模形式和费马大定理

在数论里，费马大定理(或者费马猜想)是说：当n是大于或等于三的正整数时，方程

$$\mathrm{FLT(n)}: \quad x^n + y^n = z^n, \quad xyz \neq 0$$

没有整数解。这与$n = 1$或2的情形完全不一样，因为那两种情况下，方程都有无穷多的解。

费马大定理是由法国数学家费马(Pierre de Fermat)在1637年提出的，这样一个看似简单的关于整数的问题困扰了数学界350多年，最终由英国数学家Andrew Wiles证明。Wiles的证明在1994 年发布出来，于1995年正式发表。Wiles的证明被评价为“惊人的进展”，其中汇集了无数数学家在椭圆曲线、模曲线、Galois表示等方面的成果，也包含了许多突破性和创新性的工作，为后来相关方向的发展和相关问题的解决打下了坚实的基础。

关于费马大定理的历史和发展历程，已经有许多的文献资料(参见[14, 40, 51]及其参考文献)，文献[14]的开始部分简略介绍了Fermat、Euler、Germain、Kummer等的成果，并介绍了问题与Faltings、Mazur等研究的关系。在这篇文章里，我们主要介绍Wiles关于模性猜想的证明框架，解释主要结果的证明思路，并通过具体实例描述其应用价值。首先，我们介绍五位数学家以及他们的在这个问题上的深刻观点，正是由于他们的洞察力和贡献，最终导致了Wiles的证明(参见[14, 52])。

Gerhart Frey (1985) 首先提出方程FLT(n)解的存在性有可能与Shimura-Taniyama-Weil提出的模性猜想相矛盾。

Jean-Pierre Serre (1985-6) 提出了一个深刻猜想，描述了模形式和模p的Galois表示之间的关系，并指出猜想的一部分，即ϵ-猜想和模性猜想一起可以导出费马大定理。

Ken Ribet (1986) 证明了ϵ-猜想，从而要证明费马大定理，我们只需要证明模性猜想。

Richard Taylor (1994) 和Wiles一起，证明了Wiles判别方法中的极小情形。

Andrew Wiles (1994) 给出了关于半稳定椭圆曲线的模性的证明，从而完成了费马大定理的证明。

Wiles的方法后来被数学家简化并推广，在了解了证明框架之后，本文的章节4将详细解释相关数学家及其贡献。限于篇幅，本文写作是在假设读者对椭圆曲线、模曲线、模形式、Galois表示等的定义和基本性质有一定了解的基础上。相关预备知识可以参考文献[17, 27, 49, 50]，以及[12]的相关章节。由于这是一篇综述文章，文章中某些结论会强于另外的结论，并且提到的若干猜想随着理论的发展也成为了定理或者部分得到了证明。我们将在相关部分给出注解，也希望这些非标准的风格不会给读者带来困扰。最后$n = 3,\ 4$ 时，费马大定理在Euler时代就已经被证明，并且要证明费马大定理，我们可以假设n是一个素数。所以，若没有特别说明，在本文中我们考虑FLT(p)，$p \geq 5$ 为素数。

在章节1中，我们将从Frey的想法出发，把费马大定理的证明一步步归结为模性猜想的证明，并解释Wiles的证明思路。在这部分，我们将集中于上面提到的五位数学家的思路，让读者对大概框架有一定的了解；在此过程中，我们也将介绍费马大定理与Szpiro猜想、abc猜想、Serre模性猜想的关系。在章节2中，我们将介绍Wiles的证明中用到的一个重要工具——伽罗华表示的形变理论，并将模性猜想的证明归结为证明两个特殊环之间的同构，即所谓的$R = T$定理。在章节3中，我们介绍被Diamond简化后的Taylor-Wiles系统的构造，即所谓的patching过程，并构造一个Diamond-Taylor-Wiles系统来证明$R = T$定理，从而完成(部分)模性猜想和费马大定理的证明。

在章节4中，我们将介绍Wiles证明方法的若干发展和与模性猜想相关的其它科研课题，包括BSD猜想，Kisin的patching，Fontaine-Mazur猜想，Breuil-Mézard猜想等。

正如上面提到的，Wiles的证明汇集了无数数学家的工作成果，在这样一篇综述文章中不可能面面俱到，把所有背景和问题都解释清楚，在某些重要问题上必有所取舍。本文的重点将放在介绍Wiles的证明思路上，作者将尽最大的努力把证明中的基本方法，特别是那些在后来二十多年间被数学家推广和改进的、对数论发展起到了推动作用的部分以简明的形式呈现给大家。

目录

1 证明思路

1.1 一条“remarkable”的椭圆曲线

在这小节里，从方程的$a^p+b^p+c^p=0$的假设解出发，我们构造一条椭圆曲线E_{a^p,b^p,c^p}。

1.1.1 曲线E_{a^p,b^p,c^p}的构造

对任意的两两互素的非零整数数组(A,B,C)，若$A+B+C=0$，Gerhart Frey [23]构造了一条椭圆曲线$E_{A,B,C}$，其对应的Weierstrass方程为

$$E_{A,B,C}:\ y^2=x(x-A)(x+B).$$

对我们而言，假设费马方程有非平凡整数解，即$a^p+b^p+c^p=0$，则令$(A,B,C)=(a^p,b^p,c^p)$，这样我们得到椭圆曲线E_{a^p,b^p,c^p}。不失一般性，我们假设$a\equiv -1 \pmod 4$，$2\mid b$。对于曲线E_{a^p,b^p,c^p}，直接计算容易得到下面的结果。

引理1.1. *令$p\geq 5$为素数，令a,b,c为两两互素的非零整数且满足：$a\equiv -1 \pmod 4$，$2\mid b$，$abc\neq 0$。假设$a^p+b^p+c^p=0$，则椭圆曲线E_{a^p,b^p,c^p}是半稳定的，并且其最小判别式和导子由下面的公式给出：*

1. $\Delta_{a^p,b^p,c^p}=2^{-8}\cdot(abc)^{2p}$，
2. $N_{a^p,b^p,c^p}=\prod_{l\mid abc} l$.

