趣味数学丛书

生动有趣的数学故事

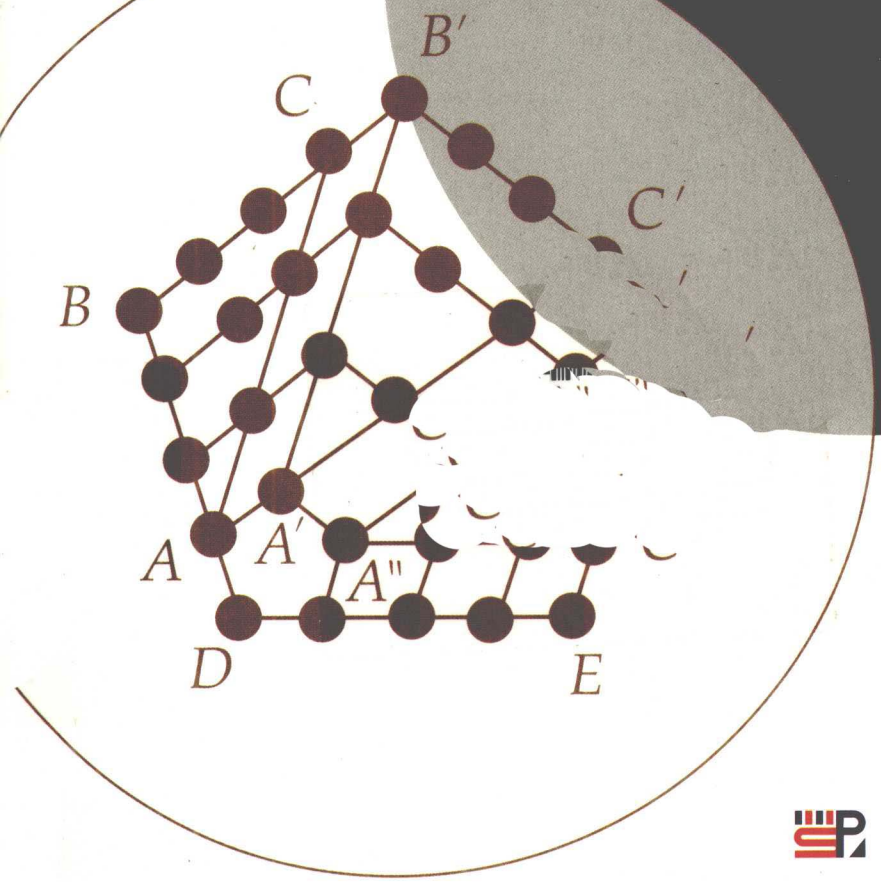
奥秘无穷的数字难题

哭笑不得的历史失误

证明推理　妙不可言

数学奇趣

徐品方　徐　伟／著

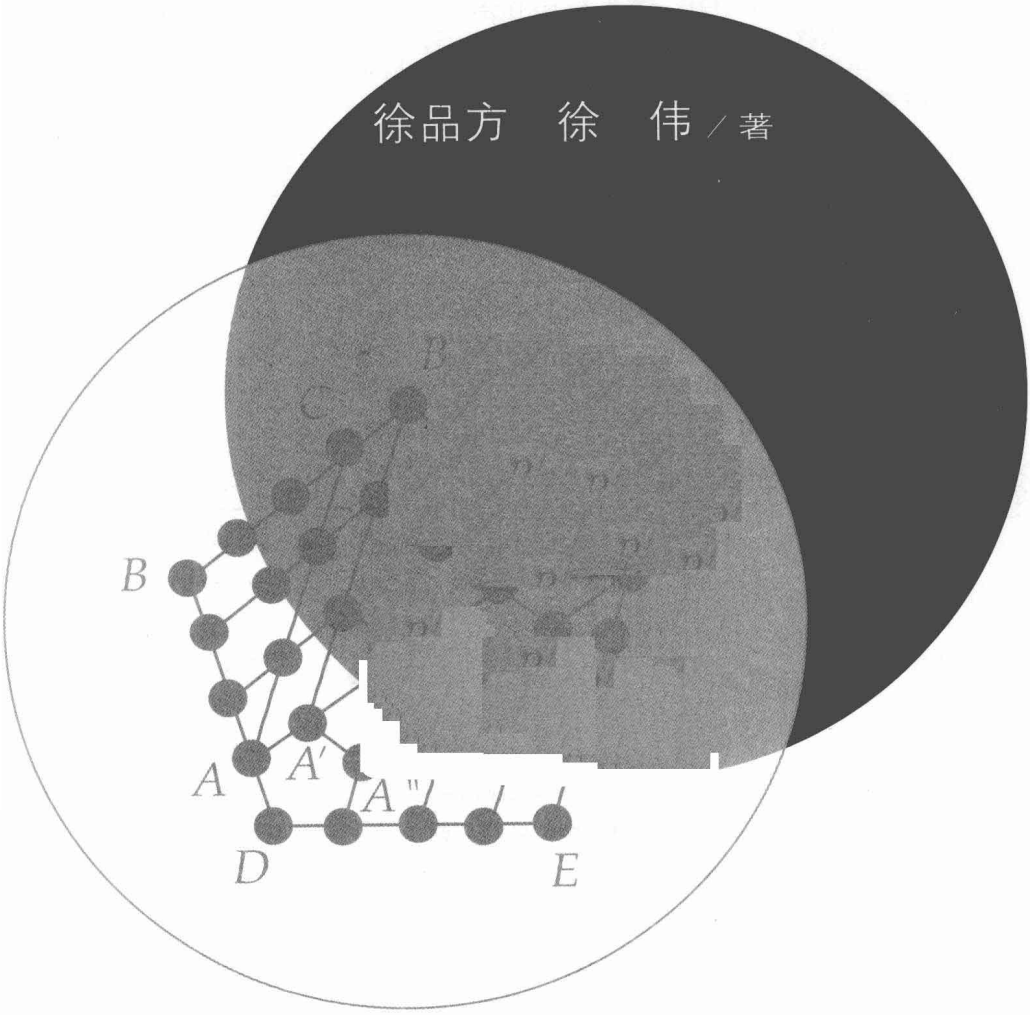


科学出版社

趣味数学丛书

数学奇趣

徐品方　徐　伟／著



科学出版社
北京

内 容 简 介

数学很奇妙，它就像是一座由数字、字母、符号和图形构成的迷宫。利用思维的力量去寻找迷宫正确道路的过程，充满着挑战，也充满着乐趣。

本书介绍了一些充满奥秘与奇趣的数学知识和数学历史故事，包括神秘而有趣的自然数、妙趣横生的墓志铭，以及数学历史上的失误等，这些内容发人深思，令人惊讶，有些还会让你会心一笑。相信本书能够激发你对数学的兴趣，锻炼你的逻辑思维能力，提升你的创新意识。

本书语言通俗易懂，集知识性与趣味性于一体，非常适合小学高年级以上文化程度的大众读者阅读。

图书在版编目(CIP)数据

数学奇趣/徐品方，徐伟著．—北京：科学出版社，2012.3

（趣味数学丛书）

ISBN 978-7-03-033464-0

Ⅰ.①数… Ⅱ.①徐… ②徐… Ⅲ.①数学-普及读物 Ⅳ.①O1-49

中国版本图书馆 CIP 数据核字（2012）第 016504 号

责任编辑：胡升华 张 凡 房 阳 /责任校对：张 林

责任印制：赵德静 /封面设计：黄华斌

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2012 年 3 月第 一 版 开本：B5（720×1000）

