综合报告

Andrew Wiles 的绝妙证明

Henri Damon

众所周知，Fermat (费马) 曾宣称发现了 Fermat 大定理的 “一个真正绝妙的证明”, 但是由于他持有的 Diophantus (丢番图) 所著的《算术 (Arithmetica) 》一书的页边空白太小而没有记录下来. 虽然后人失去了这个证明 (如果它真的曾经存在过), 但是 Andrew Wiles (怀尔斯) 的绝妙证明已经面世 20 多年了，并且目前已经为他赢得了 Abel (阿贝尔) 奖. 据这个奖项的颁奖辞称, Wiles 应该得到这样的认可, “因为他利用关于半稳定椭圆曲线的模性猜想给出了 Fermat 大定理令人震撼的证明，开创了数论的新时代. ”

几乎没有人面对 Fermat 大定理的诱惑会无动于衷. 它是一个根源于古希腊数学，并且简单得以至于一个初学者 (如在当地公共图书馆书架上浏览的 10 岁大的 Andrew Wiles) 都可以理解和欣赏的谜题，但是却经历了世界上最聪明的头脑长达 3 个多世纪的共同努力仍悬而未决. 在这段长期的历史过程中，Fermat 大定理成为巨额奖项，如 Wolfskehl 奖, 追逐的对象. 更重要的是, 它导致了一系列重大发现: Fermat 的无穷递降法, Kummer (库默尔) 的理想论，ABC 猜想，Frey 处理三元 Diophantus 方程的方法，Serre (塞尔) 关于模 p Galois (伽罗瓦) 表示的猜想， ...

即使没有与 Fermat 大定理貌似偶然的联系，Wiles 的模性定理仍是关于椭圆曲线的基本论断 (如，它在发表于本卷的 Karl Rubin (鲁宾) 文章中定理 2 证明中所起的关键作用就是一个例证), 也是 “Langlands 纲领 (朗兰兹 Program)” 的核心，而 “ Langlands 纲领” 是一个由结论和猜想构成的壮丽而宏伟的大厦，它支配着数论学家对于该领域的观点. 这一纲领也被称为数学的 “大一统理论”. 从一个挪威人的角度看，它把 Niels Hendrik Abel 的工作中出现的对象如椭圆曲线及与之伴随的椭圆积分和 Galois 表示与 Sophus Lie (李) 所开创的连续变换群的线性表示 (通常是无限维的) 联系起来. 这个报告关注 Wiles 的定理及其 “绝妙证明” 在 Langlands 纲领中的作用，以便证实颁奖辞的结束语：Wiles 的证明如何地开创了 “数论的新时代”, 并且继续对数学产生持续而深远的影响.

我们对于 Langlands 纲领的 “初级旅程” 只能是对全貌投以局部的并且无疑是片面的一瞥，这既反映了给一般读者讲述这个问题的固有局限性，也反映了作者的缺陷. 我们将从讨论 *Diophantus 方程* 入手引入 Langlands 纲领：为此，所谓 Diophantus 方程是指如下方程

$$\mathcal{X}: \quad P(x_1, \ldots, x_{n+1}) = 0, \tag{1}$$

译自：Notices of the AMS, Vol. 64 (2017), No. 3, p. 209–216, Andrew Wiles's Marvelous Proof, Henri Damon.
作者是 McGill 大学的 James McGill 数学讲座教授，和 CICMA 及 CRM 的研究员. 他的邮箱地址是 darmon@math.mcgill.ca.

其中 P 是关于变量 $x_1, \ldots, x_{n+1}$ 的整系数 (有时或是有理系数) 多项式. 对于任意环 F, 我们可以考察方程 (1) 在 F 中的解构成的集合 $\mathcal{X}(F)$. 尽管在我们的头脑中整数解的集合 $\mathcal{X}(\mathbb{Z})$ 和有理数解的集合 $\mathcal{X}(\mathbb{Q})$ 是最重要的, 但我们将会看到, 这项研究通过深刻而精妙的方式使得各个解集彼此产生了共鸣, 从而展示了巨大的魅力. Diophantus 方程包括 Fermat 方程 $x^d + y^d = z^d$, Brahmagupta-Pell (婆罗摩笈多 – 佩尔) 方程 $x^2 - Dy^2 = 1$, $D > 0$, 以及形如 $y^2 = x^3 + ax + b$ 的椭圆曲线方程, 其中 a, b 为有理数, 等等; 对于后者, 有理数解 (x, y) 是人们感兴趣的对象.

在处理 Diophantus 问题时, 首先研究它在一些 **较简单** (*simpler*) 的环 —— 如实数域和复数域这样的完备域 —— 中的解是有益的. 对于任意整数 $n \geq 2$, 由整数被 n 除的余数构成的集合

$$\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-1\} \tag{2}$$

上可以自然定义加减乘运算, 从而构成另一个特别简单的 **有限基数** (*finite cardinality*) 的数集. 如果 $n = p$ 是 **素数** (*prime*), 这个环甚至是一个域: 其上可以定义被非零元素除的运算, 就像熟知的有理数、实数, 或复数那样. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ 是域这一事实是对于素数的一个代数刻画, 也是大多数已知有效的素性检测和分解算法的基础. 除了在 Wiles 的工作中起到非常关键作用的同名理论 [1)] 外, Evariste Galois 的又一个伟大贡献在于: 对于任一个素数幂 p^r, 他发现了基数为 p^r 的域. 而这个域, 通常记为 $\mathbb{F}_{p^r}$, 并称为含有 p^r 个元素的 Galois 域, 在同构意义下它甚至是 **唯一的** (*unique*).

