ISSN 1003-3092

数学译林

国际数学进展

MATHEMATICS

Математика

MATHEMATIK

mathématiques

2014 2

中国科学院数学与系统科学研究院
数学研究所《数学译林》编辑委员会

数学译林

第33卷 第2期

目 录

本期责任编委: 陆柱家 谌稳固
封面设计: 戴树培

János Bolyai 的真面孔

Tamás Dénes

纪念 János Bolyai (波尔约) 逝世 150 周年 [1)]

在《美国数学会通讯 (Notices of the AMS)》第 56 卷第 11 期上，我看到一篇迷人的文章："改变着的面孔 —— Legendre (勒让德) 的弄错的肖像画". 作者 Peter Duren 以可以理解的疑惑写到："这样异乎寻常的错误竟失察这么多年，似乎是难以置信的." 这鼓励我在同一份杂志上发表 —— 不失精彩 ——János Bolyai 的真面孔的故事.

在 János Bolyai 的情形，解释单词 "面孔 (face)" 的两种不同释义是理所应当的：肖像 (油画，素描) 用词 "面孔"，以及作为抽象概念的 "面孔". 本文的第 1 部分引入他的唯一肖像画的惊人的故事，该肖像画尽管被普遍接受，结果却根本不是他的. 第 2 部分探索他的智力或 "思想面孔 (mind-face)" (这是我自己构造的词)，并概述对 Bolyai 的创造性的生平和工作的新的认识.

在 Bolyai 家族的历史上，位于中欧特兰西瓦尼亚 (Transylvania) 之心脏的毛罗什瓦萨尔海伊 (Marosvásárhely) 镇占有一个重要的地位：János 一生的大部分时间在这里生活，而且他的大多数手稿保存在当地的图书馆. 读者会奇怪地发现，虽然 János Bolyai 是世界知名的杰出的匈牙利数学家，但却在罗马尼亚边境之内发现特兰西瓦尼亚 (以及毛罗什瓦萨尔海伊)[2)]. 通过特兰西瓦尼亚动荡的历史，这是可以解释的. 如果我们仅回看 19 世纪，主要居住着匈牙利人的特兰西瓦尼亚的那部分有时是自治的，有时属于匈牙利. 在二战后的 1947 年，巴黎条约把这个地区给予罗马尼亚，因此在今天的地图上是这样的.

本文的标题 "János Bolyai 的真面孔" 源于我与 Elemér Kiss 教授的交谈. 不幸的是，重病之后他在 2006 年去世，使我们合作文章的写作受挫. 这项工作旨在填补这一空白.

1. 仅有两幅 János Bolyai 画像出现过，无一存世

在匈牙利的数学史上，János Bolyai (1802 年 12 月 15 日 —1860 年 1 月 29 日) 的出现像一颗彗星.

位于特兰西瓦尼亚的毛罗什瓦萨尔海伊改革派教堂 (the Roform Church) 中 János Bolyai 的逝世记录写道："他是一位具有伟大思想的杰出数学家；绝对一流." 1823 年 11 月 3 日，他从蒂米什瓦拉 (Temesvar) 写信给他的父亲，包含后来著名的话："我从无中创造了一个新的，不同的世界."

Tamás Dénes 是匈牙利数学家和密码学家. 他的邮箱地址是 tdenest@freemail.hu.

1) 纪念 Elemér Kiss 教授 (1929—2006).—— 原注

2) 匈牙利文 Marosvásárhely 与罗马尼亚文 Târgu Mureş (特尔古穆列什) 所指是同一地方.—— 译注

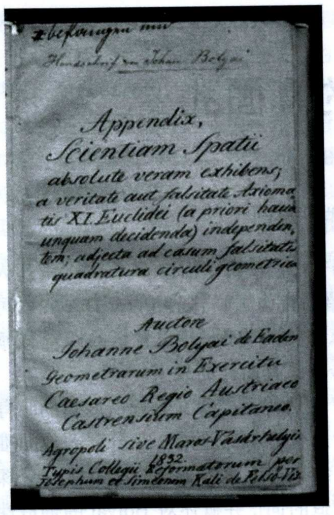


图 1　János Bolyai 的 "附录" 的标题页
来自匈牙利科学院科学图书馆

这个 "新世界" 他指的是双曲几何学的想法，概述于 1832 年，并作为 Farkas Bolyai[1)] 的著作《尝试集 (Tentamen)》的一个附录，标题是 "绝对真实的空间的科学 (Scientiam Spatii absolute veram exhibens)". 在 "附录" 的名下，这成为他最广为人知的作品.

按照 1894 年在国际数学科学文献大会上的决定，在这一著作中概述的理论被称为 "Bolyai-Lobachevsky (罗巴切夫斯基) 几何学". 在 2009 年 1 月，这个 "附录" 被加入到联合国教科文组织的《世界记忆登记册 (Memory of the World Register)》中.

János Bolyai 是 Farkas Bolyai——19 世纪匈牙利数学的关键性人物，他经常与 Gauss (高斯) 通信 —— 的儿子. 由此，同时代的艺术家既用油画又用素描使 Farkas Bolyai 和他的妻子 Zsuzsanna Árkosi Benkö 流芳百世，也许没有什么惊奇的. 所以，可以假设他们的孩子，在世时已经成名，以类似的方式名垂青史.

但是，基于同时代的资料，仅有两幅 János Bolyai 画像出现过，但无一存世. 一幅是在 1821 年 9 月 3 日 Farkas Bolyai 本人写给他的儿子的信中提到的 "维也纳画像". 根据其他资料，到 1837 年，已不能再找到这幅画了.

另一幅是当他服役当尉官时制作的. János Bolyai 本人叙述了这幅画的毁坏："因为我配不上我的父亲，我撕了这幅画，它是在军队阅兵时画的. 我不渴望其他人狂热倡导的外在的不朽."

由 Tibor Weszely[2)] 教授和 Elemér Kiss[3)] 教授最近对 Bolyai 的研究，也支持了现在不存在 János Bolyai 的真实肖像的看法.

2. János Bolyai 的肖像画，否

问题是：这张 —— 被认为是真实的 —— 肖像画怎样以 János Bolyai 之名传遍全世界？

不错，恰好 50 年前，在 János Bolyai 逝世 100 年的时候，上面带有 Bolyai 的名字的匈牙利邮票和罗马尼亚邮票发行了. 此后，这张肖像画日益在各处出现：书中，明信片上，最近也在互联网上. 今天，我们确定地知道，这张肖像画不是 János Bolyai 的.

