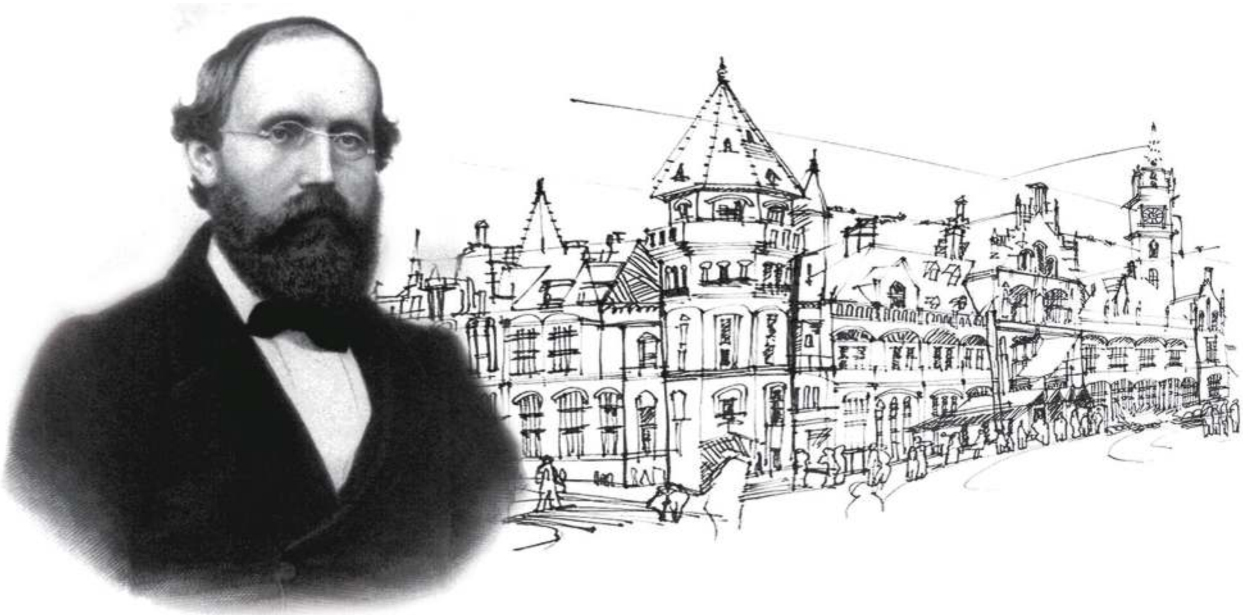
Riemann



黎曼猜想漫谈(六)

卢昌海

32 从模算术到有限域

“山寨版”黎曼猜想这枚坚果该从哪里啃起呢？为了彰显将科普进行到底的决心，让我们从小学算术啃起吧！

这并不是搞笑，在它背后其实有一段小小的故事——一段与美苏冷战有关的故事。那是在半个多世纪前的 1957 年。那一年，苏联先于美国将一颗人造卫星送入了近地轨道，迈出了航天时代的第一步。这一在太平年代可以令全人类共同自豪的成就，由于发生在冷战时期，带给美国的乃是巨大的震动和反思。作为反思的结果，美国初等教育界兴起了一场以革新教材为主旨的所谓“新数学”运动（New Math），试图“从娃娃抓起”，加强教育、奋起直追。在这场运动中，许多原本晚得多才讲述的内容被加入到了小学和初中教材中，其中包括公理化集合论（axiomatic set theory）、模算术（modular arithmetic）、抽象代数（abstract algebra）、符号逻辑（symbolic logic）等[注 32.1]。这种“拔苗助长”般的革新不仅远远超出了普通中小学生的接受能力，甚至也超出了一部分中小学教师的教学能力，因此只尝试了几年就被放弃了。不过对我们来说，这场“小跃进”式的“新数学”运动却是一

注 32.1

与本系列的上下文不无巧合的是，这些新内容的选择在一定程度上受到了韦伊参与创立的布尔巴基学派的影响。

Riemann

个很好的幌子，让我们能够宣称从小学算术开始本节的科普，因为我们将要介绍的“山寨版”黎曼猜想，可以从“新数学”当中的一种——模算术——说起。

模算术的一个典型的题目是：现在时钟的时针指向 7，请问 8 小时之后时针指向几？这个题目与“7+8=?”那样的传统小学算术题的差别，就在于时钟上的数字是以 12 为周期循环的，从而不存在大于 12 的数字。这种带有“周期”的算术题就是典型的模算术题目，它通常被表述为“7+8=? (mod 12)”，其中的“(mod 12)”表示以 12 为周期，而这周期的正式名称叫做“模”(modulus)，模算术之名因此而来[注 32.2]。

模算术是数论中一种很有用的工具，数学大腕欧拉、拉格朗日、勒让德等人都使用过，但对它的系统研究则要归功于高斯。1801 年，这位被后世尊为“数学王子”，且当时正值“王子”年龄（24 岁）的年轻数学家在其名著《算术研究》(Disquisitiones Arithmeticae）中系统性地运用了模算术，证明了许多重要命题，并为后世奠定了该领域的若干标准术语。由于讲述模算术的最通俗例子就是上面所举的有关时钟的题目，因此模算术也称为“时钟算术”(clock arithmetic)，而为了纪念高斯对这一领域的贡献，那时钟则被一些科普作家称为高斯时钟(Gauss clock)。

高斯时钟所包含的刻度数目不一定非得像普通时钟那样为 12，而完全可以是其它数目。事实上，对于我们的真正兴趣而言，刻度数目为 12 的高斯时钟是一个很糟糕的特例，因为在它上面虽然可以进行加减法和乘法，但作为乘法逆运算的除法却并不总能够进行的（请读者自行证实这一点）。在数学上，一个集合的元素之间如果加、减、乘、除全都可以进行，而且无论怎么折腾，都像孙悟空翻不出如来佛掌心一样，仍在那集合之中，那样的集合有一个专门的名称，叫做域（field）[注 32.3]。域的概念在数学上有很大的重要性，并且也是我们真正感兴趣的东西，因为我们熟悉的有理数、实数、以及表述黎曼猜想时用到过的复数的集合全都是域，即将介绍的“山寨版”黎曼猜想也离不开域。而所含刻度数目为 12 的高斯时钟由于无法保证除法的进行，便无法用来表示域，从而是一个很糟糕的例子。

对于域，我们可以粗略地分为两类：一类是像有理数、实数和复数的集合那样所含元素数目为无限的，另一类则是所含元素数目有限的。这两类域各有一个很直白的名字，前者叫作无限域（infinite field)，后者叫做有限域（finite field)。我们真正感兴趣的东西粗略地讲是域，确切地说其实是有限域，因为它在某些方面比无限域来得简单，是构筑“山寨版”东西的好材料。

虽然所含刻度数目为 12 的高斯时钟——如前所述——无法用来表示域，但某些高斯时钟确实可以用来表示域——当然，这里的域是指有限域。比如，有限域的一个最简单的例子就是只含 0 和 1 两个刻度的高斯时钟（请读者自行列出这个有限域中的加、减、乘、除结果），这个有限域通常记为 F_2——下标 2 表示元素的数目（等同于高斯时钟的刻度数目）。

很简单吧？不愧是小学算术，但我们的科普很快就要提速了。

既然含有两个元素的有限域记为 F_2，那么大家一定可以猜到，含有 p 个元素的有限域的记号就是 F_p。完全正确！不过，细心的读者也许会提出一个问题：那就是 p 这个字母在我们这个系列中通常是表示素数的，这里为何不用一个更普通的字母，比如 n 呢？答案是：这是存心的。我们刚才提到过，某些高斯时钟可以用来表示有限域，到底是哪些高斯时钟呢？正是那些所含刻度数目为素数的高斯时钟。这一点的普遍证明并不困难，感兴趣的读者可

注 32.2

需要说明的是，普通时钟与以 12 为模的模算术略有差异：前者包含的数字是从 1 到 12，后者则是从 0 到 11。这两者是等价的，因为 12=0 (mod 12)，但后者对数学研究来说更方便，因为否则的话，就必须接受一个不方便的事实，那就是 12 这个看起来非零的数字具有 0 的算术性质。

注 32.3

在加、减、乘、除这四种运算中，加和乘是基本运算，减和除作为加和乘的逆运算，可以由每个元素相对于加和乘必须存在逆元素（唯一的例外是 0 相对于乘不存在逆元素）这一要求引申出来。此外，我们在小学算术中就已熟悉的交换律、结合律和分配律也是域的定义的一部分，感兴趣的读者请参阅域的完整定义。

以从前面所说的刻度数目为 12 的高斯时钟不能表示有限域的原因入手，来琢磨一下普遍证明的思路。

能够用高斯时钟来表示，对于有限域来说无疑是一个很利于科普的特点，但却不是必不可少的条件。事实上，不能用高斯时钟来表示（即元素数目不是素数）的有限域也是存在的。而更微妙的是，有限域的元素数目虽然可以不是素数，却也不是完全任意的。那么，究竟什么样的元素数目才是可能的呢？答案是：它必须为素数的正整数次幂。换句话说，如果我们用 F_q 表示有限域，那么 q 只能是 $q=p^n$（n=1, 2, 3, ...）[注 32.4]。现在我们可以对所含刻度数目为 12 的高斯时钟做出更完整的评价：它确实是一个很糟糕的例子，因为 12 不仅不是素数，连素数的正整数次幂都不是，因此根本就不存在元素数目为 12 的有限域，更遑论用那样的高斯时钟来表示。

好了，从模算术开始，我们引出了有限域这个概念，并宣称这是我们在本节中真正感兴趣的东西。那么，对于有限域，究竟有什么东西值得我们研究呢？答案是：方程。事实上，域的概念的引进，本身就与研究方程有着密切关系，因为减法与除法这两种运算的引进，在很大程度上就是为了研究诸如 a+?=0 和 a×?=1 那样的方程。研究方程是数学中最古老的探索之一，像方程是否有解？有多少个解（即解的数目）？如何求解？那样的课题，从古至今都有一些数学家在研究。

