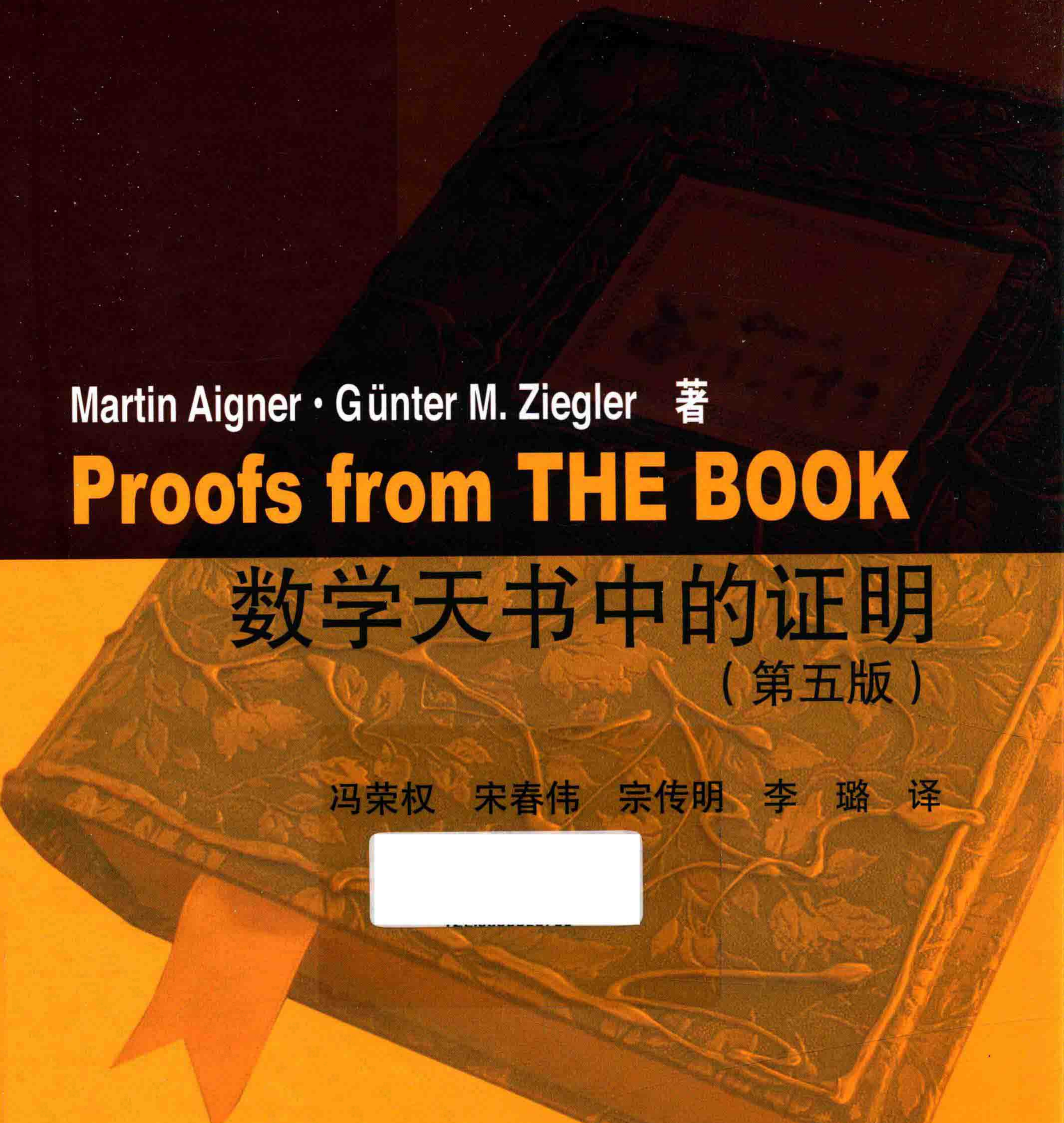
Martin Aigner · Günter M. Ziegler 著

Proofs from THE BOOK

数学天书中的证明

（第五版）

冯荣权　宋春伟　宗传明　李　璐　译



高等教育出版社

Martin Aigner
Günter M. Ziegler 著

Proofs from THE BOOK

数学天书中的证明
(第五版)