图 2　这张肖像，不是 János Bolyai 的 (在匈牙利和罗马尼亚 1960 年的邮票上)，在世界流传

1) János Bolyai 的父亲.—— 原注

2) 在罗马尼亚特尔古穆列什的智慧大学 (Sapientia University).—— 原注

3) 他是智慧大学的数学教授，直至去世 (2006 年).—— 原注

图 3　1864 年 Mór Adler 绘的油画

图 4　Károly Lühnsdorf 基于 Mór Adler 油画的素描. 他在它上面手写的注记误导了世人，直到现在

2010 年是 János Bolyai 逝世 150 周年的纪念，所以是时候 —— 在沉寂了 50 年之后 —— 解开了这个不光彩的悬疑，把最新的 Bolyai 研究的成果公布于众. 为了做到这一点，首先我需要向读者简略介绍 Bolyai 的两个同时代人：两个匈牙利画家，和一幅在这个故事中起关键作用的油画.

Mór Adler (1826—1902) 是匈牙利油画的先驱者之一. 在魏斯恩贝格 (Weisenberger) 图画艺术学校，他是一个有某些长处的出色的学生，他从这里进入维也纳学院. 1842—1845 年之间，在维也纳学院他受教于当时知名的历史和宗教画家们. 为了研究 Zimneirmann 和 Schnorr von Carolsfeld[1] 的作品，他在 1845 年到慕尼黑旅行，为了进一步学习，他在 1846—1847 年在巴黎. 接着他在 1848 年定居佩斯 (Pest)[2]，在他事业的末期，他在这里成了艺术世界的一个受尊敬的人物. 1851 年，他参加了佩斯艺术家组织的展览，而且在接下来的 58 年，他年年参加. 他以他精细的写实风格绘制的肖像和静物油画著称.

1864 年 Mór Adler 创作了上面的大油画 (150×100 cm^2).

在这幅油画中描绘的人物的名字既没有出现在这幅画的正面或反面，也没有在任何当时的文件中被提到. 我们确切知道的一件事是，根据这幅油画，Károly Lühnsdorf (1893—1958)[3] 画了一张素描. 在这张素描的底部，他写上 János Bolyai 的名字，并伴有如下的注记：“我依据仅存的 János Bolyai 的画像绘制这幅肖像画，它是由来自欧布达 (Óbuda)[4] 的艺术家 Mór Adler (1826—1902) 在 1864 年写生绘制 ——Károly Lühnsdorf.” Károly Lühnsdorf 的原始素描现在由 Bolyai 家族拥有，但它的照片和 Mór Adler 的油画可以在 János Bolyai 数学会的墙上见到.

总结一下，考虑 Mór Adler 和 János Bolyai 两人传记上的日期以及这幅油画上是一个 20 来岁的年轻人的这一事实，我们能得出如下的结论. 如果这幅油画是 János Bolyai 的，它必定是在 1822 年前后创作的，那时 Mór Adler 还没有出生.

Lühnsdorf 说他的画 “依据 Adler 写生的原始油画” 绘制，很清楚，他假设 Adler 绘制了 Bolyai 本人的这幅画. 然而，我们从 Mór Adler 的传记的日期知道 Mór Adler 在欧洲到处旅游，直到 1848 年. 只是在这之后他定居匈牙利 —— 这时 Bolyai 已经 46 岁了.

假设这个画家不是写生而是由记忆画的，这仍是一个错误，因为在 Mór Adler 出生

1) Schnorr von Carolsfeld, 1794—1872, 与拿撒勒 (Nazarene) 运动有关的德国画家. 19 世纪初，一群旨在在基督教艺术中重振诚实和灵性的德国浪漫主义画家发起了拿撒勒运动.—— 校注

2) 布达佩斯由多瑙河西岸的布达 (Buda) 和东岸的佩斯两部分组成.—— 校注

3) 1921—1928 年他在匈牙利艺术学院学习. 他的主要兴趣是肖像画和圣经场景的绘制；他在肖像画领域获得名声. 这些画描绘了科学家，历史人物，来自宗教和公共生活中的人物.—— 原注

4) 匈牙利语中，Óbuda 意为 “老布达”.—— 校注

的 1826 年，Bolyai 已经 24 岁了. 如果他们在接近 19 世纪 40 年代末相见，那时 Adler 正开始他的艺术生涯，而 János Bolyai 已年过四旬.

因此，Mór Adler 的油画不可能是 János Bolyai 的，而且 Károly Lühnsdorf 一定是依据错误的信息写下了他的注记，由此误导了后代. 这就是这幅肖像画 —— 它 不是 János Bolyai 的肖像—— 怎样开始它的世界之旅，被数学家，学生和研究机构误认为是他的仅有的原始肖像画的.

3. János Bolyai 的真面孔

“他是创造了世界著名的某些东西的第一位匈牙利数学家 (根据 Loránd Eötvös)[1]. 不幸的是，关于这位科学巨人没有画像留存，对未来的一代一代的人，他的容貌永远隐而不见. 描述他外貌的仅有的来源是他的护照 (在他 48 岁时制作): 他体形适中，蓝眼睛，长脸.” (Elemér Kiss)

从当时的描述，我们可以了解到他的样子. 我们知道他蓄着引人注目的深棕色的胡须，头发是同一种颜色，眼睛是深蓝色的. 依据 József Koncz (毛罗什瓦萨尔海伊学院的历史学家) 所说，János Bolyai 看起来很像 György Klapka[2] 将军. 另一个重要的事实：他的儿子 Dénes Bolyai 说，自己和父亲之间存在着巨大的容貌相似.

对此我想得更远. 在毛罗什瓦萨尔海伊文化宫的正面的窗户之上，有 19 世纪 6 个智力天才的石制浮雕. 在他们的下面，是褪了色的但仍可读出的辨识每个人物的标牌.

左起的第 3 个是 Farkas Bolyai, 第 4 个是 János Bolyai. 除了 János Bolyai, 我们有其他所有人的可靠的图片. 我比较这些图片与浮雕，发现特征是容易辨认的.