对于像 (1) 中的 Diophantus 方程 $\mathcal{X}$, 它在 $\mathbb{F}_{p^r}$ 上的解集

$$\mathcal{X}(\mathbb{F}_{p^r}) := \{(x_1, \ldots, x_{n+1}) \in \mathbb{F}_{p^r}^{n+1} |\ P(x_1, \ldots, x_{n+1}) = 0\} \tag{3}$$

的最基本的不变量当然是它的 **基数**

$$N_{p^r} := \#\mathcal{X}(\mathbb{F}_{p^r}). \tag{4}$$

序列

$$N_p, N_{p^2}, N_{p^3}, \ldots, N_{p^r}, \ldots \tag{5}$$

会遵循什么模式 (如果存在的话)? 这个序列可以整合为下面的生成级数

$$\sum_{r=1}^{\infty} N_{p^r} T^r \quad \text{或} \quad \sum_{r=1}^{\infty} \frac{N_{p^r}}{r} T^r. \tag{6}$$

由于技术原因, 最好考虑后一个级数的指数形式

$$\zeta_p(X; T) := \exp\left(\sum_{r=1}^{\infty} \frac{N_{p^r}}{r} T^r\right). \tag{7}$$

这个关于 T 的幂级数就是 $\mathcal{X}$ 在 $\mathbb{F}_p$ 上的 **ζ 函数** (*zeta function*). 它是整系数的, 并且具有下面的惊人性质:

1) 即 Galois 理论.—— 译注

(1) 它是关于 T 的 **有理函数** (*rational function*):

$$\zeta_p(\mathcal{X};T)=\frac{Q(T)}{R(T)}, \tag{8}$$

其中 $Q(T)$ 和 $R(T)$ 是关于 T 的多项式, (除有限个 p 以外) 其次数 **不依赖于** p (*independent of* p), 并且由复数域内的解集 $\mathcal{X}(\mathbb{C})$ 的形状 —— 复拓扑 —— 决定.

(2) 多项式 $Q(T)$ 和 $R(T)$ 在复数域范围内根的倒数的绝对值为 $p^{i/2}$, 其中整数 i 满足 $0\leq i\leq 2n$.

第 1 个论断 ——ζ 函数的有理性, 由 Bernard Dwork 于 1960 年代初证明 —— 是 Weil (韦伊) 猜想的一个关键部分. 20 世纪 40 年代提出的 Weil 猜想曾在算术几何领域掀起了一场革命, 促使了 Grothendieck (格罗滕迪克) 和他的学派在艾达尔 (étale) 上同调方面的发展. 第 2 个论断说的是复变函数 $\zeta_p(\mathcal{X};p^{-s})$ 的根都在实直线 $\Re(s)=i/2$ 上, 其中 i 同上; 这通常被称为关于有限域上 Diophantus 方程 ζ 函数的 Riemann (黎曼) 假设. 这个 Riemann 假设于 1974 年被 Pierre Deligne (德利涅) 证明, 这也是他于 2013 年获得 Abel 奖的主要成就之一.

N_p 的渐近表现可以引起对相应 Diophantus 方程的表现的洞察, 这一点正是 Birch (伯奇) 和 Swinnerton-Dyer (斯温纳顿 – 戴尔) 猜想背后的关键思想. 对于 Langlands 纲领, 理解函数

$$p\longmapsto N_p \quad \text{或} \quad p\longmapsto \zeta_p(\mathcal{X};T) \tag{9}$$

随着 **素数** p **的变化** (*as the prime* p *varies*) 所遵循的模式也可以作为我们的激发问题.

将所有有限域上的 ζ 函数按照如下方式

$$\zeta(\mathcal{X};s)=\prod_p \zeta_p(\mathcal{X};p^{-s}), \qquad \text{其中}\, p\, \text{遍历所有素数} \tag{10}$$

组合在一起得到一个关于复变量 s 的函数是有益的. 对于最简单的非平凡 Diophantus 方程 $x=0$, 它在 $\mathbb{F}_{p^r}$ 上的解集是单点集, 对于所有的 p 都有 $N_{p^r}=1$, 因此

$$\zeta_p(x=0;T)=\exp\left(\sum_{r\geq 1}\frac{T^r}{r}\right)=(1-T)^{-1}. \tag{11}$$

由此即得

$$\zeta(x=0;s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1} \tag{12}$$

$$=\prod_p\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}+\cdots\right) \tag{13}$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}=\zeta(s). \tag{14}$$

于是, 即便最简单的 Diophantus 方程的 ζ 函数, 也是数学的核心研究对象: 著名的 Riemann ζ 函数, 它与涉及到素数分布的一些深刻问题联系在一起. Riemann 在其 1860 年的伟大论文中证明了, 尽管 (13) 和 (14) 仅在半平面 $\Re(s)>1$ 上绝对收敛, 但是 $\zeta(s)$ 可以开拓

为关于 $s \in \mathbb{C}$ 的亚纯函数 (仅在 $s=1$ 处有单极点), 并且具有一个简洁的函数方程，将它在 s 处和 $1-s$ 处的取值联系在一起. 关于 $n+1$ 个变量的线性方程 $\mathcal{X}$, 由于 $N_{p^r} = p^{nr}$, 所以它的 ζ 函数只是 Riemann ζ 函数的平移，因此 $\zeta(\mathcal{X}; s) = \zeta(s-n)$.