SHUXUE TIANSHU ZHONG DE ZHENGMING

含 Karl H. Hofmann 提供的插图

冯荣权　宋春伟　宗传明　李　璐　译

高等教育出版社·北京

图字：01–2015–3393 号

图书在版编目（CIP）数据

数学天书中的证明：第5版／（德）艾格纳（Aigner, M.），（德）齐格勒（Ziegler, G. M.）著；冯荣权等译. -- 北京：高等教育出版社，2016.3

书名原文：Proofs from THE BOOK

ISBN 978-7-04-044409-4

Ⅰ. ①数… Ⅱ. ①艾… ②齐… ③冯… Ⅲ. ①数学－普及读物 Ⅳ. ①O1-49

中国版本图书馆 CIP 数据核字（2015）第 297889 号

策划编辑 王丽萍　　责任编辑 李　鹏　　封面设计 张　楠　　版式设计 马敬茹
责任校对 刘娟娟　　责任印制 尤　静

出版发行	高等教育出版社	网　　址	http://www.hep.edu.cn
社　　址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印　　刷	北京佳信达欣艺术印刷有限公司		http://www.hepmall.com
开　　本	850mm × 1168mm　1/16		http://www.hepmall.cn
印　　张	22.5		
字　　数	370 千字	版　　次	2016年3月第1版
购书热线	010-58581118	印　　次	2016年3月第1次印刷
咨询电话	400-810-0598	定　　价	59.00 元

物 料 号　44409-00

第五版译者序

《数学天书中的证明》第三版和第四版的中译本面世以来, 受到读者的广泛欢迎, 目前两个版本都几近售罄. 2014 年, Springer 出版社出版了本书英文版的第五版, 此次中译本也随之同步更新, 以飨读者.

第五版与第四版相比, 主要增加了四章内容, 包括 "谱定理和 Hadamard 判别式问题" (第 7 章) 、"Borromeo 链环不存在" (第 15 章)、"有限 Kakeya 问题" (第 34 章)、"积和式与熵的威力" (第 37 章); 此外, 原作者还更新、增补了 "素数无限"、"代数基本定理的引理" 等一些定理的新证明, 并对部分章节的内容进行了修订.

李璐博士承担了第五版中译本相关内容的补译和修订工作, 我们在此表示衷心的感谢!

宗传明

北京大学, 2015 年 10 月

第四版序言

我们在近 15 年前开始这项工作的时候, 实在难以想象我们的天书将会获得那样一种不可思议的和持久的反响. 我们收到了热情的来信、有趣的评论, 还推出新版, 至今已有 13 种外文译本. 毫不夸张地说, 它已经成为我们生命的一部分了.

除了诸多改进 (部分来源于读者建议), 现有的第四版新添了五章: 两章经典, 分别是二次互反律和代数基本定理; 两章关于拼装问题以及它们奇妙的解法; 还有一章是关于图论里 Kneser 图的色数.

感谢这些年来帮助和鼓励我们的所有人: 其中在第二版时帮助我们的人包括 Stephan Brandt, Christian Elsholtz, Jürgen Elstrodt, Daniel Grieser, Roger Heath-Brown, Lee L. Keener, Christian Lebœuf, Hanfried Lenz, Nicolas Puech, John Scholes, Bernulf Weißbach, 还有很多其他人. 第三版特别感谢以下诸位的投入: David Bevan, Anders Björner, Dietrich Braess, John Cosgrave, Hubert Kalf, Günter Pickert, Alistair Sinclair 和 Herb Wilf. 现在这一版则特别感谢以下各位的贡献: France Dacar, Oliver Deiser, Anton Dochtermann, Michael Harbeck, Stefan Hougardy, Hendrik W. Lenstra, Günter Rote, Moritz Schmitt 和 Carsten Schultz. 此外, 我们感谢 Springer 出版社海德堡的 Ruth Allewelt 以及柏林的 Christoph Eyrich, Torsten Heldmann 和 Elke Pose, 谢谢他们这些年来的帮助和支持. 最后, 假如没有 Karl-Friedrich Koch 的建议, 以及 Karl H. Hofmann 为每一版提供的精彩插图, 这部书绝不会如此赏心悦目.