1.1.2 Szpiro猜想

一般情况下，对于定义在$\mathbb{Q}$上的椭圆曲线，其极小判别式和导子被相同的素数整除，因而我们有理由怀疑极小判别式和导子之间有密切的联系。Szpiro猜想给出了一种可能的关系(参见[58])。

猜想1.2 (Szpiro). 对任意的$\epsilon > 0$，存在一个正常数$C > 0$，使得对任意的定义在$\mathbb{Q}$上的椭圆曲线E，都有

$$|\Delta_E| < C \cdot N_E^{6+\epsilon}.$$

这里，Δ_E和N_E分别是E的极小判别式和导子。

通过引理1.1不难看出，如果假设Szpiro猜想成立，则对足够大的p，费马大定理FLT(p)成立。

1.1.3 abc-猜想

这里我们简单介绍abc-猜想和费马大定理的关系。首先我们回顾一下Oesterlé和Masser给出的abc-猜想的具体内容(参见[28])。

猜想1.3 (Oesterlé-Masser). 对任意给定的$\epsilon > 0$，都存在一个常数κ_ϵ，使得对任意的两两互素的正整数a, b, c，若$a + b = c$，则

$$c \leq \kappa_\epsilon(\prod_{\substack{p \text{ prime} \\ p|abc}} p)^{1+\epsilon}.$$

这个猜想和费马大定理有什么关系呢？假设我们有两两互素的正整数x，y，z，满足$x^n + y^n = z^n$。如果猜想1.3成立，容易得到对任意$\epsilon > 0$，

$$z^n \leq \kappa_\epsilon(z^3)^{1+\epsilon}.$$

令$\epsilon = 1/6$，且$n \geq 4$，得到

$$z^n \leq \kappa_{1/6}^8.$$

于是我们证明了当$n \geq 4$时，方程FLT(n)只有有限多正整数解。

更强形式的abc-猜想提出，猜想1.3对$\epsilon = \kappa_\epsilon = 1$成立。这时，类似上面的推导告诉我们$n \geq 6$ 时，FLT(n)没有正整数解。而当$n = 3,\ 4,\ 5$ 时，十九世纪初数学家就证明了费马大定理是成立的(参见[40])。

1.2 一个"remarkable"的伽罗华表示

1.2.1 伽罗华表示的基本概念

记$\bar{\mathbb{Q}}$是有理数域$\mathbb{Q}$在复数域$\mathbb{C}$中的代数闭包，记$G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$并且给$G_{\mathbb{Q}}$ Krull拓扑。

定义1.4. 一个拓扑环A上的n-维的伽罗华表示是指一个连续同态

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A).$$

在这篇文章里，拓扑环A将会是Mazur提出的所谓系数环。

定义1.5. 一个系数环是一个完备的、诺特的局部环，并且其剩余类域是特征p的有限域。

定义1.6. 1. 若ρ是一个定义在A上的n-维伽罗华表示，ρ的行列式

$$\det(\rho) : G_{\mathbb{Q}} \to A^{\times}$$

是指ρ和$\det : \mathrm{GL}_n(A) \to A^{\times}$的复合。

2. $(\ell \neq p)$ 若ρ是一个定义在A上的n-维伽罗华表示，我们称ρ在素数ℓ处非分歧，如果$I_\ell \in \mathrm{Ker}(\rho|_{G_{\mathbb{Q}_\ell}})$。这里$G_{\mathbb{Q}_\ell}$ 和I_ℓ 分别是$G_{\mathbb{Q}}$在ℓ处的分解群和惯性群。

3. $(\ell = p)$ 若ρ是一个定义在A上的n-维伽罗华表示，我们称ρ是平坦的，如果对任意理想$I \subset A$，若A/I 是有限的，则$\rho|_{G_{\mathbb{Q}_p}} : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(A/I)$是一个定义在$\mathbb{Z}_p$上的有限平坦群概型的一般纤维。

4. 若ρ是一个定义在A上的2-维伽罗华表示，我们称ρ是奇的，如果对复共轭c，有$\det(\rho(c)) = -1$。

5. 我们称表示$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$在$p$处是正规的，如果在一组合适的基下，有$\rho|_{I_p} = \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$。

6. 我们称表示$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$在$\ell$处是半稳定的，若它满足

- ($\ell = p$)时，ρ在p处是平坦的或者是正规的；
- ($\ell \neq p$)时，在一组合适的基下，有$\rho|_{I_\ell} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$。

如果表示$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$在每个$\ell$处都是半稳定的，我们便称$\rho$是半稳定的。

1.2.2 椭圆曲线构造的伽罗华表示

伽罗华表示在数论和几何中自然出现，且这些伽罗华表示都有着良好的性质。令X是定义在$\mathbb{Q}$上的代数簇，则X的etale上同调群$H^*_{\mathrm{et}}(X \otimes \bar{\mathbb{Q}}, \mathcal{F})$就给出了伽罗华表示，且这个伽罗华表示在除了有限个素数外都是非分歧的。特别地，当X是交换代数簇时，我们可以从其Tate模来构造伽罗华表示。这时令

$$T_p(X) := \varprojlim_n X[p^n] \cong \mathbb{Z}_p^{2d}.$$

这里$d = \dim X$，$G_{\mathbb{Q}}$在$T_p(X)$上有自然作用。从而我们从X构造出一个p-进的伽罗华表示

$$\rho_{X,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_p(X)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_p).$$