再来考虑二次方程，一般的一元二次方程形如 $ax^2+bx+c=0$, 其行为由 *判别式* (*discriminant*)

$$\Delta := b^2 - 4ac \tag{15}$$

支配. 这个纯代数的事实对于有限域仍然正确，对于素数 $p \nmid 2a\Delta$ 总有

$$N_p = \begin{cases} 0 & \text{如果}\Delta\text{是模}p\text{的二次非剩余}, \\ 2 & \text{如果}\Delta\text{是模}p\text{的二次剩余}, \end{cases} \tag{16}$$

最初，判定 $N_p = 2$ 或 0—— 整数 Δ 是否模是 p 的二次剩余 —— 似乎是关于 p 的一个微妙的条件. 为了更好地理解这个条件，以方程 x^2-x-1 为例，此时 $\Delta = 5$. 对于素数 $p \le 101$, 计算 5 是否模是 p 的二次剩余，如下：

$$N_p = \begin{cases} 2 & p = 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, \ldots \\ 0 & p = 2, 3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, \ldots \end{cases} \tag{17}$$

这个试验呈现出一个明显的规律：$N_p = 0$ 或 2 似乎只取决于 p 的最右边数位上的数字，即，p 模 10 的余数. 这导致了一个猜测

$$N_p = \begin{cases} 2 & \text{如果}p \equiv 1, 4 \pmod 5, \\ 0 & \text{如果}p \equiv 2, 3 \pmod 5, \end{cases} \tag{18}$$

这个公式反映了对公式 (16) 的戏剧性的改进，比如说，它大大提高了 N_p 的计算效率. 事实上，猜想 (18) 是著名的 Gauss (高斯) 二次互反律的结论.

定理 (二次互反律) *对于任意方程 ax^2+bx+c, $\Delta := b^2-4ac$, 函数 $p \mapsto N_p$ (对于 $p \nmid a\Delta$) 的值仅依赖于 p 模 4Δ 的剩余类，因此其周期整除 $4|\Delta|$.*

N_p 随着 p 的变化所满足的周期性的规律为处理二次方程的 ζ 函数提供了很大的方便. 例如，方程 $\mathcal{X} : x^2-x-1=0$ 的 ζ 函数为

$$\begin{aligned} \zeta(\mathcal{X}; s) = \zeta(s) \times \Bigg\{ &\left(1 - \frac{1}{2^s} - \frac{1}{3^s} + \frac{1}{4^s}\right) + \left(\frac{1}{6^s} - \frac{1}{7^s} - \frac{1}{8^s} + \frac{1}{9^s}\right) \\ &+ \left(1\frac{1}{11^s} - \frac{1}{12^s} - \frac{1}{13^s} + \frac{1}{14^s}\right) + \cdots \Bigg\}. \end{aligned} \tag{19}$$

上式右侧的级数是 *Dirichlet L级数* (*狄利克雷 L-series*) 的典型例子. 这些 L 级数在关于算术级数中素数无限性的 Dirichlet 定理的证明中起到关键作用，它们和 Riemann ζ 函数有许多相同的解析性质：可以解析开拓到整个复平面，并且它们在 s 处和 $1-s$ 处的函数值通过一个函数方程联系起来. 关于这些 L 级数也有相应的 Riemann 假设，这既是 Riemann 最初的论述的推广，又和它同样深刻和难以琢磨.

事实上 (并不是完全平凡), 一般的 n 元二次方程

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c = 0 \tag{20}$$

的 ζ 函数和一元二次方程的情形相同, 也包含着相同的基本组成部分 ——Dirichlet 级数. 这意味着任意多个变量的二次 Diophantus 方程都是为人所熟悉的, 至少在只涉及它们的 ζ 函数的意义下.

考虑更高次的方程时, 问题变得复杂起来. 例如考虑三次方程 $x^3-x-1=0$, 其判别式 $\Delta=-23$. 对于所有的 $p\neq 23$, 这个三次方程在 $\mathbb{F}_{p^r}$ 上无重根, 因此 $N_p=0,1$ 或 3. Hecke (赫克) 的如下定理给出了这种情形 N_p 的一个简单表达:

定理 (Hecke) 对于所有的素数 $p\neq 23$, 总有:

(1) 如果 p 不是模 23 的二次剩余, 则 $N_p=1$.

(2) 如果 p 是模 23 的二次剩余, 则对于某些 $a,b\in\mathbb{Z}$ 有

$$N_p=\begin{cases}0 & \text{如果 } p=2a^2+ab+3b^2,\\ 3 & \text{如果 } p=a^2+ab+6b^2.\end{cases}\tag{21}$$

Hecke 的定理表明

$$\zeta(x^3-x-1;s)=\zeta(s)\times\sum_{n=1}^{\infty}a_n n^{-s},\tag{22}$$

其中生成级数

$$F(q):=\sum a_n q^n=q-q^2-q^3+q^6+q^8-q^{13}-q^{16}+q^{23}+\cdots\tag{23}$$

由显式公式

$$F(q)=\frac{1}{2}\left(\sum_{a,b\in\mathbb{Z}}q^{a^2+ab+6b^2}-q^{2a^2+ab+3b^2}\right)\tag{24}$$

给出. 在 (24) 中令 $q=e^{2\pi iz}$ 得到的函数 $f(z)=F(e^{2\pi iz})$ 是 模形式 (*modular form*) 的一个典型范例: 即, 在形如 $z\mapsto\frac{az+b}{cz+d}$ 的所谓 模代换 (*modular substitutions*) 下, 满足如下变换法则

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)f(z),\quad \text{其中 } a,b,c,d\in\mathbb{Z},\ ad-bc=1,\ 23\mid c,\ \left(\frac{a}{23}\right)=1.\tag{25}$$

应用 *Poisson* 求和公式 (泊松 *summation formula*) 于 (24) 便可得到此性质. 根据 (25), $\mathcal{X}$ 的 ζ 函数可以像 Riemann ζ 函数和 Dirichlet L 级数一样巧妙地处理. 事实上, Hecke 证明了与模形式 $\sum_{n=1}^{\infty}a_n e^{2\pi inz}$ 伴随的 L 级数 $\sum_{n=1}^{\infty}a_n n^{-s}$ 具有非常类似的解析性质, 特别是可以解析开拓及具有一个 Riemann 型的函数方程.