Martin Aigner, Günter M. Ziegler

柏林, 2009 年 7 月

第三版序言

准备这本书的第一版时, 我们绝没想到出版后会有如此的成功. 自出版以来, 这本书已被翻译成许多种语言出版. 这期间我们收到了许多读者的热情来信, 其中有许多非常好的关于修改和增加新内容的建议 —— 这使我们忙了好几年.

第三版增加了两章 (分别为 Euler 的分拆恒等式和洗牌), 关于 Euler 系列的三个证明成了独立的一章. 当然, 还有许多其他改进, 如 Calkinwilf-Newman 关于 “有理计数” 的处理. 目前也就是这些.

我们对过去 5 年中支持这一项目的每个人, 和对新版做出贡献的每个人表示衷心的感谢. 他们包括 David Bevan, Anders Björner, Dietrich Braess, John Cosgrave, Hubert Kalf, Günter Pickert, Alistair Sinclair 和 Herb Wilf.

Martin Aigner, Günter M. Ziegler

柏林, 2003 年 7 月

第二版序言

本书的第一版受到了读者广泛的欢迎. 我们也收到了许多读者来信, 其中有的给出中肯的评论, 有的指出一些错误和缺陷, 有的则对另外的证明和新的讨论题目提出了很好的建议 (显然, 当我们希望展现完美证明时, 我们的表述并不完美).

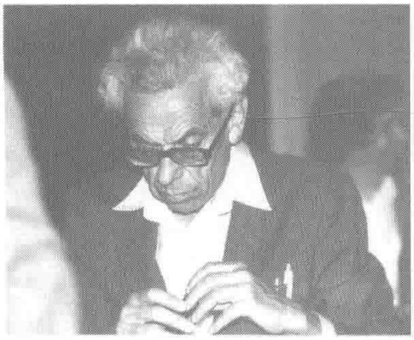
本书的再版给我们提供了改善的机会: 新版增加了三章, 并对有的章节做了实质性的修改和给出新的证明, 同时还有一些小的改动. 这些改进不少是基于读者的建议. 另外, 我们删掉了第一版中关于 “十三球问题” 的一章, 因为该问题的完整证明需要很多细节, 很难做到简洁优美.

在此我们非常感谢那些来信的读者, 他们的来信对我们很有帮助, 他们中有 Stephan Brandt, Christian Elsholtz, Jürgen Elstrodt, Daniel Grieser, Roger Heath-Brown, Lee L. Keener, Christian Lebœuf, Hanfried Lenz, Nicolas Puech, John Scholes, Bernulf Weißbach 以及许多其他读者. 同样, 我们再次对 Springer 海德堡的 Ruth Allewelt 和 Karl-Friedrich Koch 以及柏林的 Christoph Eyrich 和 Torsten Heldmann 提供的帮助和支持表示衷心的感谢. Karl H. Hofmann 提供了一些高质量的新插图, 在此一并致谢.

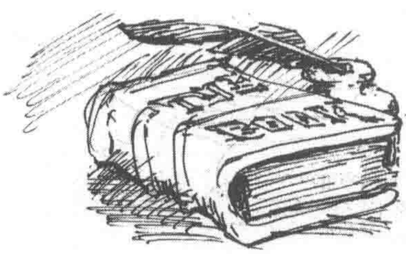
Martin Aigner, Günter M. Ziegler

柏林, 2000 年 9 月

第一版序言



Paul Erdős



"The Book"

Paul Erdős 喜欢谈论数学天书 (The Book), 上帝在其中保存着数学定理的完美证明. 这是根据 G. H. Hardy 的说法: 丑的数学是不会有永久地位的. Paul Erdős 也讲过, 作为数学家, 你可以不相信上帝, 但你应该相信数学天书. 几年前, 我们建议他勾画一下数学天书的轮廓. 他立即动手, 充满热情地一页一页提了很多建议. 本书原计划作为 Paul Erdős 的 85 岁生日献礼于 1998 年 3 月出版. 由于他于 1996 年夏天不幸去世, 他没有被列为我们的合作者. 而本书却是作为对他的纪念.