2012 年 3 月第一次印刷 印张：14

字数：280 000

定价：28.00 元

（如有印装质量问题，我社负责调换）

前　言

数学很奇妙，它是数字、字母、符号和图形构成的一座迷宫。不少人爱做迷宫游戏，用逻辑思维的武器，寻找走出迷宫的正确道路，一旦顺利走出迷宫，成功的愉悦令人兴奋，会使人再向新的或更复杂的迷宫挑战。这就是数学奇趣的魅力。

数学的定义、定理等，使一些人感到神秘莫测，有些人把数学设想成受冷酷无情的法则、定理统治的专制王国，认为里面充满着机械与单调。其实，数学是个充满趣味、充满生气、瑰丽多姿的大千世界，是人类思维开出的灿烂花朵，是思维高原上的一座宏伟殿堂。好玩的数学，永远向每一个人敞开迷宫的大门。

数学是人类的伊甸乐园。它虽然没有文学那样的故事情节，没有那样多愁善感、曲折动人，不像音乐那样有动听的旋律，也不像绘画艺术那样让人目眩或有着栩栩如生的缤纷色彩；但是，数学以严谨的逻辑推理、精确的计算和抽象思维而著称，它的色彩是简洁和明快的，有首诗说得更明白：

数学能令你的思维纯净，
会为你的思维增添活力，
它赋予你想象的翅膀，
为你开通推理的渠道。

历史上有些曾经被人所掌握的知识，随着时间的流逝，渐渐销声匿迹了，人们只能在故纸堆中寻觅它的踪影。然而，另外一些知识，尽管它们源于古老的年代，至今却仍然光彩夺目，焕发出旺盛的生命力。有些古老的数学好似铁树开花，成为珍稀的火花，点燃和照亮了现代的科学技术。让我们珍视古老的数学文化遗产，让它再开放出更