生成级数 $F(q)$ 也可以表示为无穷乘积:

$$\frac{1}{2}\left(\sum_{a,b\in\mathbb{Z}}q^{a^2+ab+6b^2}-q^{2a^2+ab+3b^2}\right)=q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}).\tag{26}$$

这个幂级数恒等式的前几项很容易通过数值验证, 但是这个等式的证明却远远不是显然和直接的. 它利用了诸如满足 (25) 及某些增长条件的关于 z 的全纯函数空间是一维复向

量空间这样的细节，当然也包括了上面的无穷乘积. 事实上，后者等于 $\eta(q)\eta(q^{23})$, 其中

$$\eta(q) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) \tag{27}$$

是 Dedekind (戴德金) η 函数，其对数的导数 (通过变换 $q = e^{2\pi iz}$ 将 η 看作 z 的函数) 由

$$\frac{\eta'(z)}{\eta(z)} = -\pi i\left(-\frac{1}{12} + 2\sum_{n=1}^{\infty}\Big(\sum_{d|n} d\Big)e^{2\pi inz}\right) \tag{28}$$

$$= \frac{i}{4\pi}\sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^2} \tag{29}$$

给出，其中最后一个求和中去除了相应于 $(m,n) = (0,0)$ 的项. Dedeking η 函数和表示正整数 n 拆为若干个正整数之和的方法数的分拆函数 $p(n)$ 的生成级数有如下关系

$$\eta^{-1}(q) = q^{-1/24}\sum_{n=0}^{\infty}p(n)q^n. \tag{30}$$

在最近一部关于 Srinivasa Ramanujan (拉马努金) 的电影中，这个公式与 Jeremy Irons 和 Dev Patel 一起成为主角.

Martin Eichler (艾克勒) 曾对 “模形式的不可思议的有效性和普遍性” 给出这样的评论：“存在 5 种基本的算术运算：加，减，乘，除， ...和模形式. ” 方程 (26), (29) 和 (30) 只是像芬芳的野兰花似的外来物种一样充斥于 Roger Godement 所谓的 “模趣的花园” 中的众多奇妙的恒等式中的几个例子而已.

上面的例子以及很多其它类似的例子在 Jean-Pierre Serre 的怡人的专著 [Se] 中都有所描述，2003 年 Serre 在 Abel 奖的颁奖典礼上演讲的也涉及到这些主题.

Hecke 建立了所有的一元三次多项式都是模的这一结论，即它们的 ζ 函数的系数服从像 (24) 和 (25) 中那样的规律. 而 Wiles 的成就在于将这个结论推广到有理数上的一大类二元三次 Diophantus 方程：椭圆曲线 (*elliptic curve*) 方程是指经过适当的变量代换可化为如下形式

$$y^2 = x^3 + ax + b, \tag{31}$$

并且是非奇异的，所谓的非奇异等价于判别式 $\Delta := -16(4a^3+27b^2)$ 非零.

为了用一个具体例子来说明 Wiles 定理，考虑方程

$$E : y^2 = x^3 - x, \tag{32}$$

其判别式 $\Delta = 64$. 置

$$\zeta(E;s) = \zeta(s-1)\times(a_1 + a_2 2^{-s} + a_3 3^{-s} + a_4 4^{-s} + \cdots)^{-1}, \tag{33}$$

与其伴随的生成级数满足下面的类似于 (24) 和 (26) 的恒等式：

$$F(q) = \sum a_n q^n = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} + \cdots \tag{34}$$

$$= \sum_{a,b} aq^{(a^2+b^2)} \tag{35}$$

$$= q\prod_{n=1}^{\infty}(1-q^{4n})^2(1-q^{8n})^2, \tag{36}$$

其中 (35) 中的求和是遍历那些使 Gauss 整数 $a+bi$ 与 1 关于 $(1+i)^3$ 同余的 $(a,b)\in\mathbb{Z}^2$. (这个等式来自 Deuring (多伊林) 对 *有复乘* (*with complex multiplication*) 的椭圆曲线的 ζ 函数的研究, 并且有可能在此之前就为人们所知.) 全纯函数 $f(z):=F(e^{2\pi iz})$ 依然是模形式, 它满足一个稍微不同的变换法则

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^2f(z),\quad \text{其中}\, a,b,c,d\in\mathbb{Z}, ad-bc=1,\, 32\,|\,c. \tag{37}$$

注意上面公式中的指数 2. 由此, 函数 $f(z)$ 被称为一个 *权为 2 水平为 32 的模形式* (*modular form of weight 2 and level 32*). 尽管式 (25) 中隶属于一元三次方程的模形式是权为 1 的, 但是 (35) 和 (36) 与 (24) 和 (26) 的对比却惊人地相似. Shimura-Taniyama (志村 – 谷山) 和 Weil 最初的猜想断言所有椭圆曲线遵循同样的规律:

猜想 (Shimura-Taniyama-Weil) *设 E 是椭圆曲线, 则*

$$\zeta(E;s)=\zeta(s-1)\times\left(\sum_{n=1}^{\infty}a_nn^{-s}\right)^{-1}, \tag{38}$$

其中 $f_E(z):=\sum a_ne^{2\pi inz}$ 是一个权为 2 的模形式.

