题 1 多的多。大多数人甚至都没有耐心去完成最终的解答。

问题 1 比问题 2 更简单，这意味着什么？问题 1 要求两个数的乘积，更具体地说是两个 6 位数的素数的乘积（素数是指它的因子仅有 1 和它本身），而问题 2 是要求将一个可以表示成两个素数乘积的数进行分解而得到这两个素数。（即已知 s 是某两个素数 p 与 q 的乘积，求解 p 与 q.）

大部分人都认为还没有一个真正的快速算法可以在一部普通的电脑上快速地分解整数。但同时，人们也没有任何结果表明整数的分解是一个 NP-complete 的难题。NP-complete 问题是指一类难度一样的问题，也即如果这些问题的其中一个可以被多项式级别的时间求解的话，那么所有这一类问题都是多项式时间可解的。另一方面，如果其中一个问题需要指数级别的时间求解的话，那么所有这一类问题都是指数级别的时间可解的。不过，虽然很多人都认为一些问题需要指数级别的时间求解，但事实上这一点也没有人可以完全肯定。大家认为没有简单算法可以对一个大整数进行因子分解，而且直到不久前，人家也不知道究竟是否有办法用多项式级别的时间来验证一个数是否是素数。所以当马尼卓•阿格拉瓦尔（Manindra Agrawal）、尼瑞艾•卡亚尔（Neeraj Kayal）和尼廷•塞克希纳（Nitin Saxena）三人提出一个验证素数的多项式算法时，人们感到十分意外。现在有很多快速算法可以验证一个数是否是素数。有意思的是，其中最快的一些算法的确可以在绝大多数情况下检验素数，但偶尔也会把一个复合数误认为是素数。验证素数的多项式算法方面的进展也意味着我们有可能找到实现整数的因子分解的多项式算法。（值得一提的是，不是每个多项式算法在求解实际问题的时候都很快。而有些指数算法，例如求解线性规划的单纯型法，在求解实际问题时却十分有效。原因是实际碰到的很多问题并不会令单纯型法无效。）

下面简单介绍一下广为人知并被广泛使用的 RSA 公钥密码系统。我们假设已经将一段要发送的原始信息的文字（例如英文）分成一块一块的结构，而原始信息的每一块也用一个数字 M 来表示。我们需要考虑怎么安全地发送 M。接下来，我们产生两个大素数 p 和 q。相对来说，这比较容易（也有人认为如何选这样的素数直接影响到最后的加密安全）。现在我们选一个大于 1 的整数 e，它要与乘积 $(p-1)(q-1)$ 互素。两个整数称为互素，如果能被这两个整数都整除的最大整数是 1。例如，12 和 35 都不是素数，但它们互素。然后，我们找一个整数 s 使得

$$(e)(s) \equiv 1 \text{ modulo } (p-1)(q-1),$$

之后，再计算 p 和 q 这两个秘密的素数的乘积 $n = pq$。为了发送 M 这个信息，我们计算 C 来产生一段密码电文：

$$C = M^{e} \text{ modulo } n,$$

其中 e 和 n 的值即是公钥。注意 n 是两个大素数的乘积。如果 n 不能分解的话，它的值对密码电文 C 而言毫无价值。

解密者通过以下计算来解密：

$$C^{s} \text{ modulo } n,$$

其中解密者的私钥可以由 s 和 n 生成。这些值用于恢复原始信息 M。

为什么这样计算就可以得到 M 呢？其中原因（我们省去细节）涉及到了数论中的两个经典定理，一个是费马（1601-1665）提出的“费马小定理”：

$$a^{p-1} \equiv 1 \text{ modulo } p,$$

其中 p 是素数，而 a 与 p 互素。另外一个定理是欧拉（1707-1783）提出的，它涉及到一个表示与 x 互素的整数个数的函数。我们记这个函数为 $\varphi(x)$，也称为欧拉函数或者熵函数。对于任意的素数 p,

$$\phi(p) = p - 1.$$

而且，如果 x 与 y 是互素的整数，我们有以下关系：

$$\phi(xy) = \phi(x)\,\phi(y).$$

于是，对于不同的素数 p 和 q, 我们有

$$\phi(pq) = (p-1)(q-1).$$

欧拉还证明了一个涉及到 ϕ 函数 $\varphi(x)$ 的有关费马小定理的非常漂亮的推广：

$$a^{\phi(x)} \equiv 1 \text{ modulo } x,$$

其中 x 是一个与整数 a 互素的正整数。

由于 RSA 系统的安全性依赖于大整数分解的复杂性，使用 RSA 系统的公司对数学家和计算机学家提出了很多有关整数分解的难题。最近，有人分解了一个 193 位的数，而这在之前是被认为十分困难的。现在也有不少人悬赏可观的奖金来求解一些整数分解问题，不妨看看这个网站 (http://www.emc.com/domains/rsa/index.htm?id=2093)！

最近，一个有关 RSA 和其它公钥系统安全性问题的担忧出现了。这一担忧关乎复杂度。随着传统计算机的速度变得越来越快，人们不禁要问是否可以用穷举的方法来破解加密系统。之前使用很多年的商用传统编码基本都是 IBM 公司制定的 DES(Data Encryption Standard) 标准。由于 DES 不再安全，一种新的标准也应运而生。这个新的标准被称之为“高级加密标准”，并以其发明者 Joan Daemen 和 Vincent Rijmen 的名字组合而命名为 Rijndael。在取代 DES 而成为新标准之前的试用阶段，Rijndael 经过了极其严格的检查和考验并通过了各种测试，最终才投入使用。不过，大家认为 Rijndael 在数学上是极其“完美”的，以至于有人认为它会因为数学上的太过完美而最终被弃用。也许最后我们还是可以根据 Rijndael 系统漂亮的数学结构来找到还未被发现的漏洞去破解它吧。

与计算机以及计算机技术支持的电信业紧密相关的数字革新发展，都是基于使用功能强大的单片机或者是使用多芯片技术的并行机。不过，科学家们正在努力发展一种基于物理学中的量子力学概念的全新计算方式。这种新的计算方式被称为量子计算。数学家彼得 • 绍尔（Peter Shor）等人认为，一旦量子计算机成为现实，那么有些需要通过常规计算机花费很长时间求解的问题，其计算时间将会大大缩短。其中，Shor 指出整数的因子分解这个问题如果用量子计算机来处理的话，就会比用传统电子计算机快很多。因此，如果量子计算机出现了，那么 RSA 系统就无法再保证密码系统的安全了。这个涉及到物理、数学以及计算机的新兴学科究竟会发展到什么情况，人们正拭目以待。

互联网已经改变了美国人以及世界各地所有人的交流方式，也改变了人们的生活。如果互联网还像人们所期望的那样继续给人们的生活带来正面影响，那么数学家也将继续参与互联网的发展。

后记：有关互联网安全的文献的更新速度是非常快的。一些对电脑运算速度要求不高的安全保障方法以及在一定时间里最好的算法经常没过多久就失效了。读者可以在网上查阅互联网安全的最新发展趋势。

本文原文链接：http://www.ams.org/samplings/feature-column/fcarc-internet

注：译者袁晓明博士是香港浸会大学数学系副教授。

数据贵过黄金?

Joseph Malkevitch ／文　　曾铁勇／译

在不同的时期，不同的地方，黄金一直备受人类社会的推崇。2011 年，某些地方黄金的价格每盎司突破了 1900 美元。多年来，黑金一直是对石油（目前每桶超过 100 美元）的重要性和价值的形象比喻。但是数据有可能成为未来真正有价值的商品吗？如果是这样，这与数学有什么关系呢？

2012 年的四月是数学宣传月，这一年的宣传主题是：数学、统计和海量数据。

本文的目的是要探讨短语“数据挖掘”的含义，以及为了促进这个领域的发展采用了哪些数学工具和思想。数据挖掘的起源之一是减小数据的占用空间，从而产生了对收集到的数据进行分析的需求。本文将给出一个非数学问题引起数学界关注后，相关的数学又如何发展的经典例子。人们不止一次看到，过去所发展的数学，只因为其“美”及智力上的吸引力，常常是洞悉新的应用环境的工具。在描述问题的背景后，我将给出一些引起广泛关注的和数据相关的例子，并探讨涉及数据挖掘的“人工智能”的方法。

无处不在的数据

什么是“数据”？作为多重领域使用的术语，数据最常代表的是“事实”或数值形式的统计。然而，有时这个术语又被用来表示将要被分析或用来做决断的信息，最近出现的对于数据的“定义”又涉及到用计算机处理或分析的数字、符号、字符串和表格。

虽然数据长伴我们，但利用数据进行更深入的探索并（或）影响决策的想法则相对较新。几何和代数之根源可上溯千年，而“数据”数学则是近代产物，在过去的 150 年间发展迅猛。产生这种现象的部分原因是人们需要计算或分析大规模数据以获得重要信息，但这往往非常耗时，且受制于人为错误。因此，人们很自然地求助计算机来大规模采集和分析数据，以达到快速和准确的目的。

在看到不因噪音或偶然测量误差而出现的

模式这一意义下，要了解数据，需要懂得概率论。概率论和统计学是在许多方式下共存的两个科目。然而，概率是一个困难与微妙的学科。尽管概率论的数学基础相当坚实，但在数学之外的学科中用概率来数学建模，却异常复杂。当我们给出一个陈述：一枚硬币出现正面的机会稍大于出现背面的的机会，比如假设出现正面的概率为 0.501，而出现背面的概率为 0.499，如何诠释这个陈述呢？如果在投掷方式不影响硬币出现正面或者背面的情况下（注意：某些技高一筹者可以多次投掷一枚硬币使得每次都出现正面）多次投掷硬币，将得到一个关于出现 H（代表正面）和 T（代表背面）的模式。例如，投掷一枚硬币 10 次而得到下面的模式：

TTHHHTTTTH

现在，基于这个有限的、很小的硬币投掷集合，出现正面的相对频率为 4/10（10 次投掷出现 4 次正面），而出现背面的相对频率为 6/10（10 次投掷出现 6 次背面）。由此你也许看到了这里出现的一个困难：对于任何一次固定数量的投掷，甚至是一次非常大数量的投掷，得到出现正面的相对频率为 0.501 和出现背面的相对频率为 0.499 的情况十分罕见！概率的“稳定的相对频率”的解释为：从长远来看，随着投掷次数变得越来越多，得到正面和背面的相对频率将分别为 0.501 和 0.499。不幸的是，似乎没有方法使得产生这种论点背后的直觉很“严谨”。除此之外，有些说法比如，这个电厂在未来 10 年将会发生核事故的概率为 0.00000001，或者明天在波士顿某些地区将会下雨的概率为 4/10 都没有很清晰的含义。

现代概率的观点是概率是受制于某些规则（公理）的系统，概率“直观的”性质产生于这个系统。这些规则意味着当有人使用“相对频率”的观点时，在一定意义上不会被误导。然而，这些年出现了其它的途径来“解释”概率的含义。显然，对于滚动骰子、投掷硬币及孩子的出生性别模式，可以较合理地理解概率意义下稳定的相对频率。然而，对于一个核电厂的燃料棒在未来 10 年内发生熔毁的可能性，概率的相对频率意味着什么呢？出现这类事件的历史非常短，所以对其稳定的相对频率的理解变得毫无意义。即使对于天气报告中经常出现的预报，比如明天下雨的可能性（概率）是 80% 的预报，我们应该如何理解呢？

因数学家长期纠结于对概率这个概念所赋予的意义，导致了许多不同的“矛盾的”观点的出现。有鉴于此，概率和统计学的杰出贡献者伦纳德 • 萨维奇（Leonard Savage, 1917-1971）指出：“众所公认，统计学在某种程度上依赖于概率。但是，对于概率是什么以及它如何与统计学相联系，很少像今天如此激烈地争论并产生完全不同的观点。”

伦纳德 • 萨维奇（1917-1971）

问题之一是如何使用共同的语言（无论是英语、法语等）来表达不同环境下涉及到的“噪声”、“随机性”、“可能性”，或者是“意外”。放射性衰变机制显然不同于龙卷风会将袭击哪个州，或将会在哪天袭击这样的问题。

目前对于概率意义有多种诠释。作为一个例子，概率论的一种解释涉及到可根据经验获得的知识来帮助主观判断。这种方法也称为贝叶斯概率（即使是这个术语也存在几种不同的版本），它试图量化当和目标事件相关的某事件发生的概率正知后，如何来修正目标事件发生的概率。由这种角度产生的“概率”与数学家的正规方法产生的“概率”遵循相同的基本规则。然而，基于概率的不同表示所得到的推理方法也会有所不同。因此，会存在一些情况，因为采用不同的概率表示方法，做决断时就要从不同的可能中选择一种。估计这个复杂的议题将长期被数学家、统计学家和哲学家大范围地讨论。

概率和统计的先驱

在数学中，重要的思想凭空出世是非常罕见的。许多国家的科学家都为概率和统计的发展做出了贡献。本节将简要介绍一小部分重要贡献者。毫无疑问，概率论中相对频率的早期先驱之一是法国哲学家和数学家布莱士•帕斯卡（Blaise Pascal, 1623-1662）。帕斯卡的出发点是赌徒在实际赌局中的机会问题，在此前提下他提出了一些较深刻的见解。

布莱士•帕斯卡（1623-1662）

英国牧师托马斯•贝叶斯（Thomas Bayes, 1702-1761）对概率论有了更深刻的理解，并且作出了极其重要的贡献。

托马斯•贝叶斯（1702-1761）

贝叶斯的著名成果涉及到条件概率这个概念，这些条件概率可以针对于人们在实验中看到的或者在某些假设下产生的。这样实验或假设出现的结果称为事件。当无偏地投掷硬币（这时出现正面或背面的相对频率假定为 1/2）10 次，那么 10 次中正好出现 7 次背面的概率是多少，或者 10 次中正好出现 7 次正面的概率是多少？假设生男生女的概率为 1/2，以及不同的出生事件是彼此独立的（即一个小孩的出生不影响其他小孩的出生），那么，一对夫妇生的前两个小孩都是女孩的概率是多少？如果有序的字符串 GGB 表示第一个小孩是女孩，第二个小孩是女孩，第三个小孩是男孩，那么所询问的概率可表示为 $P(GG)$ 是多少？我们也可以利用角标来表示出生的顺序，如 B_1, G_2, G_1B_2 分别代表三个事件：第一个小孩是男孩，第二个是女孩，第一个是女孩且第二个是男孩。现在假设我们知道第一个小孩是女孩。问两个小孩都是女孩的概率是多少？这里我们问的是在给定第一个小孩是女孩的条件下，两个小孩都是女孩的“条件概率”。更一般地，令 $P(X|Y)$ ＝事件 Y 发生的条件下事件 X 发生的概率，也可以记 $P(Y|X)$ ＝事件 X 发生的条件下事件 Y 发生的概率。不难看出，直观上假设 $P(Y)$ 不为零，则

$$P(X\mid Y)=\frac{P(X\text{且}Y)}{P(Y)};$$

利用两个集合 X 和 Y 的交集的符号，上式可以转变为

$$P(X\mid Y)=\frac{P(X\cap Y)}{P(Y)}.$$

经过片刻的思考，我们就知道当 $P(X)$ 和 $P(Y)$ 都不为零时，$P(X|Y)$ 和 $P(Y|X)$ 并不需相等。

例如，对于上面的小孩出生问题，我们可以知道 $P(G_1G_2|G_1) = 1/2$, $P(G_1|G_1G_2) = 1$; 这里我们用到的下面的事实：$P(G_1G_2) = 1/4$, $P(G_1) = 1/2$.

在计算条件概率时，贝叶斯给出了著名的贝叶斯定理，这个定理在贝叶斯死后才得以

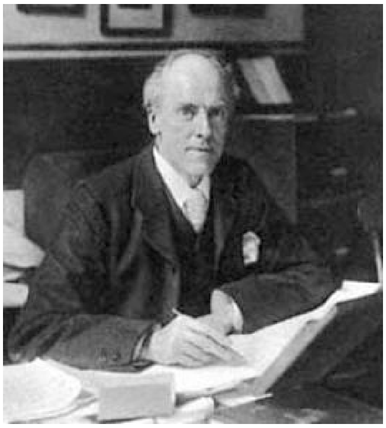
发表。直观上理解，贝叶斯定理提供了一个框架，可以从中排序出对导致事件发生的“因素”（事件）有“相对”影响力的事件。更具体地说，假设我们有一系列事件 $X_1, X_2, \cdots, X_k$，事件间相互排斥，即只可以有一个事件发生。因此，在同样一个空间中，一个实验的结果属于由这些事件组成的集合。假定 E 是一个概率不为零的事件。假设我们知道 E 一定发生，那么如何计算 $P(X_i|E)$？贝叶斯定理是一个“公式”，由这个公式可以计算出 $P(X_i|E)$ 的值，即已知 E 发生，一个特定因素 X_i 发生的概率。

数学史的较早期，即 18 世纪或者更早时，几乎所有对数学做出重大贡献的人同时也是伟大的物理学家。如牛顿（Isaac Newton, 1643-1727），欧拉（Leonhard Euler, 1707-1783），拉普拉斯（Pierre-Simon Laplace, 1749-1827），勒让德（Adrien-Marie Legendre, 1752-1833），高斯（Karl Friedrich Gauss, 1777-1855），他们不仅是杰出的数学家同时也是杰出的物理学家。作为物理学家，他们对数据中的“噪声”，即物理量的测量误差，均有所关注。统计和概率论的某些理论正是源于这种考虑。上面提到的数学家高斯以不同方式思考这个问题，由此产生了“最小二乘法”。正态分布的相关思想亦由此产生。另外，统计学不仅关注自然科学，而且关注社会科学。在这方面的先驱者之一是比利时的数学家和科学家阿道夫•凯特勒（Adolphe Quetelet, 1796-1874），他利用正态曲线来研究人类的特点，并从分析的角度来研究犯罪规律。其工作属于将统计思想用于社会学的早期实践。

阿道夫•凯特勒（1796-1874）

在现代，越来越多的人对统计及统计与概率论的结合做出贡献。在这里，我将要展示的不仅是来自不同背景不同国家的人们对统计和概率的贡献，更要说明有多少成果根源于近代。当然了，把这个话题说透彻大概需要一本书的内容。

卡尔•皮尔逊（Karl Pearson, 1857-1936）在英格兰出生及去世。皮尔逊曾就读于剑桥大学，而他的大部分职业生涯在伦敦大学的大学学院度过。皮尔逊对利用数学的思想来研究进化感兴趣，这也促使他提出了新的统计思想和方法。他 1894 年提出的标准偏差这个术语为众多文科修读统计的学生所知，标准偏差也成为度量数据发散程度的通用术语。皮尔逊还促进了使用大样本的统计检验思想的发展。



卡尔•皮尔逊 (1857-1936)

像所有的数学分支一样，在精细的审视下，统计学的发展有着丰富而复杂的历史，其推动者的身份不仅仅是数学家，他们同时也从事其他学术领域的智力活动。凯恩斯（John Maynard Keynes, 1883-1946）在经济学领域大名鼎鼎，然而他在剑桥大学学习了数学，并于 1921 年出版了关于概率论的一本重要专著。凯恩斯的工作被数学家、哲学家罗素勋爵关注，同时也引起了弗兰克•拉姆齐（Frank Ramsey）的注意。除了组合数学方面的著名成就（今天我们称为拉姆齐定理），拉姆齐同样在概率论和统计学方面做出了重要的贡献。最初凯恩斯的概率观点趋向于稳定的相对频率方法，但随着时间的推移，他的观点逐渐趋向于主观性更强的信念体系，可能在经济学中这个更有吸引力吧。

约翰•梅纳德•凯恩斯（1883-1946）

罗纳德•费舍尔（Ronald Fisher, 1890-1962）是另一个曾受教于剑桥大学的英国数学家，他在统计学研究中硕果累累。所谓的 F 检验即以他的名字命名。费舍尔同时也对实验设计感兴趣。他在英国罗森斯德（Rothamsted）的一个农业试验站工作多年，在那里他参与了一个实验，研究不同的培育方式对植物生长的影响。培育方式包括浇水制度、土壤的不同类型、施肥方案等。利用统计分析这一工具，可以找出不同的培育方式对不同类型的植物所产生的影响，并可根据结果改进方案来增加粮食的产量。很遗憾的是，费舍尔和皮尔逊在他们职业生涯中曾一度因费舍尔的统计思想和方法发生过激烈的争执。

罗纳德•费舍尔（1890-1962）

耶日•奈曼（Jerzy Neyman, 1894-1981）出生于俄罗斯，但后期研究主要在美国进行。期间他也曾在伦敦住过一段时间，在那里，他与卡尔•皮尔逊的儿子、统计学家埃贡•皮尔逊（Egon Pearson 1895-1980）相互交流。后来，奈曼在加州大学伯克利分校工作，并使该校的统计系闻名世界。

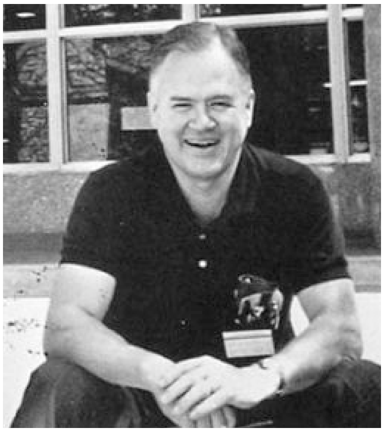
耶日•奈曼（1894-1981）

布鲁诺•德费奈蒂（Bruno de Finetti, 1906-1985）出生于奥地利，在意大利接受教育，最后在罗马去世。他以提倡从“主观”的角度理解可能性的含义而闻名。

布鲁诺•德费奈蒂（1906-1985）

随着计算机功能不断增强，数学家开始借助这个强大工具来探索和发现数据中隐藏的信息。约翰•图基（John Tukey, 1915-2000）是这一领域的先驱之一，他创造了二进制数字中的术语“比特”。图基一开始是化学系的学生，

但最终从普林斯顿获得数学博士学位。他长期在贝尔实验室工作，并曾担任实验室副主任。为了从数据中获得尽可能多的信息，图基和他的同事研究如何开发计算机的新功能、增大内存及加快计算机的处理速度。人眼对视觉模式异常敏感，所以图基和贝尔实验室的同事还探讨了如何利用人类视觉系统来显示数据以探索数据。他最传世的工作应该是他和合作者詹姆斯•库利（James Cooley）于1965年提出的快速傅里叶变换，这是信号处理领域最重要的工具之一。



约翰•图基（1915-2000）

数据密集型课题

有时我们会称最近在数据里“溺水”了。出现这个说法的部分原因是有非常多的数据正在被生成、收集及存储，可我们大多数人并没有时间去浏览这些数据，更不要说去思考数据里蕴含的意义。从某种意义上来说，21世纪美国人生活的各个方面都在被数据驱动。为了更清楚理解这一点，下面将列举几个“数据密集”的领域。

即使是在高速计算机出现之前，某些领域已经在广泛地收集数据了。下面会简短给出几个这样的领域，科学家不断研究新的统计方法，以便对付这些领域中的大数据问题。

天气

获得好的天气预报通常需要求解数学中的偏微分方程，而这些方程需要数据作为输入。不同来源的详细信息收集到一起，可以从中获得精确的天气信息。人们对天气一直比较感兴趣，这导致了大量数据的生成。这不仅是因为天气关系到上班时带不带伞的问题，而且有助于庄稼种植和庄稼收割等重要民生问题。与天气同时收集的信息有气压、温度、相对湿度、风力强度和方向、雨雪量等。这些数据都可用来做决策或规划，比如利用这些数据可以分析冰川和极地冰盖的融化及这些变化对临海国家的影响。

医学成像

医学成像数量及使用量急剧增多，许多成像的突破都受益于数学的支持。例如，约翰•拉东（Johann Radon）的工作，即拉东变换，使得层析成像成为可能。其他技术，包括计算机速度和存储，也在促进医学成像的发展。随着医学信息系统的不断完善，在治疗同一个病人时，医生们可以共享诸如CT和MRI扫描及验血所获得的数据。这些数据可以帮助医生正确诊断症状复杂的病人。

新药物的开发

开发安全且有效的新药物非常重要，这时数学工具也常被用来理解疾病治疗的本质，特别是遗传病和传染病的治疗。例如，数学已经被用来为不同阶段的艾滋病人寻找合适的治疗方案。人们知道，随着时间的推移，一些药物（抗生素和抗疟疾药物）的作用会逐渐减小，这是因为引起疾病的病原体会随着药物的使用产生抗体。所以人们需要不断寻找新的方法来调整现有的药物，以提高药效，或在病原体产生抗体之前更新药物。从病人处收集到的数据及药物的结构形式，是用数学和统计思想来研制更好的药物治疗方案的原始材料。

基因组学 / 计算生物学 / 生物信息学

克里克（Francis Crick）和沃森（James Watson）提出了著名的遗传学模型，为生物学和数学同时开辟了一个崭新的领域，这不仅吸引了统计与概率，亦吸引了其他数学分支。概括地说，作为间接遗传分子，DNA可以看成是由四个字母ACGT组成的序列，这里每个字母都是一个

特定的核苷酸的简称。每个个体都有自己特殊的由这些字母序列组成的基因。基于 DNA 模型，每个物种都有一个区别于其他物种的特定的基因组成，不同的物种具有不同数量的染色体及染色体基因组的数量。越来越快的序列分析仪，产生了越来越多的关于个体基因组和不同物种基因组的数据。生物学家声称地球上有超过一百万个物种，但也有人说目前地球上的物种的数量远大于这个数字。关于物种的正确定义的部分问题是统计的问题。判别两个对象是否属于同一类，可设计一些基于对象间一系列的“度量”作为距离。给定一些 DNA 序列，我们可以利用各种“距离”来度量这些序列是否相似。在此环境下发展的统计研究，诞生了生物信息学这个全新的领域。