我们没有数学天书中的证明的定义或标准. 这里我们所呈现给大家的是一些具有高超的思想、聪明的观察和出色的洞察力的例子. 但愿读者与我们一样对它们富有热情并喜欢它们, 尽管我们的表述并不完美. 本书内容的选取, 在很大程度上受到 Paul Erdős 的影响. 其中许多章节是他建议的, 许多证明是他给出的或者源于他富有洞察力的问题或猜想. 所以, 这本书很大程度上反映了 Paul Erdős 关于什么是数学天书中的证明的观点.

限制我们选题的一个因素是可读性: 本书中的所有章节应该能被具有大学数学水平的读者所理解. 一点线性代数、数学分析和数论以及一些离散数学的初等概念和思维方式就足够理解和欣赏本书的全部内容.

我们对那些为本书的出版提供过帮助和支持的人表示衷心的感谢 (其中包括初稿讨论班上的学生): Benno Artmann, Stephan Brandt, Stefan Felsner, Eli Goodman, Torsten Heldmann 和 Hans Mielke. 此外, Margrit Barrett, Christian Bressler, Ewgenij Gawrilow, Michael Joswig, Elke Pose 和 Jörg Rambau 对本书的出版提供了技术支持, Tom Trotter 通读了初稿, Karl H. Hofmann 提供了一些优美的插图, 在此一并致谢. 当然, 我们要特别感谢已故的伟人 Paul Erdős 本人.