然后我观看 György Klapka 和 Dénes Bolyai 的肖像画，并把它们放在来自文化宫的 János Bolyai 的肖像的旁边. 我被它们的相像所迷惑：好似它们显示的是同一个人.

毛罗什瓦萨尔海伊文化宫建于 1911 年和 1913 年之间. 那时，有知道或见过 János Bolyai 的人生活在这座城市，包括他的儿子 Dénes Bolyai. 他是一个退休法官，参加了 1911 年 6 月 7 日对他的父亲和祖父坟墓的发掘. 在石头上表现 János

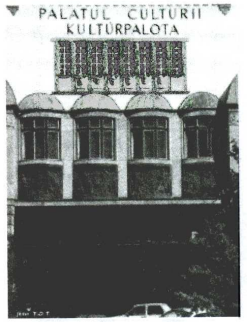


图 5　这里是位于 (罗马尼亚) 毛罗什瓦萨尔海伊文化宫正面的 János Bolyai 仅有的可靠的浮雕的照片

图 6　János Bolyai 仅有的可靠的浮雕

1) Loránd Eötvös (1848—1919) 因为他关于重力的实验工作而至今被记忆，尤其是他对引力质量和惯性质量等价 (所谓的弱等价原理) 的研究，以及他对地球表面的重力梯度的研究. Eötvös 的毛细作用定律 (弱等价原理) 被用作 Einstein (爱因斯坦) 的相对论的一个基础，而且在 Einstein 1916 年的论文 “广义相对论的基础” 中，他引用了 Eötvös 的实验. (毛细作用：推斥的毛细吸引的性质或努力 (exertion), 液体与固体接触时液体中的附着力，内聚力和表面张力的合力，引起液体表面凸起或凹陷.) Eötvös 扭秤是全球通用的大地测量学和地球物理学的一种重要仪器，用于研究地球的物理性质.—— 原注

2) György Klapka 是 1848—1849 年匈牙利自由战斗中的一位英雄将军.—— 原注

Bolyai 特征的艺术家们必定 —— 自然而然地 —— 为了他的父亲的相貌而咨询他的儿子 (Dénes Bolyai) 和他的熟人.

4. 计算机图形学的帮助

基于以上的推理，我们必须接受不存在 János Bolyai 的任何真正的肖像画. 我们已经证明 Mór Adler 的油画和 Károly Lühnsdorf 的素描不是 János Bolyai 的，而且在档案里面几乎没有可能会出现一张他本人的照片或绘画. 然而，非常重要的是，我们有他的父亲 Farkas Bolyai, 他的母亲 Zsuzsanna Benkö, 以及他的儿子 Dénes Bolyai 的可靠的肖像.

从这些数据，借助计算机图形学的帮助 (Meesort SmartMorph 软件), Róbert Oláh-Gál[1] 和 Szilárd Máté[2] 已创作了的 János Bolyai 的虚拟肖像 [20]. 这个实验的目的是在确定哪个肖像更精确上减少主观因素，肖像是 Mór Adler 在 1864 年的油画与在毛罗什瓦萨尔海伊文化宫建筑上的 János Bolyai 的半身浮雕.

经过许多实验，使用计算机上面部变换技巧，他们得出如下结论：十有八九，这些图像中仅有一个接近 János Bolyai 的真容，这就是毛罗什瓦萨尔海伊文化宫上的半身浮雕.

图 7　面孔的计算机变换：János Bolyai–Dénes Bolyai

图 8　面孔的计算机变换：Dénes Bolyai–Farkas Bolyai (孙子和祖父的相像仅能从 János Bolyai 在这两人之间的基因中介解释)

图 9　面孔的计算机变换：György Klapka–János Bolyai

经过几十年的沉寂之后，注意力应被引向这一事实：公众意识中的 János Bolyai 的面容不是他的真面容. 他的逼真肖像的唯一可靠来源是毛罗什瓦萨尔海伊的文化宫 (图 6). 作为数学史上一个有影响的大人物，在未来他应该与他的真正的面容相联系.

我高兴地向读者介绍下面两件艺术作品，它们遵循了这一思路 (图 10 和图 11).

此外，对于他的外貌的这一令人震惊的论断，能同等地用于关于他的职业活动 ("思想面孔") 的 "人所共知" 的事实.

1) 智慧大学数学与信息系，Miercurea-Ciuc, 罗马尼亚.—— 原注
2) 智慧大学数学与信息系，Miercurea-Ciuc, 罗马尼亚.—— 原注

5. 作为数学家的 János Bolyai 的真正的 "思想面孔" (基于 E. Kiss 的《来自 Bolyai 箱子中的数学珍宝》[16])

在 János Bolyai 的一生，他发表的著作仅有更以 "附录" 知名的 "绝对真实的空间科学". 这足以令他世界著名，但这也把他的智力创造约减为这篇单一的著作.

当 János Bolyai 去世时，当时的军事统治者扣押了他的所有手稿，并把它们放在箱子中运到一座城堡，以便为了军事秘密对它们做出检查. 这样他的文稿才为后人被保存了下来，手稿约有 14,000 页. 研究者面临的任务并不轻松. 手稿很少有日期，没有页码，有丢失的页，写在信封和戏院节目单上的笔记，个人癖好的数学记号，以及新发明的词语.

然而，János Bolyai 不是仅给我们留下 "附录"，而是留下了由写给他父亲的信和手稿构成的 14,000 页的一份遗产，它现在保存在毛罗什瓦萨尔海伊的 Teleki-Bolyai 图书馆的箱子里. 在这些箱子里人们能发现数学理论 —— 用 Bolyai 的词语是珍宝 —— 它们避开公众将近 100 年了. 这些纸张使我们确信，纯粹地以几何学家知名的 János Bolyai, 其实是一个全面的数学天才，他在许多数学分枝上工作，不时在冠着他人大名的重要发现上超前几十年.

Elemér Kiss 的任务是解读 (deciphering)"Bolyai 箱子" 中手稿的内容，这导致了不平凡的结果. 措辞 "解读" 描述了几十年单调乏味的行动，通过它可能重构这些材料的内容. 它的内容，语法，数学符号，与现代的显著不同，往往是难认的. 今天我们知道，这项艰苦的工作的结果留给我们 一张全新的 János Bolyai 的 "思想面孔".