宇宙学 / 天文学

人们在远离灯光的晴朗的夜晚用肉眼就可以看到数量令人惊叹的星星。现在，使用安装在山顶的望远镜（越来越多的安装在南半球，因为那里人造光源比较少）、人造卫星、太空望远镜（特别是哈勃望远镜），海量的关于天体的数据正在被收集。利用成像技术和统计思想，天文学家正在尝试更深入地理解我们宇宙的本质，并寻找适合人类生存的星球。这与物理学家试图了解时间、空间和引力的本质工作相辅相成。

赌博与投资

在赌博或投资追逐利益的过程中，大量的数据生成。纽约证券交易所（NYSE）每天都产生大量的数据。在越来越短的时间跨度内，成百上千种股票被追踪并试图预测其规律，以便吸引更多股民在这些交易所投资。许多与股票打交道的人被称为技术分析师。这些人研究股票价格的变化趋势（通常是用复杂的统计工具），再结合其他的一些信息以期投资获利。金融数学中的新思想与统计学这个重要工具，已经被用来辅助一些国家在影响最低的条件下控制商业周期，并用来帮助他们更好地理解世界金融市场。

粒子物理

在美国和欧洲，用来加速原子运动速度的机器已建成多年，包括著名的费米实验室的粒子加速器和欧洲核子研究组织（CERN）的大型强子对撞机。建造这种机器的目的是为了帮助物理学家了解物质的本质以及组成物质的粒子。虽然所谓的标准模型已经可以成功地解释大部分关于物质的原理，但仍有许多物理学家关注的谜团无法解开。谜团之一是希格斯玻色子是否存在。虽然可以找到这种粒子的能量水平的范围在减小，但是在各种粒子加速机的大量实验中还未发现这种粒子（2012 年 7 月，欧洲核子研究组织称其发现了与希格斯玻色子特征基本相符的新粒子。2013 年 3 月 14 日，欧洲核子研究组织宣布，先前探测到的新粒子是希格斯玻色子。——编者注。）每次用这些加速器做实验时，通常会有大量的图像和数据生成。数据挖掘技术被用来辅助检查这些数据，来寻找代表意想不到的事物的个别“粒子衰变”，或寻找可以支持我们对已知现象的理解的证据。

交通信息

住在城市的居民非常关心能否准时上下班或能否准时参加约会。这时，没有比因交通堵塞而迟到更令人沮丧的事情了。目前正在开发的许多系统通过配置传感器和相机来检测交通流量，并试图利用由这些系统产生的数据给司机实时的建议，让他们合理地规划路线以便减少塞车的时间。这些数据同样有助于了解在一座桥上如何设置收费亭，以及决定在有双向车道的桥上如何合理分配车道。

教育

作为监控教育行业发展的手段之一，数据收集愈发重要。学校，不论是中小学、大学、研究生院还是专业学院，都要平衡学生的数量和学生的质量。各级政府都努力使公立学校有足够的承载力，并通过数据判断这些学校是否满足社会的需求。

电子邮件和互联网

现在越来越多的人花大量的时间查阅电子邮件或上网。从个人或商业角度看，查电邮或上网都产生了大量数据。目前许多公司都在关注收集用户或群体（通常是基于用户的邮政编码来得到）的信息，用来改进浏览器的搜索结果。有些公司甚至会花钱使自己出现在网页搜索中显眼的位置上，而数据也会告诉商家广告某些特定的搜索词可能会给公司带来收益。社会学家、经济学家也对电子邮件和互联网相关数据收集到的信息感兴趣。

数据挖掘的工具

数据挖掘的基础是统计数学，同时又受益于人工智能和计算学习理论（computational learning theory）。

人工智能领域已经吸引了数学家、计算机学家和哲学家的关注。严格地说，这个领域是指由人类设计和编程的计算机在“创造”和“思考”的时候可以表现出类似人类的能力。

历史上，人工智能的目标是令计算机可以玩人类需要投入高层次思考的游戏，这些游戏强调技巧而不存在运气的因素，如跳棋、象棋和围棋。例如，在人工智能的早期历史上，有人相信当计算机“武装”上优秀玩家用到的规则就可以下象棋，然而这种方法并不十分成功。随着计算机拥有越来越快的处理速度和越来越大的内存，人工智能开始借助计算机的这些特征再往前发展。今天，对于象棋盘上的任何一个给定的位置，计算机可以找到所有可能的走法以及对手相应的走法，利用这个“暴力”方法，结合“位置评估”可找到最佳的移动和应对方法，正因如此，IBM 的深蓝计算机终于击败了一位世界冠军。

最近，IBM 设计了一个名为沃森（Watson）的计算机系统，它击败了在著名智力抢答节目 Jeopardy 中最成功的人类选手，这个节目使参与者在语言诙谐的气氛下挑战一系列复杂而广泛的知识。选手选择一个具有特定分数的主题，问题的难度与所附分数的值成正比。参与者不时地选择问题，如果答对了，则使收到的金钱加倍。有时对于一个特殊类别中的问题，选手可以拿已得到的金钱中的一部分来对正确答案“下注”。因此，这里有一个“终极危险”的回合，如果选手确信自己给出的是正确答案，则可以尝试通过拿已得的部分资金下注以期超过对手。2011 年 2 月 14 至 16 日，在黄金时间播出的一系列特别电视节目里，尽管在回答问题时出现一些奇怪的“行为”，IBM 的沃森计算机“系统”打败了两名非常优秀的人类对手。沃森的信号手的技能（当它准备好回答问题时就按铃）非常好，但是当主持人叫它回答问题必须简短的时候其反应就会差一些。

计算学习理论主要是指探索可以使机器针对一个具体的目标改进自身性能的算法。例如，处理大量电子邮件的人的一个困扰是垃圾邮件的增长。垃圾邮件包含通过电子邮件发送的无用信息，没有人愿意收到它们。已经开发出软件用于将有可能的垃圾邮件和推销信息放到一个目录下，如果在一定的时间段内没有被查看，则这些邮件会被自动删除。用户通常可以设置垃圾邮件过滤器的参数，以便尽可能地避免删除那些用户愿意阅读的邮件。利用贝叶斯统计思想，可以设计出越来越成功的垃圾邮件过滤器，即使在邮箱的用户没有指出过滤器哪部分的决策不满意的情况下也很成功。

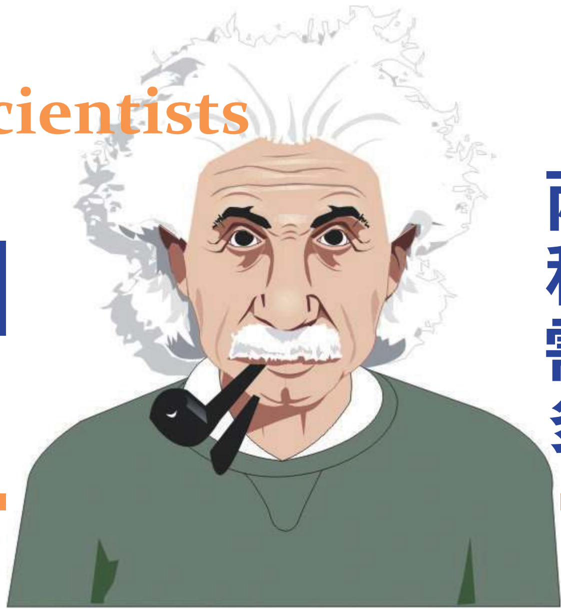
理解数据的一种方法是找到可以解释这些数据的数学模型。这方面一个成功的例子是利用均值和标准偏差来对数据的集中趋势和变化程度建模。实际上，无论是从物理实验、心理学实验收集到的数据，还是英语教授观察莎士比亚戏剧中句子的长短，都可以用同样的数学工具来分析。另外一个展现数学魅力的例子是概率密度函数和概率分布函数的思想的产生，这使得探讨数据是服从正态分布还是服从其它分布成为可能。然而，生成数据的数量越来越大，以及在哪些领域数据可以发挥更大的作用，对我们依然是重大的挑战。数学家、统计学家和计算机科学家正在努力应对这一挑战。

原文链接：http://www.ams.org/samplings/feature-column/fc-2012-04

注：译者为曾铁勇博士，香港浸会大学

Two Views: How Much Math Do Scientists Need?

两种观点：科学家需要多少数学？



E. O. Wilson , E. Frenkel / 文　　丁 玖 / 译

2013 年 4 月 5 日的《华尔街邮报》发表了哈佛生物学家 E. O. 威尔逊（E. O. Wilson）的一篇随笔：《好科学家≠数学好》。2013 年 4 月 9 日，伯克利数学家爱德华 • 弗兰克尔（Edward Frenkel）在 Slate 上回应了此文。《华尔街邮报》和 Slate 允许我们如下转载这两篇随笔。

On April 5, 2013, The Wall Street Journal published an essay by the Harvard biologist E. O. Wilson, "Great Scientist ≠ Good at Math". Berkeley mathematician Edward Frenkel responded to it in Slate on April 9, 2013. We reprint the two essays below, with permission from The Wall Street Journal and Slate.

好科学家≠数学好

E. O. 威尔逊揭秘：发现源于想法，而不是数字运算

对于许多立志成为科学家的年轻人，大感头疼的是数学。没有高级的数学，科学上你怎能做出严肃的工作？好吧，我有一个职业秘密与您分享：当今世界上许多最成功的科学家，在数学上差不多是半文盲。

在我哈佛几十年的生物学教学生涯中，我伤心地目睹大有前途的本科生转身离开可以跻身其中的科学职业生涯，只因担心如果数学能力不强而会导致失败。这种错误的假设已经从科学界里夺走了不可估量的急需人才。它已经产生了要急需止住的脑力大出血。

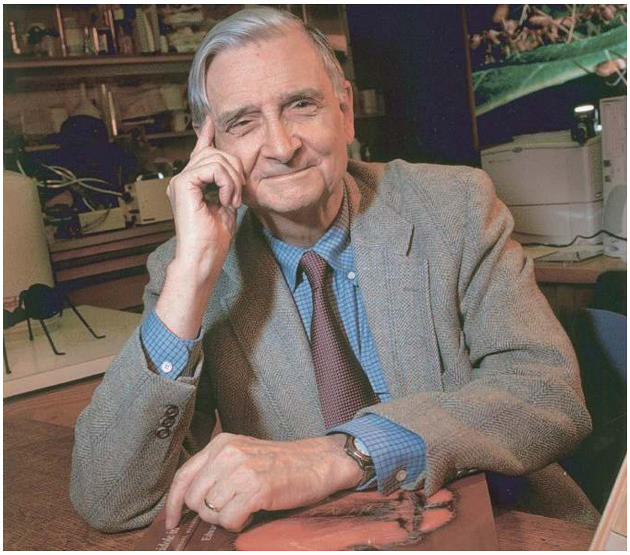
就这个论题而言我可以一个权威的身份说话，因为我

Great Scientist ≠ Good at Math

E. O. Wilson Shares a Secret: Discoveries Emerge from Ideas, Not Number-Crunching

For many young people who aspire to be scientists, the great bugbear is mathematics. Without advanced math, how can you do serious work in the sciences? Well, I have a professional secret to share: Many of the most successful scientists in the world today are mathematically no more than semiliterate.

During my decades of teaching biology at Harvard, I watched sadly as bright undergraduates turned away from the possibility of a scientific career, fearing that, without strong math skills, they would fail. This mistaken assumption has deprived science of an immeasurable amount of sorely needed talent. It has



E. O. 威尔逊

自己就是一个极端的例子。在相对较差的一所南方学校度过了我几年的大学预科后，直到在阿拉巴马大学上大一时我才修了代数课。作为一个 32 岁有终身教职的哈佛教授，我终于和微积分面对面了，和比我岁数的一半只大一点点的那些本科生坐在同一个课堂里，我是那么地不舒服。他们中的几个是我教的进化生物学课上的学生。我吞下了我的自尊心，学会了微积分。

在迎头赶上期间，我从未是一个 C 以上的学生，但我以此发现感到安心：卓越的数学功底和流利的外语能力是相似的。经过更大努力及与内行人多交谈，我可能会更流利，但沉浸于野外和实验室的研究，让我只有少量的进步。

幸运的是，出色的数学才华只在少数几个学科中需要，如粒子物理、天体物理和信息论。整个科学其余部分更为重要的是形成概念的能力，在此期间，研究者以图形想象，凭直觉行事。每个人有时都像科学家那样浮想。立足而起且训练有素，幻想是创造性思维的源泉。牛顿梦想过，达尔文梦想过，你也梦想。其诱发的图像在开始时是模糊不清的。它们在形式上可以转移，淡入或淡出。当在纸上勾勒出图形时，它们会变得更坚实一点，而当寻找真实的例子并有发现后，它们便活生生起来。

科学先驱者鲜有从纯数学的想法中提取发现。大部分在黑板上研究成行方程的科学家的刻板照片上，展示的是解释已作出的发现的教师。真正的进展出现在充满笔记的现场，堆积乱涂乱画纸张的办公室，向朋友奋力解释的走廊上，或独自吃午饭之时。灵光一现需要努力工作和全身心的投入。

当出于自身需要而对世界的某些领域进行研究之时，

created a hemorrhage of brain power we need to stanch.

I speak as an authority on this subject because I myself am an extreme case. Having spent my precollege years in relatively poor Southern schools, I didn’t take algebra until my freshman year at the University of Alabama. I finally got around to calculus as a thirty-two-year-old tenured professor at Harvard, where I sat uncomfortably in classes with undergraduate students only a bit more than half my age. A couple of them were students in a course on evolutionary biology I was teaching. I swallowed my pride and learned calculus.

I was never more than a C student while catching up, but I was reassured by the discovery that superior mathematical ability is similar to fluency in foreign languages. I might have become fluent with more effort and sessions talking with the natives, but being swept up with field and laboratory research, I advanced only by a small amount.

Fortunately, exceptional mathematical fluency is required in only a few disciplines, such as particle physics, astrophysics and information theory. Far more important throughout the rest of science is the ability to form concepts, during which the researcher conjures images and processes by intuition.

Everyone sometimes daydreams like a scientist. Ramped up and disciplined, fantasies are the fountainhead of all creative thinking. Newton dreamed, Darwin dreamed, you dream. The images evoked are at first vague. They may shift in form and fade in and out. They grow a bit firmer when sketched as diagrams on pads of paper, and they take on life as real examples are sought and found.

Pioneers in science only rarely make discoveries by extracting ideas from pure mathematics. Most of the stereotypical photographs of scientists studying rows of equations on a blackboard are instructors explaining discoveries already made. Real progress comes in the field writing notes, at the office amid a litter of doodled paper, in the hallway struggling to explain something to a friend, or eating lunch alone. Eureka moments require hard work. And focus.

Ideas in science emerge most readily when some part of the world is studied for its own sake. They follow from thorough, well-organized knowledge of all that is known or can be imagined of real entities and processes within that fragment of existence. When something new is encountered, the follow-up steps usually require mathematical and statistical methods to move the analysis forward. If that step proves too technically difficult for the person who made the discovery, a mathematician

最容易产生科学的想法。这些想法源于严谨而有序的知识。而所有这些知识或是已知的，或是能由真正的实体以及尚不完整的现实进程所勾画。遇到新的东西时，后续步骤通常需要数学和统计方法来将分析向前推进。如果对发现者而言该步骤证明技术上太困难，数学家和统计学家可以加进来成为合作者。

20 世纪 70 年代末，我与数学理论家乔治 • 奥斯特 (George Oster) 一道研究社会性昆虫的等级制度原则及其劳动分工。我提供了已在自然界和实验室中发现的细节，而他用其定理和假设的工具库来捕捉这些现象。即便没有这样的信息，奥斯特先生也许能开发出一个一般理论，但他不会有任何的方式来推断出可能排列中的哪些在地球上实际存在。

多年来，我曾和数学家及统计学家共同撰写多篇论文，所以我有信心提供下面的原理。这叫威尔逊第一原理：科学家从数学家和统计学家获得所需合作远比数学家和统计学家找到科学家能够运用他们的方程更加容易。

这种不平衡在生物学中尤其如此，在那里现实生活中的现象经常被误解，或未摆在首要位置而被注意。理论生物学的编年史塞满了数学模型，而它们要么可以放心地忽略，或测试时失败。当中超过 90% 的可能没有任何持久的价值。只有那些与活生生的系统知识有扎实联系的模型才有许多被用的机会。

如果你的数学竞争力级别低，规划提升它，但同时应知道你现有的知识也能做出优秀的科学工作。不过，对于专攻需要实验和定量分析密切更替的那些领域，要三思而后行。这些包括：大部分的物理和化学，以及分子生物学中的一些专业。

牛顿为了给他的想象力实质内容而发明了微积分。达尔文几乎没有什么数学能力，但由于积累了大量的信息，他能够构想出一种过程，后来才用到了数学。

对于有抱负的科学家，关键的第一步是要找到一个他们极感兴趣并专注于此的学科。这样做的话，他们应该记住威尔逊第二原理：对于每一位科学家，存在一门学科，在当中他或她的数学能力足以使其走向辉煌。

——E. O. 威尔逊，哈佛大学荣休教授

or statistician can be added as a collaborator.

In the late 1970s, I sat down with the mathematical theorist George Oster to work out the principles of caste and the division of labor in the social insects. I supplied the details of what had been discovered in nature and the lab, and he used theorems and hypotheses from his tool kit to capture these phenomena. Without such information, Mr. Oster might have developed a general theory, but he would not have had any way to deduce which of the possible permutations actually exist on earth.

Over the years, I have co-written many papers with mathematicians and statisticians, so I can offer the following principle with confidence. Call it Wilson's Principle No. 1: It is far easier for scientists to acquire needed collaboration from mathematicians and statisticians than it is for mathematicians and statisticians to find scientists able to make use of their equations.

This imbalance is especially the case in biology, where factors in a real-life phenomenon are often misunderstood or never noticed in the first place. The annals of theoretical biology are clogged with mathematical models that either can be safely ignored or, when tested, fail. Possibly no more than 10 percent have any lasting value. Only those linked solidly to knowledge of real living systems have much chance of being used.

If your level of mathematical competence is low, plan to raise it, but meanwhile, know that you can do outstanding scientific work with what you have. Think twice, though, about specializing in fields that require a close alternation of experiment and quantitative analysis. These include most of physics and chemistry, as well as a few specialties in molecular biology.

Newton invented calculus in order to give substance to his imagination. Darwin had little or no mathematical ability, but with the masses of information he had accumulated, he was able to conceive a process to which mathematics was later applied.

For aspiring scientists, a key first step is to find a subject that interests them deeply and focus on it. In doing so, they should keep in mind Wilson’s Principle No. 2: For every scientist, there exists a discipline for which his or her level of mathematical competence is enough to achieve excellence.

—E. O. Wilson

Harvard University, Emeritus

莫听 E. O. 威尔逊的

数学可以帮助你从事几乎任何职业，没有理由害怕它

E. O. 威尔逊是一位杰出的哈佛生物学家和畅销书作者。我为他的成就向他致敬。但他最近的一篇《华尔街邮报》短文（改编自他的新书《给一个年轻科学家的信》）是不能再错的了，其中他告诉那些满怀抱负的科学家，他们不需要数学就能茁壮成长。他以这样的话开始："当今世界上许多最成功的科学家，在数学上差不多是半文盲。……就这个论题而言我可以一个权威的身份说话，因为我自己就是一个极端的例子。"如果他接下来说："但是你，年轻的科学家，不必像我一样，所以让我们来看看我是否可以帮助你克服对于数学的恐惧"，那倒是很好。唉，这位年逾八旬的社会性昆虫权威却反其道而行之。原来他居然相信不仅恐惧是有道理的，而且大多数科学家并不需要数学。"我得到的，所以你也可以得到"是他的态度。可悲的是，从这篇文章清晰可见，威尔逊犯下这等错误的原因是，基于他自己有限的经验，他不明白什么是数学以及它如何用于科学。

倘若数学是美术的话，那么威尔逊对它的看法将是：这一切都是在你家的后院篱笆上涂油漆。当你可以雇人来做时，为什么要学习如何自己做呢？但是美术不是油漆围栏，而是大师的画作。同样，数学不是关于如同威尔逊的文章所指的"数字运算"。它是关于概念和想法，它们把我们武装起来描述现实，并发现世界是怎样工作的。伽利略的名言说："自然法则都是用数学语言书写的。"

数学代表着客观的知识，这使我们能够打破教条和偏见。正是通过数学，我们才了解到地球不是平的，它围绕太阳旋转，我们的宇宙是弯曲的、扩张的，充满了暗能量，并

爱德华•弗兰克尔

Don't Listen to E. O. Wilson

Math Can Help You in Almost Any Career. There's No Reason to Fear It

E. O. Wilson is an eminent Harvard biologist and bestselling author. I salute him for his accomplishments. But he couldn't be more wrong in his recent piece in *The Wall Street Journal* (adapted from his new book *Letters to a Young Scientist*), in which he tells aspiring scientists that they don't need mathematics to thrive. He starts out by saying: "Many of the most successful scientists in the world today are mathematically no more than semiliterate …… I speak as an authority on this subject because I myself am an extreme case." This would have been fine if he had followed with: "But you, young scientists, don't have to be like me, so let's see if I can help you overcome your fear of math."Alas, the octogenarian authority on social insects takes the opposite tack. Turns out he actually believes not only that the fear is justified, but that most scientists don't need math. "I got by, and so can you" is his attitude. Sadly, it's clear from the article that the reason Wilson makes these errors is that, based on his own limited experience, he does not understand what mathematics is and how it is used in science.

If mathematics were fine art, then Wilson's view of it would be that it's all about painting a fence in your backyard. Why learn how to do it yourself when you can hire someone to do it for you? But fine art isn't a painted fence, it's the paintings of the great masters. And likewise, mathematics is not about "number-crunching", as Wilson's article suggests. It's about concepts and ideas that empower us to describe reality and figure out how the world really works. Galileo famously said, "The laws of Nature are written in the language of mathematics." Mathematics represents objective knowledge, which allows us to break free of dogmas and prejudices. It is through math that we learned Earth isn't flat and that it revolves around the sun, that our universe is curved, expanding, full of dark energy, and quite possibly has more than three spatial dimensions. But since we can't really imagine curved spaces of dimension greater than two, how can we even begin a conversation about the universe without using the language of math?

Charles Darwin rightfully spoke of math endowing us "with something like a new sense." History teaches that mathematical ideas that looked abstract and esoteric yesterday led to spectacular scientific advances of today. Scientific progress would be diminished if young scientists were to heed Wilson's advice.

It is interesting to note that Wilson's recent article in *Nature* and his book claiming to show support for socalled group selection

且很可能有三个以上的空间维度。但是，因为我们真的不能想象维数大于二的弯曲空间，不用数学语言我们还怎么能开始与宇宙对话？

查尔斯•达尔文理所当然地谈到数学赋予我们以“一个新意义上的东西”。历史告诉我们，昨日还显得抽象和深奥的数学思想，今日就导致科学壮丽的突飞猛进。如果年轻的科学家听取威尔逊的建议，科学进步就会被削弱。

有趣的是注意到威尔逊最近的一篇刊登在《自然》上的文章和他声称有证据支持的所谓群选择的一本书遭到了理查德•道金斯(Richard Dawkins)和其他许多人尖锐的批评。一些批评者指出，错误的来源之一在于威尔逊的数学。因为我不是进化理论的专家，所以我不能提供我的意见，但从威尔逊的论断“伟大的科学家不需要数学”来看，我觉得这场争论有趣。

有一件事应该是清楚的：虽然我们感知的物理世界总有可能被扭曲，我们对数学真理的感知却不可能是这样的。它们是客观的、持久的、必要的真理。一个数学公式对任何人，在任何地方，都意味着同样的事情——无论什么性别、宗教，或肤色；对任何人，从现在开始的一千年，它的意思总是不变。这就是为什么数学在科学和技术上发挥着越来越重要的作用。

数学的关键功能之一是信息的排序。随着 3-D 印刷等新技术的到来，我们曾经习以为常的现实正在经历一个激进的变革：一切都将从现实的物理层迁移到信息层和数据。我们很快就能很容易地通过使用 3-D 打印机将信息变成所需的物质，就像我们现在将一个 PDF 文件转换成一本书，或将一个 MP3 文件转换成一段音乐。在这个勇敢的新世界，数学将是王者：它将被用来组织和整理信息并促进信息转换成物质。

在某些领域，仍有可能“数学不好”（但是我相信任何人都可以数学好，如果它能被正确的方式解释）却能成为一个好科学家，但这大概不会太长久。但是，这是一个缺陷，没什么可骄傲的。诚然，某些科学领域目前使用的数学比其它领域少，但是这些领域的工作者后来更从学习数学中受益。

威尔逊的文章如果仅仅限制在他个人的经验范围内，那没问题。对于现代生物学的学生，这是一个过时的职业生涯道路。然后我们就可以讨论真正的问题，这就是如何改善我们的数学教育并消除如他所说的对数学的恐惧。相反，通过制造恐惧，威尔逊给下一代特别是未来的科学家做出一个远离数学的错误建议。这不只是使人误入歧途，导致不良后果，更在于像他这样的领头科学家嘴里说出来，这简直是一种耻辱。不要接受这个建议——它是一个自我破灭的策略。

——爱德华•弗兰克尔，加州大学伯克利分校

have been sharply criticized, by Richard Dawkins and many others. Some of the critics pointed out that one source of error was in Wilson's math. Since I'm not an expert in evolutionary theory, I can't offer an opinion, but I find this controversy interesting given Wilson's thesis that "great scientists don't need math."