而对这些课题的研究，往往与在什么域中研究有着很大关系。比如说，曾经难住数学家们长达 358 年（这个记录连黎曼猜想也未必能打得破）才被解决掉的费马猜想（如今已荣升为费马大定理）如果放到实数域中，根本就不是问题。既然对方程的研究与在什么域中研究有着很大关系，那么有限域上的方程自然也就成为了研究课题之一。这其中很受数学家们钟爱的一类方程叫做代数方程（algebraic equation），也叫多项式方程（polynomial equation），它只包含变量的整数次幂（费马大定理所涉及的方程就是一种代数方程）。我们接下来要讨论的就是有限域上的代数方程。

作为有限域上代数方程的最简单例子之一，我们考虑有限域 F_q 上的二元代数方程 $F(x, y)=0$，其中 $F(x, y)$ 是一个所有系数及变量 x、y 都在 F_q 中取值的多项式（“所有系数及变量 x、y 都在 F_q 中取值”是该方程作为“有限域 F_q 上”的方程所须满足的定义性条件）。我们知道，像 $F(x, y)=0$ 这样的二元方程在实平面上的解（即 x、y 都为实数的解）的集合通常是曲线，借用这种术语，数学家们把二元代数方程 $F(x, y)=0$ 的解的集合称为代数曲线（algebraic curve）[注 32.5]，如果该二元代数方程是有限域上的方程，则相应的解的集合称为有限域上的代数曲线。当然，这种所谓的“曲线”实际上只是有限多个点的集合，因为它所在的整个“平面”$F_q \times F_q$ 总共也只有 q^2 个点。

另一方面，一个代数方程 $F(x, y)=0$ 如果是有限域 F_q 上的方程，当然也是以 F_q 为子域（subfield）、但比 F_q 更大的有限域上的方程，从而可以表示那些更大的有限域上的代数曲线。那些更大的有限域称为 F_q 的扩张域（extension field）。可以证明，F_q 的扩张域是那些所含元素个数为 q 的正整数次幂的有限域，即 F_{q^m}（m=1, 2, 3, ...）。因此，有限域 F_q 上的代数方程 $F(x, y)=0$ 可以被视为是所有有限域 F_{q^m}（m=1, 2, 3, ...）上的代数方程。

以上这些貌似与黎曼猜想风马牛不相及的东西，就是“山寨版”黎曼猜想赖以存身的那座“山”。

注 32.4

细心的读者可能还会提出这样一个问题：我们用 F_q 来表示元素数目为 q 的有限域，但如果那样的有限域有不止一个怎么办？用什么办法来区分它们呢？答案是，元素数目为 q 的有限域彼此是同构（isomorphic）的，即彼此的元素及运算关系全都是一一对应的。对于数学研究来说，这样的有限域可以视为等同，从而无需区分。另外补充一点：不仅有限域的元素数目必须为素数的正整数次幂，而且对于任何一个素数的正整数次幂 p^n，都必定存在一个元素数目恰好为 p^n 的有限域。

注 32.5

效仿普通解析几何的做法，由 $F(x, y)=0$ 的解的集合所定义的代数曲线本身也可以用 $F(x, y)=0$ 来表示，称为代数曲线 $F(x, y)=0$。另外要提醒读者的是，代数曲线不仅可以用像 $F(x, y)=0$ 那样的代数方程来表示，也可以用方程组来表示，就好比普通空间中的曲线：比如一个圆既可以用一个方程 $x^2+y^2=1$ 来表示，也可以用方程组 $x^2+y^2+z^2=1$ 和 z=0 来表示。为行文简洁起见，我们在正文中一律以方程为例。

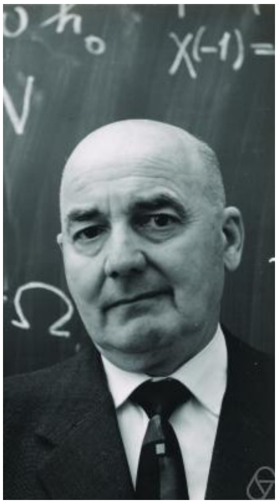
Riemann

33 “山寨版” Riemann 猜想

现在我们要往“山寨版”黎曼猜想靠拢了。由于黎曼猜想是关于黎曼 ζ 函数零点分布的猜想，因此很明显，要想有黎曼猜想，首先得有黎曼 ζ 函数。只不过，黎曼猜想如果是“山寨版”的，作为其“核心部件”的黎曼 ζ 函数当然也只需是“山寨版”即可。这“山寨版”的黎曼 ζ 函数从何而来呢？正是从有限域上的代数曲线中来。

为此，我们要引进有限域上代数曲线 $F(x, y)=0$ 的一个重要性质，那就是它所含点的数目。这个性质之所以重要，因为它实际上就是有限域上代数方程 $F(x, y)=0$ 的解的数目。如前所述，解的数目对于研究方程来说是一个重要课题，相应的，所含点的数目对于代数曲线来说也是一个重要性质。我们在前面说过，有限域 F_q 上的代数方程 $F(x, y)=0$ 可以被视为是所有有限域 F_{q^m}（m=1, 2, 3, ...）上的代数方程。用代数曲线的语言来说，这意味着有限域 F_q 上的代数曲线 $F(x, y)=0$ 可以被视为是所有有限域 F_{q^m}（m=1, 2, 3, ...）上的代数曲线。另一方面，代数曲线 $F(x, y)=0$ 所含点的数目，或代数方程 $F(x, y)=0$ 的解的数目，显然是与定义域 F_{q^m} 的选取有关的。为了体现这种关系，我们用 N_m 表示定义域为 F_{q^m} 时的这一数目。

埃米尔·阿廷
Emil Artin



海尔穆特·哈塞
Helmut Hasse

有了这些准备，现在我们可以定义“山寨版”的黎曼 ζ 函数了，那就是：

$$\varsigma_C(s)=\exp\left(\sum_{m=1}^{\infty}N_m(C)\frac{q^{-ms}}{m}\right)$$

如此定义的“山寨版”黎曼 ζ 与“正版”黎曼 ζ 一样，是关于复变量 s 的函数，它有一个比较正式的名字，叫做有限域上代数曲线的 ζ 函数。在这一函数的定义中，我们特意引进了一个表示代数曲线的字母 C，因为此定义所给出的函数显然与代数曲线的选取有关。上述定义中还含有 q，这也是显而易见的，因为代数曲线 C 的原始定义域是 F_q。

有了“山寨版”的黎曼 ζ 函数，我们就可以表述有关其零点分布的“山寨版”黎曼猜想了。由于这个猜想是关于有限域上代数曲线的 ζ 函数零点分布的，因此我们称其为有限域上代数曲线的“山寨版”黎曼猜想。

> 有限域上代数曲线的“山寨版”黎曼猜想：有限域上代数曲线的 ζ 函数的所有零点都位于复平面上 Re(s)=1/2 的直线上。

由于“山寨版”黎曼 ζ 函数与代数曲线的选取有关，实际上有无穷多种。因此上述“山寨版”黎曼猜想实际上也是无穷多个猜想的统称。对于特定的代数曲线及原始定义域，该猜想可以通过对“山寨版”黎曼 ζ 函数的直接计算加以验证，有些甚至是相当容易的，但涵盖所有代数曲线及原始定义域的普遍证明却大为不易。

我们在 31 节中曾经提到，安德烈·韦伊（André Weil, 1906-1998）并不是“山寨版”黎曼猜想这一研究方向的开创者。事实上，早在 1923 年，奥地利数学家埃米尔·阿廷（Emil Artin, 1898-1962）就提出了有限域上一类被称为超椭圆曲线（hyperelliptic curve）的特殊代数曲线上的 ζ 函数，以及相应的“山寨版”黎曼猜想。1933 年，德国数学家海尔穆特·哈塞（Helmut Hasse, 1898-1979）则证明了有限域上一类被称为椭圆曲线（elliptic curve）的特殊代数曲线上的“山寨版”黎曼猜想（请注意，阿廷只是提出猜想，哈塞则是证明猜想，不过两人针对的是不同情形下的猜想——前者针对超椭圆曲线，后者针对椭圆

曲线）[注 33.1]。

阿廷的猜想及哈塞的证明虽都有一定的广泛性（都涵盖了无穷多的个例），但针对的仍只是特定类型的代数曲线。韦伊的贡献则在于给出了上述“山寨版”黎曼猜想的普遍证明（即针对任意代数曲线）。不过，在 31 节提到的他给埃利 • 嘉当（Élie Cartan, 1869-1951）的信件中，他给出的只是证明的大致思路，完整的证明直到二战结束后的 1948 年才发表。韦伊对“山寨版”黎曼猜想的贡献还不止于此。完成了对上述猜想的证明后的第二年，即 1949 年，韦伊对该猜想进行了一次重要推广。这个推广的证明是如此困难，不仅他自己未能给出，在接下来二十四年的时间里，参与研究的所有其他数学家也都未能给出完全的证明。他的这一推广因此而被称为了韦伊猜想（Weil conjectures）。

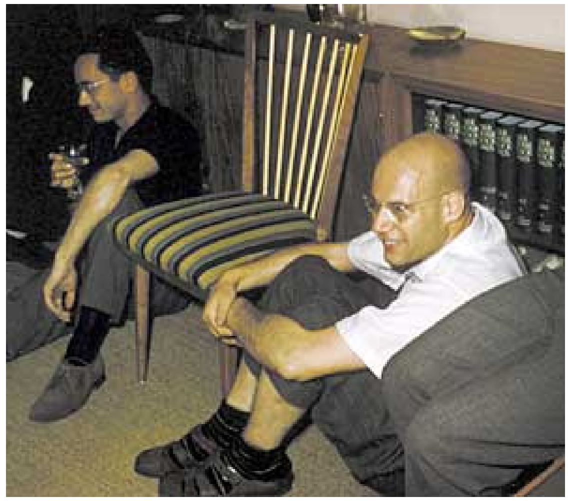
韦伊猜想包含了若干个命题，“山寨版”黎曼猜想是其中之一，并且从历史上讲是证明最为不易的一个。不过，韦伊猜想中的“山寨版”黎曼猜想的证明虽然困难，其由来却是对上述“山寨版”黎曼猜想的很直接的推广，即将上述猜想中的代数曲线推广为高维几何对象。这种高维几何对象有一个专门的名称，叫做代数簇（algebraic variety），它也是用代数方程（或方程组）来定义的，并且也可以定义在有限域上。与有限域上代数曲线的 ζ 函数完全类似，也可以引进有限域上代数簇的 ζ 函数。对于这种 ζ 函数，也存在“山寨版”的黎曼猜想，我们称其为有限域上代数簇的“山寨版”黎曼猜想，它是韦伊对有限域上代数曲线的“山寨版”黎曼猜想的推广，也是韦伊猜想的一部分。