Elemér Kiss 的书由 Typotex 和匈牙利科学院出版社在 1999 年以匈牙利文和英文出版，随后是 2005 年的增订第 2 版 [16].

图 10　应用 Bolyai 时代的文本和其他来源，由 Attila Zsigmond (1927—1999 年生活在毛罗什瓦萨尔海伊的画家) 用墨绘制的重构的肖像素描. 此画在毛罗什瓦萨尔海伊的 Bolyai 博物馆能见到

图 11　由 Kinga Széchenyi 为 Bolyai 诞辰 200 周年 (在 2002 年) 准备的纪念奖章，基于毛罗什瓦萨尔海伊的文化宫上的浮雕

第 1 章 "János Bolyai 的生平和空间的科学 (The life of János Bolyai and the science of space)" 给出了这位科学家创造一种新的几何学所走的旅程的一个简要叙述. 此外，在第 1 章 §6 有真正新的东西，基于 Bolyai 的通信的事实，考虑非欧几何学的发现. 对在 Bolyai-Gauss-Lobacsevszky 的关系中 Bolyai 的优先权，作者得出了一个有说服力的推理.

在第 2 章，我们能读到对 "Bolyai 箱子" 的系统的而且全面的描述. 这一章的一些部分解释了 Bolyai 在慎密的研究之后所用的语言和符号，因为一些原始的文本就好象复杂的谜语.

在第 4 章 §3 我们能读到 Bolyai 笔记的一则，他写道："我长期培育的期待和希望已

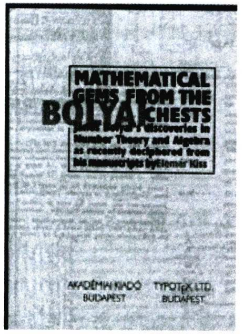


图 12　Elemér Kiss 的书揭开了 János Bolyai 的数学工作的全新面貌

经渐长且升高，即是，仅仅根据素数在它们的序列中的顺序，我能独立地或直接地找到它们 ...，换言之，给出一个仅定义素数的公式是可能的."

他找不到有理整素数的公式，直到今天其他人也找不到，但 János Bolyai 的研究把他引向一个重要的发现：他发现了第一个伪素数. [1)]

Bolyai 相信在 Fermat (费马) 小定理 [2)] 中他已经发现了素数公式. 由于他父亲的催促，他尝试证明 Fermat 小定理的逆，但是一些尝试令他信服这样的证明是不可能的，而且在一般情况下 Fermat 小定理的逆不成立. [3)] 他没有发现素数公式，但他发现了第一个伪素数. 在写给他父亲的一封信中，他告知了对最小的伪素数 (相对于 2) 341 的发现：

"...最紧迫且适当的问题. 即使 m 不是一个素数，情形 $2^{\frac{m-1}{2}} \equiv 1 \pmod{m}$ 仍是可能的 (这当然可能被即使一个例子证明，正如我偶然发现的下面的例子，但没有理论上的考虑): $2^{340} \equiv 1 \pmod{341}$ 能被 $341 = 11 \cdot 31$ 整除，这极易从 $2^{10} = 1024$ 确定，它除以 341 余 1，所以 $2^{10^{17}} = 2^{170} = 2^{\frac{341-1}{2}}$ 的余数与 $2^{341-1} \equiv 1 \pmod{341}$ 相同，因此对于 $2^{\frac{m-1}{2}}$，不仅 Fermat 定理不成立，而且这个不错的猜想也不成立 (既不在一般的情形，也不在 $a = 2$ 的特殊情形)，这是令人惋惜的，因为它们本可能为素数的辨识 (准则) 提供一个出色且非常适宜的新方法 ..."

从这封信，尤为有趣的是这一片段："但没有理论上的考虑". 这些早期的笔记能包含些什么？János Bolyai 检查了在什么条件下同余式

$$a^{pq-1} \equiv 1 \pmod{pq} \tag{1}$$

被满足，这里 p 和 q 是素数，a 是既不能被 p，也不能被 q 整除的一个整数. 他的推理如下：根据 Fermat 小定理，$a^{p-1} \equiv 1 \pmod{p}$ 且 $a^{q-1} \equiv 1 \pmod{q}$. 通过提升第 1 个同余式的两边到 $q-1$ 次幂，提升第 2 个同余式的两边到 $p-1$ 次幂，我们得到：

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p} \text{ 和 } a^{(p-1)(q-1)} \equiv 1 \pmod{q} \Rightarrow a^{(p-1)(q-1)} \equiv 1 \pmod{pq}. \tag{2}$$

其次，Bolyai 观察到，如果同余式 $a^{p+q-2} \equiv 1 \pmod{pq} = a^{p-1} \cdot a^{q-1} \equiv 1 \pmod{pq}$ 是真

1) 对许多合数 m，表达式 $a^{m-1} \equiv 1 \pmod{m}$ 成立. 自 1904 年起，伪素数的数目是无穷的为人所知 [5]. 存在合数 m 对每个 a 满足这个表达式，这里 a 与 m 互素. 为了纪念它们的发现者，这些数被称为 Carmichael (卡迈克尔) 数 [1]. 数论的最近结果之一是证明 Carmichael 数在超过所有的界之外存在 (基于杰出的匈牙利数学家 Paul Erdős (爱尔迪希) (1913—1996) 1956 年的一个想法). 1939 年，J. Chernick 证明的一个定理可以用于构造 Carmichael 数的一个子集. 数 $(6k+1)(12k+1)(18k+1)$ 是一个 Carmichael 数，如果它的 3 个因子全是素数. 在 1994 年，W. R. Alford, Andrew Granville 和 Carl Pomerance 证明确实存在无穷多个 Carmichael 数. 尤其是，他们证明对于充分大的 n，在 1 和 n 之间至少有 $n^{2/7}$ 个 Carmichael 数. 对伪素数的研究完成于 20 世纪，而且其更重要的应用领域是密码学 [7]. 在此我愿意提及 Carmichael 数有实际应用，即攻击 RSA 密码系统 [21].—— 原注

2) 这个定理说，如果 p 是一个素数且 a 是不被 p 整除的一个整数，则差 $a^{p-1} - 1$ 能被 p 整除；对此的一个常用的简短表示是：$a^{p-1} \equiv 1 \pmod{p}$.—— 原注

3) Fermat 小定理的逆是：如果 $a^{p-1} \equiv 1 \pmod{p}$ 成立，得出 p 是素数不是必然的.—— 原注

的 [1)]，然后通过把早先得到的两个表达式相乘，能得到想要的同余式 (1).