One thing should be clear: While our perception of the physical world can always be distorted, our perception of the mathematical truths can't be. They are objective, persistent, necessary truths. A mathematical formula means the same thing to anyone anywhere——no matter what gender, religion, or skin color; it will mean the same thing to anyone a thousand years from now. And that's why mathematics is going to play an increasingly important role in science and technology.

One of the key functions of mathematics is the ordering of information. With the advent of the 3-D printing and other new technology, the reality we are used to is undergoing a radical transformation: Everything will migrate from the layer of physical reality to the layer of information and data. We will soon be able to convert information into matter on demand by using 3-D printers just as easily as we now convert a PDF file into a book or an MP3 file into a piece of music. In this brave new world, math will be king: It will be used to organize and order information and facilitate the conversion of information into matter.

It might still be possible to be "bad in math" (though I believe that anyone can be good at math if it is explained in the right way) and be a good scientist——in some areas and probably not for too long. But this is a handicap and nothing to be proud of. Granted, some areas of science currently use less math than others. But then practitioners in those fields stand to benefit even more from learning mathematics.

It would be fine if Wilson restricted the article to his personal experience, a career path that is obsolete for a modern student of biology. We could then discuss the real question, which is how to improve our math education and to eradicate the fear of mathematics that he is talking about. Instead, trading on that fear, Wilson gives a misinformed advice to the next generation, and in particular to future scientists, to eschew mathematics. This is not just misguided and counterproductive; coming from a leading scientist like him, it is a disgrace. Don't follow this advice—it's a self-extinguishing strategy.

—Edward Frenkel
University of California at Berkeley

在复旦大学数学科学学院2013年度迎新大会上的讲话

李大潜

各位同学：

很高兴参加为今年本科生与研究生联合举行的迎新大会。刚才同学们的发言非常精彩，院领导也做了重要的讲话，希望大家认真记取，我在这儿想和大家拉拉家常，谈谈想到的几个方面，一是热烈欢迎，二是殷切期望，三是郑重建议，供大家参考。

首先是对大家来到复旦、参加本科和研究生阶段的学习，表示热烈的欢迎。人们常说："铁打的营盘流水的兵"，复旦数学学院也是这样。每年一大批同学毕业离校，又有一大批新同学进校学习，形成了一个生生不息的良性循环状态。你们的到来，为我们数学学院增添了活力和朝气，是学院兴旺发达的标志和保证，更给学院带来了动力和希望。我们坚信，评价一个学校，靠的不是那些暂时性的指标和政绩，例如每年发表了多少篇论文之类，而是要看她的主要产品，即学生，在毕业后走上社会，为国家、为人民、为人类建功立业的实际表现，看经过岁月的考验和环境的变迁，涌现出多少出类拔萃的科学家、企业家、政治家，出现了多少为人们称道并引以为豪的人物。从这个意义上说，你们的成长与成才，不仅是你们个人的事，也密切关系着我们学校和学院的未来。正因为如此，我们对大家的热烈欢迎，绝不是应景的客套，而是发自内心的。

下面对你们要谈的是期望，同样不是客套话，而是十分殷切的。我们殷切的期望是什么呢？是期望你们真正懂得珍惜：珍惜你们复旦人的身份，珍惜你们所学的专业，珍惜你们在复旦的宝贵学习时光。

李大潜院士在复旦大学数学科学学院2013年度迎新大会上讲话

能够成为复旦的学子，无疑是值得庆幸的，相信你们也一定会引以为荣。但是，入学不应是你们的终极目标，也不能自动转化为你们今后的成功与辉煌。取得了复旦学子的身份，不等于能最大限度地利用复旦这个成长与进步的平台，不等于在复旦将会一帆风顺，不等于在毕业时能毫无悔色地面对自己的一切，不等于能为自己一生的发展打好一个坚实的基础。因此，希望大家务必珍惜这个珍贵的起点，用加倍的努力来实现自己的理想和抱负。

那些进了复旦就觉得自己壮志已酬的人，看中的只是复旦的这块招牌，而不珍视与这个招牌相应的真才实学的内涵，是很难走得远的。有人一考入复旦，就急着想下一步到哪儿去，就又在为自己设计一个新的前程（例如出国、找一个好的工作等等），甚至不务正业，忙着为进入下一阶段进行种种自认为必要的准备。这样做看来很精明，但实际使自己沦为一个匆匆来去的过客，人在复旦，却心浮气躁，放松了正规的学习和严格的训练，将来难免悔对在复旦虚度的岁月，这是很不明智的。只有脚踏实地，认真地把握现在，才是对未来发展最好的铺垫和准备，才有光辉的未来。苏步青先生曾经说过："要把自己的学校看成最好的学校，要把自己的老师看成最好的老师。"我的理解，就是强调要面对现实，在自己所处的实际客观环境下尽最大的努力做得更好，这是前辈先贤给我们的忠告，希望大家铭记在心，充分珍惜复旦学子这一身份，全身心地在复旦茁壮地成长。

要珍惜你们所学的数学类专业。数学是一个人一生中学得最多的功课，然而，为什么要学习数学？为什么要学好数学？可能并没有太多的人认真地思考过。大家是数学的本科生及研究生，希望能够认真地想想清楚。你们为什么选修现在的专业深入学习，也希望认真思考一下。我想，相当一部分同学是真正非常热爱数学的，希望将来能成为一个数学家，一辈子献身数学。对他们来说，如饥似渴地学习数学应该是不成问题的。还有很大的一部分同学，既对数学有兴趣，也深知数学的重要性，但他们是希望先打好一个数学基础，将来转入到其他各行各业发挥作用的。这也是学习数学的一个良好的出路和动机，众多有着良好数学基础和修养的毕业生进入各行各业，不仅会从根本上改变这些行业的面貌，而且对数学发展本身也提供了良好的外部环境和带来极大的推动，同样是值得鼓励和支持

李大潜院士 2008 年获法国荣誉勋位骑士勋章

的。但是，尽管将来要进入各行各业，你们和其他人相比的优势不在别的地方，而在你们数学上的积淀；你们将来在新的环境中能不能脱颖而出，靠的也只能是你们在数学上的优势，而不是其他！因此，对所有的同学来说，努力学习数学，学好数学，尽可能学得出类拔萃，不仅是现阶段对你们的学习要求，也是对你们未来发展的战略性的投资，是终生受用不尽的。

希望大家要充分珍惜在复旦的学习时光。三年、四年、五年，看起来时间很长，但如果不抓紧，一晃就会过去。本科新生中的大多数同学在中学阶段经过了漫长的应试教育的训练，想必是相当累了。到了大学，没有老师盯得你们紧紧的，课业表面上也不太重，你们中的相当一些人还可能缺乏自制的能力，很容易在一开始处于一种松垮的状态，优哉游哉一下，甚至沉醉于上网、玩一些无聊的游戏等等。这一放松，时间很快就过去了。等到发觉大事不好，想要抢救过来就难了。为什么呢？数学这个学科逻辑性强，整个体系十分严谨，一环扣一环，前面没有很好掌握和理解，后面学习就会有本质上的困难。形象地说，数学学习和在食堂里打饭不同，是不能“插队”的！一开始放松，就很难抓得回来，就可能永远被动下去，甚至一蹶不振。一开始不抓紧，往往就可能输在起跑线上！而到了临近毕业的时候，相当大的一部分人要忙着找工作或找出路，往往像热锅上的蚂蚁，想要静下心来学习恐怕就成了一个奢望了。因此，*在你们刚进校的时候就要提醒你们：你们的时间不多了！一定要有一种紧迫感，对在复旦的学习岁月加倍地珍惜。*

总之，机不可失，时不再来。对学校、对专业、对时光，要高度的珍惜。决不可掉以轻心，使时光虚度，岁月蹉跎，将来后悔莫及。

最后，为了在复旦这一段有限的时间中能认真地学好数学，郑重地给大家下面一些建议：

第一，从中学到大学，从本科生到研究生，学习要求和学习环境都有重大的变化，但大家一开始可能没有感觉，而一旦感觉到了，往往为时已晚。建议大家认真体验、讨论与总结，将自觉地改变自己的学习方法作为开始阶段的第一要务，力争在转折点处掌握先机，抓住学习的主动权。

第二，从学习态度的层面，要坚持认真、刻苦的学习，不能松懈。有一分劳动，就有一分收获，这是永恒的真理，数学更不能例外。不出气力，玩小聪明，偷工减料，含糊敷衍，都是不行的。我们有少数研究生，学习不刻苦，不投入，平时的办公室在晚上往往是乌灯熄火，到了周末，办公室里更是很少见到他们的身影。他们的劳动强度不要说远远比不上那些发愤图强的同学，甚至远远不如我们一些年纪大的老师，对此，我们是很有意见的。这样的师兄师姐，不应该成为你们的榜样。希望从你们开始，能够开辟出一个崭新的局面。

第三，从学习方法的层面，要掌握学习数学的诀窍，达到事半功倍、举一反三的效果。我们有些同学，学习积极性是很高的，劲头来了，胃口很大，总希望学得更多一些，学得更快一些。他们选修了很多课程，甚至外加了很多额外的负担，把时间排得满满的；同时追求那种一目十行、七步成诗的高速度和才子风范，但效果往往不好，甚至适得其反，越搞越被动。这不是一个学习数学的正确方法。最近我在和一些同学的谈话中，针对他们在学习上贪多求快、不求甚解的情况，明确总结了一个学习数学的“四字诀”，现在告诉大家。哪四个字呢？少、慢、精、深。我觉得，数学学习的好坏要看是否理解深入、运作熟练及表达简明这三个方面，关键是要深入的理解，达到精深的地步。而为了达到精深，不能多、快，只能少、慢。要学好微积分，一本真正好的教材就够了，用不着像文科那样博览群书、一口气看上好多本。平时的学习也不宜平均分散力量，要集中力量打歼灭战，打下一个据点就牢固占领一个据点。这样，虽然一开始不贪多，但日积月累就会根基扎实地积少成多，实现由少到多的转化，不断扩大自己的知识结构和范围。而只有慢，不片面地追求速度，才能细嚼慢咽，反复思考，才能深入地理解，透彻地领会，真正掌握数学的真谛。我在上大学的时候，陈建功先生给我们上实变函数论的课。这门课很难，一堂课下来，真正弄清楚的不太多。我课后要认真地破译他那本相当浓缩的自编油印讲义，改正一些印刷上的错误，补充不少证明的细节和自己的点滴体会，一直到彻底弄懂为止。这样做，通常要花上二、三倍的时间，可以说是慢到极点。但破译了这一本“天书”，以后碰到再难的“天书”也不害怕了。这在当时就给我带来了深切的感受和极大的愉悦，而且影响和造就了我的一生。应该说，这是我在大学中收获最大的一门课程，因为它不仅锻炼和考验了我的自学能力和方法，而且极大地增加了我的信心和勇气。这不是“快”的功劳，而是“慢”的功劳。精工才能出细活，也才能逐步实现由慢到快的转化。这样得到的快，才是真快，才是无后顾之忧的快，才真正进入到一个新的境界。

少、慢的目的是要达到精、深。怎样达到呢？需要大家不断地总结经验。我这儿只向大家介绍华罗庚先生提倡的一个读书方法：由薄到厚，由厚到薄。首先要由薄到厚。要反复思考、分析有关内容的关键和重点，抓住论证的核心和要害，了解材料的来龙去脉，读出自己的体会，读出书本及教师没有直接说出来的深刻的内涵，也包括提出自己的问题与困惑，等等。这样读书，书自然由薄到厚，认识也逐步走向深入了。但这不是全部，还要在此基础上进一步抓住问题的本质和核心，做到由厚到薄。真理总是朴素的，本质的东西往往是简明扼要的，到了一定阶段，通过认识的升华，就会发现你所面对的这一大堆东西其实很简单，三言两语就可以点出它的本质，这就由厚转向了薄。这样的薄，经过了否定之否定的过程，已与原来的“薄”有了本质的不同，可以说，已经在一定程度上达到融会贯通的地步了。

第四，学好数学，要重视严格的数学训练，其中很重要的一环，是要认真做好习题。苏步青先生曾经做过一万道微积分题，他功底扎实，再烦再难的推导及计算都不在话下，决不是偶然的。你们平时看书、听课，有些东西一时弄不明白，有些习题一下子做不出来，并不是一件不光彩的事情，是很正常的，深入思考一下或过一定的时间，学到后面，往往会自然得到解决。但是，有一件事却是很不光彩的，就是依赖市场中贩卖的“习题解答”，

做不出的题目一抄了事，甚至自己可以做的题目也一抄了事。这使老师布置的训练要求，使严肃的学习任务，统统化为泡影，自己更得不到应有的锻炼与考验，自欺欺人，害人不浅。想想看，是怎样一些人为了盈利的目的去提供这些充斥市场的东西呢？我们数学学院有老师在干这些无聊而有害的勾当吗？你们这些堂堂复旦大学的大学生，这些抱负和眼界都甚高的青年学子，难道没有一点自尊心和荣誉感，心甘情愿地让这些“习题解答”牵着鼻子跑吗？将这些货色作为自己的拐杖和依靠，不应该觉得惭愧甚至羞耻吗？！我在这里郑重地希望大家，将这些“习题解答”像学习上的毒品那样坚决予以抵制与抛弃，像过街老鼠人人喊打那样与之作坚决的斗争，以净化我们周围的学术和学习风气，努力学到一些货真价实的本领。

第五，最后一点，学习贵在创新。对数学的学习，当然不应生吞活剥、死记硬背，也不能只提倡培养分析问题和解决问题的能力，更要注意培养发现问题和提出问题的能力。希望大家的脑筋一直处于一个活跃的状态，不断对老师、对书本、也对自己提出种种问题，努力促进自己的好奇心和求知欲，努力培养自己成为一个具有创新意识和创新能力的优秀人才，从这个意义上说，鸦雀无声、座无虚席的听、讲课的状态，不是一个理想的状态。要勇于质疑，大胆提问，使讨论和争论成为风气，你们的成才才有可靠的保证，数学的发展才有真正的希望。

今天就讲到这里，谢谢大家！

作者简介：

李大潜，著名数学家，复旦大学数学院教授，中科院院士，法国科学院外籍院士，曾任中国数学会副理事长，中国工业与应用数学学会理事长。

微博上的数学漫游（连载六）

歌之忆 http://weibo.com/wildmath

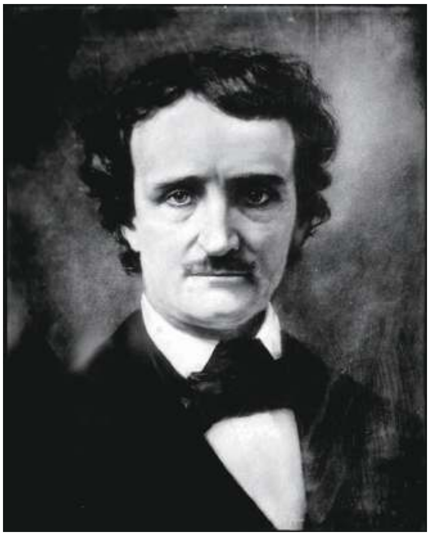
数学思想的每一次历险，都丰富了人类文明中最具力与美的景观，展示了来自心灵自由的深刻的创造。二十世纪的数学家们，不但像他们先辈那样穷天极地，更是将人类的心智列入了数学探索的对象。如果说许多世纪以来的数学探险家们发现了一个又一个新大陆，那么开辟了信息时代的数学家们，则是用他们创造的数学，极大地升华了人类的心智。

俄罗斯文学家普希金（1799-1837）

数学家用磐石一样坚不可摧的逻辑，建立了一个超然于世、却又充满诗意的自由王国。在数学上挥洒自如的超一流大师柯尔莫哥洛夫（Andrey Kolmogorov），一生多次撰文探索普希金的诗歌。数学本是从理性出发，但理性的至高境界却是大海般的自由，是普希金吟唱出的"我只愿意歌颂自由，只向自由奉献诗篇"的诗情。

屹立在智慧之巅、如入无我之境的数学大师柯尔莫哥洛夫，最初能读到的仅仅是支离破碎、被肢解的香农（Claude Shannon）——冷战伊始，苏联在翻译"敌对阵营"的学术论文时，习惯于修修剪剪、来一番过滤。但柯氏以无与伦比的功力，靠一份残缺的译文准确解读了香农的原意，从此他为香农深邃的直觉激赏不已。

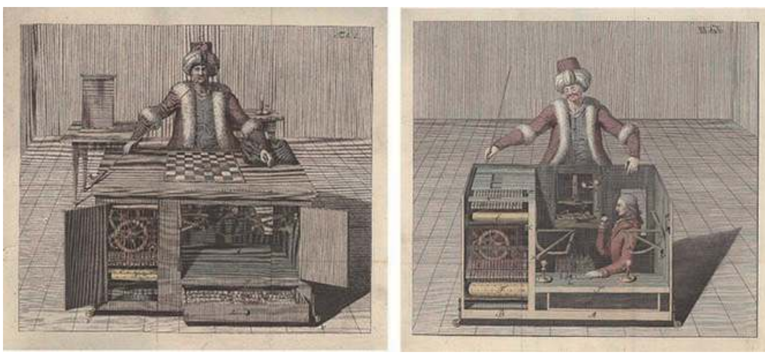
苏联数学家柯尔莫哥洛夫（1903-1987）



美国文学家爱伦•坡（1809-1849）

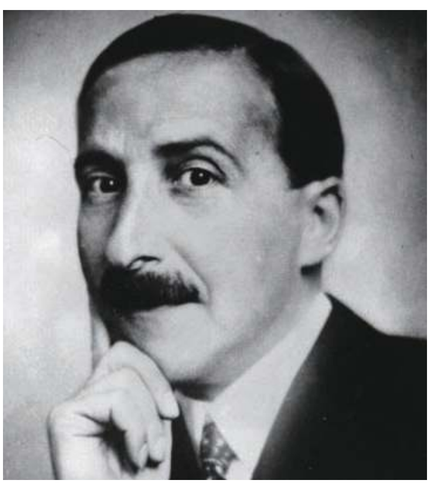
但彼时的逆天之才香农，其实早已不满足于挑战人类的智力。少年香农曾沉迷于爱伦•坡在小说《金甲虫》设下的迷局，如今他开始琢磨爱伦•坡的《梅尔策尔象棋手》。自古以来，人们就幻想有个能和人类对弈的象棋机器人，但梅尔策尔实则是一桩骗局——那个自动象棋的箱子里暗藏着一位象棋高手。

40 年代末，电子计算机发明不久，图灵已经开始探索如何用计算机下象棋，而真正的象棋高手香农更是棋高一招，在其 1948 年的信息论名作发表之后仅仅 2 年的时间，香农在《哲学期刊》发表了计算机象棋程序。他的论文提出了两种程序思想——暴力搜索或选择性搜索，分别称为 A 型策略和 B 型策略。

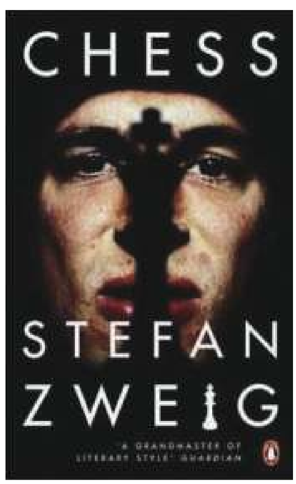


梅尔策尔象棋手

《金甲虫》



奥地利文学家茨威格（1881-1942）

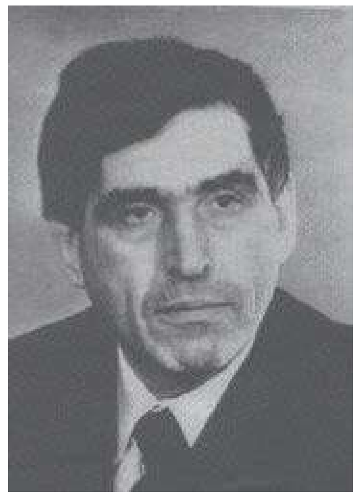


茨威格的《象棋的故事》

茨威格有篇小说名为《象棋的故事》。说的是在驶向南美的客轮上，一位在象棋上没有任何想象力、完全靠冰冷的逻辑推理打遍天下无敌手的象棋冠军琴多维奇，意外栽倒在业余棋手 B 博士手下——后者因被盖世太保长期关押及至精神濒于崩溃之际、靠一本棋谱打发时间最终练得了令人称奇的棋艺。

美国人工智能学者麦卡锡（1927-2011）

现实却比茨威格的小说更加精彩。1966-1967 年间，美国人工智能先驱者麦卡锡（John McCarthy）在苏联接受数学家的挑战，莫斯科理论与实验物理研究所（ITEP）和美国斯坦福大学展开了计算机象棋比赛，历时 9 个月，结局是 3:1，苏联获胜。但这场较量的真正赢家却是香农——比赛双方分别采用了香农的 A、B 策略。



苏联数学家、计算机科学家克罗洛德（1921-1986）

茨威格的小说中，白痴棋手琴多维奇输掉首局之后，靠不义之招，将曾饱受纳粹摧残的 B 博士，置于强大的精神压力之下，令其彻底崩溃。虽然现实的美、苏计算机象棋大战中，持香农 A 策略的苏联靠着堂堂正正的计算机程序击败了持香农 B 策略的美国。但胜利后的苏联队，悄然继续着茨威格的故事。

俄罗斯诗人叶赛宁（1895-1925）

在冷战期间，任何一场胜利都会被大书特书。但领导苏联取得计算机象棋竞赛胜利的杰出数学家克罗洛德（A. Kronrod），不久却被剥夺了工作。藉口是计算机象棋消耗了 ITEP 的计算资源；但实际的原因，却是他参与了 99 位数学家的联名呼吁：要求当局释放被强制关进精神病院的一位优秀的同行。

数学家渴望自由，却深知在学术上只能沿着逻辑的阶梯去达到最高的自由。但懂逻辑的数学家或许能理解诗歌、却不懂社会。在苏联那样的社会讲逻辑，意味着失去自由。1965 年 12 月 5 日，数学家叶赛宁 - 沃尔品（Alexander Esenin-Volpin）跑到普希金广场发起呼吁，要求苏联当局严格遵守法律。于是，等待他的便是精神病院。

俄裔美国数学家叶赛宁 - 沃尔品（1924-）

正是在普希金雕像前的 1924 年 6 月 6 日，数学家叶赛宁 - 沃尔

苏联的 Kaissa 程序夺得了第一届计算机象棋比赛世界冠军

品的父亲朗诵过一首自己创作的《致普希金》——“我命中注定要受压迫，但我还要长久地歌吟”。这位歌吟的诗人，就是深受俄罗斯人民拥戴的诗人叶赛宁。诗人不接受压迫，他的数学家儿子也不接受压迫。数学和诗，都是心灵自由的产物。

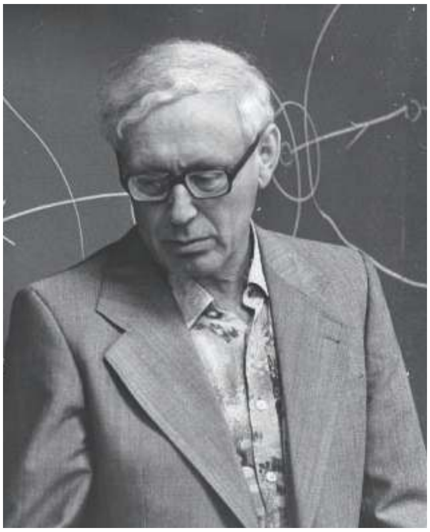
和诗人相比，数学家更需要心灵的自由。因为愤怒可以出诗人，却出不了数学家。与柯尔莫哥洛夫同出于大师鲁津门下的数学博士克罗洛德，只能悲愤地告别数学，一门心思研制起抗癌药物，甚至拿自己做起了药物试验。一个用数学为祖国争得荣誉的数学家，在连续三次中风之后，悲凉地悄然离世。

在冷战空前激烈之际，莫斯科 ITEP 的数学家克罗洛德向美国发起计算机象棋挑战赛，最终战胜了斯坦福大学。但这位计算实验室主任，却因同情叶赛宁 - 沃尔品被赶出了莫斯科。不幸中的万幸，苏联的计算机象棋团队顽强生存下来，并且在 1974 年第一届国际计算机象棋比赛中，他们的 Kaissa 程序顺利拿下了冠军。

苏联计算机象棋一连串的胜利，背后自然有高人。这位幕后高手就是电子工程博士鲍特维尼克（Botvinnik）——这位国际特级大师自 1948 年为苏联拿到国际象棋世界冠军后，将冠军头衔几乎完整地保持了 15 年——期间仅仅两次丢失冠军。他开启了国际象棋的苏联时代，名将卡尔波夫和卡斯帕罗夫都出自他的门下。

无论是围棋还是国际象棋，竞技场上的求道派往往棋下得漂亮却常与胜利失之交臂，而那些力战派的棋却经常在丑陋不堪中笑到了最后。鲍特维尼克也许算不上才华横溢，但他个性坚强、冷峻，擅长以学院派的思维系统地研究棋局。身为国际特级大师的电子工程博士还精深研究了香农的选择性搜索。

一代棋王鲍特维尼克领导苏联的计算机象棋，在 80 年代



开创了国际象棋苏联时代的国际象棋特级大师、国际象棋世界冠军、电子工程博士鲍特维尼克（1911-1995）

末已接近国际大师的水准。这位电子工程博士对算法颇有心得，在残局的算法上抛弃了香农的路线图。但他的团队每周只能有 16 个小时去用一台陈旧的 IBM。老爷货每秒只能执行 40 万条指令，仅是 PC 机的 1/5。而美国的先进电脑，对苏联是禁运的。