有读者可能会问：将曲线推广为高维几何对象这样直截了当的推广，那是中学生都能想到的事情，为何要等到 1949 年才问世？答案是：有限域上代数簇的“山寨版”黎曼猜想与普通（即有限域上代数曲线的）的“山寨版”黎曼猜想以及“正版”黎曼猜想有一个绝非显而易见的差异，那就是它所要求的零点分布并非是单一直线，而是与代数簇的维数有关的一系列直线。具体地说，韦伊猜想中的“山寨版”黎曼猜想是这样的：

> 有限域上代数簇的“山寨版”黎曼猜想：有限域上的 d 维代数簇的 ζ 函数的所有零点都位于复平面上 $\mathrm{Re}(s)=1/2, 3/2, \ldots, (2d-1)/2$ 的直线上。

如前所述，这一“山寨版”黎曼猜想只是韦伊猜想的一部分，而非全部。韦伊猜想还包括了关于有限域上代数簇的 ζ 函数的另外几个命题。虽然与普通（即有限域上代数曲线的）“山寨版”黎曼猜想及“正版”的黎曼猜想都有所不同，这个推广了的“山寨版”黎曼猜想与后两者的相似性还是很显著的，不算有负“山寨版”的“光荣称号”。此外，在 d=1 的特殊情况下，该猜想可以自动给出有限域上代数曲线的“山寨版”黎曼猜想，这也印证了它作为“山寨版”黎曼猜想的地位。

韦伊猜想提出后引起了很多数学家的兴趣，在试图证明这一猜想的数学家中，包括了阿廷的学生 Bernard Dwork（1923-1998）、阿廷的儿子迈克尔 • 阿廷（Michael Artin, 1934-）、1954 年菲尔兹奖得主塞尔（Jean-Pierre Serre, 1926-）、1966 年菲尔兹奖得主格罗滕迪克（Alexander Grothendieck, 1928-）等人。经过这些数学家的努力，韦伊猜想的某些部分在二十世纪



菲尔兹奖 1954 年得主塞尔（左）与 1966 年得主格罗滕迪克摄于 1958 年。

注 33.1

超椭圆曲线是指形如 $y^2=f(x)$ 的代数方程所表示的代数曲线，其中 $f(x)$ 为满足特定条件的四次以上多项式。椭圆曲线是指形如 $y^2=f(x)$ 的代数方程所表示的代数曲线，其中 $f(x)$ 为满足特定条件的三次多项式。

Riemann

六十年代得到了证明，但有限域上代数簇的“山寨版”黎曼猜想部分，则直到 1974 年才由格罗滕迪克的学生、比利时数学家皮埃尔•德利涅（Pierre Deligne, 1944-）所证明，他的证明借助了格罗滕迪克的工作。四年之后，德利涅因这一工作获得了 1978 年的菲尔兹奖。在证明包括“山寨版”黎曼猜想在内的韦伊猜想的过程中，数学家们发展出了一些很有用的东西，比如格罗滕迪克创立了一种全新的数学工具：平展上同调（Étale cohomology），对数学——尤其是代数几何——的发展起到了促进作用。从这个意义上讲，“山寨版”黎曼猜想与其它一些重要的数学猜想一样，是一只“会下金蛋的鹅”（这是希尔伯特对费马猜想的评价）。这也是它的证明虽迄今不曾为人们提供证明“正版”黎曼猜想的有效思路[注 33.2]，却依然被视为重要成就的主要原因。当然，“山寨版”黎曼猜想的证明，多多少少使一些人对“正版”黎曼猜想的成立抱有了更大的信心。

在结束本节前，还有一件事情需要交代一下。细心（或挑剔？）的读者也许还会提出这样一个问题：我们说了半天的“山寨版”黎曼猜想，作为基础的那个所谓“山寨版”的黎曼 ζ 函数跟“正版”的黎曼 ζ 函数并不像啊？难道就凭它的零点也都在直线上，就将它称为“山寨版”的黎曼 ζ 函数，既而将有关其零点分布的猜想称为“山寨版”的黎曼猜想吗？如果那样的话，炮制“山寨版”黎曼猜想可就忒容易了，因为构造一个所有零点都在直线上——甚至在 Re(s)=1/2 的直线上——的函数其实是很容易的事情（请读者自行构造几个那样的函数），难道那样一来它们就都可以跟黎曼猜想攀上亲？

这些问题的答案是：这里引进的“山寨版”黎曼 ζ 函数及黎曼猜想与“正版”黎曼 ζ 函数及黎曼猜想的相似性，绝不仅仅是因为它们的零点都分布在直线上，而有着更深层的理由。比方说，“山寨版”黎曼 ζ 函数跟“正版”黎曼 ζ 函数一样，可以写成类似于欧拉乘积公式那样的表达式，而且也满足类似于“正版”黎曼 ζ 函数所满足的函数方程。不仅如此，与“正版”黎曼猜想的成立可以给出对素数分布的最佳估计（即与素数定理之间的最小偏差——参阅第 5 节）相似，“山寨版”黎曼猜想的成立可以给出对有限域上代数簇所包含的点的数目（即定义代数簇的方程或方程组在有限域上的解的数目）的某种最佳估计。可惜的是，这些结果，以及“山寨版”黎曼猜想的证明，都不是省油的灯（比方说“山寨版”黎曼 ζ 函数所满足的函数方程——对有限域上的代数簇而言——其实是韦伊猜想的一部分）。考虑到它们毕竟只是关于“山寨版”的，而我们还想保留几枚牙齿去啃点别的东西，在这个方向上就不多逗留了。如果本节的介绍让读者大致知道了“山寨版”黎曼猜想是怎么一回事，比诸如“它是黎曼猜想在代数簇上的类似物”之类口诀式的介绍强一点，我们的目的就算达到了。

聊完了“山寨版”的黎曼猜想，接下来，我们要走向另一个极端，去领略几款“豪华版”的黎曼猜想。

34 “豪华版” Riemann 猜想

本节我们来介绍“豪华版”的黎曼猜想。所谓“豪华版”，顾名思义，就是要比“普通版”更高一筹，后者有的前者都得有，而且还得有新东西。对于数学命题来说，这意味着得比原命题更强、更普遍，将原命题包含为自己的特例。那样的命题如果成立，原命题就自动成立，但反过来则不然（否则两者就等价了，对不住“豪华版”这一光荣称号）。

“豪华版”黎曼猜想与第 33 节介绍的“山寨版”黎曼猜想虽分属不同类别，有一点却是共同的，那就是都得从对黎曼 ζ 函数的变通入手，因为黎曼猜想所关注的无非就是黎曼 ζ 函数非平凡零点那些事儿，对它的各种变通，归根到底也就是对黎曼 ζ 函数的变通。只不过“山寨版”黎曼猜想中的黎曼 ζ 函数只需与普通黎曼 ζ 函数有抽象的对应即可，而“豪华版”黎曼猜想中的黎曼 ζ 函数却必须将后者包含为自己的特例，以保证猜想的“豪华”性。黎曼猜想的“豪华版”有不止一款，我们将着重介绍其

注 33.2

韦伊年轻时曾对“山寨版”黎曼猜想有可能为“正版”黎曼猜想提供借鉴或证明抱有乐观看法。他甚至设想，如果自己因此而证明黎曼猜想的话，将会有意推迟到 1959 年——黎曼猜想提出 100 周年时——才公布。不过，他的这种乐观到晚年时已不复存在，他曾对一位友人表示，自己希望能在有生之年看到黎曼猜想的解决，但这是不太可能的。

Riemann

狄利克雷
Johann Dirichlet

中有代表性的两款。

我们首先介绍一款较浅显的，叫做广义黎曼猜想（Generalized Riemann Hypothesis）。当然，这里所谓的“浅显”，绝不是指容易证明（挂有“黎曼猜想”这一招牌的东西哪会有容易证明的？），而是指相对来说比较容易介绍。这一“豪华版”黎曼猜想所采用的变通后的黎曼ζ函数叫做狄利克雷L-函数（Dirichlet L-function），它是一个级数的解析延拓，那个级数叫做狄利克雷L-级数（Dirichlet L-series），通常记为$L(s,\chi_k)$，其定义是（k、n为正整数）[注 34.1]：

$$L(s,\chi_k)=\sum_n \chi_k(n)^{-s} \quad (\mathrm{Re}(s)>1)。$$

读者们想必还记得，普通黎曼ζ函数也是一个级数，即（n为正整数）

$$\zeta(s)=\sum_n n^{-s} \quad (\mathrm{Re}(s)>1)$$

注 34.1

本定义中的χ看起来很像英文字母x（从计算机屏幕上看更是如此），其实是希腊字母 Chi。另外要提醒读者的是，有些文献将$L(s,\chi_k)$记为$L_k(s,\chi)$。

的解析延拓（不记得的读者请参阅第 2 节）。这个级数有一个不太常用的名称，叫做p-级数（p-series）。这个名称之所以不常用，是因为它一般只表示s为实数的情形，比上述黎曼ζ函数级数表达式的定义域小得多。不过为行文便利起见，我们在本节中将用它来称呼上述级数。

对比这两个级数，不需要很厉害的眼力就可以看出两者间的相似性，以及狄利克雷L-级数是p-级数的推广这一表观特点——因为后者无非就是前者中各项系数$\chi_k(n)$全都等于 1 的特例。不过，要想确认这一表观特点，必须得知道$\chi_k(n)$的定义，尤其是得知道$\chi_k(n)$是否真的能全都等于 1，因为$\chi_k(n)$并不是任意的系数，而是一组被称为狄利克雷特征（Dirichlet character）的东西[注 34.2]，它们能否全都等于 1 不是可以随意假定，而必须是由定义决定的。那么，$\chi_k(n)$的定义是什么呢？是由以下三个条件共同构成的（k为正整数，m、n为整数）：

1、对一切n，$\chi_k(n)=\chi_k(n+k)$，
2、对一切m和n，$\chi_k(m)\,\chi_k(n)=\chi_k(mn)$，
3、对一切n，若k和n互素，则$\chi_k(n)\neq 0$，否则$\chi_k(n)=0$。