令$\bar{\rho}_{X,p} := \rho_{X,p} \pmod p : G_{\mathbb{Q}} \to \mathrm{GL}_{2d}(\mathbb{F}_p)$，这个表示给出了伽罗华群$G_{\mathbb{Q}}$在

$$X[p] \cong \mathbb{F}_p^{2d}$$

上的作用。更特别地，若$X = E$是一条椭圆曲线，这时$d = 1$，我们有下面的结果(参见[45])。

定理1.7. *令E是定义在$\mathbb{Q}$上的椭圆曲线，N_E和Δ_E分别是E的导子和极小判别式。令$\rho_{E,p}$是由E构造的p-进伽罗华表示，则*

- $\det(\rho_{E,p}) = \chi_p$，*这里$\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$是$p$-进分圆特征；*
- $\rho_{E,p}$*在pN_E外都是非分歧的。*

特别地，$\rho_{E,p}$是奇的。如果进一步假设E是半稳定的，则$\rho_{E,p}$和$\bar{\rho}_{E,p}$都是半稳定的，并且$\bar{\rho}_{E,p}$有如下性质

- 若$\ell \neq p$，则$\bar{\rho}_{E,p}$在ℓ处非分歧当且仅当$p \mid \mathrm{ord}_\ell(\Delta_E)$；
- $\bar{\rho}_{E,p}$在p处平坦当且仅当$p \mid \mathrm{ord}_p(\Delta_E)$。

1.2.3 伽罗华表示$\bar{\rho}_{a^p,b^p,c^p}$

现在令$E := E_{a^p,b^p,c^p}$是我们在节1.1.1中构造的椭圆曲线，从而我们得到伽罗华表示

$$\bar{\rho}_{a^p,b^p,c^p} := \bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}).$$

Gerhart Frey [22, 23]和Jean-Pierre Serre [45]证明了这个表示有着非常特殊的性质。

定理1.8. 令$p \geq 5$是素数，a，b，c是非零整数且满足$a^p + b^p + c^p = 0$。假设$a \equiv -1 \pmod 4$且$2 \mid b$，则

1. $\bar{\rho}_{a^p,b^p,c^p}$绝对不可约，即$\bar{\rho}_{a^p,b^p,c^p} \otimes \bar{\mathbb{F}}_p$不可约；
2. $\bar{\rho}_{a^p,b^p,c^p}$是奇的；
3. $\bar{\rho}_{a^p,b^p,c^p}$在$2p$外非分歧，在p处平坦；
4. $\bar{\rho}_{a^p,b^p,c^p}$在2处半稳定，即

$$\bar{\rho}_{a^p,b^p,c^p}|_{I_2} \cong \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

注1.9. 上世纪80年代，数学家怀疑满足条件(1)-(4)的伽罗华表示是不存在的。Ribet的结果(参见[41]，定理1.21)告诉我们，满足条件(1)-(4)的伽罗华表示必定不是模性的(定义1.16)；Khare-Winterberger证明了Serre模性猜想后(参见[31, 32]，猜想1.22)，这类表示的不存在性得到证实。从这个方向来说，我们给出了费马大定理的另一个证明。

1.3 模性猜想

1.3.1 Eichler-Shimura的结果

令E为定义在$\mathbb{Q}$上的椭圆曲线，E的L-函数定义为

$$L(E,s)=\prod_{p\nmid N_E}\frac{1}{1-a_pp^{-s}+p^{1-2s}}\prod_{p|N_E}\frac{1}{1-a_pp^{-s}}.$$

这里

$$a_p=\begin{cases}p+1-\sharp E(\mathbb{F}_p) & \text{若}p\nmid N_E,\\ 1 & \text{若}E\text{在}p\text{处为分裂乘法约化},\\ -1 & \text{若}E\text{在}p\text{处为非分裂乘法约化},\\ 0 & \text{若}E\text{在}p\text{处为加法约化}.\end{cases}$$

令$S_k(\Gamma_1(N),\chi)$表示权重为k、水平为$\Gamma_1(N)$、特征为χ的尖形式组成的空间。(为方便起见，若f的水平为$\Gamma_1(N)$，我们也称f的水平为N。)令$f\in S_k(\Gamma_1(N),\chi)$ 为一个特征形式，$f(z)=\sum_{n\geq1}a_ne^{2\pi inz}$ 为f的q-级数展式。f的L-函数定义为

$$L(f,s)=\prod_{p\nmid N}\frac{1}{1-a_pp^{-s}+\chi(p)p^{k-1-2s}}\prod_{p|N}\frac{1}{1-a_pp^{-s}}.$$

更进一步，若$k=2$，$f\in S_2(\Gamma_0(N))$的q-级数系数全为有理数，Eichler-Shimura构造了一条椭圆曲线E_f，使得E_f的L-函数和f的L- 函数“基本相等”。具体地说，我们有下面的结果。

定理1.10 (Eichler-Shimura). 令$f(z)=\sum_{n\geq1}a_ne^{2\pi inz}\in S_2(\Gamma_0(N))$是一个规范新形式且$a_n\in\mathbb{Q}$。存在$E_f$为定义在$\mathbb{Q}$上的椭圆曲线，满足

$$L_p(E_f,s)=L_p(f,s)\ \text{对}p\nmid N.$$

注1.11. 事实上，Eichler-Shimura的构造比上面的结果要更一般。具体地说，若$f\in S_2(\Gamma_1(N),\chi)$，Eichler-Shimura构造了一个Abel簇，它是模曲线$X_1(N)$的Jacobian的商簇，并且其维数是$[K_f:\mathbb{Q}]$，这里$K_f=\mathbb{Q}(a_n(f):n\in\mathbb{Z})$是$f$ 的所有Fourier系数生成的域，是$\mathbb{Q}$的一个有限扩张。特别地，若f的系数都是有理数，构造出来的Abel簇是一维的，即为椭圆曲线。