接下来的一步一定是寻找确保后一同余式成立的条件. 因为 $a^{p-1} \equiv 1 \pmod{p}$ 和 $a^{q-1} \equiv 1 \pmod{q}$，Bolyai 继续往下做，一定存在整数 h 和 k，使得 $a^{p-1} = 1 + hp$ 和 $a^{q-1} = 1 + kq$. 换言之，(1) 成立的条件是

$$hp + kq = (a^{p-1} - 1) + (a^{q-1} - 1) \equiv 0 \pmod{pq}. \tag{3}$$

如果 p 是 k 的一个因子且 q 是 h 的一个因子，则 (3) 被满足，根据 Bolyai，这意味着 $a^{pq-1} \equiv 1 \pmod{pq}$ 对使 $\frac{a^{p-1}-1}{pq}$ 和 $\frac{a^{q-1}-1}{pq}$ [2)] 是整数的素数 p 和 q 是正确的，在这种情形

$$\frac{a^{p-1}-1}{p} \quad \text{和} \quad \frac{a^{q-1}-1}{q} \text{ 也是整数.} \tag{4}$$

在 $a = 2$ 的简单情形，Bolyai 代入满足 (4) 的素数并得到 $p = 11$ 和 $q = 31$. 这就是 János Bolyai 是怎样发现最小伪素数的.

在上面引用的他的信中，尽管他强调 "即使一个例子" 就够了，但在其余的手稿中有许多反例. 他构造了更多的同余式：

$$2^{340} \equiv 1 \pmod{341}, \quad 4^{14} \equiv 1 \pmod{15}, \quad 2^{2^{32}} \equiv 1 \pmod{2^{32}+1}. \tag{5}$$

Bolyai 说，如果同余式 (1) 中 $a = 2$，则同余式

$$2^{pq-1} \equiv 1 \pmod{pq} \text{ 成立.} \tag{6}$$

这个同余式恰好相当于 James Hopwood Jeans (金斯) (1877—1940) 的定理，他的定理在 János Bolyai 去世的几十年之后，发表于 1898 年 [15]. 这就是与 Jeans 定理相关的情形. Bolyai 的除了 "附录" 之外的许多其他发现，甚至没有与他的父亲交流. 这就是 Bolyai 的一些优美的定理中的一个定理没有冠上 János Bolyai 的名字，而冠上它的再发现者的名字的原因.

Bolyai 目标是把他的方法 (6) 推广到 n 是 3 个素数之积的情形："...但它对 3 个因子的情形将更加困难." 这样的同余式由 R. D. Carmichael 在 [1], [2] 中构造. Bolyai 的尝试建议了如下的推广 Jeans 定理的想法：设 $p_1, p_2, \cdots, p_n$ 是素数，$n \geq 1$，并令 a 是一个不被这些素数中任何一个整除的整数.

$$\begin{aligned} \text{如果} \quad & a^{p_1 p_2 \cdots p_{n-1} - 1} \equiv 1 \pmod{p_n}, \\ & a^{p_1 p_2 \cdots p_{n-2} p_n - 1} \equiv 1 \pmod{p_{n-1}}, \\ & \cdots \\ & a^{p_2 p_3 \cdots p_{n-1} p_n - 1} \equiv 1 \pmod{p_1}, \\ \text{则} \quad & a^{p_1 p_2 \cdots p_n - 1} \equiv 1 \pmod{p_1 p_2 \cdots p_n}. \end{aligned} \tag{7}$$

第 4 章 §6 揭示了 János Bolyai 也被 Fermat 数 [3)] 迷住. 在写给他父亲的一封信中，有

1) 此处原文最后的同余式误为 "$a^{p-1} \cdot a^{q-1} \equiv (\text{mod } pq)$".—— 校注

2) 原文误为 "$\frac{a^{q+1}-1}{pq}$".—— 校注

3) 形为 $F_n = 2^{2^n} + 1$ 的数，这里 n 为自然数. Fermat 坚信所有这样的数是素数，即使他只计算了 $F_0 = 3$，$F_1 = 5$，$F_2 = 17$，$F_3 = 257$，$F_4 = 65637$. 他的猜想当 1732 年 Euler (欧拉) 表明下一个 Fermat 数 $F_5 = 641 \times 6700417$ 不是素数时而被反证. 到 20 世纪 80 年代早期，对所有的 $5 \leq n \leq 32$，已知 F_n 都是合数.—— 原注

两处他提及他对 Fermat 数的探讨："顺便提一下，我先前对完全数的证明以及关于 $2^{2^m}+1$ 形的数的证明是好的和漂亮的 ..."

"我打算证明形为 2^p-1 的数是素数，如果 p 是素数，同时我在对 $2^{2^m}+1$ 努力，因为正如我所写的表明，我认为对任意的素数 p, 2^p-1 总是素数 ..."[1)]

这一章代表了一种特别的价值，其中介绍了关于 Fermat 数的 Bolyai 定理. 根据这个定理 "Fermat 数总有形式 $6k-1$，所以永远不能被 3 整除." 他证明这个命题如下：

$2^{2m-1}+1=(2+1)(\ldots)$; 由此, $2^{2m-1}+1=3n$, 于是 $2^{2m-1}=3n-1$, 因此, $2^{2m}=6n-2$, 这就是，2 的偶数次幂具有形式 $6n-2$. 则 $2^{2m}+1$, 且因此 $2^{2^m}+1$ 具有形式 $6n-1$, 其中 m, $n\geq 0$ 是自然数.

这一定理的国际重要性和 Elemér Kiss 的研究的份量已被出版物 [18] 所支持，其中定理 3.12 被称为 "Bolyai 定理".

这是第一个有高度声望的来源，其中 János Bolyai 的名字在作为几何学的对立面的数论领域被提到，在揭示 János Bolyai 真的 "思想面孔" 的道路上这是一块真正的里程碑.

