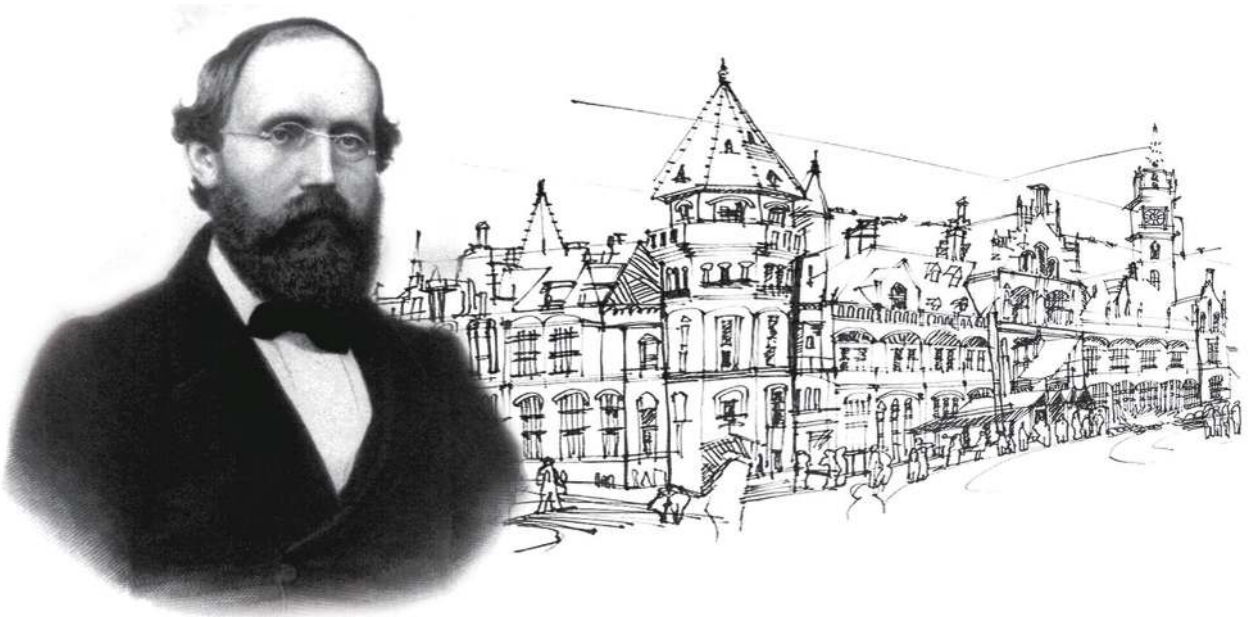
Riemann



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。

Riemann

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 $q=p^n$（$n=1, 2, 3, \ldots$）[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 $a\times?=1$ 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}（$m=1, 2, 3, \ldots$）。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}（$m=1, 2, 3, \ldots$）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。

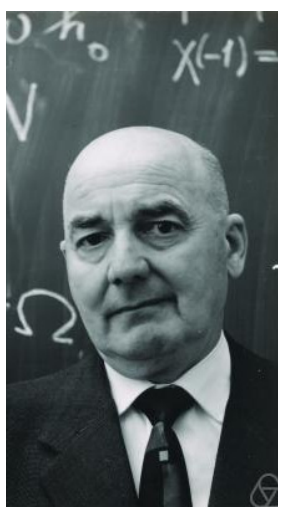
Riemann 33

“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}（$m=1, 2, 3, \ldots$）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}（$m=1, 2, 3, \ldots$）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 $\mathrm{Re}(s)=1/2$ 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，不过两人所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

Riemann

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）。

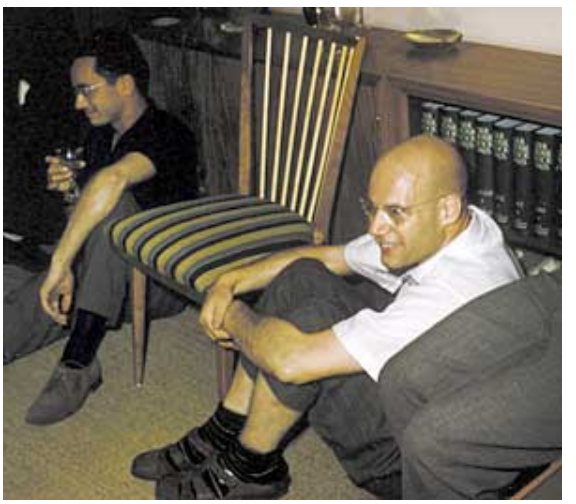
韦伊猜想包含了若干个命题，“山寨版”黎曼猜想是其中之一，并且从历史上讲是证明最为不易的一个。不过，韦伊猜想中的“山寨版”黎曼猜想的证明虽然困难，其由来却是对上述“山寨版”黎曼猜想的很直接的推广，即将上述猜想中的代数曲线推广为高维几何对象。这种高维几何对象有一个专门的名称，叫做代数簇（algebraic variety），它也是用代数方程（或方程组）来定义的，并且也可以定义在有限域上。与有限域上代数曲线的ζ函数完全类似，也可以引进有限域上代数簇的ζ函数。对于这种ζ函数，也存在“山寨版”的黎曼猜想，我们称其为有限域上代数簇的“山寨版”黎曼猜想，它是韦伊对有限域上代数曲线的“山寨版”黎曼猜想的推广，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 $\mathrm{Re}(s)=1/2$ 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。