Martin Aigner, Günter M. Ziegler

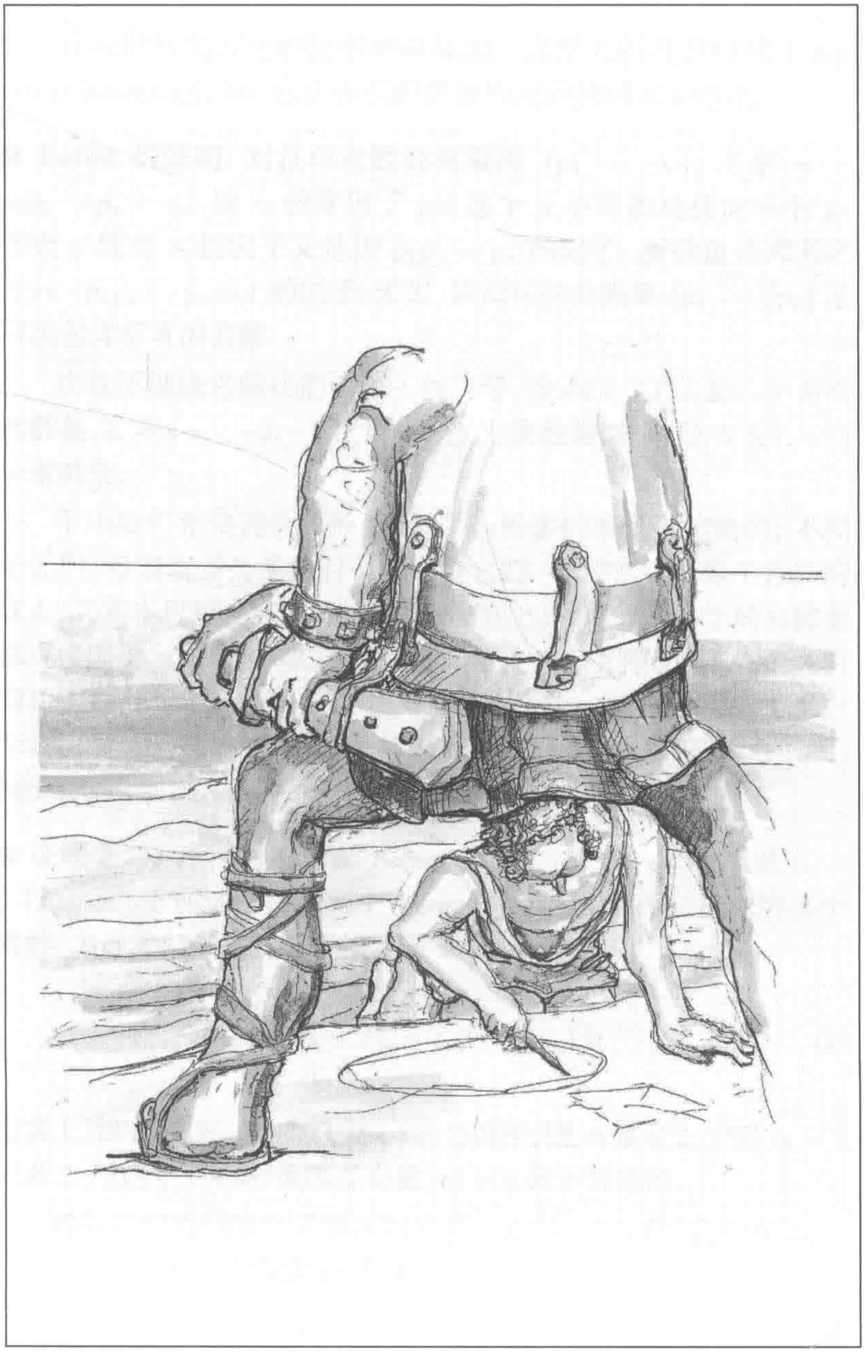
柏林, 1998 年 3 月

目录

组合数学 201

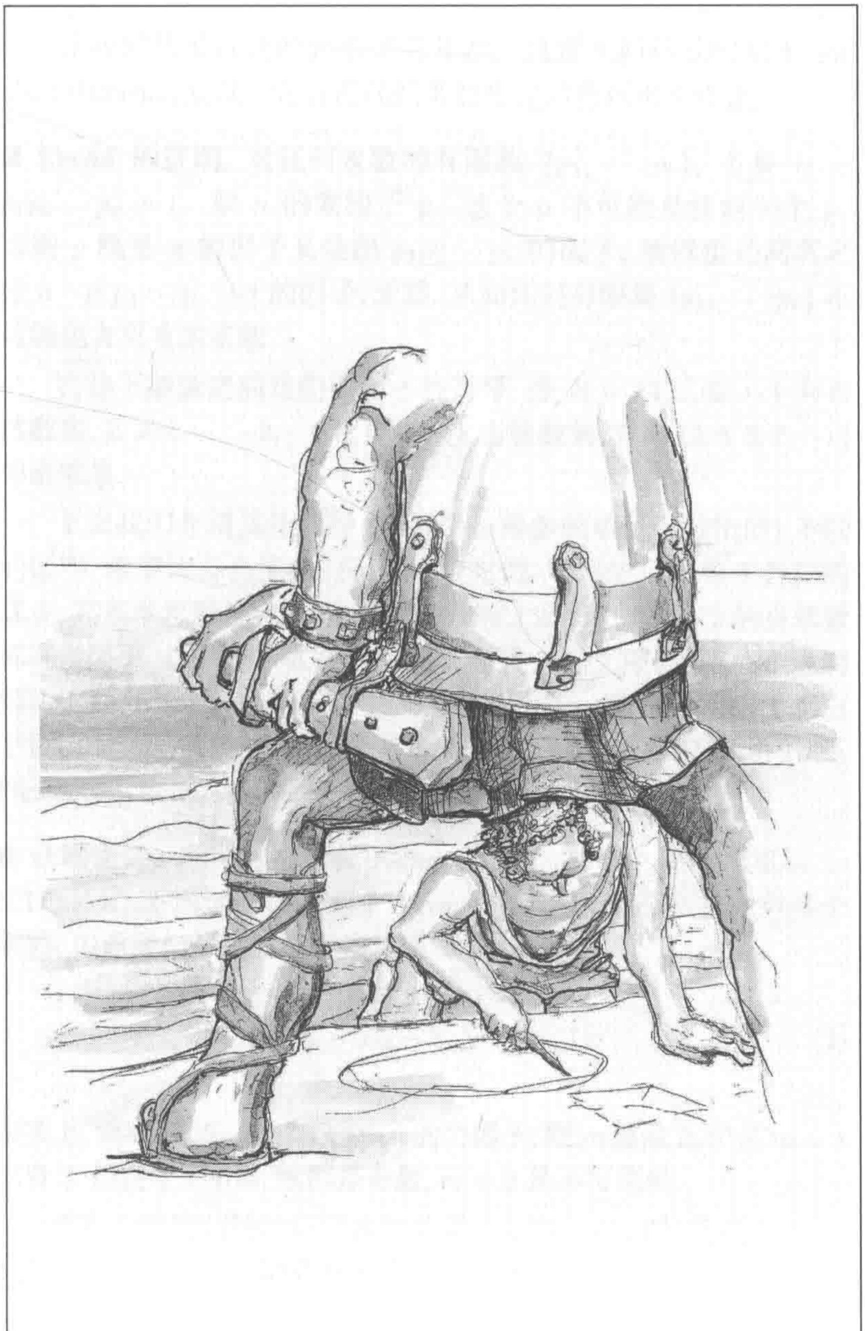
图论 273

数论



"无理性和 π"

数论



"无理性和 π"

素数无限的六种证明

第 **1** 章

让我们从最古老的天书证明开始. 通常人们将其归功于 Euclid (Elements IX, 20). 它告诉我们素数构成的数列永不终止.

■ **Euclid 的证明.** 对任何素数的有限集 $\{p_1, \cdots, p_r\}$, 考察 $n = p_1p_2\cdots p_r + 1$. 取 n 的素因子 p. 这个 p 不可能是任何一个 p_i: 否则 p 既是 n 的因子又是积 $p_1p_2\cdots p_r$ 的因子, 所以也是两者之差 $n - p_1p_2\cdots p_r = 1$ 的因子, 矛盾. 从而任何有限集 $\{p_1, \cdots, p_r\}$ 不可能包含所有的素数. □

在往下继续之前我们引入一些符号. 令 $\mathbb{N} = \{1, 2, 3, \cdots\}$ 为自然数集, $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ 为整数集, $\mathbb{P} = \{2, 3, 5, 7, \cdots\}$ 为素数集.

下面我们介绍其他几种 (从一个长得多的单子上选出的) 不同的证明, 希望读者会像我们一样喜爱它们. 尽管它们来源于各异的观点, 其基本思想是相同的: 自然数没有上界, 而每个 $\geqslant 2$ 的自然数都有素因子. 这两个事实放在一起将导致 $\mathbb{P}$ 是无限的. 下一个证明归功于 Christian Goldbach (在 1730 年致 Leonhard Euler 的信里), 第三个证明显然是通俗的, 第四个是 Euler 自己给出的, 第五个由 Harry Fürstenberg 提出, 而最后一个是 Paul Erdős 的.