加绚丽鲜艳的花朵。

本书选介一些充满奥秘的数学奇趣，供你赏析，会让你过目难忘。若能撞响你思维的洪钟，激发你对数学的兴趣，提高你的创新能力，甚至有助于提高全民科学素质的话，作者也就心满意足了。

由于作者水平有限，不当之处，欢迎批评指正！

徐品方　徐　伟

初稿于2008年11月于四川西昌学院（南校区）

2011年3月修改

目　　录

1 充满奥秘的数学

数学是个万花筒，里面有许多形形色色的美丽、和谐的趣事，十分奇妙、有趣。

公元前3世纪，古希腊的阿基米德对数学十分痴迷。“仿佛他家中有一个绝色的仙女，与他形影不离，使他神魂颠倒，忘了吃，忘了喝，也忘了自己。有时，甚至在洗澡时，也用手指在炉灰上画几何图形，或者在涂满擦身油的身上画线条，他完全被神女缪斯的魅力征服。”这是近两千年前的古希腊历史学家、传记作家普鲁塔克（Plutarch，约46～约127）对阿基米德的评述（解延平等，1987）[96]。

1.1 破译密码王中王

先讲一个有趣的故事。

稻田边立着穿蓑衣的稻草人。几天过去，鸟儿便知道这是假人，大胆地饱食快成熟的稻谷，还故意站在稻草人头上鸣叫“假假假”。后来，稻田主人自己穿上蓑衣站在田边。鸟儿又像过去一样来吃谷子，吃完后站在“稻草人”头上，最终被稻田主人抓住。稻田主人大笑道：“你天天在叫假假假，今日叫你撞上真真真！”

下面要讲的密码的故事，绝不是假假假，而是真真真！

密码一般是用0～9的10个数字中的一些数字组成的秘密记号，只有自己（如银行卡密码、电脑密码等）或双方（如通信密码）知道。

密码通信在军事、政治、经济上都是必不可少的。

1. 密码的历史悠久

密码的历史悠久，我国自古有之。例如，宋朝曾将40个军用短语密码用序号1，2，…，40表示；另用一首只有40个字（没有重复字眼）的五言诗中的字一一对应。若送密码，写一普通公文，其中包含诗中对应序号的一个字眼，并在此字上加盖图章。例如，要求增兵，从密码中查“请添兵”是第14个军用短语，诗中对应的第14个字是“别”字。于是写一封信夹进“别”字，并在其上盖章。收信人一看便知是要求增兵援助了（徐品方等，2007a）[64～65]。

又传说，北宋年间，辽国奸细王钦若打入宋朝内“卧底”。辽国要送密件给

他时，为逃避路上盘查，把密件蜡丸塞入送信人切开的大腿肌肉里，待伤愈后送给王钦若。这是历史上最野蛮的传送密件的方法之一。

在国外，历史上为保卫祖国破译敌人密码的数学家也不乏其人。

16 世纪，在一次法国与西班牙的战争中，西班牙人编制了一份自认为极其安全的密码，没想到法国数学家韦达（F. Vieta，1540～1603）利用数学方法破译了这份数百字的密码，使法国军队打败了对方。西班牙国王开始还不相信他们的密码能被破译，认为法国人采用了邪术，后来得知是韦达搞的，愤怒的西班牙宗教裁判所缺席判处烧死韦达的极刑。当然，韦达远隔异国，宗教裁判所鞭长莫及，无法得逞。

第二次世界大战（1939～1945）中，英国数学家图灵（A. M. Turing，1912～1954）于 1943 年根据数学原理设计了一台叫“乌尔特拉”的密码自动破译机，又称图灵机。德国谍报部门用性能最优良的发报机发送出的各种密码，都能被图灵机自动译出，致使德军连连失败。德军统帅部直到战争结束时，还一直相信他们优良的发报系统绝对安全，认为失密是内部出了叛徒，当时还千方百计在内部捉拿“奸细”。然而，他们做梦也没有想到，密码是被年轻的数学家图灵用数学方法破译的。英国首相丘吉尔称图灵机为“英国的秘密武器”，为此，图灵荣获了帝国勋章。

无独有偶，在第二次世界大战时，美军科学家也用数学方法成功地破译了日军的密码电报，得知日本空军头目山本五十六的动向，预先设下埋伏，一举击落了山本五十六的座机，使这个日本侵略军的头目葬身孤岛。