由上述定义不难证明（请读者自行完成），对一切n，$\chi_1(n)=1$。因此$\chi_k(n)$全都等于 1 的确是$\chi_k(n)$的一组可能的取值（即k=1 的特殊情形）。这表明狄利克雷L-级数确实是p-级数的推广。当然，这也意味着作为相应级数解析延拓的狄利克雷L-函数是黎曼ζ函数的推广。

与p-级数在$\mathrm{Re}(s)>1$的区域内可以写成连乘积表达式（即欧拉乘积公式）相类似，狄利克雷 L-函数在$\mathrm{Re}(s)>1$的区域内也可以写成连乘积表达式：

$$L(s,\chi_k)=\prod_p\left[1-\chi_k(p)p^{-s}\right]^{-1},$$

注 34.2

更具体地说，$\chi_k(n)$是所谓模为k的狄利克雷特征 (Dirichlet character to the modulus k)。另外，对于狄利克雷L-函数的某些方面（比如函数方程）的研究往往要求k为$\chi_k(n)$的最小模——即不存在k的因子$d<k$，使得对一切n，$\chi_k(n)=\chi_d(n)$。这样的狄利克雷特征也被称为 primitive Dirichlet character。

Riemann

其中右边的连乘积针对所有的素数进行。与黎曼 ζ 函数及欧拉乘积公式包含了素数分布的信息（参阅 第 3 节）相类似，狄利克雷 L- 函数及上述连乘积表达式可以用来研究算术级数（arithmetic progression）中的素数分布 [注 34.3]。1837 年，德国数学家狄利克雷（Johann Dirichlet, 1805-1859）进行了那样的研究，得到了所谓的狄利克雷算术级数定理。这个定理的内容是：如果正整数 n 和 k 互素，则序列 $n, n+k, n+2k, \cdots$ 中存在无穷多个素数。狄利克雷对这一定理的证明方法类似于我们在 第三节 中介绍过的欧拉 (利用欧拉乘积公式) 对素数有无穷多个这一命题的证明。

他那项研究在数论历史上有着重要地位，被视为是解析数论（analytic number theory）这一分支领域的开山之作。正是为了纪念狄利克雷的重大贡献，人们以他的名字命名了狄利克雷 L- 级数、狄利克雷 L- 函数、以及狄利克雷特征等术语。

可以证明，狄利克雷 L- 函数作为狄利克雷 L- 级数的解析延拓，与黎曼 ζ 函数一样，是复平面上的亚纯函数（其定义请参阅第 2 节）。狄利克雷 L- 函数与黎曼 ζ 函数的相似性是相当广泛的，比如它也满足类似于黎曼 ζ 函数所满足的那种函数方程。此外，狄利克雷 L- 函数的零点也有平凡与非平凡之分，非平凡零点也全都位于 $0<\mathrm{Re}(s)<1$ 的带状区域（即 critical strip）内。而所谓的广义黎曼猜想，则是宣称狄利克雷 L- 函数的所有非平凡零点也全都位于 $\mathrm{Re}(s)=1/2$ 的直线（即临界线）上，即：

广义黎曼猜想：狄利克雷 L- 函数的所有非平凡零点都位于复平面上 $\mathrm{Re}(s)=1/2$ 的直线上。

由于狄利克雷 L- 函数是黎曼 ζ 函数的推广，因此广义黎曼猜想显然是黎曼猜想的推广。在所有“豪华版”黎曼猜想中，广义黎曼猜想是被引述得最为广泛的，有大量数学命题的成立是以这一猜想的成立为前提的。不仅如此，与黎曼猜想的成立可以给出对素数分布的最佳估计相类似，广义黎曼猜想的成立可以给出对算术级数中的素数分布的最佳估计。

我们要介绍的第二款“豪华版”黎曼猜想叫做扩展黎曼猜想（Extended Riemann Hypothesis）[注 34.4]，它所采用的变通后的黎曼 ζ 函数则叫做戴德金 ζ 函数（Dedekind zeta function），是以德国数学家理查德 • 戴德金（Richard Dedekind, 1831-1916）的名字命名的。这一函数也是一个级数的解析延拓，只不过该级数的定义是需要多费一些口舌才能介绍清楚的。我们先把定义写下来：

$$\zeta_K(s)=\sum\nolimits_I N(I)^{-s} \quad (\mathrm{Re}(s)>1)\text{。}$$

粗看起来，这个定义并不复杂，与普通黎曼 ζ 函数的 p- 级数表达式相比，只不过是在左侧的函数名称上添了一个下标 K，把右侧级数中的 n 换成 $N(I)$，再把对 n 的求和换成了对 I 的求和而已。不过，这种简单性纯粹是数学符号的简洁性带来的幌人耳目的表面现象。事实上，这里的每一处看似细小的差别，即 K、I 和 $N(I)$ 的背后都大有文章。我们先把它们的名称写下来，让大家感觉一下它们一个比一个递进的陌生性。它们的名称是什么呢？

- K 是数域；
- I 是数域 K 的整数环的非零理想；
- $N(I)$ 是数域 K 的整数环的非零理想 I 的绝对范数。

如果你不是很熟悉代数学的话，上面这些名称看了估计就跟没看一样——如果不是更犯晕的话。数学是一个高度抽象的领域，试图了解一个陌生数学分支中的概念，有时就像初学英语者拿着英 - 英词

注 34.3

这里所说的 arithmetic progression 是指形如 $n, n+k, n+2k, \cdots$ 的序列 (n、k 为正整数)。中文译名“算术级数”(也叫“等差级数”) 来自于《英汉数学词汇》(科学出版社, 1987 年第二版)。不过这一译名在我看来并不恰当，因为“级数”一词对应于英文的 series，通常是指序列的和，与 arithmetic progression 所指的序列本身颇为不同。如果让我建议的话，arithmetic progression 宜译为“算术序列”或“等差序列”。

注 34.4

Extended Riemann Hypothesis 似乎尚无标准中译名，有时也被称为“广义黎曼猜想”。Extended Riemann Hypothesis 与 Generalized Riemann Hypothesis 之间的这种名称混淆不仅存在于中文中，也存在于英文中。在个别英文资料中这两者的名称与内容间的对应与本节介绍的恰好相反，此外也有人用 Generalized Riemann Hypothesis 来表示类似于本节末尾提到的 Grand Riemann Hypothesis 那样更“豪华”的黎曼猜想。但多数文献对这两个猜想的命名方式与本节介绍的相同。

典（English-English Dictionary）查找单词一样，往往在查找到的解释之中又夹杂着新的陌生词汇，大有发生“链式反应”（chain reaction）之势。上面的努力就是一个例子，我们想知道什么是戴德金 ζ 函数，于是查找到它的级数表达式，但在级数的定义中却冒出了诸如“数域”（number field）、“整数环”（ring of integer）、“理想”（ideal）、“绝对范数”（absolute norm）之类的陌生名称。而为了解释这些陌生名称，天知道会不会遇到其它陌生名称。但既然我们已决定要介绍“豪华版”的黎曼猜想，就只好硬着头皮一个一个啃下去了。

先说说“数域”这个概念。这是一个相对简单的概念，对多数读者来说，可能是上述诸名称中唯一一个眼熟的概念，尤其是我们在第 32 节中还刚刚介绍过什么是“域”。但简单归简单，它却也没有简单到可以望文生义成“数字组成的域”（否则它跟“域”基本就是一回事了）。那么，究竟什么是数域呢？它是有理数域（field of rational numbers）的有限次代数扩张域（finite algebraic extension field）。果然，不解释还好，一解释“链式反应”就又来了：什么是有理数域的“代数扩张域”？什么又是“有限次”代数扩张域呢？所谓有理数域的代数扩张域，指的是那样一个域，其中所有元素都是系数为有理数的代数方程的解（忘了什么是“代数方程”的读者请温习第 32 节）。那样的元素（即数域中的数）被称为代数数（algebraic number），而数域本身则因此也被称为代数数域（algebraic number field）。数域的一个很简单的例子是所有形如 $a+b\sqrt{2}$（a, b 为有理数）的数构成的域（请读者自行证明这样的数构成一个域，并且每个这样的数都是一个系数为有理数的代数方程的解）。$a+b\sqrt{2}$ 这一形式让人联想起向量空间（vector space）中用一组基（basis）表示向量的做法——其中 1 和 $\sqrt{2}$ 扮演基的作用，a 和 b 则是任意向量在该组基下的分量。这种从向量空间角度看待代数扩张域的做法有一定的普适性，相应的向量空间的维数（对 $a+b\sqrt{2}$ 这一例子来说是 2）称为代数扩张域的度数（degree）。度数有限的代数扩张域就称为有限次代数扩张域。这样我们就解释了什么是有理数域的有限次代数扩张域，即数域了。

中文中常见的“实数域”、“复数域”那样的名称容易给人一个错觉，以为实数、复数的全体也构成数域。其实，它们的全体虽然构成域，却并不是数域，因为它们并不是有理数域的代数扩张域，更不是有限次代数扩张域。这方面英文的名称比较好，在英文中“实数域”、“复数域”分别是“field of real numbers”和“field of complex numbers”，突出了“field”（域）的概念，却不包含“number field”（数域）这一组合，从而不像中文那样容易望文生义。

接下来说说数域的“整数环”这一概念。要说整数环，首先得说说“整数”，因为这里所谓的整数并不仅仅是大家在小学课上学过的那些整数，而是所谓的代数整数（algebraic integer）。我们上面说过，数域中的元素都是代数数，即系数为有理数的代数方程的解。如果那代数方程的系数不仅为有理数，而且是整数，并且首系数（即幂次最高项的系数）为 1，那么它的解就是所谓的代数整数[注 34.5]。粗看起来，这种数跟整数似乎没什么共同点，它们为什么被称为代数整数呢？原因有好几条：

- 首先，所有普通整数都是代数整数（请读者自行证明）。
- 其次，所有代数数都可以表示为代数整数的商，就如同所有有理数都可以表示为普通整数的商。
- 最后，代数整数与普通整数一样，对加法、减法和乘法封闭，但对除法不封闭（即两个代数整数的商未必仍是代数整数）。

可以证明，一个数域中的所有代数整数构成一种特殊的代数结构，叫做环（ring）。环这一概念是戴德金提出的（名称则是希尔伯特引进的），它是一种比域更简单的结构，相当于在域的定义中去除了乘法交换律，及每个非零元素存在乘法逆元素这两个要求。当然，这是指环的一般定义，对于整数环来说，由于其元素都是数域中的数，因此乘法交换律是