■ **证明之二.** 让我们先看看 *Fermat* 数 $F_n = 2^{2^n} + 1$, 这里 $n = 0, 1, 2, \cdots$. 下面证明任意两个 Fermat 数互素; 从而必有无穷多个素数. 为此我们只需验证递推关系

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geqslant 1). \tag{1}$$

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$
$F_5 = 641 \cdot 6700417$
前几个 Fermat 数

事实上, 设 m 是 F_k 和 F_n $(k < n)$ 的公因子, 则 m 整除 2, 于是 $m = 1$ 或者 2. 但由于 Fermat 数都是奇数, $m = 2$ 是不可能的.

现在我们用归纳法证明递归关系 (1): 当 $n = 1$ 时, 我们有 $F_0 = 3$ 及 $F_1 - 2 = 3$. 由归纳假设即得

$$\prod_{k=0}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) F_n = (F_n - 2)F_n$$
$$= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

证毕. □

■ **证明之三.** 假设 $\mathbb{P}$ 有限且令 p 为最大的素数. 我们考虑 *Mersenne* 数 $2^p - 1$, 并证明 $2^p - 1$ 的任意素因子 q 皆大于 p, 由此导出素数无限. 令 q 为整除 $2^p - 1$ 的一个素数, 则有 $2^p \equiv 1 \pmod q$. 因为 p 为素数, 前一公式说明在域 $\mathbb{Z}_q$ 的乘法群 $\mathbb{Z}_q \backslash \{0\}$ 中元素 2 的阶就是 p. 而该乘法群有 $q-1$ 个元素. 由 Lagrange 定理, 我们得到 $p \mid (q-1)$ 并由此可以导出 $p < q$. □

Lagrange 定理

若 G 是一个有限 (乘法) 群且 U 是它的一个子群, 则必有 $|U|$ 整除 $|G|$.