事实上, 猜想更为精细, 并且断言了 f_E 的水平 —— 即出现在 f_E 所满足的变换法则中类似于式 (25) 中的 23 和式 (37) 中的 32 的整数 —— 等于椭圆曲线 E 的 *算术导子* (*arithmetic conductor*). 这个导子是椭圆曲线 E 的算术复杂性的一种度量, 可以利用 Tate (泰特) 算法通过 E 的方程精确地计算出来. 如果导子被某个素数 p 整除, 那么定义 E 的方程模 p 后一定是奇异的. 椭圆曲线称为 *半稳定的* (*semistable*), 如果其导子无平方因子. 这类椭圆曲线中包括如下形式的曲线:

$$y^2=x(x-a)(x-b), \tag{39}$$

其中 $\gcd(a,b)=1$, 并且 $16|b$. 这类曲线中最著名的椭圆曲线是那些最终被证明并不存在的: 由假定 Fermat 方程 $a^p+b^p=c^p$ 有解而得到的 "Frey (弗雷) 曲线" $y^2=x(x-a^p)(x+b^p)$. 在承认这些曲线的模性的前提下, 其不存在性此前已由 Kenneth Ribet 在其里程碑式的文章 [1)] 中给出. 恰恰是对于半稳定椭圆曲线证明了 Shimura-Taniyama-Weil 猜想为 Andrew Wiles 赢得了 Abel 奖:

定理 (Wiles) *设 E 是一条半稳定椭圆曲线, 则 E 满足 Shimura-Taniyama-Weil 猜想.*

Wiles 定理中半稳定的条件后来被 Christophe Breuil, Brian Conrad, Fred Diamond, 和 Richard Taylor 于 1999 年去掉了 (见当时发表于《美国数学会通讯 (Notices of the AMS) 》的报道 [Da]).

在描述其证明中的一些重要思想之前, 我们首先必须对 Wiles 定理为什么在数学中占据如此核心的位置做一个解释. Langlands 纲领大大推广了 Diophantus 方程 "相应于一个模形式" 的涵义, 从而将它置于一个更大的框架之中. 其关键在于, 将 (24) 或 (34) 中

1) 见本卷 229 页对新任美国数学会理事长 Ribet 的采访.—— 原注

相应于三次方程或椭圆曲线的模形式看作局部紧拓扑群

$$GL_2(\mathbb{A}_{\mathbb{Q}}) = \prod_p' GL_2(\mathbb{Q}_p) \times GL_2(\mathbb{R}) \tag{40}$$

(其中 $\prod_p'$ 表示对所有素数做限制直积，其元素形如 $(\gamma_p)_p$, 除有限个素数外，对应于 p 的分量 γ_p 属于 $GL_2(\mathbb{Z}_p)$ 的极大紧子群) 的某个无穷维不可约表示中的向量. 将重点从模形式转移到其张成的所谓 自守表示 (*automorphic representations*) 是决定性的. 对于任意一个约化的代数群 G, 如矩阵群 GL_n 和更一般的 Lie 型代数群就是典型的例子，Langlands 证明了 $G(\mathbb{A}_{\mathbb{Q}})$ 的任何一个不可约的自守表示都相应于一个 L 函数. 这就大大扩充了 "模" 这一概念的涵义：至此，如果一个 Diophantus 方程的 ζ 函数可以表示为相应于自守表示的 Langlands L 函数的形式，我们就说它具有这个性质. Langlands 纲领的一个基本的目标就是建立下述猜想的进一步的例证：

猜想 *在上面的意义下，所有的* Diophantus *方程都是模的.*

这个猜想可以看作是对二次互反律的深刻推广，并且也是在 Andrew Wiles 的成果中处于核心位置的非 Abel 互反律的基础.

在 Wiles 的证明之前，已知是模的 Diophantus 方程只有以下几类：

- 二次方程，利用 Gauss 二次互反律；
- 一元三次方程，利用 Hecke 和 Maass 的工作；
- 一元四次方程.

最后一个情形需要更深入的探讨，因为前面没有讨论过它并且它在 Wiles 的证明中起到根本性的作用. 四次方程的模性源于 Langlands 和 Tunnell 在他们的讨论班中的工作. 尽管讨论他们的方法超出了这篇概述的范围，仍须强调指出 Langlands 和 Tunnell 充分利用了一般的四次方程 (其 Galois 群包含于置换群 S_4 中) 可根式解这一事实. 可解扩张可以通过 Abel 扩张的复合得到，而这就进入了 19 世纪和 20 世纪前半叶发展出的类域论的研究范围. 另一方面，由于一般的次数 > 4 的一元方程不可根式解，其模性似乎远远超出了 "前 Wiles 时代" 的技术所及的范围. 如果读者坚持读完本文，就会大致了解到我们关于一般五次方程的模性知识是怎样受到 Wiles 的成果的激发而取得了显著的进展.

在 Wiles 的证明之前，对于任何有意义的多元方程 (比如次数 > 2) 的模性并没有任何一般性的结论；特别地，对于 $\mathbb{Q}$ 上的椭圆曲线，人们只是在 $\overline{\mathbb{Q}}$ 同构意义下对有限多个曲线证明了模性 (包括 $\mathbb{Q}$ 上有复乘的椭圆曲线，如 (31) 中的椭圆曲线就是一例). Wiles 的模性定理在椭圆曲线这一重要的情形证明了 Langlands 猜想；虽然椭圆曲线看上去只是 (事实上也是) 特殊的 Diophantus 方程，但是 Wiles 定理却不但在理论方面而且在应用方面 (密码学，编码理论，...) 都大大开拓了算术研究的领域.

回到这个报告的主题, Wiles 证明的重要性还体现在它引入了开创性的新方法从而为 Langlands 纲领的许多进展开启了大门.