计算机象棋竞技，既是人类的自我超越，也是信息科技总体水平的全面较量。如果说 80 年代末，美苏在信息理论和算法等数学化领地的竞争难分胜负，那么在微电子领域，美国却一枝独秀。理论、算法的均势，再加上集成电路技术的绝对优势，终于成就了美国在 90 年代计算机象棋领域划时代的成就。

香农与世界冠军鲍特维尼克对弈

美国信息科学家汉明（1915-1998）

信息科学大师汉明（Richard Hamming）曾经深刻地指出——“对于信息科技而言，如果说信息论是方向盘，那么集成电路则是发动机”。从这个意义上看，香农远远超越了他的远亲、伟大的发明家爱迪生。香农创立了信息论，他的那篇被誉为二十世纪最伟大的硕士论文，则用逻辑电路成就了未来的大规模集成电路。

1990 年，香农的信息论被《科学美国人》誉为信息时代的《大宪章》。通信传输必然受物理条件制约，它不可能超越物理信道的天然屏障。这恰如 13 世纪诞生于英国的《大宪章》——王权不可以无法无天、为所欲为，王权之上还有大宪章。在现实的物理世界，通信的极限，就是香农定义的信道容量。

香农的信息论被誉为信息时代的《大宪章》

从逻辑电路，到信息论，再到人工智能，屹立

IBM 深蓝计算机与国际特级大师、世界冠军卡斯帕罗夫对弈

在人类心智最顶峰的香农，曾经自豪地宣称：“与其说我是个科学家，毋宁说我更是一位诗人。”海德格尔说“真正的诗人是为人类寻找生存尺度的人”，而为信息社会立下《大宪章》的巨匠香农，为人类构建信息化社会，奠定了理论基础和技术基础。

少年香农曾为爱伦•坡的《金甲虫》所倾倒。小说示范了如何解谜：面对一长串符号文本，先列出各个符号的频度。小说中符号 8 出现的次数最多，于是把它替换成英文字母里最常见的 e。如此等等，这样由频度进行解谜的思想，不但被后来的柯南•道尔用在小说里，更在信息论中成为思想的原型。

从迷恋爱伦•坡的《金甲虫》，到津津乐道于他的《梅尔策尔棋

信息论创始人、杰出数学家香农。左为香农在演讲，右下为香农在驾驶飞机

爱伦·坡《乌鸦》

手》，香农向超越人类智慧迈出了计算机象棋的第一步。那是一条充满艰辛的路，是光荣的荆棘路。47 年后的 1997 年，IBM 深蓝计算机击败国际特级大师卡斯帕罗夫。但这一刻的荣耀，香农却未能享受。因为命运和超级天才开起了玩笑。

人类智力的冲浪者香农，在密西根大学获得数学和电子工程双料学位后，投身 MIT 师从美国科技政策的缔造者万尼瓦尔·布什；在普林斯顿聆听了冯·诺依曼、外尔、爱因斯坦、哥德尔；在贝尔实验室曾与图灵和其他信息技术开拓者切磋。正是这样一位成就斐然、才华横溢的学者，却在晚年患上了老年痴呆症。

以挑战人类智力极限为乐、敢以诗人自居的香农，伴随着老年痴呆症走向生命的终点。迷恋爱伦·坡的科学家，恰如爱伦·坡的《乌鸦》里的身处绝境的诗人，向乌鸦不断倾诉，乌鸦却答以十一个“Nevermore”——生命渐逝，永不复焉。曾经的辉煌，被命运无情地推向悲凉，渐入荒芜。那，几乎是一切天才的归宿。

晚年的香农

通向现代数学的一扇门：《数学译林》

陈 跃

在我们学习与研究数学的过程中，除了学习书本和研读论文外，还离不开好的综述文章，因为后者能够帮助我们了解一些重要数学领域的成就与概貌，了解现代数学形成的过程。《数学译林》就是一份主要登载这样的综述文章的季刊，它早已经被国内数学界公认为是办得非常成功的好杂志。

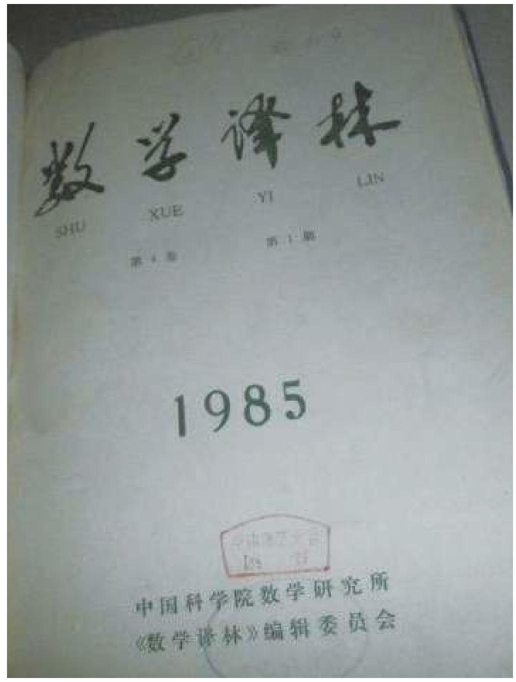
《数学译林》是一本什么类型的杂志

《数学译林》实际上是一本以综述类译文为主的综合性中文数学杂志，由中国科学院数学与系统科学研究院数学研究所主办。这本杂志是在 1980 年开始出版试刊的，1982 年正式创刊，每年一卷，每卷 4 期，1982 年的这一卷作为第一卷。而在 1980 和 1981 这两年，每年各出了 3 期试刊，所以总共有 6 期试刊。试刊的封面底色呈淡蓝色，但从第一卷开始，采用了非常朴素的纯白色底色。一直到 1992 年的第十一卷，才改成了比较厚重的褐色，并且从杂志的特点出发，在封面上分别用英、俄、德和法文标出了“数学”一词，这个封面沿用至今。

在为纪念《数学译林》创刊十周年而出的总目录增刊上，由《数学译林》编辑部写的一段话最能说明该杂志的主旨：

> 近几十年来，述评类文章倍受学界重视。它们往往由数学大师、或某一学科领域的高手撰写，具有综述性，批判性和历史性的特征，是在大量原始文献的基础上经认真消化、归纳、总结后的成果。这些文章所附的参考文献，因经过精心筛选而不愧为进入某一研究前沿的海图。《数学译林》最青睐此类作品。我们选择的综合报告、学科与专题介绍、数学史文章中不乏此类佳作。

在重视综述文章的同时，《数学译林》也非常注意给出数学家们创造数学的过程，提供



他们所生活的时代背景材料，努力展现鲜活生动的数学思想。为此《数学译林》还设立了人物与传记、数学圈以及数学争鸣等栏目，登载了不少数学家们的回忆录、访问记以及生卒纪念文章。此外还有一些关于数学教育的文章和国外数学竞赛的试题集等。

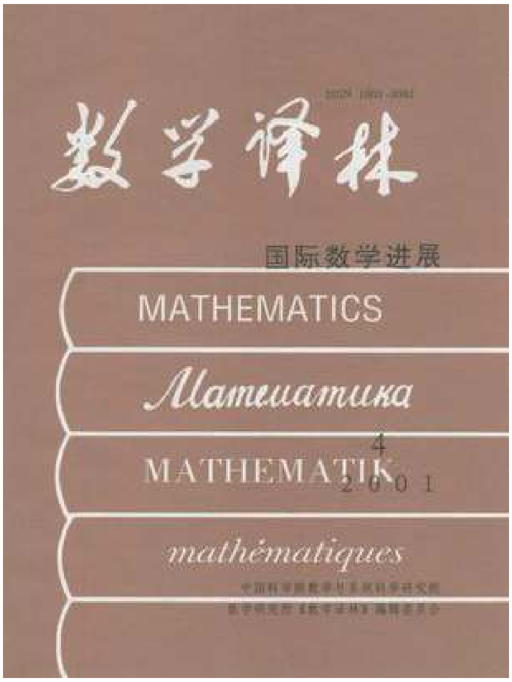
《数学译林》杂志是怎样产生的

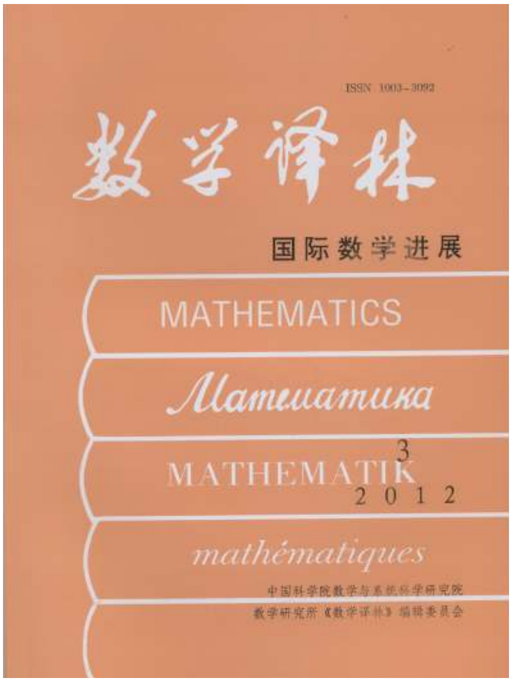
在 33 年前的中国，怎么会想到创办这样一份以译文为主的数学杂志？据另一本为纪念《数学译林》创刊二十周年而出的总目录增刊介绍，该杂志的创意是这样产生的：“《数学译林》是上个世纪七十年代末由中国科学院数学研究所的同仁创办的，它由张耀成提议，经与李培信、沈信耀、江嘉禾等酝酿、发起，成立了一个松散的由部分研究室人员参加的临时编委会。到 1982 年正式出刊时，才成立了一个编委会。”

今天来看，《数学译林》的诞生似乎是一个偶发的事件，其实不然。在世界各国出版的各种综合性介绍数学的杂志中，基本上都是以发表原创文章为主，而极少有主要刊登翻译文章的杂志。《数学译林》能够诞生在上世纪 70 年代后期的中国，有其一定的必然性。在 36 年前的 1977 年，我国在经历了“文革”的十年动乱之后，数学事业处于百废待兴的状态。改革开放伊始，打开了以往封闭的大门，才发现我们已经远远落在了后面。于是中国的数学工作者们埋头苦干，急起直追，除了迅速恢复以前比较熟悉的传统数学领域的研究外，他们还迸发出了极大的学习与研究新的现代数学的热情。这个时候就需要有一种能比较快地了解世界数学发展状况的途径，而直接翻译国外优秀的综述类文章就是一个很有效的应急方法。

让我们比较仔细地来看一看 1980 年的第一期《数学译林》试刊。在该期的相当于创刊词的“试刊说明”中这样写道：

> 近数十年来世界数学迅速发展，数学研究中心星罗棋布，文种各异的出版物不断涌现，正式或非正式的数学文献汗牛充栋。要从这些浩如烟海的文献中及时抓住数学发展的方





向，显然并非易事。因此，我们试办《数学译林》这个刊物，希望能对读者提供有益的资料。本刊是以翻译为主、既有提高也有普及的综合性数学刊物，目的是介绍国外数学的进展，普及已成熟的现代数学知识，促进我国数学的发展和水平的提高。读者对象是广大数学工作者，……

这一期所介绍的现代数学大部分属于几何与拓扑的范畴，虽然这些基本知识现在已经普遍为人们所熟知，但在当时的中国却很少有人知道。第一篇文章由编委钟家庆翻译，译自丘成桐在 1978 年国际数学家大会上的报告，其中比较全面地总结了整体微分几何与复几何中的一部分最新的研究成果。第二篇文章主要介绍多复变函数论中最基本的$\bar{\partial}$方程方法。第三篇文章通俗解说了代数拓扑学主要解决什么问题，以及采用什么方法。第四篇文章是一篇由著名数学家阿蒂亚（Atiyah）写的通俗短文，他从 3 个简单的小例子出发，论证了在代数、几何、拓扑以及分析之间存在着本质上的联系，从而显示了现代数学的内在统一性。第五篇讲微分流形的文章其实只是在介绍微分拓扑学中新得到的几个定理。第六篇文章是一份关于 Hodge 理论的讲课提纲，这个理论是现代数学中连通几何、拓扑与分析的一个比较基本的理论。而第七篇文章也是一篇短文，由著名数学家马宁（Manin）撰写，他在极少的 3 页篇幅内，清楚明确地解释了希尔伯特第 15 问题是怎样通过运用现代代数几何的工具加以解决的，让人看到抽象的概形理论到底用在了什么地方。在接下来的几篇数学家的人物介绍文章中，着重于解释他们的数学思想，而不是只有他们的生平和经历。在该期杂志的结尾处，除了介绍美国两所大学的数学课程设置外，还有一篇标题为“发展数学”的很有意思的争鸣文章，大意是说发展中国家的数学教育容易偏向于实用，他们的数学研究容易陷入“高度专门化”，这应该是对我们的一种善意提醒。第一期最后一篇讲 Morse 理论的文章实际上是米尔诺（Milnor）的经典同名讲义的第一部分。

《数学译林》就是在这样一种急切需要了解世界数学潮流的特殊环境中产生的，它对当

时普及现代数学的知识，促进我国数学研究水平的提高，确实发挥了不可替代的重要作用。《数学译林》出版至今，已经有超过一千多篇、总数超过两千多万字的学术译文面世，它们主要译自英、法、日、俄等文种的几百种数学期刊和图书资料，它们凝聚了前后几十位《数学译林》编委、几百位进行翻译的数学专家们的辛勤劳动和心血。可以说《数学译林》伴随了改革开放后中国的整整一代数学工作者的成长。

《数学译林》部分文章分类索引

最近我将《数学译林》中写得比较好的文章按分支学科做了一个分类，以便于自己的学习。我发现经过分类以后，《数学译林》的价值显著增加，内容体系更完整，前后更连贯。考虑到这样的分类可能对人们了解现代数学的帮助会更大，我将整理后的这些文章的标题列在下面，供大家参考。我对文章的选取标准主要是看其对重要数学思想的阐发，而不仅仅是对重大数学事件的新闻报道以及对数学家们日常社会生活的描述，并且主要偏向于基础数学。在每个大类中，按照文章发表的先后顺序进行排列，在每篇文章标题后的括号内，冒号前的数字表示文章所在的卷数（试刊的两年则写年份），冒号后的数字是文章所在的期数。

对现代数学的整体看法方面的文章

数学的统一性 (1980:1)、N. Bourbaki 与现代数学 (2:1)、当代数学问题 (2:2, 3, 4)、数学发展中的某些倾向 (3:1)、纯数学最近的动向 (3:2)、近三十年来 Bourbaki 学派的工作 (3:3)、数学与数学模型 I,II(4:1,2)、M. Atiyah 访问记 (4:2)、数学科学：一种统一的、大有潜力的资源 (6:2)、Riemann 传 (6:3)、Jean-Pierre Serre 访问记 (6:3)、数学中的几个大问题 (9:2)、近期研究成就和有关的机会 (10:3, 4)、数学的进展慢下来了吗 ?(11:1, 2)、只要可能，什么都想干 (11:1)、几何学中的新维数 (11:2)、Princeton 大学半个世纪会议 (12:3)、拓扑和抽象代数：理解数学的两种途径 (15:1)、下个世纪的数学问题 (17:3)、与 Nicolas Bourbaki 相处的二十五年 (1949-1973)(17:3)、数学及其在中国的发展 (18:3)、从菲尔兹奖看现代数学 (18:3, 4; 19:1, 3, 4; 20:1)、André Weil 的生平和工作 (19:1)、André Weil: 一个开拓者 (19:2)、Jean Leray(1906-1998)(19:3)、著名数学家介绍七个新千年数学奖问题 (20:1, 2)、普林斯顿高等研究院的数学学部 (20:4; 21:1)、二十世纪的数学 (21:1)、Armand Borel (1923-2003)(23:4; 24:1)、Hermann Weyl(1885-1955)(24:4)、Alain Connes 访谈录 (27:3, 4)、Henri Poincaré 的水晶球 (28:1)。

数论方面的文章

Pierre Deligne(1980:1)、数论今昔两讲 (1981:2; 3:1)、有限域上方程解的 p 进位处理法 (1:3)、什么是模形式 ?(1:4)、Mordell 猜想的证明 (4:2)、第九问题：一般互反律 (4:3)、椭圆曲线的 L- 级数 ,Birch-Swinnerton-Dyer 猜想和高斯类数问题 (4:4)、虚二次域的 Gauss 类数问题 (5:4)、Mordell 猜想 (5:4)、椭圆曲线的最新进展 (6:4)、Gerd Faltings 对数学的一些贡献 (7:4)、Vladimir Drinfeld 的工作介绍 (11:3)、费马大定理介绍 (12:4)、Wiles 证明了 Taniyama 猜想；由它推出了 Fermat 大定理 (12:4)、有关 Wiles 剑桥讲演的报告 (14:1, 2)、R. Taylor 和 A. Wiles 对费马大定理的证明 (14:4)、椭圆曲线 (15:4)、局部域上的非阿贝尔互反律 (20:3)、Riemann 假设 (22:4; 23:1)、代数数论历史及其在 ICM 上的反映 (23:1)、解析数论 (26:3)、模的奇迹 (28:1)、密码学背后的算术 (29:3)、椭圆曲线的黎曼假设 (30:1)。

代数与代数几何方面的文章

Hilbert 第 15 问题 (1980:1)、Emmy Noether(1980:1, 2)、有限单群 (1980:2, 3)、奇点 (1980:3)、Hilbert 第 14 问题 (1980, 3)、群的西表示论的起源和早期历史 (1981:1)、代数几何和有关的代数历史漫谈 (1981:2, 3; 1:1, 2)、二十面体 (1:1)、有限单群的分类 (1:3)、

代数K-理论:历史的回顾(2:1)、有限群的特征标及其应用(2:1)、代数曲面(2:3)、代数学的现代趋势(2:4)、伽罗华传(2:4)、辛几何中的矩映射(4:4)、数学究竟是什么?(5:1)、代数课程的内容和方法(5:1)、交换环论五十年(6:2)、有限单群分类(6:4)、解析性研究300年(7:2)、Daniel Quillen的工作(7:3)、交换代数15年(7:4)、Chevalley(7:4)、椭圆曲线,阿贝尔曲面与正二十面体(9:1)、代数簇的极小模型理论(9:2)、代数几何(9:3)、数学中的千古一文(11:1)、一百周年纪念:Wilhelm Killing和例外群(11:1)、交换数学与非交换数学(11:2)、代数几何(11:3)、回顾与……(11:3)、从Frobenius到Brauer的有限群表示论(12:3)、Van der Waerden所建立的代数几何基础(14:4)、黎曼曲面与代数曲线(15:2)、群表示与调和分析——从Euler到Langlands(16:1,2)、Dynkin图和代数表示论(17:2)、周炜良(17:2)、有限群的表示一百年(18:1; 21:4)、椭圆曲面(19:1)、小平变形理论及后来的发展(19:2)、不变量理论的两个转折点(20:4)、Kac-Moody李代数创立之路(22:1)、Donald C. Spencer(1912-2001)(23:3)、什么是Motive?(24:1)、仿佛来自虚空:Alexander Grothendieck的一生(24:2,3,4)、计数几何学Schubert演算法(24:4)、Alexander Grothendieck之数学人生(26:3)、代数几何学基础:从Severi到Anndré Weil(26:3)、Motive——Grothendieck的梦想(28:3)、忆Grothendieck和他的学派(30:1)、从线性代数到同调代数(30:3)。

几何与拓扑方面的文章

代数拓扑学(1980:1)、微分流形(1980:1)、Hodge理论大纲(1980:1)、同伦论五十年(2:2, 3)、关于新老Morse理论的讲演(3:1, 2)、Cauchy-Riemann方程和微分几何(3:1)、双曲几何学一百五十年(3:1)、八十年代的分析和几何(4:1)、复微分几何的某些最新进展(4:2)、半个世纪来的同伦论(4:3)、Yang-Mills方程与四维流形的结构(4:3)、谱相同的流形(4:3)、Sophus Lie(5:1)、几何中的非线性分析(5:3, 4)、Lie群一百年(5:3)、Dirac算子的特征值(5:4)、D. S. Freed与K. K. Uhlenbeck著《瞬子与四维流形》(5:4)、四维流形上的怪异结构(6:1)、纽结与奇点(6:1)、让研究工作行之自然(6:2)、非交换微分几何简介(6:4)、一个新的纽结多项式与von Neumann代数(6:4)、Л. С. Понтрягин(庞特里亚金)自传(6:4)、混合Hodge理论的通俗导引(7:1)、规范理论作为低维拓扑学者的工具(7:4)、45年来的群扩张(7:4)、论Simon Donaldson的工作(7:4)、3维和4维流形中的新不变量(8:2)、软硬辛几何(8:2)、几何学在美国的复兴:1938-1988(9:2)、拓扑漫谈(9:4)、瞬子及其近亲(10:3)、局部Atiyah-Singer指标定理(11:1)、循环上同调与非交换微分几何(11:2)、同调三维球的Floer同调群(11:3)、辫子和环链理论的最新进展(11:3)、李群论发展中的怪事(11:4)、数学陶冶我一生(12:2)、4维拓扑中的问题(12:4)、辛拓扑引论(13:1)、Hermite对称空间的射影秩(13:3)、纽结理论中的新观点(13:4; 14:1)、不可征服的Morse理论(15:3)、几何及非线性微分方程的现状与前景(16:1)、漫谈Gauss-Bonnet定理的历史发展(16:1)、拓扑对分析的影响(16:3)、几何学的未来发展(16:4)、Samuel Eilenberg(1913-1998)(18:2)、André Weil与代数拓扑(18:4)、在老范氏楼中成长(20:1)、拓扑学的发展(20:3)、Raoul Bott访问记(20:3)、九十九年后的Poincaré猜想:进展报告(22:3)、Dirac方程和几何(23:2)、从四元数到宇宙学:常曲率空间(23:3)、陈省身(24:1)、Poincaré猜想(25:3)、Poincaré猜想和三维流形分类的近期进展(25:4)、二十世纪的拓扑学(26:2,3)、怀念陈省身(27:3)、你也能发明谱序列(28:3)、陈省身的成就和生涯(28:4)、拓扑与复分析中的亏格(29:4)。

分析方面的文章

微分方程在微分几何中的作用(1980:1)、复分析中的偏微分方法(1980:1, 2)、拟共形映照、Teichmuller空间和Klein群(1980:2)、von Neumann代数(1981:3)、Dirichlet问题(1:3)、拟凸性与Levi问题(2:3,4)、常微分方程五十年(3:3,4)、泛函分析五十年(3:3)、单值化定理(3:4)、算子代数——前40年(6:4)、几何偏微分方程的近期进展(7:2)、复分析中的映射问题和$\bar{\partial}$问题(9:4)、偏微分方程和微分几何(10:4)、复分析(11:4)、Harish-

Chandra 及其工作 (13:3)、多复变函数论 (14:4)、L. V. Ahlfors 的数学工作 (17:4)、求学时代——从 1945 年到 1953 年在明斯特 - 巴黎，苏黎世与普林斯顿学习复分析 (20:4)、Laurent Schwartz(1915-2002)(23:2)。

现代数学与物理相互作用方面的文章

正规范场的几何 (2:1)、对 Manin 的“几何学中的新维数”的评论 (7:2)、物理对几何的影响 (10:2)、分析力学在数学发展中的作用 (11:4)、弦，纽结和量子群 (12:4)、物理法则的几何化 (13:1)、可积模型在数学发展中的作用 (13:4)、规范理论寿终正寝了！不，规范理论长命百岁 !(14:4)、规范理论与 4 维几何的新展开 (15:2)、量子理论与几何学 (15:3)、两个理论的故事 (16:2)、群和物理 (16:4)、神奇，神秘和矩阵 (18:2)、向子孙后代讲讲 P. Dirac(23:1)、构成我们的场 (24:2)、Feynman 图应用的微分几何与物理基础 (28:2)。

对《数学译林》杂志的期望

当我做完了这个分类索引，才意识到《数学译林》中已经有了相当多难得一见的好文章，它们完全可以称得上是一座宝库。仔细地观察以上的这些文章的标题，可以看出它们基本上涵盖了 20 世纪基础数学的主要内容，这也从一个侧面显示了《数学译林》各位编委们的深厚数学素养和长远眼光。虽然这些文章所谈的还只是浩如烟海的现代数学中一小部分具有代表性的问题，却已经是蔚为壮观了。将它们组合在一起，无疑就是一部用中文写的简略的现代数学辉煌发展的历史，或者也可以看成是一部通俗的人性化的现代数学百科全书。

在今天，也许是因为人们已经有了更多与世界交流的机会，《数学译林》的作用与地位已经不如以前那么重要了。此外又由于经费和版权方面的原因，近几年来《数学译林》文章的选择范围也明显缩小了（文章的来源只能局限于少数的几种杂志），这样就会使一些分散在各种书籍杂志上的好的综述文章无法译成中文。尽管如此，我们还是需要《数学译林》这样一份杂志，这主要是因为现代数学已经变得高度抽象、无比庞大与深奥，我们与世界主流数学前沿的隔阂依然存在，所以我们期望今后在《数学译林》上能继续读到好的综述类文章。

《中国数学会通讯》是该刊编辑委员会编辑出版的内部刊物，季刊。主要刊登国内外数学界的重要信息，报道中国数学会与各省市自治区数学会、学科分会等的活动情况。主要栏目包括：学术活动信息，数学教育与普及，数学精品文章（数学的历史、进展、价值、趣事等），人物专栏，学科介绍，书讯与书评等。

2013 年《中国数学会通讯》全年的总订费为 50 元（含邮费）。欢迎各省市自治区数学会、学科分会和有关单位以及广大数学工作者、数学爱好者订阅本刊并踊跃投稿。

订阅办法： 请将订费邮汇至北京中关村东路 55 号（邮政编码：100190），中国数学会办公室；或行汇至中国数学会，同时请给中国数学会办公室来信告知（或在汇款单附言中注明）订购份数、收刊单位（或个人）详细地址及邮政编码，以便我们及时准确地投寄本刊。