注 34.5

这里要说明的是：系数为有理数的代数方程实际上等价于系数为整数的代数方程（请读者自行证明），因此代数整数定义中的系数是整数并不是新要求，真正的新要求是在系数为整数的情况下要求首系数为 1。另外顺便说一下：首系数为 1 的代数方程有一个专门名称，叫做首一代数方程（monic algebraic equation）。

自动满足的。另外要提醒读者注意的是，有些文献在环的定义中还去除了乘法结合律，在这种定义下满足乘法结合律的环（即普通定义中的环）被称为结合环（associative ring）。由一个数域 K 中的所有代数整数构成的环就叫做该数域的整数环。作为一个例子，如果数域是有理数域，则可以证明代数整数正好就是普通整数（事实上，对任意数域，一个代数整数如果是有理数，它就必定是一个普通整数），而整数环则恰好就是全体整数的集合，即整数集。

说完了整数环，再说说整数环的“理想”。这“理想”当然绝不是中国大陆读者们从小耳熟能详的“无产阶级革命理想”之类的东西，而是一个不折不扣的数学概念。这个概念也是戴德金提出的，是环的一种子集，是对德国数学家恩斯特•库默尔（Ernst Kummer, 1810-1893）早些时候提出的一个叫做“理想数”（ideal number）的概念的推广（其名称也由此而来）。对于我们所讨论的情形来说，理想是整数环的一个子集，对加法、减法和乘法封闭，包含零元素，并且它的任意元素与整数环的任意元素的乘积仍在该子集内 [注 34.6]。从某种意义上讲，理想这个概念跟“0”这个概念有一定的相似性，因为 0 乘以任何数仍然是 0，与理想所满足的“它的任意元素与整数环的任意元素的乘积仍在该子集内”相似。事实上，以 0 为唯一元素的子集确实是任何环的理想，称为零理想（zero ideal），而理想这个概念与 0 之间的相似性，则可以用来对环中的元素进行约化，即通过把理想视为广义的 0，把通常建立在两个元素之差等于 0 基础上的元素相等概念中的 0 换成理想，而对环中的元素进行分类（大家很快就会看到一个例子）。一个环的理想是不唯一的（否则戴德金 ζ 函数的级数表达式中对理想 I 的求和就没什么意义了），比如对于整数集（即有理数域的整数环）这一特例来说，所有形如 $\{\cdots, -2n, -n, 0, n, 2n, \ldots\}$（$n$ 为非负整数）的集合都是理想（请读者们依据理想的定义予以验证），这种集合通常被记为 nZ（Z 是表示整数集的符号），整数集的所有理想

> **注 34.6**
>
> 对于一般情形，由于环上的乘法未必满足交换律，因此在理想的定义中需区分左乘积与右乘积，相应的理想也有左理想 (left ideal) 与右理想 (right ideal) 之分。

都具有这种形式。

最后要介绍的是理想的“绝对范数”。我们刚才说过，从某种意义上讲，理想这个概念跟“0”这个概念有一定的相似性。这一点，连同整数集的理想是 nZ（n 为非负整数）这一结果，使我们联想起第 32 节中介绍过的模算术，因为一个以 n 为模的模算术的基本特点就是 n 具有 0 的算术性质——比如在以 12 为模的模算术（即刻度数目为 12 的高斯时钟这一特例）中，12 具有 0 的算术性质（参阅 [注 32.2]）。事实上，不仅 n，所有等于 n 整数倍的数，即形如 $\cdots, -2n, -n, 0, n, 2n, \ldots$ 的数（也就是理想 nZ 中的所有元素），在以 n 为模的模算术中都具有 0 的算术性质，而任意两个其差等于这种数（也就是属于理想 nZ）的数则被视为相等，这正是我们上面所说的用理想来对环中的元素进行约化的一个例子。一般地讲，用理想对一个环中的元素进行约化类似于模算术的推广，即将两个数的相等定义为其差属于该理想。那么什么是一个理想的绝对范数呢？它就是用该理想对环中的元素进行约化后不同元素的数目。对于整数集的理想 nZ 这一特例来说，约化后的不同元素只有 n 个，即 $0, 1, \cdots, n-1$（这也正是相应的高斯时钟的刻度数目），因此该理想的绝对范数是 n。

这样，我们就走马观花般地完成了对戴德金 ζ 函数的级数表达式的介绍。不仅如此，在介绍的过程中——不知读者们有没有意识到——我们其实已完成了对 K 为有理数域这一特例下戴德金 ζ 函数的计算！计算的结果是什么呢？让我们来挑明一下：

- 首先，在介绍整数环时我们说过，有理数域 K 的整数环恰好就是整数集；
- 其次，在介绍理想时我们说过，整数集的理想 I 全都是形如 nZ 的集合；
- 最后，在介绍绝对范数时我们说过，理想 nZ 的绝对范数是 n。

把这些结果合并起来，我们可以看到，对于 K 为有理数域这一特例，戴德金 ζ 函数中对非零理想 I 的求和实际上是对正整数 n 的求和（因为 n=0 所对应的是零理想，从而被排除），而相应的绝对范数 $N(I)=n$，因此戴德金 ζ 函数的级数表达式可以写成（其中数域 K 的符号被换成了有理数域的符号 Q）：

$$\zeta_Q(s)=\sum_n n^{-s} \quad (\mathrm{Re}(s)>1) 。$$

这个表达式大家一定认出来了，它就是普通黎曼 ζ 函数的级数表达式 p- 级数。因此，$\zeta_Q(s)=\zeta(s)$，这表明黎曼 ζ 函数是戴德金 ζ 函数的特例，而戴德金 ζ 函数与狄利克雷 L- 函数一样，是黎曼 ζ 函数的推广。与后两者一样，戴德金 ζ 函数也可以写成类似欧拉乘积公式的连乘积表达式：

$$\zeta_K(s)=\prod_P\left[1-N(P)^{-s}\right]^{-1}。$$

其中连乘积所针对的是所谓的“素理想”（prime ideal），通常表示为 P。这里我们不幸再次遇到了“链式反应”，即“素理想”这一概念。什么是素理想呢？对于我们所讨论的情形来说，它是这样一种理想，如果整数环中的两个数的乘积在该理想之中，那么两个数中至少有一个数本身就在该理想中。对于有理数域的整数环——即整数集——来说，一个理想 nZ 为素理想当且仅当 n 为素数（这一点的证明十分容易，请读者们自己完成）。显然，在这种情况下，上述连乘积公式完全等同于欧拉乘积公式（因为对素理想 P 的求积就是对素数 p 的求积）。

当然，以上介绍的还只是戴德金 ζ 函数在 $\mathrm{Re}(s)>1$ 上的级数表达式。不过与狄利克雷 L- 函数一样，它也可以被解析延拓为整个复平面上的亚纯函数，而且也满足类似于黎曼 ζ 函数所满足的函数方程。这些结果是德国数学家（又是德国数学家，本节几乎从头至尾都在介绍德国数学家的成果）Erich Hecke（1887-1947）所证明的。不仅如此，戴德金 ζ 函数的零点也同样有平凡与非平凡之分，非平凡零点全都位于 $0<\mathrm{Re}(s)<1$ 的带状区域（即 critical strip）内。有了这些结果，扩展黎曼猜想的表述也就一目了然了，那就是：

> 扩展黎曼猜想：戴德金 ζ 函数的所有非平凡零点都位于复平面上 $\mathrm{Re}(s)=1/2$ 的直线上。

注 34.7

Grand Riemann Hypothesis 似乎也尚无标准中译名，并且如 [注 34.4] 所说，有时也被混同于 Generalized Riemann Hypothesis（广义黎曼猜想）。“大黎曼猜想”这一名称系本文作者自拟的译名。

由于戴德金 ζ 函数是黎曼 ζ 函数的推广，因此扩展黎曼猜想也显然是黎曼猜想的推广，从而是“豪华版”的。

从上面的介绍中我们看到，广义黎曼猜想与扩展黎曼猜想作为普通黎曼猜想的推广，是建立在对黎曼 ζ 函数的两种不同推广之上的，前者是狄利克雷 L- 函数，后者则是戴德金 ζ 函数。我们还看到，无论狄利克雷 L- 函数还是戴德金 ζ 函数，都与普通黎曼 ζ 函数有着极大的相似性。这种令人瞩目的相似性也许会启示读者问这样一个问题，那就是这些彼此相似的函数是否可以被统一起来，纳入一个更宏大的框架中，成为一类更广泛的函数的特例呢？这是一个好问题，它的答案是肯定的。事实上，狄利克雷 L- 函数与戴德金 ζ 函数都是一类被称为自守 L- 函数（automorphic L-function）的涵盖面更广泛的函数的特例。大家也许还会进一步问：自守 L- 函数是否也有相应的“豪华版”黎曼猜想呢？答案也是肯定的，这种涵盖面更广泛的函数也有一个“豪华版”的黎曼猜想，堪称是“史上最豪华”的黎曼猜想，它的名字很气派，叫做“大黎曼猜想”（Grand Riemann Hypothesis）[注 34.7]。不过，自守 L- 函数这一概念所牵涉的“链式反应”十分剧烈，而建立在这一概念之上的大黎曼猜想的应用却极少（这种应用的多寡主要体现在有多少数学命题以假定其成立为前提），我们就不详加介绍了。在这里，我们只把大黎曼猜想的内容叙述一下（其实不叙述大家想必也不难猜到），那就是：

> 大黎曼猜想：自守 L- 函数的所有非平凡零点都位于复平面上 $\mathrm{Re}(s)=1/2$ 的直线上。

当然，这里的“非平凡零点”仍是指位于 $0<\mathrm{Re}(s)<1$（即 critical strip）内的零点。大黎曼猜想包含了普通黎曼猜想、广义黎曼猜想、扩展黎曼猜想、以及若干有名字或没名字的其它“豪华版”黎曼猜想为其特例，它若能被证明，则黎曼猜想这一研究领域几乎就被一锅端了。不过从目前的情况来看，我们距离这一天还差得很远。事实上，别说是大黎曼猜想，有关自守 L- 函数的许多简单得多的性质，比如它的解析延拓及函数方程等，也都还是未被普遍证明的东西。