■ **证明.** 考虑二元关系

$$a \sim b :\Longleftrightarrow ba^{-1} \in U.$$

从群的定义易见 $\sim$ 是一个等价关系. 包含元素 a 的等价类即陪集

$$Ua = \{xa : x \in U\}.$$

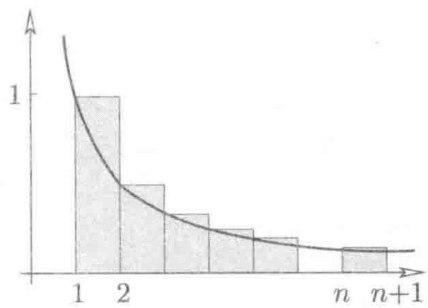
显然 $|Ua| = |U|$, 所以 G 可以被划分为阶数均为 $|U|$ 的若干陪集, 从而可以导出 $|U|$ 整除 $|G|$. □

在 U 是循环子群 $\{a, a^2, \cdots, a^m\}$ 的特殊情况, 可见 m (使 $a^m = 1$ 的最小正整数, 称为元素 a 的阶) 一定整除 $|G|$ 的阶数. 特别地, 我们有 $a^{|G|} = 1$.

下面是一个用到初等微积分的证明.

■ **证明之四.** 令 $\pi(x) := \#\{p \leqslant x : p \in \mathbb{P}\}$ 表示不超过实数 x 的素数个数. 将 $\mathbb{P} = \{p_1, p_2, p_3, \cdots\}$ 排为升序. 我们考虑由 $\log x = \int_1^x \frac{1}{t} dt$ 定义的自然对数 $\log x$.

现在将曲线 $f(t) = \frac{1}{t}$ 之下的面积与稍高的阶梯函数之下的面积进行比较. 对 $n \leqslant x < n+1$ 我们有



在函数 $f(t) = \frac{1}{t}$ 上面的阶梯

$$\log x \leqslant 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}$$
$$\leqslant \sum \frac{1}{m},$$

这里 $\sum$ 表示对所有的仅含 $p \leqslant x$ 的素因子的 $m \in \mathbb{N}$ 求和. 因为每个被求和的 m 可以唯一地表为 $\prod\limits_{p \leqslant x} p^{k_p}$ 的形式, 最后一个和式等于

$$\prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \Big(\sum_{k \geqslant 0} \frac{1}{p^k}\Big).$$

由于上面的内和是公比为 $\frac{1}{p}$ 的几何级数, 所以

$$\log x \leqslant \prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

显然, $p_k \geqslant k+1$, 因而

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leqslant 1 + \frac{1}{k} = \frac{k+1}{k},$$

所以

$$\log x \leqslant \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x)+1.$$

众所周知 $\log x$ 无界, 所以 $\pi(x)$ 也无界, 从而素数有无穷多个. □

■ **证明之五.** 在用了分析之后现在轮到用拓扑了！我们考虑整数集 $\mathbb{Z}$ 上的一种奇特的拓扑. 对 $a, b \in \mathbb{Z}, b > 0$, 令

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

每个集合 $N_{a,b}$ 都是正负无界的算术级数. 我们称集合 $O \subseteq \mathbb{Z}$ 为开集, 如果 O 是空集, 或者对任意的 $a \in O$ 存在 $b > 0$ 使得 $N_{a,b} \subseteq O$. 显然, 开集的并总是开集. 另外, 如果 O_1 和 O_2 是两个开集, 对任意的 $a \in O_1 \cap O_2$, $N_{a,b_1} \subseteq O_1$ 以及 $N_{a,b_2} \subseteq O_2$, 都有 $a \in N_{a,b_1b_2} \subseteq O_1 \cap O_2$. 所以开集的有限交是开的. 从而我们定义的开集族的确导出了 $\mathbb{Z}$ 上的一个拓扑.

这里我们注意两个事实:

(A) 每个非空的开集都是无界的.