开 户 行：北京工商行海淀西区支行
帐　　号：0200004509089161419
电　　邮：cms@math.ac.cn
电　　话：0086-10-62551022

2013 年第 3 期要目：

- 中国数学会正副理事长、秘书长会议纪要
- 2013 年度国家杰出青年科学基金建议资助项目申请人名单
- 优秀青年科学基金资助名单

田野荣获拉马努金奖
和算对中算的继承与创新
郑板桥的画竹与数学建模
古今建筑中的数学思想
2013 第 12 届中国女子数学奥林匹克在浙江镇海中学举行
会议纪要
数学前沿——数学与人文 • 第十辑

《中国数学会通讯》编辑部供稿

现代数学的特点、境界和应用

丁伟岳

本文是笔者在讲座中对同学们一些问题的回答。这些问题中大部分都是关系现代数学大局的问题，很深刻，也很难回答。问题本身是没有标准答案的，每个人会有不同的答案。下面是我的个人意见，不一定正确，仅供大家参考。

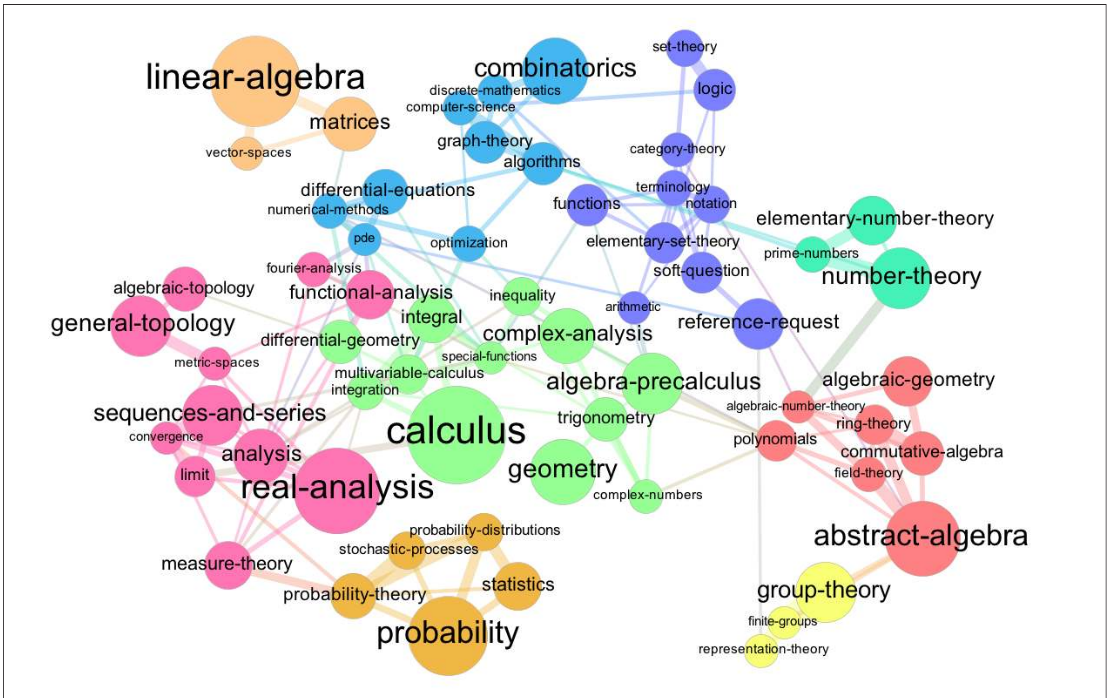
1. 现代数学的特点和现状

有的同学问：听说现代数学分支非常细，不同分支的人彼此不了解，这样还能出现总揽全局的数学大师吗？此外，数学的复杂是否使它远离“简单性”这个朴素的自然法则？

这是一个很大的问题，提这个问题的同学希望从总体上了解现代数学，这是非常好，非常值得鼓励的。但是要把这个问题说清楚并不容易。确实，现代数学分支繁多。按美国数学会的分类，数学科目可以分成 60 多个大类，每个大类下面又有几十个子类，总计有 3500 个以上的子类。肯定没有人能对所有这些分支都了如指掌，甚至于一个分支的专家也很难把分支里的所有数学了解得一清二楚。

但是，真正影响大局的数学却没有那么多。这就像世界上有 200 多个国家，但是影响全球格局的却只有少数大国。这种影响大局的数学可以叫做“主流数学”。即便在主流数学中也不是所有的问题都是平等的，还有主次之分。因此，如果能抓住主流数学中的主流问题，大体上就可以说是“总揽全局”了。至于说“大师”，他不仅能总揽全局，而且能通过他的工作影响全局。这样的人肯定很少，但也不能说一个没有，这要由历史来做定论。那么，为什么现在出不了牛顿、欧拉、高斯、黎曼这样的大师了呢？这有两个原因。首先，时势造英雄，不是每个时代都会出旷世英雄的。其次，即便是这样的英雄，他的历史地位也要经过历史的考验，并不是在当时就能确立的。

那么哪些是主流数学呢？回顾历史，现代基础数学从 17 世纪开始发源，经过 18 和 19 世纪的大发展和 20 世纪的完善，现代数学的基础部分，包括代数和数论、几何与拓扑、分析学的所有主



纯数学知识点

要分支，我们叫这些为经典分支，都进入了成熟期。所谓成熟是指，理论已经十分完善，而内在的发展动力则减弱了。因此，基础数学的单独分支的自身发展已不再是主流。取而代之的是综合与交叉，集多个分支的方法来解决以前无法解决的重要问题。费尔马猜想和庞加莱猜想相继被证明就是最好的例证。在我看来，现代数学的另一个特点是应用数学的兴起，随着现代科学技术的迅速发展，各个方面对数学的需求日益增长，推动了应用数学的崛起，它正成长为数学中一个不可忽视的主流。

从重要问题的来源看，基础数学内部一些最主要的问题是来自数论、拓扑以及几何，例如克莱研究所的 7 大问题中 4 个是关于纯数学的：两个来自数论（黎曼猜想，BSD 猜想），一个拓扑（庞加莱猜想），一个代数几何（Hodge 猜想）。另外 3 个多少与应用有关：Navior-Stokes 方程（流体力学），P-NP 问题（计算复杂性），Yang-Mills 理论（理论物理）。近年来，理论物理对基础数学的影响越来越大，这是值得注意的。

数学的复杂性不在于它的分支繁多，而在于它的深度和难度越来越大。世界既有简单的一面，又有复杂的一面。科学家的任务是把复杂的东西分析和解剖，化繁为简，找出对人类有用的东西。“复杂性”也是自然界的一个法则，它与“简单性”构成了自然界辩证的两个方面，缺一不可。

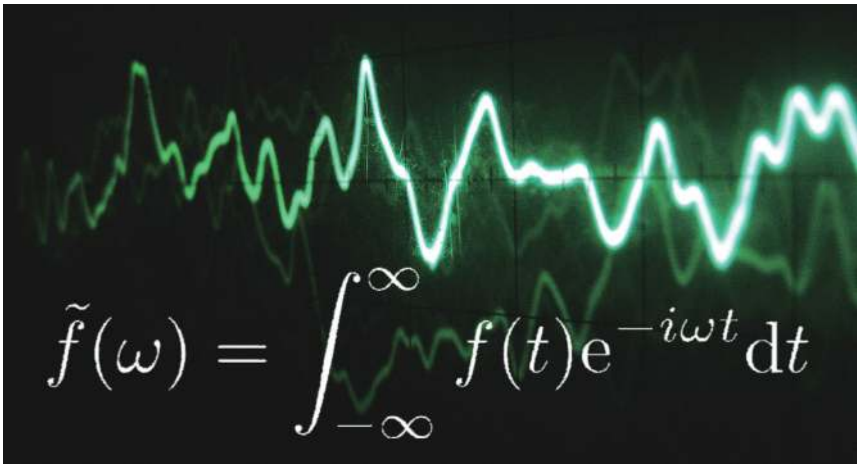
2. 数学的境界

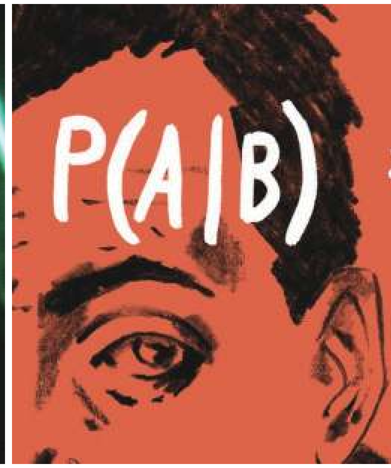
有的同学问：数学大师的精神境界是怎样的？数学的最高境界是和艺术及文学相通的吗？

在我看来数学和艺术、文学是非常不同的。艺术和文学在很大程度上是创造性地表现人对现实世界的感受和观点，表现得好就能够引起人们的共鸣和感动。而数学更像是哲学，是一种客观真理，不以人的意志为转移，你只能去发现它而不能改造它。当然，数学家同艺术家、文学家之间也有共同点，那就是他们都必须有高度的创造性。虽然创造的目标不同，创造的过程是有相似之处的。

数学家有时也赞叹某人的数学工作如何优美，遗憾的是究竟有多美只有极少的人可以欣赏。既然数学的终极目标是追求数学真理，对于美的追求就是次要的。对于有些数学家喜欢舞文弄墨不必太认真，往往他是在表达一种个人的观点，未必全对；或者他只是在自我陶醉。

我想数学大师首先是一个普通的人，要尊敬他但不要神化他；要学习他，但不要被他的思想





应用数学：现代通讯、图像技术的法宝——傅里叶变换

观点束缚住自己的思想。这一点在中国特别重要，原因是中国的文化中有一种崇拜权威的倾向；而这是创造性的大敌。还需要破除的一点是对书本的崇拜，可能对我们的同学们比较重要。书是必须读的，但不能读的太多，太多就会挤压我们头脑中自由想象的空间。数学大师们最值得我们仰慕的“最高精神境界”就是他们思想的大胆和自由，这是他们能够发现新的数学和创造新的方法的根本。

然而，大师在成为大师之前的精神更值得我们学习。我认为最要紧的大概是：对数学强烈的兴趣与好奇心；对数学问题深入细致的观察以及独立思考和分析的习惯；坚持不懈的努力。在这些基础上，才有可能达到创造性思维的最高境界。

3. 数学的应用

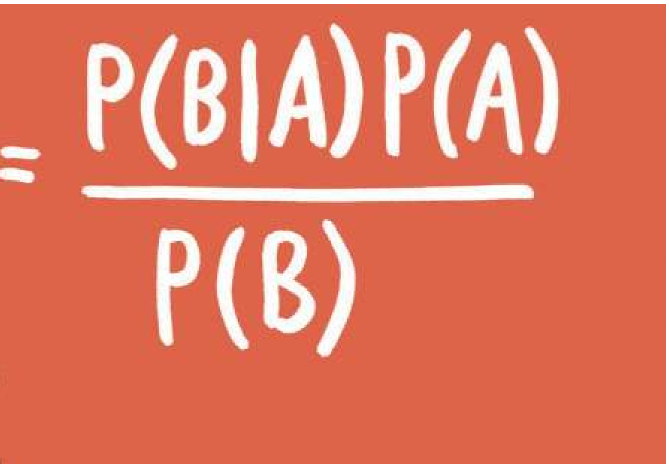
这方面的问题比较多，我选一些来回答。

Q1. 现代数学是否发展过快，以至于很多方面的理论还没有找到用武之地？

这里涉及一个问题：数学的用处究竟是什么？数学一开始是为了实用的目的而发展起来的，因为需要计算你拥有的财产、土地，等等，还要计算交易中的价格；然后，当科学发展起来的时候，必须要用数学来描述物体的运动，于是微积分就应运而生。这种例子数不胜数。但是，一旦数学发展到一定程度，它就产生了它自己的问题，不是完全为了实用，而在相当大程度上是为了满足数学家的好奇心，甚至是野心。费尔马猜想就是这样一种问题。我们知道解决这个猜想用了 300 多年，而在整个过程中这个问题对数学理论的发展，主要是代数数论和算术代数几何的发展有重要影响。现在数学理论已经发展到了极其完善的时代，数学家们仍然有很多野心，比如他们希望把流形按照各种不同的结构完全分类，他们希望建立在代数、几何、分析之间的更多深刻的联系（如 Langlands 纲领），等等。所有这些究竟有何用处是一个问题。好在我们有一个野心更大的邻居——理论物理学家，他们希望建立一种涵盖一切的物理理论，所谓“统一场论”，为了搭建理想中的宏大建筑他们把几乎所有的数学理论，特别是最新发现的理论，拿过去作为建筑材料和检验各种模型的试金石。这算不算有用还要时间的考验，因为物理学家们的理论最终是否成功，以及需要用到哪些数学，完全是未知的。我认为许多基础数学的理论是为了完善数学本身，具有方法论的意义。对于这些理论的评价要留待历史去做。

另一方面，实用的数学，通常叫做应用数学，得到了广泛的重视和迅速的发展。在我看来，这部分数学的发展最终必然会影响到基础数学本身。主流数学的概念也会随着时代的不同而变化。

最后，我想还有相当大的一部分数学是绝对无用的。原因是，这些数学的存在是由于现代大学的一些不尽合理的规定，你要求职、提升、加薪等等要看你有多少论文；于是许多没有其它用处的论文就被大量制造出来。



概率统计应用，充满应用魅力的贝叶斯公式

Q2. 我们是否可以只关心数学的应用，而只在不得已的时候去完善理论呢？

如果是以应用为目的，一开始理论总是不完善的。比如，牛顿建立微积分实际上是以力学为背景的，曲线在他看来是质点运动的轨迹，而导数被他叫做“流数”。为了应用必须归纳出微积分的运算法则，而这些法则的推导实际上是不严密的。微积分被完善成为“数学分析”用了大约 200 年的时间。其实，即使是基础数学，理论的完善也要有一个长期的过程。一开始总是从具体的问题出发，类似的问题被反复研究和解决才有可能提升为一种解决这类问题的理论。理论的产生使得解决这类问题有章可循，变得机械化。大体上说，一种研究是从问题的提出开始，而以理论的完善告终。

现在的许多实用领域，包括科学技术，也包括经济金融，给数学提出了许多新问题。面向这些问题的应用数学离成熟的理论还差得相当远。有的甚至没有办法建立比较适用的数学模型。建立数学模型的过程更像是做实验，你要试验各种不同的模型，唯一的判别标准是实践，而不是数学证明。在数学上无懈可击的模型，如果不能解决实际问题就必须加以否定。

Q3. 概率统计在数学中的地位不断上升的原因是什么？

我不是专家，只能谈一点粗浅的看法。我认为根本的原因是社会需求使得应用数学的地位不断上升，而概率统计在数学的应用中占有特殊重要的地位。随着科学技术的迅速发展，人们发现应用领域提出的大多数问题含有不确定性的因素，因而无法用完全确定的数学模型加以描述。比如，金融数学研究的对象是证券和其他金融产品的定价规律、风险控制和投资策略。各种交易对象的价格无时无刻不在变化，而影响这些变化的因素极多，比如：宏观和微观经济、国家政策、交易者的策略和心理变化，等等；而这些因素本身也在变化。这是一个极其复杂的过程，完全无法用确定性的数学来描述，只能把它看成“随机过程”；或者用过去的统计规律来推断未来。类似的情形还有许多，比如在生命科学、医药卫生、信息科学、通讯技术、心理学、企业管理等等方面，大量的问题只能用概率和统计的办法去寻找解决方案。另一方面，由于高速计算机的广泛应用，原来无法进行的大规模统计计算变得轻而易举；这使得统计方法的应用遍及几乎所有的行业。

若干年前在美国科学基金会的一份报告中提出了一种观点：数学是所有高科技的核心；而且还提出了“数学技术”的说法。我相信，数学对于现代科学技术将发挥日益重要的作用，而这将会对数学本身的发展起重要的反作用。

作者简介：

丁伟岳，著名数学家，北京大学数学院教授、中科院数学与系统科学研究院研究员，1997 年当选为中科院院士。曾任中国数学会副理事长。

学会欣赏沿途风景

金 石

数学和哥德巴赫猜想

由于工作需要我常常出差，包括许多越洋飞行。在飞机上我通常会看一些学术论文，有时候邻座看见我阅读的奇怪东西时会问我是干什么的，我回答是“研究数学”。我最常听到的回答是：“那是我最差的科目。”大部分人会再没有兴趣和我继续聊。他们会觉得我是个异类，和他们没有太多可交流的。我倒是乐得清静，继续阅读或是思考我的数学问题。现代人的生活被现代通讯工具——手机、电邮、微信等切成碎片，能有那么一整段时间不被打扰地阅读和思考，是非常奢侈的事情。我十分珍惜长途飞机上这种大段不被打扰的时光。

人们常常不理解，那么枯燥的数学为什么会有那么一些人孜孜以求地研究，并且乐在其中。当然不仅是数学家，科学家在许多人眼里每天都在做着枯燥的事情。我上中学时风靡全国的报告文学《哥德巴赫猜想》中的陈景润，在全社会塑造了科学家最典型的形象。而现在许多家长会觉得，陈景润固然伟大，但我不希望我的孩子变成那样，而科学家——尤其是数学家，大概就是那样的。

乐趣：研究者生命闪光的瞬间

为什么那些科学家要乐此不疲地从事常人看来是非常枯燥的研究工作？我们的文化从小就教育孩子长大要攀登科学高峰，将来拿诺贝尔奖。然而，如果一个人的研究是为了得大奖，那么我会劝他最好放弃。首先，他拿诺贝尔奖的概率几乎是零，如果忙碌了一辈子是为了拿奖，最后没拿到，岂不是人生完全失败？ 其次，靠这种拿奖的信念做研究，根本就是本末倒置，完全失去了研究的乐趣，甚至失去了人生的乐趣。

那么，什么是研究的乐趣？

伟大的俄国作曲家斯特拉文斯基一次坐在钢琴边接受记者采访。记者问他：“斯特拉文斯基先生，哪一个时刻是你生平最伟大的瞬间？是你最终完成你的交响曲的那一刻吗？”

“不，不，不……”

“是你第一次听到乐队演奏你的交响曲的时刻吗？”

“不，不，不……”

“那一定是你的曲子被他们封为 20 世纪最伟大的作品之一的时刻了！”

“不，不，不……”

“那到底是哪一个时刻？”

斯特拉文斯基一边弹着一首曲子一边说：“我坐在钢琴边三四个小时，一直在寻找一个音符。我一直找不到那个音符，就在琴上梆梆梆地敲了三小时。三小时后，我终于找到了我要的音符！就是那个瞬间 !! 没有比那更美妙的瞬间了 !!! That is everything !!!!”

研究者在研究过程中有挫折，有痛苦，有漫长的煎熬。然而，如果把这样一个一个闪光的瞬间连接起来，就成为一串美丽的生命的珍珠。正如西方古典音乐中的交响曲、协奏曲和歌剧一样，需要一些准备，需要一些入门知识，许多人也许觉得枯燥无味，然而一旦入门了，便会发现，那是一个绚丽多彩的世界。古典音乐爱好者从中获得的享受，绝不亚于流行音乐为它的发烧友带来的乐趣。

科学研究是很好的职业

即使不从一个理想主义者的眼光来看研究者，完全从世俗的角度出发，科学家——至少是我了解的数学家——依然是一份很好的职业。2009 年 1 月，美国《华尔街日报》登出了美国 200 个职业排名。排名基于五个标准：工作环境、薪水、就业前景、体力要求以及工作压力大小。排在第一的，不是华尔街的银行家，也不是律师和医生，而是——数学家！

这可不是数学家自娱自乐的排名，也不是号称世界数学麦加巴黎人的排名，这是《华尔街日报》登出来的排名——每个人都知道华尔街追求的是什么。沿着排名往下看，第二是统计学家，第三是精算师，这些也都是数学出身的人做的事情。

在美国买房子，房屋中介会告诉客户挑房子的三个最重要的因素是：位置、位置、位置。今后家长问我孩子应该学什么，我也会毫不犹豫地告诉他们：数学、数学、数学！

这样说，当然物理学家、化学家、生物学家等等会不高兴。其实，每个职业都可以找出一个排名说自己是最好的。我想对学生说的是，你喜欢的职业，就是最好的职业！

人们做过一个调查，问题是：假如你不愁钱，你最想做的是什么。大多数人的答案都是：度假。每天从事你喜欢的工作，就相当于每天在度假。令人不可思议的是，还有人给你付工资度假。

研究者最大的幸福，就是每天做你喜欢的事情。

学会欣赏沿途风景

之所以人们常常看到科学家对研究的痴迷，很大程度上是因为科学家对研究的专注。我常对学生说，如果你每年没有几个晚上因为想数学问题睡不着觉，你不可能成为一个好的数学家。同样，如果你每天只是朝九晚五地做数学，你也不可能成为一个好的数学家。不管做任何事情，passion 是让人成功的最基本的要素。

当然，仅有 passion 是不够的。路漫漫其修远兮。以美国大学数学系为例，从大学生到成为一个独立的研究者，平均要四年大学、五年博士生、两到三年博士后的经历，然后才能成为（助理）教授，之后还要有五年左右才能拿到终身教职（tenure）。这么漫长的历程，很容易让大学生们觉得当科学家“看上去很美”，但坚持不了十多年寒窗的煎熬。仅仅是信念和热情，能让人坚持那么久吗？激情是会很快被燃烧掉的。

我向来不觉得那么漫长的求学历程是煎熬。人生的每一段都是美丽的，虽然我们的目的地可能非常遥远，就像乘越洋飞机从美国到中国一样，十多个小时的飞行枯燥而疲惫，让人生畏。然而，无论是长途飞机和火车，如果你去欣赏旅途中窗外的云卷云舒，眼前掠过的山川、村庄、草地、麦田和晚霞；如果你有几个有趣的旅伴，或者即使没有，你也懂

得欣赏飞机或火车上的音乐、电影、甚至游戏，或是带几本喜欢的书阅读，那么即使路途遥远，即使飞机晚点，即使没有抵达目的地，你也享受了一路的风景，拥有了一路愉悦的心情。人生可以说是不虚此行。更不用说你在大学里度过的青葱岁月，师长的教诲，友谊的温暖，同窗的激励，爱情的甜美，这一切，将让你的求学生涯变得丰富多姿。如果你能多交些朋友，多读些经典，养成能陪伴你终身的兴趣爱好，这样，即使是遇到挫折和不幸，你依然会相信，前面的道路宽广无比。

当然，也有很多人做了一段时间研究，发现老做不出结果来，这时候或者觉得自己不是这块料，或者变得茫然以致于最后放弃。研究会出什么结果事先是无法预料的——能事先预料并能按部就班地做出来的不会是什么激动人心的原创性研究。最好能同时思考几个问题，一个做不通就考虑其它的问题，过一段时间再回头，很可能由于思考角度不同，或是从别的问题和方向得到启发，豁然开朗，那时候，才真正领会到“众里寻他千百度，蓦然回首，那人却在灯火阑珊处”的妙境。

制度永葆研究之树长青

美国大学能吸引并留住世界上一大批杰出人才，很大程度上是因为美国大学的终身制。美国只有两种职业是终身的，一种是联邦法院的大法官——只有 9 位，另一种职业就是大学教授。人们常以为大学终身制会让人变懒，殊不知在拿到终身教授之前 tenure-track 的磨练，已经使那些好的学者养成了一种惯性，对他们而言，研究已经成为生活方式，让他们停下来是不可能的——至少好大学里大多数教授如此。终身教职的获得，反而使他们因为没有论文篇数的压力，从而可以有充分的保险去研究重大的学术问题。

德国大诗人歌德说过：“理论是灰色的，而生命之树常青。”那些原创性的成果，是让一个大学充满生命力的表现，而那些刻板排名的数据是灰色的。一所伟大的大学，就是要提供一种制度和土壤，让其中研究者的生命之树和她的莘莘学子一样年轻。

自由思考带来无限快乐

学术研究的一大乐趣，是没有老板“管”你。科学的重大发现不是计划经济，科学家也没有老板——你自己就是老板。人们可以要求楼房、桥梁和高速公路何时和怎样建成，只要配以充分的人力和财力就可以。科学的重大发现是无法计划，也不可能有老板布置任务要一定时间完成的——牛顿发现的万有引力，世界上没有任何人事先可以为他计划好并命令他一定时间内完成。海阔天空，异想天开，标新立异，才会有原创的思想，也是科学研究迷人的地方。

集合论的创始人康托尔说过，“数学的本质在于思考的自由充分”。自由充分的思考，可以说是每一个领域研究的根本要素。人的身体受到物理时空的局限，但思想是不受羁绊的。自由思考的时候，思想摆脱了沉重的身体，自在地遨游于万物，超越时空给肉身设置的障碍。自由思考的时候，人可以与自然对话，与自己的心灵对话。自由思考的快乐在于神游于物，更在于物我两忘。当一个研究者全身心沉入数学的世界时，他是忘掉一切的，而这样的境界，总是让研究者无比快乐，汲汲以求。而当思想受到太多束缚的时候，研究也就止步不前了。

读万卷书，行万里路

研究，至少是数学研究的另一大乐趣，就是可以和世界上其他有共同爱好的人合作。数学家不需要昂贵的仪器设备，但需要经常参加学术会议以及与同行交流，因此出差很多且必要，虽然不是度假，依然可以把出差的快乐和研究工作巧妙地结合在一起。读万卷书，行万里路，在数学家的工作方式中得到了充分的体现。每个人的思维都有局限，而这种合