1.3.2 模性猜想：基本形式

粗略地说，定理1.10是指我们可以从一个新形式构造出一条椭圆曲线，而模性猜想是说我们也可以从一条椭圆曲线构造出一个新形式。

定义1.12. 令E是一条定义在$\mathbb{Q}$上的椭圆曲线。称E是模性的，若存在一个权重为2，水平为$\Gamma_0(N_E)$的新形式f_E，使得

$$L_p(f_E, s) = L_p(E, s) \text{ 对} p \nmid N.$$

猜想1.13 (模性猜想)**.** 定义在$\mathbb{Q}$上的所有椭圆曲线都是模性的。

注1.14. 在数学文献中，模性猜想也称为Weil-Shimura-Taniyama猜想或者Shimura-Taniyama猜想。

1.3.3 模性猜想：等价形式

由Eichler-Shimura的构造，从一个权重为2的新形式出发，我们可以构造出一个交换代数簇，这个交换代数簇是GL_2-型的。考虑此交换代数簇的Tate模，我们便得到一个2 维的伽罗华表示。这个从新形式到伽罗华表示的关系后来被数学家推广。具体地说，我们有下面的结果。

定理1.15 (Eichler, Shimura, Deligne, Deligne-Serre等)**.** 令$f = \sum_{n>0} a_n e^{2\pi i n z} \in S_k(\Gamma_1(N), \chi)$是一个权重为$k$、水平为$\Gamma_1(N)$、特征为$\chi$的规范新形式。对任意素数$p$，令$K$为$\mathbb{Q}_p$的一个有限扩张且$K \supset K_f := \mathbb{Q}(a_n : n > 0)$。则存在一个$p$-进的伽罗华表示

$$\rho_{f,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$$

满足

1. $\rho_{f,p}$是不可约的；
2. $\det(\rho_{f,p}) = \chi\chi_p^{k-1}$，$\rho_{f,p}$是奇的；
3. $\rho_{f,p}$在pN外是非分歧的，并且当$\ell \nmid pN$时，$\rho_{f,p}(\mathrm{Frob}_\ell)$ 的特征多项式为
$$X^2 - a_\ell X + \ell^{k-1}\chi(\ell).$$

令$\mathbb{T}(k,N) := \mathbb{Z}[T_l, \langle d\rangle : \ l \nmid N,\ d|N] \subset \mathrm{End}(S_k(\Gamma_1(N)))$为Hecke代数。注意到一个权重为$k$、水平为$\Gamma_1(N)$的新形式$f$对应到$\mathbb{T}(N)$的一个极大理想$\mathfrak{m}_f$，即映射$\mathbb{T}(k,N) \to K_f$ $(T_n \mapsto a_n)$的核。这诱导我们给出下面的定义。

定义1.16. 一个定义在系数环A上的伽罗华表示$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$称为模性的，若存在正整数$k$，$N$，以及一个同态$\pi : \mathbb{T}(k,N) \to A$，满足

- ρ在pN外非分歧；
- 对任意$\ell \nmid pN$，有

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = \pi(T_\ell),\ \det(\rho(\mathrm{Frob}_\ell)) = \pi(\ell)\ell^{k-1}.$$

现在我们可以给出模性猜想的若干等价形式。

定理1.17. *令E是定义在$\mathbb{Q}$上的椭圆曲线。下列条件等价：*

1. *E是模性的；*
2. *对某些素数p，$\rho_{E,p}$是模性的；*
3. *对所有素数p，$\rho_{E,p}$是模性的；*
4. *存在非平凡定义在$\mathbb{Q}$上的态射$\pi : X_0(N_E) \to E$；*
5. *E与某一个E_f同源，这里E_f是通过Eichler-Shimura方法构造出来的椭圆曲线。*

Wiles于1995年证明了如下结果。

定理1.18 (Wiles 1995)**.** *定义在$\mathbb{Q}$上的所有半稳定的椭圆曲线都是模性的。*

5年后，Breuil、Conrad、Diamond、Taylor合作证明了完整地模性猜想，从而模性猜想成为了定理。

定理1.19 (Breuil-Conrad-Diamond-Taylor 2001)**.** *定义在$\mathbb{Q}$上的所有椭圆曲线都是模性的。*

注1.20. 在节4.2.1中，我们将解释为什么这两个结果中间有6年的发展期。

1.4 费马大定理的证明

1.4.1 Ribet的结果

在Mazur、Serre等研究的基础上，Ribet [41]证明了如下结果。

定理1.21. *令f是一个权重为2水平为$\Gamma_0(N\ell)$的新形式，这里$\ell \nmid N$。假设模p表示$\bar{\rho}_f$绝对不可约，且满足下面两个条件中至少一个：*

- *$\bar{\rho}_f$在ℓ处非分歧；*
- *$\ell = p$且$\bar{\rho}_f$在p处平坦。*

那么存在一个权重为2、水平为$\Gamma_0(N)$的新形式g，满足$\bar{\rho}_g \cong \bar{\rho}_f$。

这个结果是Serre模性猜想的一个特殊情况，最初被Serre称为ϵ-猜想。这里我们也简单介绍一下Serre模性猜想。

猜想1.22 (Serre模性猜想：弱形式). *所有不可约的、奇的伽罗华表示*

$$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

都是模性的。

上面猜想1.22是Serre模性猜想的一部分。其另外一部分(强形式)通过$\bar{\rho}$的局部结构，预测了满足$\bar{\rho}_f \cong \bar{\rho}$的新形式$f$的所有可能的水平和权重。Serre模性猜想已经被证明，参见文献[31, 32]。文献[30]中，Khare简单介绍了猜想1.22的证明，以及猜想和Fontaine-Mazur猜想、预模性提升猜想等的联系。