(B) 每个 $N_{a,b}$ 都是既开又闭的.

第一点是显然的. 至于第二点, 我们观察

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}.$$

这说明 $N_{a,b}$ 是开集的补, 因而是闭集.

素数在哪里呢? —— 下面就来了. 每个整数 $n \neq 1, -1$ 都有某个素因子 p, 所以我们有 $n \in N_{0,p}$ 以及

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

“掷扁石, 到无穷远”

如果 $\mathbb{P}$ 是有限的, 那么 $\bigcup_{p\in\mathbb{P}} N_{0,p}$ 将是有限个闭集的并 (根据 (B)), 所以是闭的. 进而可以导出 $\{1, -1\}$ 是一个开集, 这与 (A) 矛盾. □

■ **证明之六.** 我们的最后一个证明更迈进了一大步. 它不仅证明了素数无穷多, 还证明了无穷级数 $\sum_{p\in\mathbb{P}} \frac{1}{p}$ 发散. Euler 首次证明了这个重要的结果 (那个证明也很有趣), 我们将要介绍的是由 Erdős 给出的着实漂亮的证明.

令 $p_1, p_2, p_3, \cdots$ 表示升序排列的素数, 并假设 $\sum_{p\in\mathbb{P}} \frac{1}{p}$ 收敛, 那么一定存在自然数 k 使得 $\sum_{i\geqslant k+1} \frac{1}{p_i} < \frac{1}{2}$. 这时, 我们称 $p_1, \cdots, p_k$

为小素数, 称 $p_{k+1}, p_{k+2}, \cdots$ 为大素数. 这样对任意的自然数 N 都有

$$\sum_{i \geqslant k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{2}$$

令 N_b 表示满足 $n \leqslant N$ 且至少被一个大素数整除的正整数 n 的个数, N_s 表示满足 $n \leqslant N$ 且因子都是小素数的正整数的个数. 我们将证明存在某个 N 使得

$$N_b + N_s < N,$$

从而导出矛盾. 根据定义 $N_b + N_s$ 应该是等于 N 的.

为估计 N_b, 我们注意到 $\lfloor \frac{N}{p_i} \rfloor$ 计数了满足 $n \leqslant N$ 的 p_i 的倍数. 于是由 (2) 得到

$$N_b \leqslant \sum_{i \geqslant k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{3}$$

现在再看 N_s. 把每个只有小素数因子的 $n \leqslant N$ 写成 $n = a_n b_n^2$ 的形式, 这里 a_n 是没有平方因子的部分. 每个 a_n 也就是一些互异的小素数的乘积, 所以一共恰好有 2^k 个可供选择的没有平方因子的部分. 另一方面, 由于 $b_n \leqslant \sqrt{n} \leqslant \sqrt{N}$, 至多有 $\sqrt{N}$ 个不同的平方部分, 所以

$$N_s \leqslant 2^k \sqrt{N}.$$

因为 (3) 对任意的 N 都成立, 只需找到一个满足 $2^k\sqrt{N} \leqslant \frac{N}{2}$ 亦即 $2^{k+1} \leqslant \sqrt{N}$ 的 N 就行了. 那么令 $N = 2^{2k+2}$ 即可. □

附录: 又无穷多个证明

我们证明素数无限的库藏里还有若干其他或旧或新的宝贝, 然而其中一件最近的珍品很不一般, 特别值得一提. 让我们试着确定整数序列 S, 使得能够整除 S 的某个元素的那些素数构成的集合 $\mathbb{P}_S$ 无穷. 每个这样的序列都给出了一个关于素数无限的证明. 第二个证明中研究的 Fermat 数 F_n 构成了这样一个序列, 而所有 2 的幂不行. Issai Schur 的一个定理给出了许多例子, 他在 1912 年证明, 对于每一个不为常数的整系数多项式 $p(x)$, 所有非零值集合 $\{p(n) \neq 0 : n \in \mathbb{N}\}$ 就是这样一个序列. 对于多项式 $p(x) = x$, Schur 的结果就是 Euclid 的定理. 另举一例, 对于 $p(x) = x^2 + 1$, 我们得到, "平方数加 1" 包含了无穷多个相异的素因子.