金石教授（右二）与学生们在一起

作，不仅让你从其他人那里学到新东西，更重要的是，思想的碰撞，会迸发出意想不到的火花，加速科学发展的进程。数学界有个很好的惯例，就是合作的论文作者排名多数时候是以英文字母顺序排列的，这里重要的是合作的友好和快乐，而不是对功名利禄的斤斤计较。

列宁在纪念国际歌的作曲者欧仁•鲍狄埃逝世二十五周年的文章中写道："一个有觉悟的工人，不管他来到哪个国家，不管命运把他抛到哪里，不管他怎样感到自己是异邦人，言语不通，举目无亲，远离祖国——他都可以凭《国际歌》的熟悉的曲调，给自己找到同志和朋友。"

我们也一样，凭着数学的语言，无论走到哪里，都可以为自己找到同志和朋友。

作者简介：

金石，上海交大数学系系主任，致远讲席教授。1983 年北京大学数学系毕业，1991 年获得美国亚利桑那大学应用数学博士学位。2000 年以来为美国威斯康星大学数学系正教授，并曾任该系系主任。

《数学家》的相册

林开亮

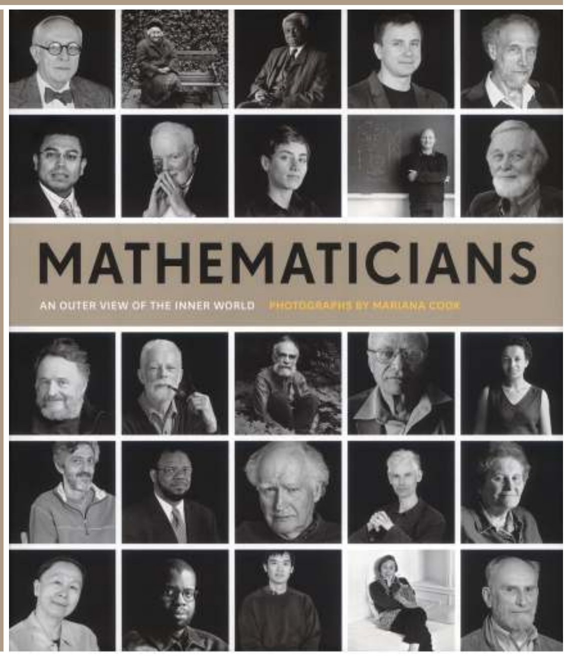
感谢普林斯顿大学出版社授权翻译并在本刊首次发表书中的部分内容。

“美者真，真者美”——此即尔等在人世所共知，所应共知。

——济慈（John Keats），《希腊古瓮颂》[1]

真实是数学中的终极权威。一个定理必须被证明是真的。经常在十多年的工作以后，一个证明的长度将缩短到只有一页。它因其简单性而优美。我曾给许多人拍过照：艺术家、作家、科学家和其他人群。在谈论其工作时，数学家比其他任何群体更惯于用“优美”、“真实”、“漂亮”。

——玛丽娅娜•库克（Mariana Cook），《数学家——内心世界的外观》序言



引 言

对一般读者而言，数学家绝对是一个神圣的职业，即便对数学专业的学生来说也是如此。由于数学学科的特殊性，数学家本身也很难为公众所了解。对于未能登堂入室的数学系学生来说，对数学与数学家也往往是一知半解。但不论怎么说，种种现象都只能增强大众对数学与数学家的好奇心。

上个世纪三十年代，美国数学家贝尔（E. T. Bell）写过一本《数学精英》（*Men of*

玛丽娅娜•库克，达斯汀•赫斯顿（Dustin Heuston）摄

[1] 济慈的《希腊古瓮颂》(*Ode on a Grecian Urn*) 有多个译本，这里我们选取的是余光中的翻译（《济慈诗八首》，刊登于《扬子江诗刊》，2009 年 05 期）。

[2] 有两个中译本：《数学精英》（在 2004 年上海科技教育出版社的再版中更名为《数学大师》），徐源译，北京，商务印书馆，1991 年；《大数学家》，井竹君等译，台北，九章出版社，1998 年。

Mathematics）[2] 介绍了古往今来的三四十个有代表性的大数学家，对数学家的宣传与数学的普及产生了深远的影响。

近些年来，也有一些作者仿照贝尔《数学精英》的模式介绍二十世纪的大数学家，但能够与之媲美的作品并不多见。不过，倒是有一本风格与众不同的书脱颖而出。这就是美国摄影师库克（Mariana Cook）的摄影集：*Mathematicians — An outer view of the inner world*（普林斯顿大学出版社 2009 年出版），暂译为《数学家——内心世界的外观》，以下简称《数学家》（笔者参与了该书的中译本翻译，见本期《译后记》一文）。

《数学家》是库克继 2004 年出版的科学家相册《科学的面孔》[3] 之后的又一部力作。虽然这两本书关注的对象不同，但它们之间颇有渊源。这中间有一个小故事，在《数学家》一书的介绍和后记中都有交代。我们略述如下，这要从勃兰登 • 弗拉德（Brandon Fradd）说起。弗拉德于一九八〇年代在普林斯顿大学数学系硕士毕业，他估计自己不适合从事理论数学的研究，就转向了医学，现在他是生物科技的投资者。几年前，一个偶然的机会，弗拉德认识了摄影师库克和她的丈夫汉斯 • 克劳斯（Hans Kraus）。后来库克将她新出的相册《科学的面孔》送给了弗拉德，弗拉德看到此书后立即提议，是否愿意为数学家也出一个相册？库克当即表示同意。于是弗拉德为库克安排与普林斯顿的老师和朋友见面摄影，之后又通过传递性将范围进一步扩大到全世界的一些有代表性的数学家（主要是在美工作或访问的），最后形成了相册《数学家》。库克还邀请普林斯顿大学教授院的前任院长、著名数学家罗伯特 • 冈宁（Robert Gunning）为该书写了引言（见该书第 8-9 页）。此外，库克告诉笔者，弗拉德本人还私人购买了两千册《数学家》赠送到全美各地的图书馆。弗拉德说，哪怕只有一个学生的命运因为这本书发生了改变，这么做就都是值得的。

全书共选入了 92 位数学家的照片，大多数都是取得了卓越成就的成名人物，囊括了许多大奖得主，如阿贝尔奖、菲尔兹奖、沃尔夫奖等等。这些数学家的工作也几乎遍历了所有的数学领域，从像数论这样的经典课题到像小波分析这样的热门应用领域。大部分数学家都上了年纪，其中有七位在该书出版前后已经过世，他们是昂利 • 嘉当（H. Cartan, 1904-2008），盖尔范德（I. M. Gelfand, 1913-2009），布莱克韦尔（D. H. Blackwell, 1919-2010），芒德布罗（B. Mandelbrot, 1924-2010），马利亚维（P. Malliavin, 1925-2010），希策布鲁赫（Friedrich Hirzebruch, 1927-2012），瑟斯顿（W. P. Thurston, 1946-2012）；当然也不乏一些年轻的新秀，如巴尔加瓦（M. Bhargava, 1974-），陶哲轩（Terence Tao, 1975-），米匝哈尼（M. Mirzakhani, 1977-），而后者是全书中最年轻的一位。除了她之外，本书还收入了其他 12 名女性，包括华裔数学家张圣容（Sun-Yung Alice Chang）。张圣容目前是普林斯顿大学数学系的系主任。除前面提到的陶哲轩、张圣容外，还有三位华裔数学家入选该相册，他们是：萧荫堂（Yum-Tong Siu）、丘成桐（Shing-Tung Yau）、田刚。

每一位入选的数学家都附有一篇简短的自述，介绍他们是如何走上数学道路的，有哪些事件对他们的数学生涯产生了深远的影响，他们又是怎样看待他们的工作以及整个数学的。这些见解很值得每一个对数学感兴趣的读者去了解。我们平常很少有机会聆听大数学家谈他们的数学经历和对数学的感悟，库克的这本相册弥补了这个缺憾。以下笔者从中译本中选取了一部分内容分享给读者，考虑到也许译文欠佳，有兴趣的读者请阅览原书。[4] 该书中译本不久将由上海世纪出版集团出版，敬请有兴趣的读者关注批评。

[3] 关于摄影师库克本人以及《科学的面孔》一书的介绍，可见本文的姊妹篇，二十世纪科学家群像——《科学的面孔》，台湾《科学月刊》第 44 卷第 527 期（2013 年 11 月号），867-870。同时，也可以登录库克的个人主页：http://www.cookstudio.com/。

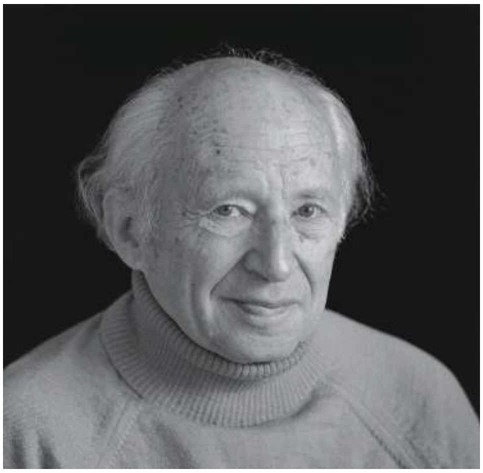
[4] 读者也许可以比照着另一本风格相近的书一起阅读：J. F. Dars, A. Lesne, A. Papillault, *The Unravelers: Mathematical Snapshots*(A K Peters, Ltd., 2008)，中译本《解码者：数学探秘之旅》，李锋译，姚一隽、张小萍校，高等教育出版社，2010 年。

全文欣赏

盖尔范德（Israel Moissevich Gelfand）

群表示，分析

罗格斯大学数学系兼职教授[5]



盖尔范德（1913-2009）

我不认为自己是先知。我只是一个学生。在我的一生中，我曾经师从于像欧拉和高斯那样的伟大数学家、比我年长或年幼的同事、我的朋友和合作者，最重要的是师从于我的学生。这就是我持续工作的方式。

许多人认为数学是一门很枯燥很形式化的科学。然而，在数学中，任何真正好的工作总是具有它优美、简单、精确和不可思议的思想。这是一种奇异的组合。在很早的时候我就从古典音乐和诗歌的例子中理解到这个组合是本质的。而这在数学中也是典型的。很多数学家欣赏正经的音乐也许不是偶然。

当我们想到音乐的时候，我们并不像通常在数学中那样将它分成一些特殊的领域。如果你问一个作曲家他的职业是什么，他会回答说，“我是作曲家。”他不大可能回答说“我是四重奏的作曲家”。也许这就是为什么当我被问及我做哪一种数学时，我只是简单地答复“我是一个数学家”的原因。我想提醒你，当音乐风格在二十世纪发生改变时，许多人说现代音乐缺少和谐，没有遵循标准规则，有不和谐音，等等。但是，勋伯格（Arnold Schoenberg）、斯特拉文斯基（Igor Stravinsky）、肖斯塔科维奇（Alfred Shostakovich）和施尼特凯（Alfred Schnittke）在他们的音乐中像巴赫、莫扎特、贝多芬一样地精确。

1930 年，年轻的物理学家泡利（Wolfgang Pauli）写了一本最好的关于量子力学的书。在这本书的最后一章，泡利讨论了狄拉克方程。他写道，狄拉克方程有瑕疵，因为它导致了不可能的、甚至是疯狂的结论：

1. 方程将预言，除了电子之外，还存在带正电荷的电子，即正电子，但没有人观测到它。
2. 而且，电子遇到正电子时的行为很奇异：它们两个将湮灭并形成两个光子。

而且完全不可思议的是：

3. 两个光子可以变成一个正、负电子对。

泡利写道，虽然如此，狄拉克方程还是非常有趣，特别是狄拉克矩阵值得注意。我很幸运地见到了伟大的保罗•狄拉克 (Paul Dirac)，我们在匈牙利一起度过了几天。我从他那里学到很多。我问狄拉克：“保罗，既然有这些批评，为什么你没有放弃你的方程而是继续追求你的结果？”

“因为它们很美妙。”[6]

现在，数学的基本语言中有根本性的改革。在这个时候，尤其重要的是，要记住数学的统一性，记住它优美、简单、精确和不可思议的思想。

---

[5] 这里指盖尔范德身兼罗格斯大学以及莫斯科国立大学两所大学的教职。

[6] 无独有偶，1954 年杨振宁与米尔斯（Robert Mills）一起提出后来发展为规范理论的杨（振宁）-米尔斯（Yang-Mills）方程时，也遭到了泡利的反对，而且杨振宁与米尔斯也同样是基于美妙的理由发表了他们的工作。见杨振宁，*Selected Papers 1945-1980 with Commentary*（W. H. Freeman and Company, 1983）一书第 19-21 页或江才健《规范与对称之美——杨振宁传》（台北，天下远见，2002 年；广州，广东经济出版社，2011 年）第九章的叙述。

格里菲斯（Phillip Griffiths）

微分几何，代数几何

普林斯顿高等研究所数学教授和前任所长

格里菲斯（1938-）

我在北卡罗来纳州的农村长大，并且主要是在农村学校上学，然后去了亚特兰大附近的军事学院。南方的一个传统是就读军事学院。而那里正是我坠入数学爱河的地方。我遇到了一个极好的数学教师威尔逊（Lottie Wilson），她让我对数学这门科学有所见识，此后我便开始心无旁骛地思考数学。我后来去了普林斯顿大学读研究生院，又在伯克利做博士后，研究的都是数学。我在哈佛教了多年的书，然后去杜克大学担任数学院院长。1991 年，我进入普林斯顿高等研究所担任所长。

对算得上数学珍品的东西，数学界往往有完全一致的评判。创造力是可遇而不可求的。你苦思冥想，穷追不舍，然而常常身陷困境不能自拔，于是暂时放开转而做别的事情，突然间豁然开朗，你看到了一些希望。我们做数学主要是出于美学的动机。当然，物理也是一门非常优美的学科，然而它与自然紧密相连。数学是科学的语言。数学的实际方面保障了我们的生活，例如各种安全码，又如各种经济部门的人控市场。

我最主要的兴趣一直是几何。我特别感兴趣的是现代几何，它与拓扑学（形状的几何学）、代数几何（代数方程及其图像与分析）与微分几何（诸如曲面、肥皂泡之类的可度量的形状）紧密相关。即使作为一个行政人员，我每天也把最初的几个小时用来做数学，而且我一直带学生。我喜欢学生。他们让我感到惊讶。他们接触一个对他们而言新鲜的学科，因而他们以不同的方式思考，而且，看着他们成长确实有趣。

在过去的十年里，我参与了世界银行的科技计划，主要是尽力帮助非洲建立一个本土的科学团体。在历史上，他们把学生送到国外学习，但这些学生往往不再回去。为了使得科学与技术对非洲的生活的各个方面——不论是农业、医疗，还是经济——产生影响，他们不得不一直引进专家，因为他们自己的人才已经移民了。

在我们国家，进入数学和科学领域的年轻人不如从前那么多了，在欧洲甚至在中国也是如此。他们想进入商业。低端和终端的新想法可以改良小玩具或生产线，这在中国、韩国与印度很盛行。而在美国，强调得更多的是能够给你全新技术的创造力：科学与数学产生的高价值的智力财富。可以发现，从麻省理工学院、加州理工学院、斯坦福大学毕业的学生并没有减少。在这些地方，那一点仍然很重要。

然而不幸的是，科学教育，特别是数学教育，从幼儿园到高中，情况都不太好。即使好学校也没把数学教好……我见过的新课本与我那时所用的课本比起来，简直令人害怕。首先，它们太厚了。如果你不能用一百五十页讲明白一门课，那么你就没有充分理解这门课。你要把最重要的东西选出来解释清楚，如果做得好，学生们可以自己领会其余的部分。

在当今世界，科学知识尤为重要。许多工作都要求具备定量的、分析的技能。科学所教给你的事实就是基于证据推理的精神，而我们正是在这一点上失败了。要成为我们国家的好公民，你需要对科学有一个一般的认识。看看进化论的争辩，看看新闻和报纸

上的种种数据。你就会发现，事实上，对于进化论的大意以及如何理解新闻报纸上的数据，许多人连最模糊的观念都没有。

造成这一问题的部分原因在于学校的教学。教师主要是通过教育院校走进教学体系。他们更多地停留在教学技能的层面而并没有深入到教育的本质部分。一个数学教师，哪怕是一个小学数学老师，都应该对这个学科有一个硕士水平的了解。只有具备了如此深刻的了解，你才能用一种简单的方式更好地去教授初等的内容。否则，你可能会弄得不必要地过分复杂。威尔逊夫人，我的第一个数学教师，绝对是一个富有天分的数学家，这一点使她成为一个伟大的教师。

萧荫堂（Yum-Tong Siu）

多复变函数

哈佛大学威廉·埃尔伍德·拜尔利（William Elwood Byerly）讲座教授

我 1943 年出生于中国，童年在澳门度过，青少年在香港度过。从香港大学本科毕业之后，我来到明尼苏达大学念研究生，1966 年在普林斯顿大学获得博士学位。从 1992 年起，我开始担任哈佛大学的拜尔莉讲座教授，并在 1996-1999 年期间担任数学系主任。在 1982 年加入哈佛以前，我曾任教于普渡大学、圣母大学、耶鲁大学和斯坦福大学。

萧荫堂（1943-）

虽然我的数学生涯已逾四十二载，但小时候我从未想过要做一个数学家，因为我最初钟爱的是中国文学，特别是古诗。我进高中以后，因为沉浸于组装收音机，才对科学和数学发生了兴趣。我常常在跳蚤市场淘废旧收音机的各种部件，利用基尔霍夫定律（Kirchhoff 's law）对电路图进行简单的修改后，我能成功地将淘来的部件组装在一起，这让我很满足。后来我发现，比起耗费时间的实验过程，我更喜欢理论科学。

数学吸引我是因为它的优美、清晰、逻辑必然性与普遍性。它超越了语言和文化障碍。它以一种完全清晰、毫无疑问的方式提取了自然结构的逻辑共性。

我的数学研究领域是多元复变函数，分析学的一个分支，与几何学紧密相关。微积分处理实数变量，代表的是测量。复数变量允许使用虚数，包括 –1 的平方根。多元复变量处理不止一个复变量，提供了研究和理解来自于物理学、天文学、工程学以及其他应用科学领域的方程及其解的几何性质的自然平台。

有时人们觉得奇怪，何以一个人会在做这样的基础研究中得到满足，它仅仅受智力上的好奇心与美妙指引，而对该研究是否有任何具体的直接应用与回报期限完全不予考虑。数学家认为，对数量的结构、对称性以及空间的真实而深刻的理解将最终导致真正新奇的实际应用，其深刻性与普遍性将远甚于那些从任务导向引发的研究。在现实方面，数学不需要任何昂贵的支出。随着计算机应用的增多，它越来越深入到所有领域的量化方面，但至今为止，数学的很多领域都与此无关。

回首我的数学生涯，我发现滋养它的一个最关键的因素是智力激发的环境。作为研究生，我从与同学的讨论那里受益良多。我的导师和楷模，如冈宁（Robert Gunning）——我的博士论文导师，卡拉比（Eugene Calabi）、格劳尔特（Hans Grauert）与孔恩（Joseph Kohn）明确地塑造了我的研究进程与数学观。

张圣容 (Sun-Yung Alice Chang)

几何分析

普林斯顿大学尤金·希金斯
（Eugene Higgins）讲座教授

张圣容（1948-）

我出生在中国的古都西安。时值中国革命，因此我们举家搬迁到香港，在我两岁时又迁到台湾。我父亲是建筑师，母亲是会计。我在台湾长大，升入了国立台湾大学。

长大以后，我对中国文学特别着迷，不过数学也很在行。我发现数学简练而优美；我欣赏这种逻辑的思维方式。第二次世界大战以后，台湾的经济很不景气，因此那些有科学和技术背景的年轻人更容易找到好工作而自立。我之所以决定在大学主修数学，部分就是出于实际的考虑。我本科同学的数学班看起来是非常特别的一届——班上四十个学生中有十二个是女生。从大一开始，我们五个人组成了一个团体[7]，一起学习一起玩耍。我们是班上最喧闹的一群，乐趣多多。只是在进入了伯克利研究生院我才知道，做女数学家可能是一种孤独的经历。

在加州大学伯克利分校的研究生院，我的课题属于经典分析。粗略地说，数学有三个分支：分析、几何与代数。在分析中，通常将事物分成许多小片；单独分析每一个小片然后将信息拼接起来。

在研究生院最后一年，我与我的一个同学结了婚。我丈夫杨建平（Paul Yang）是一个几何学家，从形状和图形的视角来看待事物。婚后早些年，我们只是粗线条地谈论数学，从不与对方讨论各自的研究计划。慢慢地，我们意识到，我们研究的一些问题既可以从几何的观点看也可以从分析的观点看。在结婚十年之后我们开始一起合作研究！我们现在研究的领域称为几何分析，用分析中的方法解决几何问题。一个主要的问题是将某些四维流形分类。这个问题与物理学中的问题紧密相关，因为我们生存的空间是三维的，但还有一个额外的时间维数。

我一直觉得，像音乐一样，数学是一门语言。为了系统地学习它，有必要一小块一小块地慢慢吸收，最终达到浑然天成的效果。从某种意义上说，数学又像古代汉语——非常典雅而优美。听一个精彩的数学讲座就好比听一场精彩的歌剧。万事齐全，一切都趋向问题的中心。我享受数学！

[7] 据张教授回函：“我大学同班有许多女同学，其中最常切磋的有胡守仁、金芳蓉、吴徵眉和刘小詠（已早逝）。”此外，陈省身先生还专门写过一篇传记《记中国的几位女数学家》（与康润芳合作）介绍张圣容、李文卿、金芳蓉、吴徵眉、藤楚莲、萧美琪六位台湾女数学家，该文最初发表于台湾《传记文学》66 卷第 5 期（1995 年），也收入《陈省身文集》第 152-161 页，张奠宙、王善平主编，华东师范大学出版社，2002 年。

米匝哈尼（Maryam Mirzakhani）

遍历理论、泰希米勒（Teichmüller）理论

普林斯顿大学数学教授

米匝哈尼（1977-）

我在伊朗长大，有一个幸福的童年。我的家人中没有科学家，但我从我的哥哥那里学到了很多，他一直对数学和科学有兴趣。在我周围，女孩被鼓励要自立并追求其兴趣。我记得曾在电视上看到关于一些女强人如居里夫人（Marie Curie）和海伦•凯勒（Helen Keller）的节目。我尊敬那些对其工作充满热忱的人，对关于梵高（Vincent van Gogh）的一本书《渴望生活》[8] 有很深的印象。然而，作为一个孩子，我梦想成为作家，而读小说则是我最喜欢的消遣。

后来我参加了数学竞赛，对学习数学越来越感兴趣。我有一些好朋友对数学也感兴趣，这使得我的本科生涯非常激动人心。我主修数学，后来到哈佛念研究生。在哈佛我跟麦克马伦（Curt McMullen）一起工作，我对与动力系统和黎曼曲面的几何相关的一些数学领域发生了兴趣。麦克马伦广泛的兴趣和深刻的见解给我很大的影响。

数学系变得更加为男性主宰，而且有时令年轻女性畏惧。然而，话虽如此，我却从来没有因为自己是女性而遇到任何麻烦，而且我的同事很支持我。不过情况也远不理想。我相信，女性能够胜任与男性同样的工作，但期限是不一样的。对男性来说，保持长时期的集中并为其工作牺牲更多是相对容易的。另外，社会对女性的期望有时不同于做研究的需要。对女性来说，很重要的一点是，要保持自信和积极。

我主要研究与曲面的几何相关的问题，也涉足其他相关的领域。复分析和遍历理论总是令我着迷。

我喜欢学习数学的不同领域并理解它们之间的联系。关于黎曼曲面的问题最精彩的方面是它与诸多数学领域之间的关联，包括遍历理论、代数几何和双曲几何。

我做研究非常慢。我不相信在数学的不同领域之间存在边界。我喜欢思考令我兴奋的有挑战性的问题，并随其所至。这使我可以与许多聪明的同事接触并向他们学习。从某方面讲，做数学的感觉就像写小说，而你的问题就像一个活生生的主人公在发展。然而，你所说的必须非常清晰：每一件事情必须像钟表中的齿轮那样衔接得有条不紊。

[8] 该书是美国作家欧文•斯通（Irving Stone）为梵高写的传记，有两种中译本，一是台湾著名作家、翻译家余光中的译本《梵高传》，一个是大陆翻译家常涛的译本，译作《渴望生活——梵高传》或《梵高传——对生活的渴求》。

片段欣赏

■ 思考数学时我更喜欢闭上眼睛。我最好的工作是在夜晚半睡眠的状态下完成的。有时候我在睡觉时想，“嗯，我有一个引理要证明或否定。”（我应该解释一下引理是什么吗？登山者从一级上到更高的一级需要登山杖，而引理就是数学家的登山杖。）当然如果打算以后发表，你需要将东西写下来。有时你会发现你所想的是错的，但那是少有的。

让－皮埃尔·塞尔（Jean-Pierre Serre），法兰西学院荣誉教授

■ 物理固然吸引我，但课程往往看起来很无聊，而且我做实验总是不成功。音乐课告诉我，我没有一点音乐细胞；哲学课则完全是海阔天空不着边际，而教写作的一个富有创造性的教授则当着全班同学的面朗诵我的诗歌作为反面教材！相对而言，在数学系我瞬间有了一种回到了家的感觉。因为我的社交能力发展缓慢，我对如何与人打交道知之甚少。但是，数学系的公共休息室是一块乐土，有活泼的对话，各种各样的棋类对弈，如国际象棋、围棋、军棋，还有在一旁胡乱支招的观战者。这个因纳粹导致欧洲数学家大量移民而造成的国际化环境，对我来说是崭新的。（我们有时将这个地方称为“蹩脚英语系”（Department of Broken English）。）在普林斯顿，像福克斯（Ralph Fox）、斯廷罗德（Norman Steenrod）和阿廷（Emil Artin）这样的专家教给我数学思想的魅力和数学问题的挑战。