Riemann

35 未竟的探索

我们的黎曼猜想漫谈到这里就接近尾声了。在过去的一个半世纪里，无数数学家从各种角度为探索这一猜想付出了艰辛的努力，但可惜的是，直到今天它仍是一个未被证明（或否证）的猜想，对这一猜想的探索迄今仍是向前延伸着的一条未竟的征途。

在数学领域中，超过一个半世纪未能解决的猜想当然不止黎曼猜想一个，比如著名的费马猜想（即如今的“费马大定理”）自提出后隔了超过三个半世纪才被解决；迄今尚未被证明（或否证）的哥德巴赫猜想（Goldbach Conjecture）也已存在了两个半世纪以上，黎曼猜想的历史与它们相比还差得很远。但在所有高难度的数学猜想中，若以它们跟其它数学分支之间的关系，乃至与物理学那样的自然科学分支之间的关系（这些关系在很大程度上决定了一个数学猜想的重要性）而论，黎曼猜想可以说是无与伦比的[注 35.1]。

与费马猜想或哥德巴赫猜想那种连中学生都能看懂题意的数学猜想不同，理解黎曼猜想是有一定“门槛”的，因为仅仅理解其表述就需要有一些复分析方面的知识。由于这一特点，这一远比费马猜想和哥德巴赫猜想更重要的数学猜想在公众中的知名度要远远低于后两者，也较少受到民科们的青睐——当然也绝非没有，但起码是不曾有任何机构收到过数以麻袋计的来信，声称自己证明（或否证）了黎曼猜想（费马猜想和哥德巴赫猜想都曾引发过此等“盛举”)。不过，尽管“杂音”相对较少，但在黎曼猜想那样艰深的数学猜想面前，无论多么精英的群体也难免会搞出意外事件来。我们在第 6 节中曾经介绍过一次那样的事件，即荷兰数学家斯蒂尔吉斯 (Thomas Stieltjes, 1856-1894) 声称自己证明了一个比黎曼猜想更强的命题，但后来却一直没有发表完整的“证明”，最终不了了之。在最近这十几年里，也出现过两次值得一提的事件。在结束我们的漫谈之前，我们先来聊聊这两次事件。

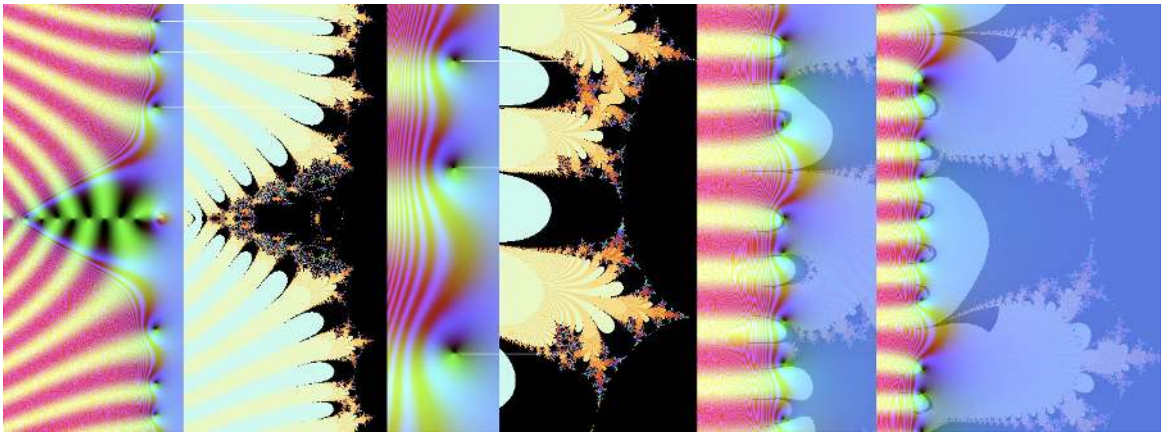
这两次事件中的第一次始于二十世纪九十年代中期，核心人物是法国数学家阿兰•科纳（Alain Connes，1947-）。科纳是一位极有声望的数学家，曾获得过 1982 年的菲尔兹奖，并且是非对易几何（Noncommutative geometry）的主要奠基者。对于小道消息相对匮乏的数学界来说，这样一位著名人物开始研究黎曼猜想的消息自然是非同小可的消息。因此早在科纳正式发表这方面的文章之前，有关他正在研究黎曼猜想的小道消息就在圈内不胫而走，并引起了很多人的兴趣。扑灭小道消息的最好手段无疑就是用“官方消息”取而代之。1997 年早春，这样的“官方消息”正式出炉了：科纳决定到普林斯顿高等研究所，向包括塞尔伯格在内的黎曼猜想研究领域的若干巨头报告自己的工作思路。

科纳的思路确实颇有来头：既继承了自二十世纪七十年代之后颇受瞩目的希尔伯特 - 波利亚猜想的路子，也借鉴了韦伊和格罗滕迪克等人在研究“山寨版”黎曼猜想的过程中发展起来的代数几何方法，甚至还用上了科纳自己参与开创的“看家本领”：非对易几何。这几条路子每一条都很吸引眼球，科纳居然将它们一起融入到自己的研究之中，确实是不简单，也很对得起“观众”们的热情。但来到普林斯顿高等研究院听报告的那几位巨头却并不是看热闹的人，那些令常人眼花缭乱的东西，在他们锐利思维的解剖下，被一一还原为冰冷的逻辑，并且显出了漏洞，那就是科纳所报告的方法存在一个“先天”不足，它无法发现不在临界线上的非平凡零点！这个漏洞是很严重的，因为科纳的方法如果无法发现不在临界线上的非平凡零点，那它就会营造出一个错觉，让人误以为所有的非平凡零点全都在临界线上。这就好比有一批不是蓝色就是红色的小球，你若戴上一副只能看见其中一种颜色的滤光镜去看它们，就有可能误以为所有小球都是那种颜色的。因此，普林斯顿高等研究院的那几位巨头在科纳报告之后所给出的最正面的表示也只是审慎的鼓励，即认为科纳确实取得了一些进展，但与黎曼猜想的

注 35.1

另一个衡量数学猜想重要性的指标，是看在研究该猜想的过程中是否发展出有价值的数学手段。从这个角度上讲，黎曼猜想也是无与伦比的。比方说，费马大定理的证明就在一定程度上受益于因研究“山寨版”黎曼猜想而发展起来的代数几何手段。

Riemann



由黎曼 ζ 函数零点及其迭代过程生成的彩图

证明仍有相当距离[注 35.2]。

这一事件原本就到此为止了，没想到后来却闹出了一点新的意外。科纳的普林斯顿演讲之后不久恰好是西方社会一个最有趣的节日：“愚人节”。很多人在这一天（4 月 1 日）的习惯是互相开玩笑，试图对别人（通常是朋友）进行善意的愚弄，出席过科纳报告的巨头之一、1974 年菲尔兹奖得主蓬皮埃利（Enrico Bombieri, 1940-）（我们在第 14 节中曾提到过他）也不例外，他给一位朋友发去了一封“愚人节”邮件，宣称有位年轻的物理学家受科纳报告的启发，终于完成了黎曼猜想的证明！由于当时数学界很多人正四处打探和传播着有关科纳工作的消息（尤其是与科纳的普林斯顿报告有关的消息），蓬皮埃利这权威之人发自权威之地的消息一出，收到邮件的数学家朋友当场就信以为真地把它传了出去。这消息传得很快，甚至连已从普林斯顿回到法国的科纳本人都很快就知道了，让他颇为不快。

当然，有道是“谣言止于智者”，一个“愚人节”玩笑在智者云集的数学家群体中是不会惹出太大动静的，不久之后有关科纳报告导致黎曼猜想被证明的消息就平息了下去。但这个误传的消息似乎将数学家们对科纳的兴趣透了支，以至于后来无论是科纳 1999 年正式发表的论文，还是他在同一方向上的进一步研究，都没有再引起当初那样的关注。不过科纳本人对此看得很开，他曾经表示：

> 对我来说，数学一直是一所教人谦虚的最好学校。数学之所以有价值，主要就是因为那些极其困难的问题，它们就像数学的喜玛拉雅山。登顶是极其困难的，甚至必须为之付出代价，但千真万确的是，如果我们能登顶，那里的风景将是奇妙的。

对于那“必须为之付出”的代价，他在 2000 年发表的一篇文章的开头曾经作过这样的表述[注 35.3]：

> 按我第一位老师 Gustave Choquet 的说法，公开面对一个著名的未解决问题是一种冒险，因为别人将更多地记住你的失败而不是其它。

尽管如此，科纳仍选择了冒险攀登数学的喜玛拉雅山，因为：

注 35.2

据说在对有关黎曼猜想的研究进行评述时有一种比较“规范”的总结词就是：“这确实是一个重要进展，但如何才能证明黎曼猜想仍不是很清楚”，普林斯顿高等研究院的巨头们对科纳的评价与那种总结词颇有异曲同工之意。

注 35.3

科纳这段话中提到的 Gustave Choquet（1915-2006）是一位著名的法国数学家，在分析与拓扑等领域作出过重要工作。

Riemann

> 在到达某个年龄之后，我意识到“安全地”等待自己生命的终点同样是一种让自己失败的选择。

有关科纳的事件大体就是如此，他目前仍在攀登，虽然已不再是镁光灯下的焦点，我们仍衷心祝愿他取得进展。

在科纳的事件之后又过了几年，2004 年，另一个事件发生了：美国普度大学（Purdue University）的数学教授路易斯 • 德勃良地（Louis de Branges, 1932-）在互联网上张贴了一篇长达 124 页的论文，宣称自己证明了黎曼猜想！由于在此前的 2000 年 5 月，美国克雷数学研究所（Clay Mathematics Institute）已经为七个所谓的“千禧年问题”（Millennium Problems）设立了每个一百万美元的巨额奖励，而黎曼乃是其中排名第四的问题[注 35.4]。因此德勃良地的宣称立刻引起了一些媒体的关注。