在第 4 章 §7, Kiss 指出, János Bolyai 能够证明 Wilson (威尔逊) 定理[2)]的逆, 但他不知道 Lagrange (拉格朗日) 较早的证明. Gauss 在《算术探究 (Disquisitione Arithmeticae)》中讨论了 Wilson 定理，但对它的逆他保持沉默. János Bolyai 从 Gauss 的这部著作中获得了大量的数论知识；这样，Bolyai 并不知道 Wilson 定理的逆的证明.

这个定理的逆对 János Bolyai 是重要的，他对各种大数的素数或合数的本性感兴趣，而且还寻找素数的公式. 他记录道："我已经证明了 Wilson 的非常美妙且重要的定理的逆." 为了读者的喜悦，我提供 Bolyai 的证明.

假设

$$(p-1)!\equiv -1 \bmod p. \tag{8}$$

令 q 是 p 的一个素因子，即 $p=q\cdot p_1$, 则

$$(p-1)!\equiv -1 \bmod q, \tag{9}$$

又根据 Wilson 定理

$$(q-1)!\equiv -1 \bmod q. \tag{10}$$

从 (9) 和 (10) 即得

$$(q-1)!\equiv (p-1)! \bmod q \Rightarrow 1\equiv \frac{(p-1)!}{(q-1)!} \bmod q. \tag{11}$$

1) 形为 2^p-1 的素数被称为 Mersenne (梅森) 素数. p 为素数, 2^p-1 不一定是素数, 如 $2^{11}-1=23\times 89$ 不是素数.—— 译注

2) 1770 年 Edward Waring (华林) (1736—1798) 宣布了他以前的学生 John Wilson (1741—1793) 的下述定理：如果 p 是素数，则 $(p-1)!\equiv -1 (\bmod\, p)$, 亦即, $(p-1)!+1$ 能被 p 整除. 这个定理由 E. Waring 发表，但他承认它首先由 J. Wilson 提出，但没有证明. 这个定理由 Joseph Louis Lagrange (1736—1813) 在 1771 年第一次证明，而且他也证明了 Wilson 定理的逆：如果 n 是 $(n-1)!+1$ 的一个因子，则 n 是素数.—— 原注

现在假设 $q<p$, 则 q 是 $(p-1)!$ 的因子，但不是 $(q-1)!$ 的因子. 因此

$$q<p\Rightarrow \frac{(p-1)!}{(q-1)!}\equiv 0 \bmod q. \tag{12}$$

同余式 (11) 和 (12) 是矛盾的；因此 $q<p$ 的假设是假的. 于是 $q=p$ 是一个素数.

从第 4 章 §8 我们能发现 János Bolyai 在小阶数幻方[1)] 的一般构建上获得的结果.

Bolyai 在包含幻方的一页纸上写下 $a=3b$ (图 13); 由此 $b=5$ 为真.

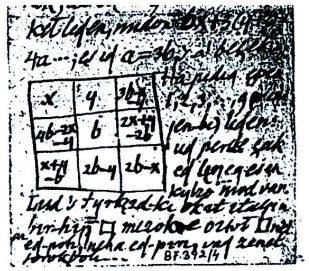


图 13 János Bolyai 的 3×3 幻方的一般作法

在这篇笔记的结尾，Bolyai 邀请读者把他的 3×3 幻方推广到 $n\times n$ 幻方："找出构造一般性 □[2)] 的方法，将一个 □ 分成任意数目的相等的 □, 不管是算术级数，几何级数还是调和级数 ..." 我想补充的是，Bolyai 的想法被 Cayley (凯莱) [3] 和 Chernick [4] 重新发现，并且幻方的一般构建可在一部百科全书般的书中找到 [6].

图 14 János Bolyai 的 3×3 幻方的具体解

第 5 章论述前所未见的 Bolyai 工作的一些结果：关于复整数[3)], Bolyai 投入了巨大的精力对它进行研究. 这些研究处理复整数的算术，Bolyai 称其为 "素数理论" 或 "虚数理论".

Gauss [12], [13] 发现并发展了复整数的可除性理论. 他证明了与数论的基本定理对应的局限于 Gauss 整数的定理，并讨论了涉及复数的同余. 在差不多相同的时间，János Bolyai 独立于 Gauss 详述了复整数的算术.

可以准确地确定 Bolyai 开始研究复数的日期，因为在给他父亲的信中，他明确地指出了这一日期："我在虚量的合适的位置寻找它们的理论，并且在 1831 年幸运地发现了这一理论." 根据他的陈述可以断言，在 19 世纪 30 年代的开端，这甚至早于 "附录" 的出版，János Bolyai 清楚地理解他自己的理论.

在他的手稿中可以释读他清楚地辨别复整数环中的素数. 他断言复素数是如下之一

$$\text{数 } 1+i,\ 1-i,\ -1+i,\ -1-i, \tag{13}$$

$$\text{形为 } 4m+3 \text{ 的有理素数}, \tag{14}$$

$$\text{形为 } 4m+1 \text{ 的有理素数的复因子}. \tag{15}$$

1) n 阶幻方是 n^2 个数，通常是不同的整数，在正方形中的一个排列，使得所有行，所有列，以及两个对角线上的 n 个数的和等于相同的常数. 一个正规的幻方包含从 1 到 n^2 的整数. 在每个行，列，以及对角线的和被称为幻常数或幻和. 一个正规的幻方的幻常数仅与 n 有关，而且具有值 $a=n(n^2+1)/2$.—— 原注

2) 这是 Bolyai 的纸页上的原始符号 (见图 13).—— 原注

3) 复整数或 Gauss 整数是其实部和虚部皆为整数的复数. 形式上, Gauss 整数是集 $Z[i]=\{a+bi|a,b\in Z\}$, $i=\sqrt{-1}$.—— 原注

Bolyai 仅把 (13) 中的数作为 "完全素数 (*perfect primes*)", 并注意到 $2=(1+i)(1-i)$, 但他明确指出 $1+i$ 不能写成两个复整数之积.

关于 (14) 中的数, Bolyai 提出它们是 "绝对素数 (*absolute primes*)" 的多种证明. 他的一个证明是: "如果素数 p 是形为 $4m+3$ 的, 则 $p=t^2+u^2$ 是不可能的, 因为, 如果 t 和 u 同时是偶数或奇数, 它们的平方和将产生一个偶数, 而这样的一个数不是素数. 如果 t 和 u 中的一个是偶数而另一个是奇数, 则它们的平方和是形为 $4m+1$ 的一个数. 于是 p 是一个绝对素数."