1.4.2 Wiles+Ribet⇒费马大定理

下面利用定理1.18和定理1.21，我们用反证法来证明费马大定理。假设$p \geq 5$，并假设有非零整数a，b，c满足$a^p + b^p + c^p = 0$。不失一般性，我们设$a \equiv -1 \pmod 4$且$2 \mid b$。令E_{a^p,b^p,c^p}是由方程$y^2 = x(x - a^p)(x + b^p)$定义的椭圆曲线，$\rho_{a^p,b^p,c^p}$是由$E_{a^p,b^p,c^p}$的Tate模给出的$p$- 进伽罗华表示。

由引理1.1，E_{a^p,b^p,c^p}是半稳定的且其导子为$N_{a^p,b^p,c^p} = \prod_{\ell|abc} \ell$。于是由定理1.18，$E_{a^p,b^p,c^p}$是模性的。从而存在一个权重为2、水平为$\Gamma_0(N_{a^p,b^p,c^p})$的

新形式f_{a^p,b^p,c^p}，使得$\rho_{a^p,b^p,c^p} \cong \rho_{f_{a^p,b^p,c^p}}$。由定理1.8，表示$\bar{\rho}_{a^p,b^p,c^p}$是绝对不可约的，并且在$2p$外非分歧，在$p$处平坦。不断使用定理1.21，我们得到一个权重为2水平为$\Gamma_0(2)$的新形式g，满足$\rho_{a^p,b^p,c^p} \cong \rho_{g_{a^p,b^p,c^p}}$。但是$\dim S_2(\Gamma_0(2))$等于模曲线$X_0(2)$的亏格，而这个亏格是0。这个矛盾就说明费马大定理成立。

2 表示的形变理论

伽罗华表示的形变理论由Mazur开始研究发展，是Wiles证明中最重要的工具之一，在数论其它相关问题的研究上(如p-进Hodge理论、p-进局部Langlands对应等)也有重要应用。在这一节里，我们介绍形变理论的基本概念和性质，并将定理1.18的证明归结为证明两个环之间的同构。关于伽罗华表示形变理论的更多内容，读者可参阅文献[27, 38]等。

为了方便读者，我们先确定一些在本节里使用的记号：

- $\mathcal{O}$: 完备的离散赋值环，剩余类域的特征为p
- λ: $\mathcal{O}$的素元
- $k := \mathcal{O}/\lambda$
- $\mathcal{C}_{\mathcal{O}}$: 完备的、诺特的、局部的、剩余类域为$k$的$\mathcal{O}$-代数组成的范畴
- $\mathcal{C}_{\mathcal{O}}^{\circ}$: 由artian对象组成的$\mathcal{C}_{\mathcal{O}}$的子范畴
- Π: 满足p-有限条件的仿有限群
- **p-有限条件**: 对任意指数有限的开子群$\Pi_0 \subset \Pi$，$\mathrm{Hom}_{\mathrm{cont}}(\Pi_0, \mathbb{Z}/p\mathbb{Z})$是有限集
- $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$: 群$\Pi$的连续表示

2.1 基本性质

2.1.1 形变函子

定义2.1. 令$R \in \mathcal{C}_{\mathcal{O}}$。我们称两个同态

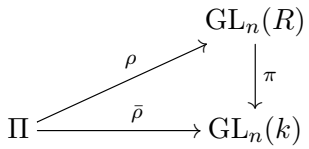
$$\rho_1,\ \rho_2 : \Pi \to \mathrm{GL}_2(R)$$

是严格等价的，如果存在$M \in \Gamma_n(R)$，使得$\rho_1 = M^{-1}\rho_2 M$。这里

$$\Gamma_n(R) := \mathrm{Ker}(\mathrm{GL}_n(R) \xrightarrow{\pi} \mathrm{GL}_n(k)),$$

$\pi : R \to k$是典范投射。

定义2.2. 令$\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$是一个表示，$R \in \mathcal{C}_{\mathcal{O}}$是一个系数环。$\bar{\rho}$ 在R上的一个形变是指一个提升$\rho : \Pi \to \mathrm{GL}_n(R)$的严格等价类。这里$\rho$ 满足$\bar{\rho} = \pi \circ \rho$，即我们有交换图



现在我们定义形变函子

$$\begin{aligned} \mathbf{D}_{\bar{\rho},\mathcal{O}} : \mathcal{C}_{\mathcal{O}} &\to \mathrm{Sets} \\ R &\mapsto \{\bar{\rho}\text{在}R\text{上的形变}\} \end{aligned}$$

令$\mathbf{F}$是定义在$\mathcal{C}_{\mathcal{O}}$上的函子。任取$(R, \mathfrak{m}) \in \mathcal{C}_{\mathcal{O}}$，我们都有

$$R = \varprojlim_n R/\mathfrak{m}^n.$$

对任意n，典范映射$R \to R/\mathfrak{m}^n$诱导了映射$\mathbf{F}(R) \to \mathbf{F}(R/\mathfrak{m}^n)$，并且它们组成一个反向系统。于是我们得到一个典范映射

$$\mathbf{F}(R) \to \varprojlim_n \mathbf{F}(R/\mathfrak{m}^n).$$

定义2.3. 定义在$\mathcal{C}_{\mathcal{O}}$上的函子$\mathbf{F}$称为是连续的，若对任意$(R, \mathfrak{m}) \in \mathcal{C}_{\mathcal{O}}$，

$$\mathbf{F}(R) \to \varprojlim_n \mathbf{F}(R/\mathfrak{m}^n)$$

是一个同构。

引理2.4. $\mathbf{D}_{\bar{\rho},\mathcal{O}}$是一个连续函子。

2.1.2 可表性和纤维积

假设我们考虑的范畴中纤维积是存在的。令A, B, C是范畴中的三个对象且有态射$\alpha : A \to C$和$\beta : B \to C$。考虑纤维积$A \times_C B$

$$\begin{array}{ccc} A \times_C B & \xrightarrow{q} & B \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \beta} \\ A & \xrightarrow{\alpha} & C. \end{array}$$