为了说明这一点，我们需要介绍 Wiles 证明中的另一个 戏剧性对象 (*dramatis personae*): *Galois* 表示 (*Galois representations*). 设 $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 是 $\mathbb{Q}$ 的绝对 Galois 群，即所有代数数构成的域的自同构群. 它是一个拟有限群，其上赋以自然拓扑：当域 L 遍历 $\mathbb{Q}$ 的有限扩张时，子群 $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ 构成了开子群基. 根据 Galois 本人最初的观点，群

$G_{\mathbb{Q}}$ 像一个置换那样自然地作用于有理系数的多项式的根集之上. 给定一个由素数构成的有限集 S, 我们可以仅考虑判别式仅被素数 $\ell \in S$ 整除的首一整系数多项式 (最终是经过变量代换的). 拓扑群 $G_{\mathbb{Q}}$ 是通过一个商群 $G_{\mathbb{Q},S}$ 作用于这些多项式的根集之上的, 其中商群 $G_{\mathbb{Q},S}$ 是 $\mathbb{Q}$ 的在 S 外 非分歧的 (*unramified*) 极大代数扩张的自同构群, 可以看作 $\mathbb{Q}$ 上 "在 S 外有非奇异约化" 的所有零维代数簇的对称群.

$G_{\mathbb{Q}}$ 的置换表示在 Galois 最初阐述其理论时是非常重要的; 除此以外, 研究其 (连续)线性 (*linear*) 表示

$$\varrho : G_{\mathbb{Q},S} \to GL_n(L) \tag{41}$$

是非常重要的, 其中 L 是完备域, 如实数域 $\mathbb{R}$, 复数域 $\mathbb{C}$, 有限域 $\mathbb{F}_{\ell^r}$ 赋以离散拓扑, 或 ℓ 进数域 $\mathbb{Q}_\ell$ 的有限扩张 $L \subset \overline{\mathbb{Q}}_\ell$.

Galois 表示在 Abel 的工作中是一个重要的主题, 并且在现代仍处于核心地位. 20 世纪的很多著名数学家都投身于此项研究, 其中就包括此前的 3 位 Abel 奖获得者: Jean-Pierre Serre, John Tate, 和 Pierre Deligne. 对于代数数论学家, 在 Galois 表示领域工作似乎成为获得 Abel 奖的必要条件.

像 Diophantus 方程一样, Galois 表示也给出了 ζ 函数的类似物. 确切地说, 对于每个素数 $p \notin S$, 群 $G_{\mathbb{Q},S}$ 中包含一个特别的元素, 称为 p 处的 *Frobenius* 元素 (弗罗贝尼乌斯 *element*), 记为 σ_p. 严格地说, 这个元素只是在 $G_{\mathbb{Q},S}$ 中的共轭意义才是良定义的, 但是这已足以定义出以下算术序列

$$N_{p^r}(\varrho) := \mathrm{Trace}(\varrho(\sigma_p^r)). \tag{42}$$

像 $\zeta(\mathcal{X}; s)$ 的定义一样, ζ 函数 $\zeta(\varrho; s)$ 也整合了这个算术序列的信息.

例如, 如果 $\mathcal{X}$ 对应一元 d 次多项式 P, $G_{\mathbb{Q},S}$ 在 P 的根集上的作用给出了一个 d 维置换表示

$$\varrho_{\mathcal{X}} : G_{\mathbb{Q},S} \to GL_d(\mathbb{Q}), \tag{43}$$

并且 $\zeta(\mathcal{X}, s) = \zeta(\varrho_{\mathcal{X}}, s)$. 事实上, 这种联系远不止于此, 可以推广到 $n+1 (n \geq 0)$ 个变元的 Diophantus 方程的情形. 在最初提出 Weil 猜想时的一个伟大的洞察是 $\zeta(\mathcal{X}; s)$ 可以用源自 $\mathcal{X}$ 的 艾达尔上同调 (*étale cohomplogy*) 的 Galois 表示的 ζ 函数来表达. 而艾达尔上同调是一种上同调理论, 具有 ℓ 进系数, 对于 $\mathcal{X}$ 指定一族有限维 $\mathbb{Q}_\ell$ 向量空间

$$\{H^i_{\mathrm{et}}(\mathcal{X}_{/\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)\}_{0 \leq i \leq 2n},$$

并在其上赋予 $G_{\mathbb{Q},S}$ 的连续线性作用 (这里 S 是素数 q 构成的集合, 包括 ℓ 以及 $\mathcal{X}$ 的方程具有奇异约化的那些素数). 这些表示推广了 (43) 中的表示 $\varrho_{\mathcal{X}}$, 因为在将后者的系数由 $\mathbb{Q}$ 扩充到 $\mathbb{Q}_\ell$ 之后就可以通过 $G_{\mathbb{Q},S}$ 在 $H^0_{\mathrm{et}}(\mathcal{X}_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ 的作用来实现了.

定理 (Weil, Grothendieck, ...) *如果 Diophantus 方程 $\mathcal{X}$ 在 S 外有好约化, 那么存在 $G_{\mathbb{Q},S}$ 的 Galois 表示 ϱ_1, ϱ_2, 满足*

$$\zeta(\mathcal{X}; s) = \zeta(\varrho_1; s)/\zeta(\varrho_2; s). \tag{44}$$

表示 ϱ_1 和 ϱ_2 分别表示 $\oplus H^i_{\text{et}}(\mathcal{X}_{/\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ $(0 \le i \le 2n)$ 中 i 为奇数和 i 为偶数的部分. 更典范地，总存在 $G_{\mathbb{Q},S}$ 的 不可约 (*irreducible*) 表示 $\varrho_1, \ldots, \varrho_t$ 以及整数 $d_1, \ldots, d_t$, 使得

$$\zeta(\mathcal{X}; s) = \prod_{i=1}^{t} \zeta(\varrho_i; s)^{d_i}, \tag{45}$$

这源于将 $H^i_{\text{et}}(\mathcal{X}_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$(半单化) 分解为不可约表示之和. 每个 $\zeta(\varrho_i, s)$ 可看作 $\zeta(\mathcal{X}, s)$ 的 "原子组件", 并且揭示出原始方程的许多 "隐藏结构". 将 $\zeta(\mathcal{X}; s)$ 分解为不同的 $\zeta(\varrho_i; s)$ 之积无异于将波函数分解为其简谐部分.