Bolyai 证明了, 只要 $p=m^2+n^2$ 是一个素数, 则复整数 $m+ni$ 没有异于它的相伴数的其他因子. 他把 (15) 中数的这一性质联系到 Fermat 圣诞定理 [1], 他写道: "形为 $4m+1$ 的每个素数是两个虚素数之积, 因为所有这样的数是两个完全平方之和." 例如: $13=(2+3i)(2-3i)$.

János Bolyai 还讨论了复整数的唯一分解, 他证明了如下的定理: "形为 $a+bi$ 的每个数能唯一地 (到诸因子的顺序) 分解为有限多的素数的一个乘积."

他不仅详述了复数的理论, 而且也做出了一些很重要的应用. 在许多数论定理的证明中, 他很技巧地应用他关于复整数的结论.

第 6 章 "代数方程论 (The theory of algebraic equations)" 揭示了在 5 次和更高次的代数方程的不可解性上 Bolyai 所作的奋斗. 他的未发表的藏品包含许多有关这个主题的笔记. 在这一章的结尾, Elemér Kiss 总结道: "János Bolyai 对这个重要的问题思考了很长时间, 不知道它在以前已被解决."

这就是 Bolyai 与代数方程论之间的联系尤其令人感兴趣的原因. János Bolyai 经常提到 Andreas von Ettingshausen (埃汀萧森) (1796—1878) 著的两卷本的《高等数学讲义 (Vorlesungen über höhere Mathematik)》, 该书于 1827 年在维也纳出版 [11]. 在这部著作中, 作者专用一个整章于解高于 4 次的代数方程的不可能性, 并引用了 Paolo Ruffini (鲁菲尼) (1765—1822) 1799 年的证明 [2][22], [23]. Bolyai 引用 Joseph Louis Lagrange 的书 [19], 它致力于为何用于解次数等于或小于 4 的方程的方法不能用于更高次的方程这一根本问题. [3] 关于 Bolyai 的阅读, 他写道: "...对 5 次或更高次数给出这种不可能性的一个证明: 由 Ruffini 给出的证明 (正如实至名归的 Ettingshausen 所写) 足够机智, 但有许多错误, 一言以蔽之, 仅在他的幻想之中."

这导致他作出这个定理无效的结论, 随后他开始以很大的热情寻找高于 4 次方程的解法, 他在 1844 年写道: "通过反驳 (Ruffini 的) 不可能性的证明 ...以一个新的方式它

1) 奇素数 p 能写成两个整数的平方和, 当且仅当 $p\equiv 1\,(\mathrm{mod}\ 4)$. 这一定理是 Fermat 在 1640 年 12 月 25 日致 Marin Mersenne 的一封信中宣布的, 故有时也称为 Fermat 圣诞定理.—— 译注
无独有偶, 两个相关的结果也是 Fermat 在另一个 12 月 25 日 (1654 年, 致 Blaise Pascal (帕斯卡)) 的信中宣布的: (a) 奇素数 $p=m^2+2n^2$, $m,n\in\mathbb{Z}$, 当且仅当 $p\equiv 1$ 或 $p\equiv 3\,(\mathrm{mod}\,8)$. (b) 奇素数 $p=m^2+3n^2$, $m,n\in\mathbb{Z}$, 当且仅当 $p\equiv 1\,(\mathrm{mod}\,3)$.—— 校注

2) Niels Henrik Abel (阿贝尔) (1802—1829) 1826 年的文章不可能包含在 1827 年发表的这部著作中. Abel-Ruffini 定理说, 对 5 次或更高次的多项式方程, 不存在用根式的一般解.—— 原注

3) 这一观察不仅推动 Ruffini 和 Abel 在这个方向上继续研究, 而且也导致 Galois (伽罗瓦) 群论的概念.—— 原注

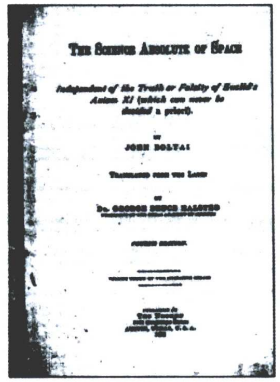
被 eo ipso (自明地) 证明."

János Bolyai 对这个重要的问题思考了很长时间, 不知道它在以前已被解决. 另一方面, 世界不知道这个 19 世纪的匈牙利科学家, 他 (也许迟了, 而且仅为了自身的原因) 已经使一个长达几个世纪的争论画上句号.

上面的事实提示, 孤立的 Bolyai 终其一生以他的巨大的创造力工作, 通过这种创造力他能 "从无中创造一个新的, 不同的世界", 并不限于几何学领域.

6. 致谢

在 150 年的沉寂之后, 在揭示 János Bolyai 的真面孔上, 很难高估 Elemér Kiss 的这部著作的价值. 使它更为有意义的是, 到目前为止 János Bolyai 的面容是未知的, 因为在全世界流传的那幅著名的画像无疑不是他的. 为了结束这一误解, 而且也为了在相关领域宣传有关文章和研究, 我们在 http://www.titoktan.hu/Bolyai_a.htm 创建了 "János Bolyai 的真面孔 (The Real Face of János Bolyai)".


THE SCIENCE ABSOLUTE OF SPACE

JOHN BOLYAI

美国数学家 George Bruce Halsted (1853—1922) 在 1896 年把 János Bolyai 的 "附录" 译成英文

在这方面, 必须记住美国数学家 George Bruce Halsted (霍尔斯特德, 1853—1922)—— 在任何其他的 Bolyai 研究者之前 —— 访问了毛罗什瓦萨尔海伊并翻译了 János Bolyai 的主要著作 "附录" [14]. 由于他的活动, 对国际上认识两个 Bolyai 他有显著的贡献.

我衷心感谢审稿人支持本文的发表, 因为这继承了由 G. B. Halsted 开始的传统. 通过这样做, 对于向世界介绍 János Bolyai 的真面孔, 他们做出了重要贡献.

没有与 Elemér Kiss 教授的私下讨论, 没有 András Prékopa 教授所写的说明, 以及没有 Róbert Oláh-Gál 在面容模拟上的支持, 本文无从写就.