然而有矛必有盾，随着一个个密码被破译，新的更为复杂的密码不断编制出来。

2. RSA 密码的诞生

物换星移几度秋，时间匆匆地进入 20 世纪 70 年代，一种亘古未有的密码，神奇般地降临大地，向数学家、计算机专家的智慧发出了挑战。

1978 年的一天，美国青年科学家里维斯特（Rivest）、夏米尔（Shomir）和阿德利曼（Adleman）三人相约悄悄来到纽约，共商设计令全球最难解的一种密码系统。三人中两人是数理逻辑学家，一人是计算机专家，他们凭借着超群的智慧和极其独特的设密技术，经过夜以继日的不懈努力，发明了一种长达 129 位的长码。这是一种最为先进、最为复杂的密码系统，起名为“RSA129”，取三位发明者姓名的头一个字母，后人统称 RSA 密码系统。

他们把这个发现写成文章，投寄给美国最有影响的科普杂志《科学美国人》。在文章中，他们以年轻人特有的幽默，诙谐地宣布说，谁能解出 RSA129

密码，将能获得 100 美元的奖励，因为他们拿不出更多的钱。

文章以最快的速度发表了，喜欢标新立异、寻找“奇闻”的美国读者，争读和传播这个“公开秘密”的信息。它首先在美国引起轰动，随后又很快在全球数学界和计算机界传开。许多专家学者跃跃欲试，倒不是为了那微薄的 100 美元的奖金，而是试图登上密码界的珠穆朗玛峰。但是，他们低估了 RSA 密码系统的难度，个个都以失败而告退。

科学家认为，解开 RSA129 这个有史以来最难的密码系统，并非是一种趣味游戏，它涉及数论里因数分解问题。解开它不仅在理论密码学、数理逻辑学和数论上都有重大意义，而且直接影响当代商业与军事部门所使用密码的生存与命运，因为一旦破译，许多银行、公司、政府和军事部门现行所使用的密码系统必须全部改换，才能防止保密系统泄密。

面对这个诱人的理论与应用重大课题，许多人运用各种办法去解开它。时间一年一年过去了，然而没有人成功，“竹篮打水一场空”。

这时，有人似贬实褒地“骂”道：“这三个野小子，十分厉害。”也有人说 RSA129 是一个根本不能破译的“大骗局”，是一个“圈套”。这话传到发明者之一里维斯特耳朵里，他平静地回答说：这绝不是骗局，也不是圈套，而是科学。并且告诉大家说，如果想靠个人单干的小打小闹或零敲碎打解开 RSA129 密码，那么人类至少要花 4000 年！他又暗示说，只有集中力量，进行连续的跨国联网大会战，才会有可能成功。

3. 智慧的较量

人们从失败中发现，这类 RSA 密码系统是一种与数的因数分解有关的数学方法，用它可以编、译密码。聪明的发明者正是利用数论专家目前还难以解决大数的因数分解之机，编制成了这种难以破译的密码系统。

我们知道，用现代计算机进行两个很大的数相乘是件极容易的事。例如，9 位数 193707721 和 12 位数 761838257287 相乘，用计算机只需几秒钟就可得出积数 $2^{67}-1$。但是反过来，如果不知道这两个因数，要求完成乘积（$2^{67}-1$）的因数分解，却不容易，积的位数越多，计算机所耗时间越多。有人统计，若进行两个 101 位数的积的因子分解，最快的计算机也要几十万亿年的时间。因此，求一个大数的因数分解，必须采用数学家们研究出新的计算方法，同时辅之以电子计算机工作才行。里维斯特三人正是利用了数学家目前对大数的因数分解的困难，研制了这一可以公开却又无法破译的密码。短短几年间，这一密码得到了一些国家安全部门的广泛应用。

RSA 密码系统的基本思想是：取两个充分大的素数的乘积，如果需要发送

秘密文电，只需公开告诉发电报的人这两个素数的乘积是多少，并说明如何用它进行编码，但不必告诉他这两个素数。发报人按编码进行发送秘密文电，而收报人只要对这两个很大的素因数严守秘密，任何人都无法破译，只有他本人知道这一密码电报。

RSA 密码系统的出现，一方面给一些国家安全部门带来了喜悦与通信的安全感，另一方面却给数学王国的数学家带来了极大的震动。顿时，数坛的能工巧匠惊惶不安，被誉为“数学皇后”的数论以及“计算之王”的计算机等的尊严受到了严重的损伤，数论再也不是“世外桃源”，再也不是与实践不沾边、纯之又纯的数学理论了。几千年来始终洁白如玉、一尘不染的素数的性质一下子败在了国家谍报工作人员的脚下，RSA 系统密码出奇地钻了数学家们暂时不知的大空子，给他们出了一道极富挑战性的难题。