约翰·米尔诺（John Willard Milnor），纽约州立大学石溪分校数学教授

■ 我一直喜欢数学。记得在我两三岁时，总爱围着祖母转。她一边擦窗户，一边跟我玩游戏。她要我说出一个数字，比如说 3，她就用清洁剂在窗子上喷出一个大大的 3 然后再擦掉。我觉得太好玩了。我小时也有一些算术练习簿。它们都很简单，比如，像 3 ＋□＝ 7 这样的等式，问方框中是几？我觉得真是有趣。对我来说，数学是唯一让我奉为真理的：3 加 4 就是 7，合该如此。永远无人可以提出新兴概念而说老答案已经是不对的。我喜欢数学的明确理性，并视它如一种抽象的玩意。我只是在后来才意识到它是如何与现实世界相关，又如何可以应用到各种事情上。

陶哲轩（Terence Chi-Shen Tao），加州大学洛杉矶分校数学教授

■ 我十二岁那年的冬天，父亲[9]坐在火炉边烤火，旁边有他的三个学生，他们在讨论着什么。我坐在他身边，一边看着一本书，一边欣赏着窗外的雪景，享受着屋里的温暖。不知什么时候，父亲和那三个年轻的学生突然停止了讨论，陷入了沉思。这突如其来的宁静吓到了我，看起来要持续到永久，然而他们每个人看起来都非常惬意，完全沉浸到他们的世界中去了。过了许久，其中一个人开口说了什么，而其他人则露出了充满喜悦的笑容。我想，不论数学究竟是什么，它一定很美。

……最重要的是，我感到很幸运，能以自己的方式经历很多年前在我父亲和他的学生身上所见到的那种惊讶和满足。

广中惠理子（Eriko Hironaka），佛罗里达州立大学数学教授

[9] 即著名的日本数学家广中平祐（Heisuke Hironaka）。

■ 我一直觉得，音乐、诗歌和数学这三个东西非常相似。在很大程度上，对所有的纯数学家来说，这都是对的。在中学里，数学一般被划分到理科的范畴。但是，对数学家来说，像音乐、诗歌与绘画一样，数学也是一种艺术创造。它们都包含——而且事实上需要——一种创造火花。它们都在努力地表达日常语言所不能表达的真理，它们都在努力地臻向于完美。

巴尔加瓦（Manjul Bhargava），普林斯顿大学数学教授

■ 在科学圈，我最富有名声的是发明了生命游戏，它开创了细胞自动机的新领域。我还发现了几个很大的对称群。这是很难做到的，而且在当时是一个很有趣的课题。然而，我最为自豪的是，发现了数的一个全新的世界，这被高德纳（Donald Kunth）[10] 命名为“超实数”。我真希望这个名字是我取的。一百多年前，伟大的德国数学家康托尔（Georg Cantor）发现了无穷数的理论；两千多年前，阿基米德创建了我们常用的实数的理论。超实数将二者包括在内，有一些超实数是康托尔的无穷数，有一些则是普通的实数；但也有一些超实数是二者与无穷小数的混合。当我发现了它们以后，我在六周的时间里陷入了永恒的白日梦，想象着探险者科蒂斯（Hernando Cortez）当时如何眺望太平洋和西方人前所未见的这一片世界。我所看见的还没有被人看到过。虽然它是完全抽象的，但它同时也是真实的。数可以比物理对象更为真实。我所发现的不仅仅是数，还有数的一个奇妙的新世界。

约翰·康威（John Horton Conway），
普林斯顿大学冯·诺依曼（John von Neumann）讲座教授

■ 课堂上，我的数学老师指着我喝到：“杜•索托伊，下课之后跟我走一趟。”当时我十二岁，害怕极了：莫非我做错了什么？下课铃声响起后，我被他带到数学区的后边。我想，“现在我真的有麻烦了。”然而老师开始解释说，他认为我应该去了解真正的数学是什么样子的。他给我指引了一些书，其中包括哈代（G. H. Hardy）的《一个数学家的辩白》[11]。他还建议我阅读加德纳（Martin Gardner）在《科学美国人》上的专栏 [12]。真是出乎意料！我读到了关于素数、对称的语言，以及拓扑的奇妙世界。我经历了第一次的证明所带来的震撼和激动。哈代写道，数学家是模式的创造者，而且创造的模式必须要美。我就像在学习一门乐器一样，开始时只允许弹奏简单的音阶和琶音，而看到这些书就好比第一次听到某个人为我演奏了一段真正的音乐。

马库斯·杜·索托伊（Marcus du Sautoy），牛津大学数学教授

■ 当我十岁时我居住在英格兰美丽的剑桥大学城，一天我在当地的图书馆偶然幸运地发现了一本书，在这本书的封面上陈述了所有最著名的数学问题，至少对那时作为外行的读者是如此。其中一个问题是著名的费马大定理，而其问题是证明：虽然很容易找到许多平方数使得它可以写成另外两个平方数的和，但同样的结论对立方数和任何的高次幂都不成立。费马是一位杰出的数学家，他曾将这个断言写在他手抄的某本希腊数学著作的页面边缘上。他宣称“我对此定

[10] 高德纳，四卷本《计算机程序设计艺术》的作者。高德纳之名是计算机专家储枫在 Donald Kunth 访问中国之前为他专门取的中文名。他曾专门为康威的超实数之发现写了一本小说，*Surreal Numbers*，有中译本，《研究之美》，高博译，电子工业出版社，2012 年。

[11] 有两个中译本：王希勇译，北京，商务印书馆，2007 年；也见于李文林、戴宗铎、高嵘所编译的哈代的非专业文集《一个数学家的辩白》，大连理工大学出版社，2009 年。

[12] 加德纳主持了《科学美国人》的数学游戏专栏多年，他的许多文章已集结成书出版，国内有中译本，例如《矩阵博士的魔法数》、《啊哈！原来如此》、《啊哈！灵机一动》、《趣味密码术与密写术》等。

理有一个精彩的证明，但是边缘的空白是如此之小而无法写下来”。此后，数学家一直在为找到一个证明而奋斗，但都未成功。找到费马大定理的证明成为了我儿时的梦想。

安德鲁·怀尔斯 爵士（Sir Andrew John Wiles），普林斯顿大学，希金斯（Eugene Higgins）讲座教授

■ 数学家为什么能够长年专注于研究某个特定的问题？也许是因为对应用或进一步的数学非常重要；也许会带来认可；结合教学，这会带来收入——因为做自己喜欢做的事情而得到报酬。但所有这些都是次要的，与无限的不确定性抗争才是最基本的回报。在我而言，只有做爱的乐趣超越了做数学，而滑雪是远远排在第三位的。

爱德华·尼尔森（Edward Nelson），普林斯顿大学数学教授

■ 另一方面，数学是一种你可以直接接触而无须任何中介工具的东西。这是数学最显著的特征。独自一人你仍然可以思考数学。你没有必要做当前很重要的数学，因为那样的话你必须阅读最新的文献。我并不是说你应该孤立地工作。如果那样，你无法取得进展。我想说的是，当真正开始要做一个数学家时，关键的一步是认识到，在某个时刻你必须停止念书了。你必须自己思考。你必须成为自己的权威。不再有你需要求助的其他权威了。在那一刻你必须认识到，一个东西是否写进书本并不重要。更重要的是，你是否有一个证明以及你是否确信它。其它的都不重要。

阿兰·孔涅（Alain Connes），法国高等科学研究所、俄亥俄州立大学数学教授

■ 虽然我父亲的工作需要数学（主要是统计），但给我深刻印象的是他对这个学科的喜爱。在很小的时候（大约十岁），我从他那里学到了正多面体和半正多面体，而且我们做了许多模型。我十六岁时发生的一件事令我特别惊讶。我告诉父亲，我们的中学数学老师明天将要开始教微积分。父亲听完后看起来有些忧虑，立即将我叫到一旁，为我熟练地演示了微积分的本质和优美。我想给我印象最深的是，他渴望成为那个将这门课程的深刻优美揭示给我的人，我由此知道了数学的这门课程是何等地值得珍视。

彭罗斯爵士（Sir Roger Penrose），牛津大学劳斯·鲍尔（Rouse Ball）讲座教授

■ 在高中时我读了贝尔（E. T. Bell）的《数学精英》。每一章描述了一个大数学家的生活与工作。从这本书中我学到了许多奇妙的东西，例如二次互反律、算术级数的狄利克雷定理。我反复地努力想象如何证明它们，当然总是徒劳的。我总是喜欢自己先思考而不愿意去读别人写好的东西。当我还是孩童时，我就不喜欢在猜谜题时翻答案，虽然那样做我能够学到更多的东西。这种以自己的方式去做事情的强烈愿望曾经是一股力量，但如果还伴有阅读别人工作的兴趣和能力就更好了。你需要平衡。

在读了贝尔书中关于阿基米德、费马、牛顿、高斯、伽罗瓦等人的章节以后，我产生了这样的想法，如果你不是天才，那么你不可能成为一个数学家。我知道我不是天才。但我觉得这一点对物理学来说不成立，因为我父亲就是一个物理学家。于是，我进入普林斯顿大学研究生院以后选择了物理。然而在第一年，我就很清楚了，数学才是我的真爱和最有天分的学科，因此我转向了数学。

我最感兴趣的定理——二次互反律——的最终推广时，当我知道我最喜欢念的书——范德瓦尔登（Bartel Leendert van der Waerden）的《近世代数》[13]——正是基于他与诺特（Emmy Noether）的讲课时，我非常震惊。阿廷是一个伟大的数学家，同时也很喜欢教课。他成为了我的指导者和博士论文导师。[14]

约翰·泰特（John T. Tate），
奥斯汀德克萨斯大学讲座教授，哈佛大学荣休教授

在我的访问快结束时，我们通宵都在计算一些积分，做一些不现实的假定。许多个小时过去以后，我们得到了一个公式，处处都有不收敛的无穷和。这个表达式中仅有一项有意义。扎吉尔（Don Zagier）问我，这一项代表的应该是什么，我预言说，它代表的应该是一个素数除以某个奇异 j- 不变量的幂次。这看起来是毫无理由的——我们所做的任何事情与 j- 不变量哪怕是遥远的关系都没有。因为已经是凌晨四点了，我建议我们等天亮以后去图书馆，那里有表可以供我们查阅不变量。然后我睡觉去了。

然而，扎吉尔继续坚持，用他的手动计算器一次一次地计算 j- 不变量，验证了我的预言在每一种情形都是正确的。中午时分我起床了，而扎吉尔还在熟睡中。客厅的地板上到处都是他的演草纸，每一页都肯定了这个猜想。当我翻到最后一页时，上面写着："赶紧叫醒我！"

这是我数学生涯中的巅峰时刻。我和扎吉尔不知道是否会得到最终的公式，但是我们知道有了一个很好的开始，而且是在一个全新的领域内工作。这是一片未经开垦的土地。没有人曾经发现这里，无需紧赶。几个月以后，我们达到了计算的终点——他对 L- 函数的推导与我对解的高度的计算——并仔细审察了许多复杂项，我们发现它们吻合得特别完美。这引出了一个简单的等式，现在被称为格罗斯 - 扎吉尔（Gross-Zagier）公式。没有人真正解释过为何它是对的，虽然达蒙（Henri Darmon）、库德拉（Steve Kudla）和张寿武每个人都对其推广做出了进展。

当你发现了一个数学真理时，每件事情都立即变得清晰了。理解起来是如此容易。你不再想碰它。见到数学的美妙真是令人愉快。

本尼迪克特·格罗斯（Benedict H. Gross），
哈佛大学乔治·莱弗里特（George Leverett）讲座教授、前任院长

[13] 有中译本《代数学》，第一卷（丁石孙、曾成肯、郝炳新译），第二卷（曹锡华、曾成肯、郝炳新译），科学出版社，2009 年。

[14] 事实上，泰特还成为了阿廷的女婿。

致谢：在本文的准备和写作过程中，清华大学高等研究中心的杨振宁教授、华东师范大学的王善平教授与首都师范大学数学院的刘瑞义、邵红亮、王丽芳、颜昭雯、张宝群、赵洁与文学院的高中华、吕鹤颖、苗勇刚等同学对初稿给出了许多有价值的建议；普林斯顿大学数学系的张圣容教授与加州大学洛杉矶分校数学系的陶哲轩教授分别对相对应的译文初稿作出了修改；摄影师玛丽娅娜·库克委托她的秘书道格·里克斯（Doug Leax）提供了文中的所有照片。作者在此一并表示衷心的感谢。

另外，还要感谢《数学传播》的一位匿名审稿人为笔者指出了初稿中的两处译文疏漏，感谢首都师范大学数学院的王永晖教授的热心推荐。

《数学家》译后记

提起当代数学家，也许最容易让人想到的就是电影《美丽心灵》的主人公原型纳什（J. F. Nash）了。影片中的纳什留给人的印象大概可以概括为：性格古怪、举止异常，痴迷于大脑中的抽象世界，而对身处的现实世界则漫不经心，仿佛来自虚空，不食人间烟火。

也许在许多人的心目中，纳什就是数学家的典型代表：如同世外高人一样高深莫测，甚至还可能有点神经兮兮。其实这只是一种误解，绝大多数的数学家都是正常的，即便是纳什本人，在现实生活中也是接地气的。

本书会帮你揭开数学家的神秘面纱，让你大开眼界，接触到当代的诸多大数学家，从而对数学家这个特殊群体获得更真切的认识。

两年前我从图书馆偶然借到本书的英文原版之后就爱不释手了，吸引我的不只是诸位数学家清澈深邃的目光，还有朴实的自述文字所传递出的心声，试听一听朗兰兹（R. L. Langlands）的这段独白：

> 最美妙的时光是在我只有数学相伴时：没有野心，无需伪装，忘怀天地。

这种境界乃是陶渊明“采菊东篱下，悠然见南山”的境界，这种情怀乃是“豪华落尽见真淳”（元好问对陶渊明诗的评价）的情怀。我等凡人，也许倾尽毕生心力也难以达到此等修为。

虽不能至，然心向往之。于是我想也许可以将这美妙的文字翻译成中文，分享给所有对数学和数学家感兴趣的朋友。这个想法得到了许多老师和同学的支持和鼓励，其中不乏一些知名的大数学家，更多的是数学圈外的朋友，数目之多难以一一列举。本书之所以能出版，我要特别感谢所有给过我们帮助的人，他们的汗水和智慧，成就了我翻译本书的梦想。

全书一共收入九十二位当代大数学家的照片，并辅以相应的自述文字回顾其生涯。虽然这些数学家遍布于世界各地，研究领域也各不相同，但从他们的文字中可以看出，数学家已在全球范围内形成了一个大家庭，恰如中国的一句古话所云，“四海之内皆兄弟也”。

数学家回顾生涯往往饮水思源，道出一些不寻常的人生经历。这在当初对他们而言也许只是偶然或运气，但对今天的我们却富有借鉴意义。他们的非凡经历往往发生在中小学时期——当然也有例外，例如对库恩（H. W. Kuhn）、卡茨（N. M. Katz）和张圣容（Sun-Yung Alice Chang）而言，大学的影响要更大一些。他们或是受到了家里一位热爱科学的长辈的启蒙，如如柯文（Frances Kirwan）、泰特（J. T. Tate）、魏吉森（Avi Wigderson）、托塔若（Burt Totaro）；或是在学校受到了某位优秀的数学教师的激励，如拉克斯（P. D. Lax）、格里菲斯（Phillip Griffiths）、莫哈维兹（C. S. Morawetz）、瓦拉德汉（S. R. Srinivasa Varadhan）；或是受到一些卓越的数学通俗读物的启蒙，据译者统计，最有影响力的几本读物分别是：加德纳在《科学美国人》上的数学游戏专栏、哈代的《一个数学家的辩白》、贝尔的《数学精英》。当然，还有一些人天生就流淌着数学家的血液，例如昂利•嘉当（Henri Cartan）、迈克尔•阿廷（Michael Artin）、田刚、巴尔加瓦（Manjul Bhargava）。许多数学天才都出生于具有科学或艺术背景的书香门第，如彭罗斯（Roger Penrose）、费夫曼两兄弟（Robert Fefferman 和 Michael Fefferman）、布劳德三兄弟（Andrew Browder, Felix E. Browder 和 William Browder），从小就在耳濡目染中对数学产生了兴趣；但也有一些数学家完全出身于引车卖浆之户，例如朗兰兹与库恩，他们的故事也许会令人倍受鼓舞。

纵观全书，也许最值得注意的是，数学家对数学和数学研究的看法。对数学本身，许多数学家持柏拉图的观点，认为抽象的数学观念很实在，有形有色有生命。做数学研究绝不是言之无物的纸上谈兵，而是一种需要创造力和想象力的艺术创作。数学家常常将数学研究比作一种艺术创作，音乐、绘画或写作，但究竟更接近于哪一种，不同的人有不同的看法。例如，琼斯（W. F. R. Jones）、高尔斯（W. T. Gowers）和乌伦贝克（K. K. Uhlenbeck）认为数学研究有似于谱曲的音乐创作，拉克斯、丘成桐（Shing-Tung Yau）和迈克达芙（Dusa McDuff）认为数学创造更接近于描摹自然或抽象绘画，奥昆科夫（Andrei Okounkov）和米匝哈尼（Maryam Mirzakhani）认为做数学好比作诗或写小说，张圣容、巴尔加瓦和盖尔范德（I. M. Gelfand）则将数学、音乐与诗歌三者相提并论，而维涅海（Marie-France Vigneras）则一言以蔽之：

> 我感觉我不同于——比方说——我的邻居，但与史学家、作家、诗人和画家差别不大。

不过也有例外，纳什在自述中写道：

> 与作诗不同，数学思维是一种逻辑和理性思维。

虽然他的观点看似孤立于主流之外，但你要坚信他并非在胡言乱语——真正的数学家会很在意他写的每一句话的真实性和清晰性。纳什所强调的正是数学有别于其它艺术形式的一个特点：数学注重逻辑理性。这个特点也正是数学比其它艺术形式更难理解的原因所在：理解数学的不二法门是实践，是思考数学、做数学。对一段音乐、一首诗、一幅画或一张照片，你往往在瞬间就能获得某种感觉（它也许会令你感动或忧伤）；但对一个不那么平凡的定理或公式，即便是齐天大圣孙悟空大概也无法一眼看出更多的东西。

数学家在自述中偶尔会举具体的例子来说明数学之美妙，出现频率最高的是欧几里得平面几何，特别是勾股定理，西方称之为毕达哥拉斯定理（古希腊数学家毕达哥拉斯是历史上第一位开山立派的大数学家，约与孔子同时代）。稍微想一想，这个简单的事实已经被发现了数千年之久，真理可真是寿与天齐啊！难怪证明了费马大定理的怀尔斯（A. J. Wiles）会如此概叹：

> 数学已经被人类研究了数千年。统治者代而复谢，国家兴而复亡，帝国盛而复衰。但数学从所有这些一路走过，并幸免于战争、瘟疫与饥荒。它是人类生活中少有的不变的事物之一。古希腊和中国历代的数学在当今如同在从前一样有效。数学也将会延续到未来。今天尚未解决的问题将在明天的世界里获得解答。成为这个悠久而迷人的故事里的一分子，我感到极其荣幸。

毕达哥拉斯的定理固然是无人不知无人不晓，可他本人毕竟离我们太远了，以至于事实上他至今还是一个神秘人物。相对而言，本书中的数学家要跟我们亲近得多，我们甚至可以通过互联网与他们直接取得联系。读者可以上网浏览你所感兴趣的数学家的个人主页，在那里你也许会有意外的发现和收获——数学家就在你身边。

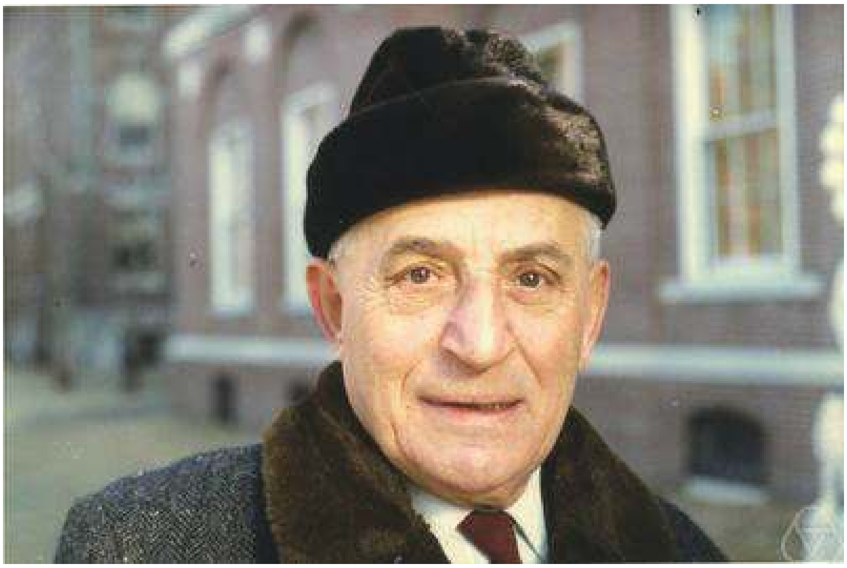
本书的翻译是合作的结晶：其他四位译者分别是首都师范大学数学院的博士研究生陈见柯——译马祖尔（Barry Mazur）篇，赵洁——译田刚篇，硕士研究生傅小虎——译瑟斯顿（W. P. Thurston）、芒德布罗（Benoit Mandelbrot）两篇，中国民航大学数学系的张雅轩老师——译梅西（W. A. Massey）、多贝西（I. C. Daubechies）两篇；三位校对分别是：北京大学数学院的博士研究生王琳、首都师范大学数学院的博士研究生张宝群与中国民航大学数学系的张雅轩老师。他们几位或是我的同学，或是我的师弟师妹，我们合作得很愉快。

当然，我们几个初出茅庐，又都是理科出身，从事文字翻译确实难以传其神而尽其妙，计较成败恐怕也是自不量力。但在数学家的灵魂深处往往有这样一种情结，要让事情趋于完美，甚至是无可挑剔的完美，就像一个无懈可击的证明那样。也许是长期受数学家熏陶的缘故，我们也有这种完美主义的倾向。所以，本书的出版并不意味着它的校对和修改同时划上句号。对于译文中的不当与可以改进之处，欢迎读者提出宝贵的意见与建议。

译者代表：林开亮
2013 年 9 月 1 日
首都师范大学图书馆

作者简介：

林开亮，湖南常德人，首都师范大学数学院博士研究生。早年死啃书本不懂交流，渐渐养成孤僻性格；后来按书追星有如渔人乍入桃花源，豁然开朗；而今见到山外青山楼外楼，武陵人欲见贤思齐。



为什么研究代数几何

——读扎里斯基的传记 *The Unreal Life of Oscar Zariski*

陈 跃

由于数学的抽象与艰深，以及与日常社会生活的严重脱节，数学家们的生活一般来说很难进入公众的视野。另一方面，也由于绝大多数数学家的生活的确是平淡无奇甚至枯燥乏味的，这些都很难成为记实和文学写作的题材。相比起其他学科来说，专门描写数学家生平与学术贡献的传记并不多。即使在仅有的这类传记中，也往往会堆砌一些与数学家真正关注的数学思想与学术生涯并无很大关系的材料，以充实相对缺乏的个人与社会生活内容。因此真正写得好的数学家传记其实是非常少见的。

由美国科学出版社在 1991 年出版的传记 *The Unreal Life of Oscar Zariski* [1] 是一本被公认为写得比较成功的数学家传记。这本书的书名本文暂且译为《不真实的人生——数学家扎里斯基传》，该书作者介绍说之所以取 Unreal Life 这个书名，是因为扎里斯基曾经说过这样一句话：几何是真实的生活（Geometry is the real life）。作为一名大数学家，扎里斯基的生活被真实地记录在了上百篇论文和几部专著中。相比之下，数学以外的日常生活就显得不那么真实或是虚幻的，这是因为在数学中，人们可以更自由充分地表达自己的个性、好奇心、乐观、骄傲、倔强、诉求以及智力上的浪漫。

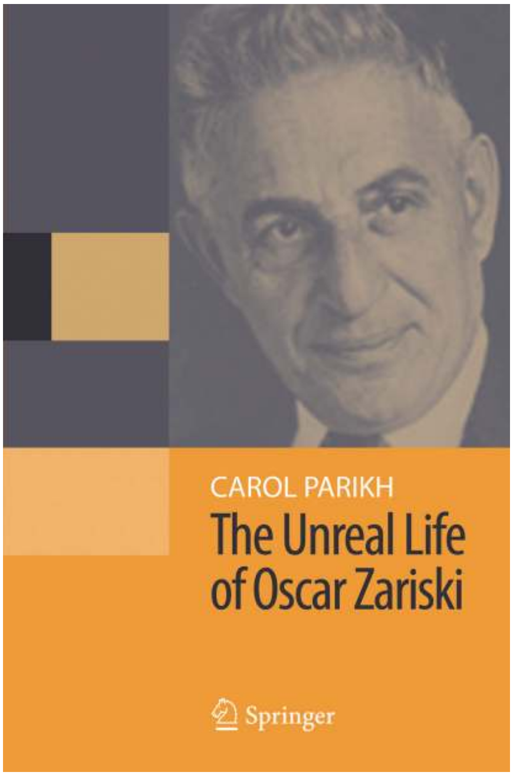
这本传记是在扎里斯基去世 5 年后推出的，内容丰富翔实，表述准确到位，生动展示了扎里斯基作为一名数学家的成长过程和研究教学的主要成就。由于颇受好评，著名的斯普林格出版社（Springer-Verlag）于 2009 年再版了这本出色的传记。目前这本书已经成为我们了解 20 世纪代数几何发展历史的重要参考文献之一。