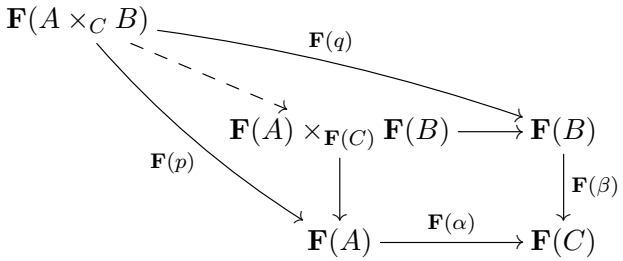
若$\mathbf{F}$是定义在这个范畴上的函子，我们得到如下的交换图

$$\begin{array}{ccc} \mathbf{F}(A \times_C B) & \xrightarrow{\mathbf{F}(q)} & \mathbf{F}(B) \\ {\scriptstyle \mathbf{F}(p)}\downarrow & & \downarrow{\scriptstyle \mathbf{F}(\beta)} \\ \mathbf{F}(A) & \xrightarrow{\mathbf{F}(\alpha)} & \mathbf{F}(C). \end{array}$$

纤维积的泛性质告诉我们，存在唯一的一个映射

$$\mathbf{F}(A \times_C B) \to \mathbf{F}(A) \times_{\mathbf{F}(C)} \mathbf{F}(B),$$

使得下面的图表交换



(2.1)

定义2.5. 若对任意图表，映射

$$\mathbf{F}(A \times_C B) \to \mathbf{F}(A) \times_{\mathbf{F}(C)} \mathbf{F}(B)$$

是一个同构，则称函子$\mathbf{F}$满足*Mayer-Vietoris*性质。

定义2.6. 令$\mathbf{F}$是定义在$\mathcal{C}_{\mathcal{O}}^{\circ}$上的函子，

- 称$\mathbf{F}$是可表的，若存在$\mathcal{R} \in \mathcal{C}_{\mathcal{O}}^{\circ}$，使得

$$\mathbf{F}(A) = \mathrm{Hom}(\mathcal{R}, A).$$

- 称$\mathbf{F}$是*pro*-可表的，若存在$\mathcal{R} \in \mathcal{C}_{\mathcal{O}}$，使得

$$\mathbf{F}(A) = \mathrm{Hom}(\mathcal{R}, A).$$

可表的函子显然满足Mayer-Vietoris性质。另一方面，我们有下面的定理(参见[29])。

定理2.7 (Grothendieck)**.** 令$\mathbf{F} : \mathcal{C}_{\mathcal{O}}^{\circ} \to \mathrm{Sets}$是一个协变函子且$\mathbf{F}(k)$是一个单点集。那么$\mathbf{F}$是*pro*-可表的当且仅当下面两个条件成立

1. $\mathbf{F}$满足*Mayer-Vietoris*性质；
2. $\mathbf{F}(k[\epsilon])$是一个有限集，这里$k[\epsilon] = k[X]/X^2$为对偶数。

注2.8. 在$\mathcal{C}_{\mathcal{O}}^{\circ}$中，纤维积总是存在的；在$\mathcal{C}_{\mathcal{O}}$中，纤维积不一定存在。这是我们考虑范畴$\mathcal{C}_{\mathcal{O}}^{\circ}$的一个主要原因(参见[38, Section 14])。

注2.9. 定理2.7的证明并不难，但是应用起来并不方便，主要是验证Mayer-Vietoris性质时需要考虑所有纤维积。在我们的学习中，一个更方便的判别可表性的准则是下一节的Schlessinger判别法。

2.1.3 Schlessinger判别法

令$\mathbf{F}$是一个协变函子

$$\mathbf{F} : \mathcal{C}_{\mathcal{O}}^{\circ} \to \mathrm{Sets},$$

且$\mathbf{F}(k)$是一个单点集。令$R_0, R_1, R_2 \in \mathcal{C}_{\mathcal{O}}^{\circ}$且有态射$\phi_1 : R_1 \to R_0$，$\phi_2 : R_2 \to R_0$。令

$$R_3 = R_1 \times_{R_0} R_2 = \{(r_1, r_2) \in R_1 \times R_2 \mid \phi_1(r_1) = \phi_2(r_2)\}$$

是纤维积。如上节所述，我们有自然的映射

$$\mathbf{F}(R_3) \to \mathbf{F}(R_1) \times_{\mathbf{F}(R_0)} \mathbf{F}(R_2). \tag{2.2}$$

定义2.10. 令$R,\ S \in \mathcal{C}_{\mathcal{O}}^{\circ}$，映射$\phi : R \to S$称为是小的，若$\phi$是满射，$\mathrm{Ker}(\phi)$是主理想，且$\mathfrak{m}_R \,\mathrm{Ker}(\phi) = 0$。这里$\mathfrak{m}_R$是$R$的极大理想。