但数学界对此事的反应却相当冷淡。

为什么呢？这还得从德勃良地是一位怎样的数学家说起，简单地讲，德勃良地堪称是一位史上最离群的数学家。数学界离群的人物为数并不少，但其他数学家再怎么离群，至多是在人际关系上离群，德勃良地却连数学工具也是离群的，他是一个几乎只用自创的数学工具进行研究的家伙，而他自创的数学工具除了他本人和为数有限的几位学生外，几乎无人通晓。这种超乎寻常的离群性大大孤立了德勃良地，他在数学界的人缘连他自己也不得不承认是很惨的。更糟糕的是（其实这才是重点），他还是一个工作很粗心的家伙，甚至颇有民科气质，经常宣称自己证明了重大数学猜想，其中包括对证明黎曼猜想的多次错误宣称，只不过在“千禧年问题”出炉之前媒体不太关注而已。当然，德勃良地如果真是一个民科，我们就不会在这里谈及他的事情了。此人的恼人之处就在于他虽然很有民科气质，却也真刀真枪地作出过一次正确的宣称，而且所解决的还是一个有着几十年历史的著名猜想：比贝尔巴赫猜想（Bieberbach conjecture）——那猜想如今已被称为了德勃良地定理（de Branges's theorem）。

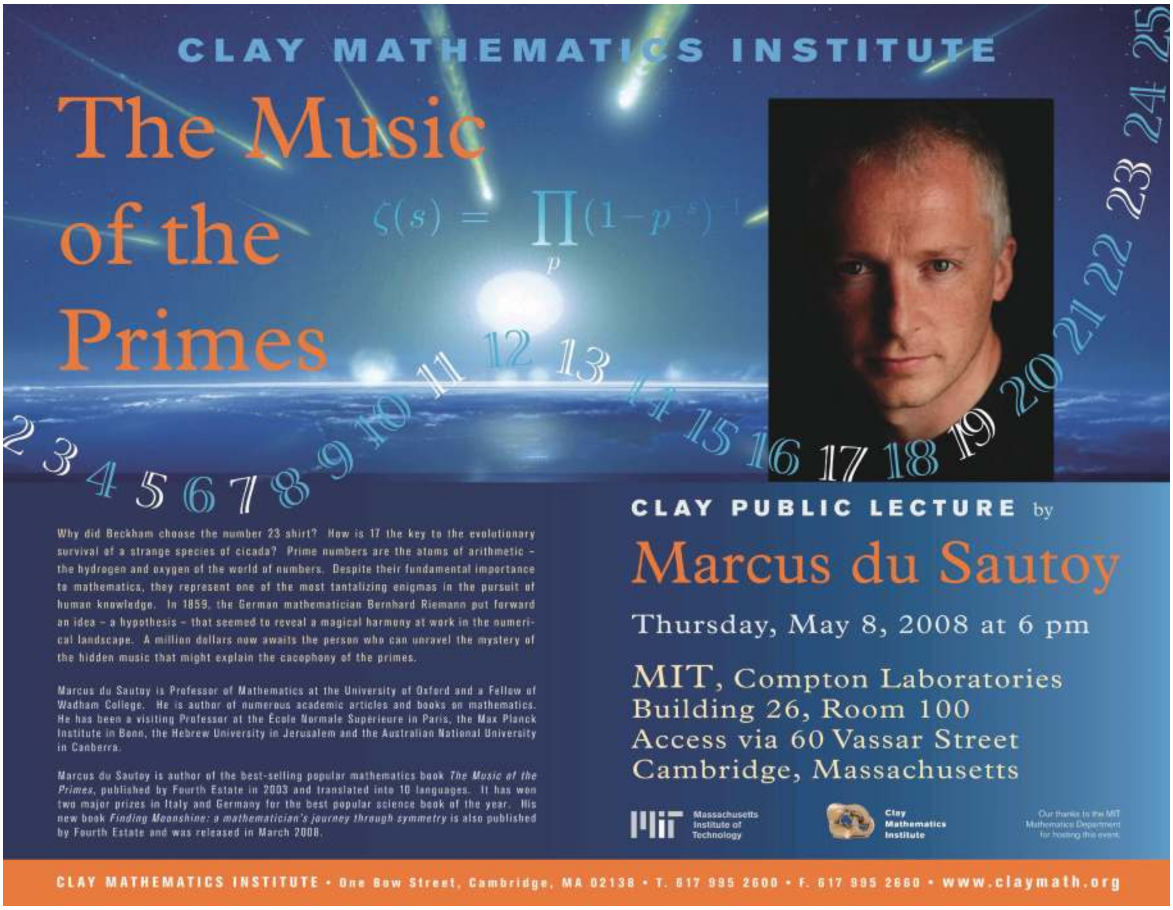
照说有过此等业绩、甚至有数学定理以其名字命名的数学家是不该受到如此冷遇的。而且德勃良地当年对比贝尔巴赫猜想的证明本身也是在有过几次错误宣称之后，才得到公认的。这似乎在从历史角度启示人们应该对他有关黎曼猜想的证明给予一点关注（或同情？）。可惜的是，德勃良地在犯错方面的名声实在太狼藉了，以至于就连对比贝尔巴赫猜想的证明也不够份量来抵消了。比如塞尔伯格就毫不客气地嘲笑说德勃良地曾经犯过所有类型的错误，他对比贝尔巴赫猜想的证明只不过说明他还犯下了“做对了”的错误（made the mistake of being right）。

德勃良地的“证明”受到数学界的冷遇还有两个重要原因：其中一个就是我们前面所说的，他几乎只用自创的数学工具进行研究，而那工具除他本人和几位学生外，几乎无人通晓。这给人们检验他的工作造成了巨大困难。当年他对比贝尔巴赫猜想的证明之所以被接受，乃是几位苏联数学家花费了几个月的时间研读他的证明，并对之进行简化的结果。而此次有关黎曼猜想的文章比当年的证明还要复杂得多，他的名声却比那时更差了，愿意花时间去研读他文章的人自然就更少了。而且要命的是，他的论文还引用了过去几十年他所撰写的其它一些无人问津的论文，从而对读者来说更是“不可承受之重”。另一个也许更致命的原因则是，虽然德勃良地的“证明”受到了数学界的冷遇，但毕竟还是有个别数学家对他的论文进行了粗略光顾。不幸的是，光顾的结果却是发现了缺陷，从而进一步坐实了他的恶劣名声。另外还有人注意到他的论文中有一些“前言不搭后语”的东西，比如序言里反复提到量子力学，正文中却完全没有呼应；文献中列举了赫尔曼 • 外尔（Hermann Weyl）的一部著作，正文中也根本没有引用，这一切都让人深切地感觉到黎曼猜想被这位已年过七旬的老人所证明实在是不太可能的事情。也许是因为缺陷遭到曝光的缘故，德勃良地后来撤掉了最初版本的论文，但他并未就此认栽。他的论文几经修改后，口气反而越改越大，目

注 35.4

“千禧年问题”的排序不是依照问题的重要性，而是依照问题英文名称的长度进行的。这种排序的目的是使列举“千禧年问题”的新闻稿看起来更加有序，从而更能吸引眼球。

Riemann



《素数的音乐》作者在美国克雷研究所的演讲广告。

前所宣称的结果甚至比我们在上节中介绍过的“豪华版”黎曼猜想之一的广义黎曼猜想还略强一些。可惜他这第 N+1 次的“狼来了”故事是真的再也无人问津了，更没有学术刊物愿意发表。

这就是有关德勃良地的事件。除德勃良地外，还有一些其他人也宣称过自己“证明”或“否证”了黎曼猜想，他们的论文往往只有寥寥几页或十几页，引起的反响则基本是零，就按下不表了。

接下来我们再聊点趣话。读者们也许还记得，在一百多年前的十九世纪末，法国数学家哈达玛（Jacques Hadamard）和比利时数学家瓦利 - 普桑（Vallée-Poussin）取得了自黎曼提出猜想三十多年以来的第一个实质性进展，即将非平凡零点的分布范围由 0≤Re(s)≤1 缩小到了 0<Re(s)<1（参阅第 7 节）。很巧的是，这两人在数学家之中都以长寿著称：哈达玛活到 98 岁，瓦利 - 普桑活到 96 岁。数学界后来流传起了一个说法，那就是如果有人证明了黎曼猜想，他就会不朽——不仅是抽象意义上的不朽（那是毫无疑问的），而且是实际意义上的不朽（即长生不老），因为哈达玛和瓦利 - 普桑这两人仅仅取得了一点点进展，就都活到了将近百岁。当然，这个传说看来是没有关怀到另一些也取得过一点点（有的甚至还不止一点点）进展的数学家，他们可就没那么好命了，比如证明了波尔 - 兰道 定理（参阅第 22 节）的波尔（Harald Bohr）和兰道（Edmund Georg Landau）就分别只活了 63 岁和 61 岁。比上述传说更厉害（或更歹毒）的传说则是 Andrew M. Odlyzko（1949-）（我们在第 16 节中介

Riemann

绍过此人）提出的，是一个与上述传说恰好“互补”的说法，即谁要是否证了黎曼猜想，他就会立刻死去！ Odlyzko 甚至开玩笑说其实黎曼猜想已经被否证了，只不过那个否证了黎曼猜想的倒霉蛋没来得及发表文章就死去了。

这些传说当然只能为我们的漫谈增添点趣话，不过，证明或否证黎曼猜想的人会“不朽”或“速死”虽是无稽之谈，黎曼猜想的极度艰深倒确实有可能对数学家的健康产生影响。事实上，数学界的确有人认为黎曼猜想的极度艰深有可能对几位数学家的精神异常起到过一定作用（不过证据都不是很强）。这方面比较著名的例子有两个：一个是广为流传的传记作品《美丽心灵》的主角、美国数学家约翰•纳什。二十世纪五十年代后期，这位已在博弈论等领域做出过重要工作的数学家对黎曼猜想产生了兴趣。不久之后，他开始宣称自己找到了黎曼猜想的证明。而数学界此时流传的却是一些有关他罹患精神分裂症的消息。这消息很快得到了证实：1959 年，纳什在哥伦比亚大学作了一次演讲。这次据说意在宣布黎曼猜想证明的演讲实际上成为了公开展示纳什精神分裂症的场合，他的演讲几乎达到了语无伦次的程度，到场听讲的数学家们只有用平时很少使用（对著名同事更是几乎从不使用）的词汇——比如“灾难性的”、“完全是胡扯”等等——才能形容那次演讲的糟糕。由于纳什罹患精神分裂症与他研究黎曼猜想发生在同一时期，一些人相信黎曼猜想对他的病症发展有可能起到过推波助澜的作用。