4. 毅力是永久的享受

在挑战面前，数学家们积极投身到大因数分解的玄机妙算之中，佐治亚大学的波梅兰斯教授说：“这种密码系统是由于无知而成功的一项应用。它的产生使更多的人热衷于研究数论了。可以说，对分解因数束手无策的数学家越多，这种密码就越好。”

数学家的科学使命遭到如此重大的打击，极大地刺伤了他们的自尊心。他们迅速地向编密码专家发出了应战的誓言：“我们必须知道，我们必将知道。”为了攻克大因数分解这座崎岖曲折的数论山峰，他们熬过无数寒暑，度过无数不眠之夜，无数次坐在计算机面前进行计算、推理与沉思。他们使用运算速度越来越快的计算机，研究改进数学计算的方法，其间又创立了新的数学分支“计算数论”。短期内取得了可喜的进展，他们进行因数分解的位数迅速增大。

例如，1984 年 2 月 13 日，美国《时代》周刊介绍了美国科学家西蒙斯、戴维斯和霍尔德里奇 3 人，用 32 小时解开了 3 个世纪之久未解决的难题——69 位数的因数分解。

时间不断在改写历史的记录，突破性的奇迹接踵而来。

1986 年末，已有一些国家能在一天之内分解一个 85 位的数；1988 年，可分解 100 位长的大数；1990 年，美国数学家 J. 波拉德和 H. 兰斯拉发现了一个 155 位数的分解方法……

数学界的消息，使美国保密机构感到震惊。因为此前美国绝大多数保密体系是使用 150 位长的大数来编制密码。现在感到不安的不再是数学家，而是那些得逞一时的国家安全部门了。

5. 破译 RSA129 密码的成功

光阴荏苒，日月如梭，距 RSA 系统问世 12 年之后，数学家们在因数分解上取得了节节胜利，鼓舞着揭开 RSA129 之谜的科学家，他们开始酝酿、策划直捣令人咋舌“要花 4000 年”解决的 RSA129“大圈套、大骗局”的难题了。

科学家们终于接受发明者的“大兵团作战”的建议。他们纷纷呼吁：集中全球的“密码学精英”和大量高性能的计算机，全力以赴“跨国联网大会战”直捣黄龙。

说起来容易，做起来太难了，举行这样的“会战”，不仅需要一笔不小的资金，而且还要有一个“愿作嫁衣裳”的机构出面组织，进行协调。

美国著名的“贝尔通信公司”负责科研的“科尔公司”的决策者们高瞻远瞩，提供资金赞助并组织了这一世界性的大会战。1990 年初，五大洲 600 多位解密专家和 1600 台高性能的计算机，汇合在一起，一场空前壮观的破译“世界密码之王”的大会战的帷幕启开了。

组织者们食不甘味，寝不安席；专家学者们送走了多少个星光交辉的夜晚，迎来了多少朝霞如火的清晨，他们有序地、科学地向密码的珠穆朗玛峰攀登。具体负责的科尔公司的阿杰恩·伦斯特博士说：“计算机已经告诉我们，破译的困难程度如同要在一堆地球一样大的干草堆中找出总共 850 万枚缝衣针。”

“天机云棉用在我，剪裁妙处非刀尺。”精英们经过整整 8 个月的连续苦战终于成功了。他们破译了 RSA129 密码。用过的草稿纸记载了多少成功和失败，凝结着多少团结合作的汗水和心血啊！

估计单干要 4000 年的工作量，集体合作只花 240 天就完成了。这不是 1 天约等于 16.6 年吗？

科尔公司在纽约举行了一次别开生面的招待会，会上伦斯特博士宣布成功地破译了 10 多年前 3 位发明家设置的这个被认为永远无法破译的“密码王中王”。发明者之一里维斯特亲手将一张 100 美元的支票“奖”给科尔公司的伦斯特博士。会场顿时爆发出一片善意的笑声，接着响起经久不息的雷鸣般的掌声和欢呼声。

人们想不到才十几年，计算机发展竟如此迅速。对此，里维斯特总结说：“由此看来，在我们这个计算机飞跃发展的时代，绝对无法破译的密码是根本不存在的。”

当然，RSA 密码系统中长达 129 位数的特殊长码破译了，但对 150 位数以上的长码，还没有找到一般的方法。有人预测，照这样形势发展，破译 RSA 密