我愿意对 János Bolyai 数学会会长 Ildikó Rákóczi 表示特别的感谢, 因为他使拍摄和发表对于这个项目有关键重要性的照片成为可能.

我也感谢我的女儿 Eszter 和 Damien Bove, 她们在本文的语言方面提供了帮助.

参考文献

[1] R. D. Carmichael, Note on a new number theory function, Amer. Math. Soc. Bull. 16 (1910), 232–238.

[2] ——, On composite numbers P which satisfy the Fermat congruence $a^{p-1}\equiv 1(\mathrm{mod}\ p)$, Amer. Math. Monthly 19 (1912), 22–27.

[3] A. Cayley, The Collected Mathematical Papers of Arthur Cayley (1889), vol. X. p. 38.

[4] J. Chernick, Solution of the general magic square, Amer. Math. Monthly 4 (1938), 172–175.

[5] M. Cipolla, Sui numeri compositi P, che verificano la congruenza di Fermat $a^{p-1}\equiv 1(\mathrm{mod}\ p)$, Annali di Matematica 9 (1904), 139–160.

[6] J. Dénes and A. D. Keedwell, Latin Squares and their Applications, Academic Press, New York, Akadémiai Kiadó Bp., English Universities Press, London, 1974.
[7] T. Dénes, The great career of the "small Fermat theorem" in encryption of information, Híradátechnika, Budapest, 2002/2. p. 59–62.
[8] ——, Complementary prime-sieve, Pure Mathematics and Applications 12 (2002), no. 2, p. 197–207.
[9] ——, Bolyai's treasure-chest (about the book of Elemér Kiss), Magyar Tudomány, 2006/5, 634–636.
[10] P. Erdös, On the converse of Fermat's theorem, Amer. Math. Monthly 56 (1949), 623–624.
[11] Andreas von Ettingshausen, Vorlesungen über die höhere Mathematik, Wiesbaden: LTR-Verlag, Neudr., 1827.
[12] C. F. Gauss, Theoria residuorum biquadraticorum, Commentatio secunda, Göttingische gelehrte Anzeigen, Göttingen 1831, Stück 64, 625–638.
[13] ——, Theoria residuorum biquadraticorum, Commentatio secunda, Commentationes Societatis Regiae Scientiarum Göttingensis Recentiores, Vol. VII. (1832), Göttingen, cl. math. 89–148.
[14] G. B. Halsted, The Science Absolute of Space (translated from the original Latin), The Neomon, Austin, Texas, USA, 1891.
[15] J. H. Jeans, The converse of Fermat's theorem, Messenger of Mathematics 27 (1897–1898), 174.
[16] E. Kiss, Mathematical Gems from the Bolyai Chests, Akadémiai Kiadó Budapest, Typotex LTD., Budapest, 1999.
[17] ——, On a congruence by János Bolyai connected with pseudoprimes, Mathematica Pannonia, 2004/2.
[18] Krizek-Luca-Somer, 17 Lectures on Fermat Numbers, Springer, 2004.
[19] J. L. Lagrange, Réflexions sur la Résolution Algébrique des Équations, Paris, 1770.
[20] R. OlÁH-GÁ and Sz. MÁTÉ Virtual portrait of János Bolyai, 6th International Conference on Applied Informatics, Eger, Hungary, January 27–31, 2004.
[21] R. G. E. Pinch, On using Carmichael numbers for public key encryption systems, Proceedings 6th IMA Conference on Coding and Cryptography, Cirencester 1997, (ed. M. Darnell), Springer Lecture Notes in Computer Science 1355 (1997) 265–269.
[22] Paolo Ruffini, Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al 4°, 2 vols., Bologna, 1798.
[23] ——, Della soluzione delle equazioni alg. determinate particolari di grado sup. al 4°, in: Mem. Soc. Ital., IX, 1802.

(赵振江 译 陆柱家 校)

****

(上接 191 页)

[3] T. H. Heath, The Words of Archimedes with the Method of Archimedes, Dover Publications, New York, 1987.
[4] D. J. Struik, ed., A Source Book in Mathematics, 1200–1800, Harvard University Press, Cambridge, 1969.
[5] I. Vardi, What is ancient mathematics? Math. Itelligencer 21 (3) (1999) 38–47.

(姜玲玉 译 陆柱家 校)

《数学译林》征订启事

由中国科学院数学与系统科学研究院数学研究所主办的以译文为主的数学刊物《数学译林》是综合性数学刊物，目的是介绍国内外数学的进展，普及现代数学知识，促进我国数学事业的发展和水平的提高. 选题内容有综合报告、专题介绍、数学史、数学小品、人物传记、数学教育以及其他等方面. 《数学译林》自 1980 年试刊以来受到广大读者的欢迎与支持.

《数学译林》每年出版一卷，每卷四期，每逢三、六、九、十二月下旬出版，国内外公开发行. 由于各项费用的上涨，原有的经费已经入不敷出. 因此，2012 年起订价改为 100.00 元 (包括国内邮费，但不含港澳台); 港澳台读者需付邮费，因此全年订价 160 元. 欲订者请直接向本刊编辑部订购，邮局汇款或银行汇款均可 (个人订阅亦可向下述银行帐号汇款).

邮局汇款地点：北京海淀区中关村东路 55 号中国科学院数学与系统科学研究院;

收款人：数学译林编辑部; 邮政编码：100190.

通过银行汇款的请注意下述信息.

开户名：中国科学院数学研究所数学译林编辑部;

开户银行：中国工商银行北京市分行海淀西区支行;

帐号：02000045090891460-90.

来函请注明寄杂志的详细地址、邮政编码和收刊人.

本编辑部尚有少量已出版的过期刊物存书，欲购者请从速.

数 学 译 林

(季 刊 1982 年创刊)
2014 年 第 33 卷 第 2 期

主管单位 中国科学院
主办单位 中国科学院数学与系统科学研究院
主 编 尚 在 久
编辑出版 《数学译林》编辑委员会
印刷装订 北京大地印刷厂

发行订购 北京中科院数学所数学译林编辑部
地 址 100190 北京中关村东路 55 号
电子信箱 yilin@math.ac.cn
出版日期 2014 年 6 月
印 数 1200 册

国内外公开发行 国内统一刊号：CN 11-2418/O1

成本价：25.00 元

ISSN 1003-3092