一个 Galois 表示称为 模的 (*modular*), 如果其 ζ 函数可以表示为相应于模形式和自守表示的生成级数; 一个 Galois 表示称为 几何的 (*geometric*), 如果它可以像上面那样实现为一个 Diophantus 方程的艾达尔上同调群. Langlands 纲领的主猜想可以修正如下:

猜想 $G_{\mathbb{Q},S}$ 的所有几何 Galois 表示都是模的.

给定一个 ℓ 进系数的 Galois 表示

$$\varrho : G_{\mathbb{Q},S} \longrightarrow GL_n(\mathbb{Z}_\ell), \tag{46}$$

可以考虑相应的模 ℓ 表示

$$\overline{\varrho} : G_{\mathbb{Q},S} \longrightarrow GL_n(\mathbb{F}_\ell). \tag{47}$$

从 ϱ 过渡到 $\overline{\varrho}$ 相当于将与所有素数方幂 p^r 相应的 $N_{p^r}(\varrho) \in \mathbb{Z}_\ell$ 用它们的模 ℓ 约化代替. 为什么研究 Diophantus 方程在不同的有限域中的解数要模 ℓ? 如果事先不知道这些解数来自系数在 $\mathbb{Z}_\ell$ 中的 ℓ 进表示, 那么这样的过渡对于序列 $N_{p^r}(\mathcal{X})$ 而言就显得很不自然. 对于 $\overline{\varrho}$ 是模的，也有相应的概念. 粗略地说，就是指诸 $N_{p^r}(\overline{\varrho})$ 和来自某个自守表示的类似数据一致. 至此，我们可以叙述 Wiles 的著名的 模性提升定理 (*modularity lifting theorem*), 它在他的整个策略中处于核心地位:

定理 (Wiles 模性提升定理) 设

$$\varrho : G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{Z}_\ell), \tag{48}$$

是不可约几何 Galois 表示, 满足若干技术条件 (包括 ϱ 在 $G_{Q,S}$ 的子群 $G_{\mathbb{Q}_\ell} = \mathrm{GaL}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ 上的限制). 如果 $\overline{\varrho}$ 是模的，并且是不可约的，那么 ϱ 也是模的和不可约的.

目前，这一惊人结果是全新的：此前从未得到过与此类似的结果！此后, "模性提升定理" 开始蔓延，关于它们的研究也越来越广泛和精细，已经催生了一个领域并导致了 Langlands 纲领中大量重要进展.

我们先来解释 Wiles 是如何利用他最初的模性定理对半稳定椭圆曲线证明 Shimura-Taniyama-Weil 猜想的. 给定这样一条椭圆曲线 E, 考虑群

$$E[3^n] := \{P \in E(\overline{\mathbb{Q}}) |\ 3^n P = 0\}, \quad T_3(E) := \varprojlim E[3^n], \tag{49}$$

其中的反向极限针对 "乘以 3 映射" 进行. 群 $E[3^n]$ 和 $T_3(E)$ 分别是 $\mathbb{Z}/3^n\mathbb{Z}$ 和 $\mathbb{Z}_3$ 上的秩为 2 的自由模，并且赋以 $G_{\mathbb{Q},S}$ 的连续线性作用，其中 S 是包含 3 和整除 E 的导子的素

数的某个素数的集合. 于是得到一个相应的 Galois 表示

$$\begin{aligned} \overline{\varrho}_{E,3} &: G_{\mathbb{Q},S} \longrightarrow \mathrm{Aut}(E[3]) \simeq GL_2(\mathbb{F}_3), \\ \varrho_{E,3} &: G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{Z}_3). \end{aligned} \tag{50}$$

Langlands 和 Tunnell 关于一般四次方程的模性定理保证了 $\overline{\varrho}_{E,3}$ 是模的. 这依赖于如下令人愉快的事实

$$GL_2(\mathbb{F}_3)/\langle \pm 1 \rangle \simeq S_4, \tag{51}$$

因此 $E[3]$ 和一般的四次方程有相同的对称群！通过考虑 $GL_2(\mathbb{F}_3)$ 在 $\mathbb{F}_3$ 上的射影直线的点集 $\{0, 1, 2, \infty\}$ 上的作用可以实现 (51) 中的同构.

如果 E 是半稳定的, Wiles 能够证明 $\varrho_{E,3}$ 和 $\overline{\varrho}_{E,3}$ 都满足应用模性提升定理的条件, 至少当 $\overline{\varrho}_{E,3}$ 不可约时是这样. 于是, $\varrho_{E,3}$ 是模的. 从而 E 也是模的, 这是因为 $\zeta(E; s)$ 和 $\zeta(\varrho_{E,3}; s)$ 是相同的.

注意, 在上述策略中, Langlands 和 Tunnell 的结果起到了关键的作用. 发现一般四次方程的根式解是意大利文艺复兴时期代数学家的伟大贡献之一, 而这恰恰使得 Langlands, Tunnell 和 Wiles 在 5 个多世纪之后证明它们的模性结论成为可能. 这也戏剧性地说明了数学的同一性和历史的连续性.