扎里斯基（1899-1986）是 20 世纪最有影响的代数几何学家中的一个，他通过运用抽象代数的思想方法，和韦伊（André Weil）、格罗滕迪克（Alexander Grothendieck）等人一起在 20 世纪的中期重新建立了代数几何的逻辑基础，澄清了经典代数几何中的许多模糊之处，从而为 20 世纪下半叶代数几何的大发展奠定了良好的基础，为

此他在 1981 年获得了沃尔夫数学奖[2]。

在现代数学众多的分支学科中，代数几何是一门非常重要而又特别的基础学科[3]，它与数学中其他分支学科有着广泛的联系，并且被深刻地应用到理论物理及其他的科学技术中。在大多数 20 世纪现代数学重大进步（例如获得菲尔兹奖和沃尔夫奖的工作）的背后，或多或少都有代数几何的身影。扎里斯基的学生、菲尔兹奖获得者芒福德（David Mumford）曾经写过如下一段话来表达他对这门奇特学科的看法："当我开始代数几何研究生涯之时，我认为有两个吸引我的原因，首先是它研究的对象实在是非常形象和具体的射影曲线与曲面；第二是因为这是一个既小又安静的领域，其中大概只有十来个人在研究，几乎不需要新的想法。然而随着时光的推移，这个学科逐渐获得了一个看上去是诡秘、孤傲而又极端抽象的名声，它的信徒们正在秘密打算接管其他所有的数学领域！从某种程度上说，上述最后一句话是对的：代数几何是一门与大量其他数学领域有着最密切关系的学科——例如复解析几何（多复变）与微分几何、拓扑学、K– 理论、交换代数、代数群和数论——并且既能给所有这些学科以各种定理、方法和例子，同时又能够从它们那里得到同样多的定理、方法和例子。"[4]

确实很难让人相信：从研究一组多元多项式的零点集合（即代数簇）中可以引发出那么多那么重要深刻而又美好的数学理论。虽然在现代数学中也有一些学科与其他学科有比较密切的联系，但这种联系远不及代数几何与其他学科的联系。抽象代数、代数拓扑与微分拓扑、整体微分几何、数论以及分析中许多重要的理论都是因代数几何的需要而提出的，同时代数几何也将分析、拓扑、几何与数论中的许多基本概念和理论抽象提升到了更高的层次，所以说代数几何是 20 世纪数学统一化的一个主要源动力。往往在别的学科中是一般性的理论，但是到了代数几何中就变成一个特例。由于数学的发展在很大程度上依赖于各分支学科之间的交叉影响和相互作用，因此可以说代数几何对 20 世纪现代数学的大发展所起的作用最大。代数几何已经成为将现代数学各主要分支学科紧密联系在一起的中心纽带。由此我们就不难理解为什么国际数学界对于和代数几何有关的重要工作总是给予较高的评价。例如获得沃尔夫奖的陈省身与丘成桐两位大师，他们最重要的工作就与代数几何密切相关：陈（省身）示性类被深刻地推广与运用到代数几何中，而卡拉比 - 丘（成桐）流形则是当前复代数几何中最热门的研究对象之一。



The Unreal Life of Oscar Zariski，斯普林格出版社 2009 年版

代数几何最早起源于在 17 和 18 世纪牛顿和贝祖（Étienne Bézout）等人关于平面代数曲线的研究工作，例如牛顿曾经仔细研究过平面三次实代数曲线的分类。到了 19 世纪上半叶的射影几何登场后，才开始出现一些关于复代数曲线与复代数簇的初步的代数几何理论。然后黎曼在研究复变函数的阿贝尔积分理论的过程中提出了内蕴的黎曼面概念和代数函数的理论，也就是从崭新的比较抽象的拓扑与几何视角来重新研究复代数曲线，并且发现了流形的拓扑不变量——亏格（拓扑学就是从这里开始的）。在此之后，以克罗内克（Leopold Kronecker）、戴德金（J. W. Richard Dedekind）和韦伯（Heinrich Martin Weber）为代表的代数学派受代数数论的启发相继引入了理想、赋值和除子等最基本的概念，特别是戴德

金和韦伯两位已经有了用纯代数的方法来研究代数曲线的超前想法。与此同时，以诺特（Max Noether）为代表的几何学派继续从经典射影几何的角度研究复代数曲线和复代数簇，发现了平面曲线奇点解消的基本方法。

从19世纪末期开始，代数几何的发展进入了一个新的历史阶段。一些数学家试图将黎曼的复代数曲线理论推广到复代数曲面上。虽然这里的维数仅仅增加了一维，但是与代数曲线完全不同，研究代数曲面需要克服许多困难，难度极大。庞加莱为此提出了代数拓扑的同调理论，莱夫谢茨（Solomon Lefchetz）用这个同调理论研究了复代数曲面的拓扑性质。当然最主要的贡献还是来自于著名的意大利学派。这个学派的三个主要代表人物是卡斯泰尔诺沃（Guido Castelnuovo）、恩里奎斯（Federigo Enriques）和塞维里（Francesco Severi），他们在20世纪初期用天才的几何直觉和高超的几何技巧，综合运用包括分析与拓扑方法在内的各种方法创造了复代数曲面的一个非常深刻的理论。但同时他们的工作也有一个致命的缺陷，就是缺少一个统一的逻辑基础，一些证明依赖于几何直观，缺乏严密性。和数学史上常见的情形类似，这种逻辑基础不稳的状况对于视严格为生命的数学家们来说是一件特别纠结和难受的事，它严重阻碍了代数几何的进一步向前发展。

扎里斯基就是在这个历史发展的关键时刻进入到代数几何领域中来的。

扎里斯基早年的经历比较曲折。扎里斯基于1899年出生于白俄罗斯的科布林，这是一个靠近波兰边境的小城市。扎里斯基是犹太人后裔，他是7个孩子中的一个，父亲早逝，靠母亲抚养长大。由于家境不错，受到良好的教育，且从小就显露出对数学的爱好。1918年扎里斯基进入乌克兰的基辅大学后开始学习数学，偏向于代数与数论。同时他在大学里还是一名关心社会、积极宣传马克思主义的进步学生，并且在游行中受过伤。当时正处于十月革命后国内战争的动荡时期，为了更好地学习数学，在经过一番周折后，扎里斯基于1921年来到文艺复兴的发源地意大利，当年秋天进入罗马大学求学。

这时的罗马大学正是当时世界代数几何的研究中心，意大利学派的所在地。由于在经典代数几何中需要用到许多代数知识，这对喜欢代数的扎里斯基来说，很自然地被吸引到代数几何这个领域中来了。他在听卡斯泰尔诺沃的“代数几何与代数函数”课的时候，还自学了所需要的复变函数论。而在恩里奎斯的课上，他不安地发现“只有几何，只看到各种曲线和图形，非常随意，没有证明”。 至于意大利学派三位大数学家中最年轻、最有影响的塞维里的课，就更随意了，所作的断言常常分不清是定理还是猜想，或是假设。尽管如此，扎里斯基以他的天赋还是从三位老师那里学到了许多东西，以至他心存感激地称罗马大学为他的“几何乐园”。他开始关心怎样完善他的意大利老师们的代数几何成果的严格证明问题，只是此时他和他的老师们都还不了解在德国哥廷根抽象代数（特别是环论）的发展。当时的看法是也许可以用拓扑和分析的方法来改造代数几何旧有的综合证明方法，所以卡斯泰尔诺沃鼓励他学习莱夫谢茨新的拓扑方法。为此扎里斯基在罗马大学获得博士学位后，于1927年来到美国的约翰•霍普金斯大学工作，以便于和在普林斯顿的莱夫谢茨进行交往。

在美国的前几年中，扎里斯基花了很大精力做的一个工作是写作《代数曲面》[5]一书。这本于1935年问世的重要著作系统总结了意大利学派关于代数曲面的经典理论，成为了后人了解意大利学派工作的必读书籍。从这本经典著作中，我们可以发现意大利学派在代数曲面方面的工作确实达到了很高的水平：奇点解消、除子与线性系、黎曼-罗赫定理（Riemann-Roch theorem）、参模、拓扑方法、分析方法等等。不过，扎里斯基更想做的是：为缺乏严密性的经典代数几何打造一个坚实的逻辑基础，所以他在书中尽量简化各定理原来的证明过程，并在其中注入严密性，正如他在《代数曲面》的前言中所说的：“在代数几何这个领域内，（定理证明）所采用的方法的重要性决不亚于定理与结论本身。”今天再读这本书，可以看到，除了大量使用旧的经典代数几何方法之外，虽然已经开始运用在当时来说是新的拓扑与分析方法（例如同调方法），但却找不到抽象代数方法的任何踪迹。

扎里斯基在完成《代数曲面》的写作后并不十分高兴。他曾经回忆说：“我试图尽我最大的努力揭示出意大利几何学家们所采用的天才几何方法背后的深刻思想，并对整个曲面理论中最

重要的一些定理给出证明，虽然做得很成功，但是付出了一个代价。这个代价就是失去了我自己的几何乐园，在这里我曾经是那样的幸福。我开始明显地对那些经我整理的原始证明的严密性感到不安和失落（虽然没有失去对弥漫在这些证明中富有想象力的几何精神的敬意）；我逐渐相信所有这些证明都必须用纯代数的方法重新来过。”例如在《代数曲面》的第一章中，扎里斯基仔细分析了复代数曲面奇点解消定理的四种不同的证明过程，这些证明所用的方法基本都是不严格的经典代数几何方法，即便扎里斯基再怎么努力也不可能消除其中的模糊之处。而奇点解消问题在代数几何中是一个非常基本的问题，它的大意是为每个有奇点的代数曲面寻找一个和它在同一类的光滑曲面。这个问题与代数曲面的分类问题直接相关，而分类问题又是代数几何的中心研究课题。

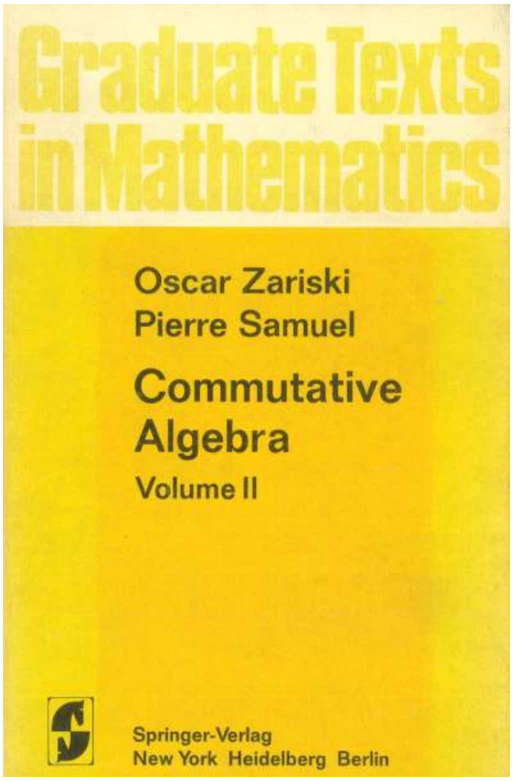
对于已经熟悉了现今用抽象代数与层论来表述代数簇性质的人们来说，当知道了 1939 年之前的代数几何基本上不用抽象代数与理想语言的时候，是有些吃惊的。这是因为用抽象代数与环的理想语言来研究代数簇实在是太确切和方便了，我们难以想象没有这种语言时的情形。例如读一下国内在前两年刚出版的范德瓦尔登（B. L. van der Waerden）在 1939 年写的《代数几何引论》中文译本[6]，就会发现如果不用现代的理想与拓扑语言时，代数簇性质的描述是非常模糊和累赘的（顺便说一下，在目前国内几乎没有代数几何初级教材的情况下，翻译出版这样一本只具有一些历史研究价值的老式教材，并将其列入必读的“数学名著译丛”丛书，容易让国内代数几何的初学者产生误解，以为现在还在用这种过时语言，因此还不如翻译一本更合时宜的引论教材[7]以应急需）。

更加让人吃惊的是，作为现代抽象代数几何鼻祖的扎里斯基，在写完《代数曲面》的时候，居然还不懂环的理想理论！他在这时候从读范德瓦尔登的《代数学》和克鲁尔（Krull）的《理想论》入手，开始自学抽象代数和环的理想理论。与我们现在常见的为学习而学习不同，扎里斯基在学习的时候有着非常明确的目的：那就是同时研究怎样用这些抽象代数的理论来重新严格地给出经典代数几何定理的证明。他尤其为克鲁尔所发现的局部环理论所震动，因为这正是研究任意域上的代数几何所需要的。此外戴德金和韦伯的用纯代数方法研究代数函数（即代数曲线）的著名文章也给扎里斯基以深深的启发。

但是“扎里斯基不久就意识到，仅仅改写证明是不够的。他必须引入不类似于他的意大利老师的几何构架的新的概念。虽然（用抽象代数重新改造代数几何的）算术化的目的是严格证明意大利学派的代数几何，从而保留其传统，但是只有引进全新的概念与方法，以此来完全取代旧的方法，这个目标才能达到。”[8]这也就是说，要想逐字逐句地运用抽象代数已有的概念和理论将经典代数几何的定理“翻译”成抽象代数的语言是远远不够的，有的时候扎里斯基必须自己重新发明新的抽象代数概念和理论才能应付研究代数簇复杂性质的需要。例如在研究改进意大利学派考虑过的代数曲面奇点解消定理证明的时候，扎里斯基就第一次成功地将环论中的整闭包与赋值环的理论运用到代数几何中，并且在戴德金等人工作的启发下还重新创造了一个新的代数概念：正规（normal）的概念（例如坐标环在其商域中整闭的代数簇称为正规簇）。在有了这些强有力的抽象代数武器后，扎里斯基就能够彻底消除原来证明中的模糊之处，于 1939 年完全严格地证明了这个重要的奇点解消定理。当然代价是改变了经典代数几何中原先比较直观简单的几何语言，代之以更加抽象和难以理解的抽象代数语言。

从此以后，扎里斯基就在代数几何的严格化与代数化这个方向上做了大量的研究工作，其影响可以从现在普遍采用的术语中反映出来：扎里斯基拓扑、扎里斯基切空间、扎里斯基主定理、扎里斯基曲面和扎里斯基空间等。扎里斯基还投入了大量精力来研究代数几何所需要的抽象代数，并且和塞缪尔（Pierre Samuel）一起写出了两大卷已经成为了抽象代数经典著作的《交换代数》[9]。就这样，扎里斯基引导着整个代数几何学科进入了一个全新的历史阶段。

与扎里斯基同时或稍后，韦依、范德瓦尔登和周炜良等人也和扎里斯基一样，在积极地推进代数几何基础的重建工作。当然对代数几何基础进行最彻底的改造还是来自于塞尔（Jean-Pierre Serre）和格罗滕迪克在 50 年代的伟大工作。人们的感觉是他们突然之间彻底重写了代数几何。其



扎里斯基与塞缪尔合著的《交换代数》

实，塞尔的层论与同调代数是整体微分几何、多复变函数、抽象代数、拓扑学得到充分发展后的产物（层论现在已经成为研究代数簇整体性质的重要工具），而格罗滕迪克是一个集大成者，他等于是综合了扎里斯基和塞尔两人的工作，即通过运用前者的交换代数和后者的层论与同调代数、以及更先进的几何与拓扑思想，将经典的代数簇理论推广成了适用面更广的概形（schemes）理论，从而将代数几何打造成了一个在很大程度上将几何、代数、数论与分析完美统一起来的逻辑推理体系。

后来的历史发展证明，当经典代数几何的逻辑基础问题被彻底解决后，代数几何便获得了急速的巨大进步[10]。这可以从扎里斯基后来在哈佛大学培养出来的一大批优秀代数几何学者的工作中得到印证，其中有两位获得了菲尔兹奖：广中平佑（Hironaka）是因为完全解决了任意维数的代数簇的奇点解消问题而在 1970 年获奖，芒福德是在 1974 年因为对参模理论的贡献而得奖。当然，代数几何在 20 世纪下半叶最辉煌的胜利应该是怀尔斯（Andrew Wiles）在 90 年代用代数几何的工具证明了数论中著名的费马大定理。这一切都充分显示了当初扎里斯基对建立代数几何基础所作的杰出贡献的重要意义和长远影响。

扎里斯基创立代数几何逻辑基础的艰难历程对于今天学习代数几何的学生也有重要的启示。如前所述，代数几何与数论、拓扑、抽象代数、多复变函数、代数群以及复微分几何等学科有着极密切的联系，只有对这些相关学科都有所涉足，才能对代数几何有比较深入的了解。实际上，“代数几何不是一门‘原创的’学科，即可以建立在一组简洁的公理或定义上的学科，它毋宁说是一门‘综合的’学科，其研究方法非常多样，不同时代、不同学派的风格千差万别，教科书也有多种模式，甚至没有大体一致的基本内容，这是与其他学科很不相同的。”[11] 在学习像代数几何这样“超级航母”般的学科时，我们尤其需要了解经典代数几何重要问题的解决过程。这是因为代数几何中许多重要的基本概念和方法都是经过了反复抽象与推广而得到的，所以它们在本质上是互相联系的。在历史上曾经引起过困惑争议因而出现较晚的理论，一般来说学生在学习的时候也会有较多的困惑与困难。应当让学生在学习较高层次的理论之前先经历较低层次的抽象过程，只有这样学生才能领悟所学知识的真正内涵。目前庞大的代数几何学科大致可以粗略地分为复代数几何[12, 13] 与现代代数几何[14-19] 两大部分：前者主要运用多复变函数论、代数拓扑学和复微分几何等学科来研究代数簇的性质（虽然这些学科已经很抽象了，但相对来讲还直观一些），而后者主要是运用交换代数和同调代数的抽象工具、以及像导出函子（Derived Functors）这样的抽象语言来进行研究，虽然难以理解和想象，但是结论精确，并且由此得到的结果适用面更广。一般的情形是：在历史上总是先有复代数几何的结果，然后在此基础上引入抽象代数的工具再进行严格化，从而可以推广到现代代数几何的高层次。因此初学者在学习代数几何的时候，应当从学习复代数几何与经典代数几何[20, 21] 开始（尽量用现代语言），这样才能更好地理解高度抽象的现代代数几何。

时代早已进入 21 世纪，与 90 年前扎里斯基来到罗马时所处的时代相比，数学的面貌已经天

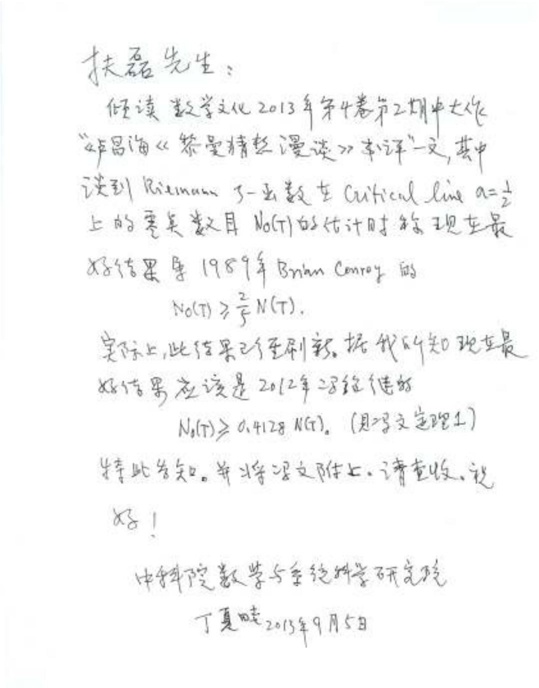
翻地覆大为改观了。现代数学真正成为了人类知识领域中最博大精深的一个，其抽象与艰深的程度登峰造极。在取得巨大进步的同时，现代数学也面临着分支学科种类繁多，研究范围越来越狭窄、概念越来越抽象等严重问题，这不免让人越来越困惑：数学研究的目标究竟是什么？一方面我们要努力使现代数学这一真正完美的人类文化遗产得到传承并发扬光大；但是另一方面应该看到：数学作为主要研究抽象逻辑结构（模式）的独特学科，与其他自然科学与社会科学学科是很不一样的，后者以大自然与人类社会作为唯一的研究对象，而在数学中，可供研究的逻辑上正确的抽象数学模式可以有任意多个，很容易迷失方向。如何避开那些意义不大的研究对象，找到真正有意义有发展前途的研究方向？对于这些难以回答的问题，我们也许可以从 20 世纪现代数学波澜壮阔的发展历史，以及像扎里斯基这样的一代数学大师的治学经历中找到一些有益的启示。

参考文献

1. C. Parikh, The Unreal Life of Oscar Zariski, Academic Press, 1991（斯普林格出版社出版社 2009 年再版）.
2. 李心灿，当代数学大师——沃尔夫数学奖得主及其建树与见解，北京航空航天大学出版社，1999.
3. 陈跃，现代数学主要分支学科的通俗介绍，数学文化，2012，第 1 期 .
4. D. Mumford, The Red Book of Varieties and Schemes, (2nd ed.,), Springer-Verlag, 1999.
5. O. Zariski, Algebraic Surfaces, (2nd ed.,), Springer-Verlag, 1971（世界图书出版公司 2010 年影印）.
6. 范德瓦尔登，代数几何引论，科学出版社，2008.
7. D. Perrin, Algebraic Geometry:An Introduction, Springer-Verlag, 2008.
8. J. J. Gray, K. H. Parshall, Episodes in the History of Modern Algebra（1800-1950）, American Mathematical Society, 2007.
9. O. Zariski, P. Samuel, Commutative Algebra, Vol . I, II, Van Nostrand, Princeton, 1958, 1960.（斯普林格出版社 1979 年重印）.
10. J. Dieudonne, History of Algebraic Geometry, Wadsworth, 1985.
11. 李克正，代数几何初步，科学出版社，2004.
12. D. Arapura, Algebraic Geometry over the Complex Numbers, Springer-Verlag, 2012.
13. P. Griffiths, J. Harris, Principles of Algebraic Geometry, Wiley, New York, 1978（世界图书出版公司 2007 年影印）.
14. A. Holme, A Royal Road to Algebraic Geometry, Springer-Verlag, 2012.
15. U. Gortz, T. Wedhorn, Algebraic Geometry I, Vieweg+Teubner Verlag, 2010.
16. S. Bosch, Algebraic Geometry and Commutative Algebra, Springer-Verlag, 2013.
17. G . Harder, Lectures on Algebraic Geometry, I, II, Vieweg, 2008, 2011 .
18. D. P. Patil, U. Storch, Introduction to Algebraic Geometry and Commutative Algebra, World Scientific , 2010.
19. R. Hartshorne, Algebraic Geometry, 1977（世界图书出版公司 1999 年影印）.
20. M. C. Beltrametti, E. Carletti, D. Gallarati, G. M. Bragadin, Lectures on Curves, Surfaces and Projective Varieties, A Classical View of Algebraic Geometry, European Mathematical Society, 2009.
21. I. R. Shafarevich, Basic Algebraic Geometry 1, Springer-Verlag, 1994（世界图书出版公司 1998 年影印）.
22. 陈跃，对话李克正教授：为什么学习代数几何，高等数学研究，2011，第 4 期 .

作者简介：

陈跃，复旦大学数学系本科毕业，上海师范大学数学系硕士，现任上海师范大学数学系副教授，主要研究代数几何的历史。


扶磊先生：
倾读《数学文化》2013年第4卷第2期中大作《卢昌海〈黎曼猜想漫谈〉书评》一文，其中谈到 Riemann ζ-函数在 Critical line σ=1/2 上的零点数目 $N_0(T)$ 的估计时称现在最好结果系1989年 Brian Conrey 的
$N_0(T) \geq \frac{2}{5}N(T)$.
实际上，此结果已经刷新。据我所知现在最好结果应该是2012年冯绍继的
$N_0(T) \geq 0.4128N(T)$.（见冯文定理1）
特此告知。并将冯文附上，请查收。祝好！
中科院数学与系统科学研究院
丁夏畦 2013年9月5日

扶磊先生：

倾读《数学文化》2013 年第 4 卷第 2 期中大作《卢昌海〈黎曼猜想漫谈〉书评》一文，其中谈到 Riemann ζ-函数在 Critical line $\sigma = 1/2$ 上的零点数目 $N_0(T)$ 的估计时称现在最好结果系 1989 年 Brain Conrey 的

$$N_0(T) \geq \frac{2}{5}N(T).$$

实际上，此结果已经刷新。据我所知，现在最好结果应该是 2012 年冯绍继的

$$N_0(T) \geq 0.4128N(T).\text{（见冯文定理 1）}$$

特此告知。并将冯文附上，请查收。

祝好！

中科院数学与系统科学研究院

丁夏畦

2013 年 9 月 5 日

Journal of Number Theory 132 (2012) 511–542

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Zeros of the Riemann zeta function on the critical line

Shaoji Feng

Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, PR China

ARTICLE INFO

Article history:
Received 7 September 2011
Accepted 26 October 2011
Available online 29 December 2011
Communicated by J. Brian Conrey

MSC:
11M26
11M06

Keywords:
Riemann zeta function
Zeros
Critical line
Mollifier

ABSTRACT

We introduce a new mollifier and apply the method of Levinson and Conrey to prove that at least 41.28% of the zeros of the Riemann zeta function are on the critical line. The method may also be used to improve other results on zeros relate to the Riemann zeta function, as well as conditional results on prime gaps.