现在我们可以列出Schlessiger判别条件：

H1 若$R_2 \to R_0$是小映射，那么映射(2.2)是满射；

H2 若$R_0 = k$，$R_2 = k[\epsilon]$，那么映射(2.2)是双射；

(如果**H2**成立，这时容易说明$t_{\mathbf{F}} := \mathbf{F}(k[\epsilon])$是一个$k$-线性空间，我们称之为$\mathbf{F}$的切空间。)

H3 线性空间$t_{\mathbf{F}}$是有限维的；

H4 若$R_1 = R_2$，$\phi_1 = \phi_2$都是小映射，那么映射(2.2)是双射。

我们有下面定理(参见[37, 44])。

定理2.11 (Schlessinger). *令$\mathbf{F}$是一个协变函子$\mathbf{F} : \mathcal{C}_{\mathcal{O}}^{\circ} \to \mathrm{Sets}$，且$\mathbf{F}(k)$是一个单点集。若$\mathbf{F}$满足条件H1-H4，那么$\mathbf{F}$是pro-可表的。即存在$\mathcal{R} \in \mathcal{C}_{\mathcal{O}}$，使得对任意$A \in \mathcal{C}_{\mathcal{O}}^{\circ}$，都有$\mathbf{F}(A) = \mathrm{Hom}(R, A)$。*

2.2 泛形变

2.2.1 泛形变的存在性

现在我们将Schlessinger判别法则运用到形变函子$\mathbf{D}_{\bar{\rho},\mathcal{O}}$上。

定义2.12. 令$\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$是一个模$p$的表示。

1. 定义

$$C(\bar{\rho}) := \mathrm{Hom}_{\Pi}(k^n, k^n) = \{P \in M_n(k) : \ P\bar{\rho}(g) = \bar{\rho}(g)P \quad \forall g \in \Pi\}.$$

2. 令$\rho : \Pi \to \mathrm{GL}_n(A)$是$\bar{\rho}$在$A$上的形变，定义

$$C_A(\rho) := \mathrm{Hom}_{\Pi}(A^n, A^n) = \{P \in M_n(k) : \ P\rho(g) = \rho(g)P \quad \forall g \in \Pi\}.$$

我们有如下结果。

定理2.13 (Mazur, Ramakrishna). *令Π是一个仿有限群且满足p-有限条件，$\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$是一个表示。则*

1. 形变函子$\mathbf{D}_{\bar{\rho},\mathcal{O}}$总是满足条件*H1-H3*。

2. 若进一步有$C(\bar{\rho}) = k$，则形变函子$\mathbf{D}_{\bar{\rho},\mathcal{O}}$也满足*H4*。从而存在$\mathcal{R} = \mathcal{R}(\Pi, k, \bar{\rho}) \in \mathcal{C}_{\mathcal{O}}$和形变

$$\rho^u : \Pi \to \mathrm{GL}_n(\mathcal{R})$$

使得对任意系数环A和$\bar{\rho}$在A上的形变$\rho : \Pi \to \mathrm{GL}_n(A)$，都存在唯一的映射$\pi : \mathcal{R} \to A$使得$\rho = \pi \circ \rho^u$。

我们称$\mathcal{R}$为泛形变环，ρ^u为泛形变。我们有下面的结果，从某种意义上说明了$\mathcal{R}$的唯一性。

定理2.14. 令$\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$是一个连续表示，且满足$C(\bar{\rho}) = k$。令$\bar{\rho}' : \Pi \to \mathrm{GL}_n(k)$是另一个连续表示，且满足$\bar{\rho}' = \bar{\rho} \otimes \chi$，这里$\chi : \Pi \to k^\times$是一个一维表示。那么存在一个典范同构

$$r(\bar{\rho}, \bar{\rho}') : \mathcal{R}(\Pi, k, \bar{\rho}) \to \mathcal{R}(\Pi, k, \bar{\rho}')$$

将$\bar{\rho}$的泛形变映射为$\bar{\rho}'$的泛形变。

例2.15. 这里我们考虑最简单的形变函子：$n = 1$的情形。这时

$$\bar{\rho} = \bar{\chi} : \Pi \to k^\times = \mathrm{GL}_1(k)$$

是一个一维表示。令$\Gamma = \Pi^{\mathrm{ab},(p)}$为$\Pi$的$p$-完备化的交换化，令$\gamma : \Pi \to \Gamma$为典范投射。令$\mathcal{O}[[\Gamma]]$为$\Gamma$在$\mathcal{O}$上的完备群环，即

$$\mathcal{O}[[\Gamma]] = \varprojlim_H \mathcal{O}[\Gamma/H],$$

这里H遍历Γ的所有指数有限的正规开子群。我们有自然的映射

$$\Gamma \to \mathcal{O}[[\Gamma]]$$
$$u \mapsto [u].$$

注意到$\mathcal{O}^\times \cong k^\times \times (1 + \mathfrak{m}_{\mathcal{O}})$，$\bar{\chi}$可典范提升为$\chi_0 : \Pi \to \mathcal{O}^\times$。有了这些准备工作，容易验证$\bar{\chi} : \Pi \to k^\times$的泛形变环是$\mathcal{R}(\Pi, k, \bar{\chi}) = \mathcal{O}[[\Gamma]]$，对应的泛形变是

$$\chi^u(x) = \chi_0(x)[\gamma(x)].$$

2.2.2 泛形变环的性质

在这一节里，我们固定一个表示$\bar{\rho}:\Pi\to \mathrm{GL}_n(k)$满足$C(\bar{\rho})=k$，于是其对应的形变函子$\mathbf{D}=\mathbf{D}_{\bar{\rho},\mathcal{O}}$是可表的。令$\mathcal{R}$为泛形变环，$\rho^u$为泛形变。我们首先考虑$\mathbf{D}$的切空间$t_{\mathbf{D}}:=\mathbf{D}(k[\epsilon])$，由可表性我们得到

$$t_{\mathbf{D}}=\mathbf{D}(k[\epsilon])=\mathrm{Hom}_{\mathcal{O}}(\mathcal{R},k[\epsilon])=\mathrm{Hom}_k(\mathfrak{m}_{\mathcal{R}}/(\mathfrak{m}_{\mathcal{R}}^2,\lambda),k). \tag{2.3}$$