在对于所有满足 $\overline{\varrho}_{E,3}$ 不可约的半稳定椭圆曲线建立了模性结论后, 对于其它的曲线, Wiles 应用他的模性提升定理于素数 $\ell = 5$ 而非 $\ell = 3$. 由于 $\mathbb{Q}$ 上的椭圆曲线不可能有 15 阶的有理子群, 此时 Galois 表示 $\overline{\varrho}_{E,5}$ 总是不可约的. 然而, 乍一看, 利用 $\ell = 5$ 这一方法貌似是没有希望的, 因为事先并不知道 $E[5]$ 的 Galois 表示是模的, 这与一般的五次方程不能根式求解如出一辙. (事实上, 对称群 $\mathbf{SL}_2(\mathbb{F}_5)$ 是五元交错群 A_5 的二重覆盖, 因此与一般的五次方程的对称群有密切的关系.) 为了建立 $E[5]$ 的模性, Wiles 构造了一个辅助的半稳定椭圆曲线 E', 满足

$$\overline{\varrho}_{E',5} = \overline{\varrho}_{E,5}, \quad \overline{\varrho}_{E',3} \text{是不可约的.} \tag{52}$$

于是, 根据前面的讨论可知 E' 是模的, 因此 $E'[5] = E[5]$ 也是模的, 从而将 E 置于 $\ell = 5$ 时的模性提升定理的适用范围之内. Wiles 的证明中这一漂亮的收尾, 即所谓的 "3–5 转换", 在当时可能被认为是权宜之计. 但是随后素数转化的观点已经牢牢地固化在这一领域, 并且它的许多变种也被利用来产生新的模性结果.

Wiles 的模性提升定理揭示了 "模性是会蔓延的", 并且经常可以从一个 ℓ 进 Galois 表示的模 ℓ 约化过渡到该 ℓ 进 Galois 表示. 正是这个简单的原理导致了模性提升定理及此后证明的各变种在这一领域的巨大影响. 事实上, 椭圆曲线的模性只是 Wiles 提出的理念的一系列壮观应用的第一个. 自 1994 年以来, 这一领域已经见证了一个黄金期, 其间许多此前完全遥不可及的未解决的问题陆续被解决了.

有关这些发展, 我们略举几个例子:

• 1923 年提出的二维 Artin (阿廷) 猜想关注的是所有奇的、二维 Galois 表示

$$\varrho : G_{\mathbb{Q},s} \longrightarrow GL_2(\mathbb{C}). \tag{53}$$

这个 ϱ 模数量矩阵的像或同构于二面体群, A_4, S_4, 或 A_5. 由于 Hecke, Langlands, Tunnell 等人的早期工作, 只有投射像 A_5 的情况还有待处理. 在 2003 年前后, 从所有来自椭圆曲线的模 5 Galois 表示的模性出发, Kevin Buzzard, Mark Dickinson, Nick Shepherd-Barron, 和 Richard Taylor 对于很多新的情形证明了二维 Artin 猜想.

• 1987 年提出的 Serre 猜想断言所有系数在有限域中的奇的、二维 Galois 表示

$$\varrho : G_{\mathbb{Q},s} \longrightarrow GL_2(\mathbb{F}_{p^r}) \tag{54}$$

是模的. 这个结果在 2008 年由 Chandrasekhar Khare 和 Jean-Pierre Wintenberger 利用 "3–5 转换技术" 的一个漂亮的推广给出证明, 这个推广本质上利用了所有的素数. (见本卷中 Khare 的报告.) 这个结果也蕴含了一般情形的二维 Artin 猜想.

• 二维 Fontaine-Mazur (方丹 – 马祖尔) 猜想关注的是满足某些技术条件的奇的、二维 p 进 Galois 表示

$$\varrho : G_{\mathbb{Q},s} \longrightarrow GL_2(\overline{\mathbb{Q}}_p) \tag{55}$$

的模性. 这个定理在很多情形下已作为 Pierre Colmez, Matthew Emerton, 和 Mark Kisin 的工作的推论被证明了.

• Sato (佐藤)–Tate 猜想关注的是: 对于椭圆曲线 E, 当素数 p 变化时, $N_p(E)$ 的分布情况. 其证明可以由与 E 伴随的所有对称幂表示的模性给出. 这一猜想的很大一部分大约在 2006 年被 Laurent Clozel, Michael Harris, Nick Shepherd-Barron, 和 Richard Taylor 证明.

• 对于一般的数域, 也可以赋予其上的 Diophantus 方程 "是模的" 的涵义. 最近, Nuno Freitas, Bao Le Hung 和 Samir Siksek 利用新近才得到的更一般且更有力的模性提升定理, 并对原先并不在模性提升定理适用范围的椭圆曲线进行了细致的 Diophantus 研究, 从而证明了所有实二次域上的椭圆曲线的模性.

• Laurent Clozel 和 Jack Thorne 证明的相应于全纯模形式的 Galois 表示的某对称幂的模性也是基于 Wiles 的理念而取得的一系列惊人的新进展之一, 见本卷中 Thorne 的文章.

对于具有划时代意义的模性提升定理而言, 这些结果只是沧海一粟. Langlands 纲领仍然是一个活跃的领域, 拥有许多等待挖掘的诱人奥秘. 虽然很难预测下一个突破口会在哪里, 但是它们肯定会利用 Andrew Wiles 的绝妙证明所遗留下来的丰富遗产.

参 考 文 献

[Da] H. Darmon, A proof of the full Shimura-Taniyama-Weil conjecture is announced, Notices of the AMS 46 (1999), no. 11, 1397–1401. MR1723249.

[Se] J.-P. Serre, Lectures on $N_X(p)$, Chapman & Hall/CRC Research Notes in Mathematics, 11, CRC Press, Boca Raton, FL. MR2920749

(曹磊 译　　赵振江 校)