另一个例子的主角是我们在第 33 节中提到过的、曾经为证明“山寨版”黎曼猜想（即韦伊猜想的一部分）作过重要铺垫工作的格罗滕迪克。这位在代数几何等诸多领域有着卓越贡献的数学家据说也有可能是因为研究黎曼猜想的缘故，使得精神出现异常，自上世纪七十年代开始就基本退出了学术界，后来发展到“离家出走”，几乎从世界上消失了。人们猜测他目前住在法国南部。关于他在做什么，则众说纷纭，有人说他正在研究一种新的经济学，有人说他在牧羊，而据个别自称与他仍有过交往的数学家说，他已沉溺于对恶魔（devil）的想象不能自拔，比如他相信是恶魔把本应该是每秒 30 万公里的数值优美的光速变成了很难看的每秒 299,887 公里（细心的读者也许注意到了，这个数值本身就是错的，实际数值应为每秒 299,792.458 公里，不知是格罗滕迪克记错了还是数学家传错了）。格罗滕迪克失踪十几年后，很多人都已搞不清他是否还健在，他却忽然于 2010 年 1 月给自己以前的学生、法国数学家 Luc Illusie（1940-）写了封亲笔信，宣布自他“消失”后所出版或再版的他的一切文字都是未经许可的，那些文字在他有生之年不得再版，已收录了那些文字的图书馆也必须将之撤除。他的这一信件被公布后，一些提供那些文字的网站已对有关内容作了撤除。这个要求对数学界是一件不幸的事情，因为他的很多文字，比如著名的《代数几何基础》（Éléments de géométrie algébrique—— 简称 EGA）和代数几何讨论班资料（Séminaire de Géométrie Algébrique du Bois Marie——简称 SGA），都早已是极重要的资料，如果不能再版或不能被图书馆收录的话，后人将会越来越难看到它们。

黎曼（Bernhard Riemann）的墓碑

格罗滕迪克这一例子，尤其是研究黎曼猜想有可能对其精神异常有过影响这一猜测来自于 Marcus du Sautoy（1965-）的《素数的音乐》（The Music of Primes）一书。该书作者是牛津大学的数学教授，为撰写此书亲自采访了很多数学家，其中包括本系列提到过的 Bombieri、Odlyzko、te Riele、Selberg、Zagier 等人，是一位比较可信的作者。不过格罗滕迪克这一例子有些例外，我虽进行了引述，对其可靠性却不无怀疑。首先是格罗滕迪克的精神是否异常，不像 Nash 的例子那样清楚，因为他自“消失”之后与社会的联系微乎其微，有关他的很多说法都只是传闻。其次，即使他的精神确实异常，那是否是研究黎曼猜想所致，du Sautoy 没有给出证据，我在其它资料中也未看到过对这一说法的支持。从行为上看，格罗滕迪克的异常始于 1970 年离开法国高等科学研究院（Institut des Hautes Études Scientifiques——简称 IHÉS）一事。但一般认为（du Sautoy 自己也持此说）此事乃是他的极端和平主义思想所致，他是因为发现 IHÉS 的经费有一部分来自军方之后，才愤然离开了这一堪称自己学术黄金之地的研究所。在那之前，格罗滕迪克的研究课题之一是韦伊猜想，他曾试图用一系列所谓的“标准猜想”(Standard Conjectures) 来证明韦伊猜想中的“山寨版”黎曼猜想部分。他在这方面的努力遭到了挫折（“标准猜想”直到今天仍未被证明），但那挫折虽在时间上与他自 1970 年开始的行为变化有些巧合，却未必有因果联系，而且那挫折对他的精神造成过多大影响也并不清楚。

写了这么多有关黎曼猜想的故事，介绍了这么多有关黎曼猜想的进展，有一个问题似乎不能不提一下——而且那想必也是读者们感兴趣的问题，那就是黎曼猜想将会被证明是正确的呢，还是会被证明为错误（即否证）？可惜的是，这个有关黎曼猜想“前途命运”的问题是一个谁都能提出，却没有人能够回答的问题，数学家们对此也各有各的倾向而毫无共识。

有些数学家坚信黎曼猜想是正确的，比如我们在第 14 节中提到过的那位输掉了葡萄酒的查基尔（Don Zagier, 1951-）。他相信黎曼猜想的理由很“纯朴”，那就是认为数值证据已经足够强大了——读者们想必还记得，他是因为有人验证了黎曼 ζ 函数前三亿零七百万个零点都在临界线上而输掉葡萄酒的。这个纪录如今早已被打破，二零零四年十月，法国人 Gourdon 与 Demichel 已经验证了黎曼 ζ 函数前十万亿（10^{13}）个零点都在临界线上。不仅如此，我们在第 16 节中还介绍过，Odlyzko 曾经验证过第 10^{22} 和 10^{23} 个零点附近的几百亿个零点也全都在临界线上。这些证据都远远强于使查基尔满意的证据。可见支持黎曼成立的数值证据确实很强大。但可惜的是，所有这些证据加在一起，也无法成为让人们信服黎曼猜想的可靠理由。其原因不仅在于从逻辑上讲再多的数值证据对于一个包含无穷多个例的猜想来说都是微不足道的，而且也因为在数学上我们已经遇到过这样的例子，即一个数学命题的反例出现在比上述所有数值证据都强得多的证据之外。那例子就是我们在第 3 节中提到过的、被李特尔伍德（John Littlewood）所否证了的关于 $\mathrm{Li}(x)-\pi(x)>0$ 的猜测。对于迄今所有被验证过的情形，$\mathrm{Li}(x)-\pi(x)>0$ 都成立，但李特尔伍德却运用分析的力量，不仅证明它不成立，而且证明了它会被违反无穷多次！那么所有验证过的情形说明什么呢？说明虽然有无穷多个 x 违反 $\mathrm{Li}(x)-\pi(x)>0$，但其中哪怕最小的 x 也大得异乎寻常 [注 35.5]。事实上，我们直到今天也不知道这个最小的 x 究竟有多大，目前对它的估计约为 10^{316}。这个数字如果用中文写出来的话，是：一万亿……亿（此处作者略去三十七个字——别想歪了，大家知道略去的是什么字）。与这个数字相比，我们对黎曼 ζ 函数非平凡零点的数值验证简直差得太远了。假如黎曼猜想的反例也出现在那样的地方（即比如出现在第 10^{316} 个零点的附近），那我们再算上几辈子也未必能碰到数值反例。因此，有关黎曼猜想的数值证据虽然不容忽视，说服力却是很有限的。

当然，除了数值证据外，我们还有许多有关黎曼猜想的解析证据，比如第 28 节中提到的康瑞（Brian Conrey）所证明的 2/5 的非平凡零点在临界线上。可惜这也远远不够（连一半都不到嘛）。支持黎曼猜想的其它理由还包括了一些在假定黎曼猜

注 35.5

这个最小的 x 被哈代称为 Skewes 数（Skewes' number），因为最早对它进行数值估计的是李特尔伍德的学生、南非数学家 Stanley Skewes（1899–1988）。

Riemann

想成立的基础上被证明过的数学命题后来被发现不假定黎曼猜想的成立也能被证明，这表明黎曼猜想与那些命题、或者说与数学的其它部分有很好的相容性。此外，我们在第 33 节中介绍过的“山寨版”黎曼猜想的成立也被认为是支持黎曼猜想的一条很强的理由。

相信黎曼猜想的数学家们各有各的理由，不相信黎曼猜想的数学家们则只要一条理由就够了，那就是：所有支持黎曼猜想的理由都不是证明。在数学上，这是一条打不倒的理由。当然，个别数学家会有自己更独特的理由，比如我们在第 9 节中提到的那位曾在黎曼猜想研究上作出过重大成就，后来却表示“假如我们能够坚定地相信这个猜想是错误的，日子会过得更舒适些”的李特尔伍德不相信黎曼猜想的理由是“一个长期不能解决的分析领域中的猜想通常会被发现是错误的，一个长期不能解决的代数领域中的猜想则通常会被发现是正确的”。由于黎曼猜想是一个“长期不能解决的分析领域中的猜想”，因此李特尔伍德认为它很可能是错误的。李特尔伍德没有为自己的理由列举具体的例子（起码我没查到），我想他对 $\mathrm{Li}(x)\text{-}\pi(x)>0$ 这一猜想的否证也许是他心目中的例子之一。但他这个理由其实也没什么说服力，比如我们上面提到过的被德勃良地所证明的比贝尔巴赫猜想就是一个几十年不能解决的分析领域中的猜想，结果却被证明是正确的。

除了上述这两种非此即彼的态度外，还有少数人由黎曼猜想的长期悬而未决联想到了著名的歌德尔不完备性定理（Gödel's incompleteness theorems），认为黎曼猜想也许是一个在现有分析体系内不可判定——即既不能证明其成立也不能证明其不成立——的命题。据说歌德尔本人就有过这种看法。不过，对于像黎曼猜想那样如果不成立就可以用明确的算法——即按虚部从小到大的顺序对零点进行逐一验证——来予以推翻的命题，如果真有人能证明它是一个不能证明其不成立的命题（有点拗口），实际上等于表明它是成立的——因为否则的话只要用那个算法，原则上总可以验证到使黎曼猜想不成立的第一个反例，从而证明其不成立。因此如果黎曼猜想真的不可判定，那实际上是表明它成立。

在本系列的最后，让我们“饮水思源”，一同去看一眼黎曼的墓碑，这位伟大的数学家只度过了 39 年 10 个月零 3 天的短暂人生，就于 1866 年 7 月 20 日在意大利的一座湖畔小镇去世了。据他生前挚友戴德金的描述，黎曼直到去世前的那一天，仍坐在一棵果树下进行着数学探索，当那最后的时刻来临时，“他的眼睛很平静，没有一丝挣扎和临终前的抽搐，仿佛他是在饶有兴致地观看着灵魂与肉体的分离”。黎曼去世后一度被葬在当地一座教堂的墓地里，可惜那墓穴却在后来的一次教堂地产的重组中遭到了损毁，如今保留下来的只有一块墓碑，嵌在离原址不远处的一堵墙上。

好了，亲爱的读者，我们的黎曼猜想漫谈到这里就正式结束了。从 2003 年 11 月写下第 1 节，到今天完成最后一节，这个系列前前后后已持续了八年多的时间，虽然有关黎曼猜想的探索还远未结束，我却要跟大家说再见了。当然，如果在我有生之年黎曼猜想被数学界公认得到了解决，我一定会续写这个系列的，但现在请允许我先说一声——

再见！

完结

2012 年 1 月