更进一步分析，令$\rho_1:\Pi\to\mathrm{GL}_n(k[\epsilon])$是$\bar{\rho}$在$k[\epsilon]$上的一个形变，则有$\rho_1(g)=(1+b_g\epsilon)\bar{\rho}(g)$。这里我们通过典范映射$k\hookrightarrow k[\epsilon]$将$k$视为$k[\epsilon]$的子集，$b_g\in M_n(k)$。换句话说，$\rho_1$诱导了一个映射$b:\Pi\to M_n(k)$。另一方面，我们知道$\rho_1$是一个同态，这个条件告诉我们$g\mapsto b_g\in Z^1(\Pi,M_n(k))$ 是一个上环。这里Π在$\mathrm{Ad}(\bar{\rho}):=M_n(k)$上的作用为共轭作用

$$g\cdot b=\bar{\rho}(g)b\bar{\rho}(g)^{-1}.$$

不难验证，上面的对应关系给出了一个k-线性空间同构

$$t_{\mathbf{D}}\cong H^1(\Pi,\mathrm{Ad}(\bar{\rho})).$$

标准的方法也告诉我们

$$H^1(\Pi,\mathrm{Ad}(\bar{\rho}))\cong \mathrm{Ext}^1_{k[[\Pi]]}(\bar{\rho},\bar{\rho}).$$

我们有

$$t_{\mathbf{D}}=\mathbf{D}(k[\epsilon])\cong H^1(\Pi,\mathrm{Ad}(\bar{\rho}))\cong \mathrm{Ext}^1_{k[[\Pi]]}(\bar{\rho},\bar{\rho}).$$

令$d_1=\dim H^1(\Pi,\mathrm{Ad}(\bar{\rho}))$，由方程(2.3)可知:

引理2.16. *$\mathcal{R}$是$\mathcal{O}[[X_1,\dots,X_{d_1}]]$的商环。*

换句话说，我们有短正合列

$$0\to I\to \mathcal{O}[[X_1,\dots,X_{d_1}]]\to\mathcal{R}\to 0.$$

一个自然的问题是：I是不是平凡的？若I平凡，那么$\mathcal{R}$即是一个级数环，结构简单。但实际情况却比较复杂。

定理2.17. 假设$C(\bar{\rho})=k$。令$\mathcal{R}=\mathcal{R}(\Pi,k,\bar{\rho})$是对应的泛形变环，令

$$d_1=\dim H^1(\Pi,\mathrm{Ad}(\bar{\rho})),\quad d_2=\dim H^2(\Pi,\mathrm{Ad}(\bar{\rho})).$$

则有

$$\mathrm{Krull}\dim(\mathcal{R}/\lambda\mathcal{R})\geq d_1-d_2.$$

更进一步，如果$d_2=0$，那么上面的不等式为等式，并且

$$\mathcal{R}\cong\mathcal{O}[[X_1,\ldots,X_{d_1}]].$$

若$d_2=0$，我们也称相关的形变问题是无障碍的。另一方面，我们有如下猜想。

猜想2.18 (维数猜想)**.** 若$\bar{\rho}:\Pi\to\mathrm{GL}_n(k)$是绝对不可约的，那么

$$\mathrm{Krull}\dim(\mathcal{R}/\lambda\mathcal{R})=d_1-d_2.$$

2.2.3 伽罗华表示

令K是一个次数为d的数域，S是K的有限个素理想组成的集合。我们假设$\{v\mid p\}\subset S$且$S_\infty:=\{v\mid\infty\}\subset S$。令$\Pi=G_{K,S}$是$K$的在$S$外非分歧的极大扩张的伽罗华群。注意到到$G_{K,S}$满足$p$-有限条件。令

$$\bar{\rho}:\Pi\to\mathrm{GL}_n(k)$$

是一个连续表示且$C(\bar{\rho})=k$。于是其对应的形变函子pro-可表，我们有泛形变环$\mathcal{R}$和泛形变ρ^u。由上节的结论，我们知道$\mathcal{R}$可以由d_1个元素生成。这时的$d_1=\dim H^1(G_{K,S},\mathrm{Ad}(\bar{\rho}))$是伽罗华上同调群的维数，我们有许多伽罗华上同调群的定理来研究它。具体地说，利用Tate的整体欧拉示性数公式(参见[59])，我们可以给出$\mathrm{Krull}\dim(\mathcal{R}/\pi\mathcal{R})$的一个比较容易计算的下界。若$M$是一个有限$G_{K,S}$-模，且$\{v\mid\sharp M\}\subset S$，欧拉示性数公式是说

$$\frac{\sharp H^0(G_{K,S},M)\cdot\sharp H^2(G_{K,S},M)}{\sharp H^1(G_{K,S},M)}=\frac{1}{(\sharp M)^d}\prod_{v\in S_\infty}\sharp H^0(G_{K_v},M).$$

在我们考虑的情形里，$M = \mathrm{Ad}(\bar{\rho})$，从而$\sharp M$是$p$的幂次。由假设条件$\{v \mid p\} \subset S$，我们可以运用欧拉示性数公式得到

$$\begin{aligned}&\dim H^0(G_{K,S}, M) - \dim H^1(G_{K,S}, M) + \dim H^2(G_{K,S}, M)\\ =&\sum_{v \in S_\infty} \dim H^0(G_{K_v}, M) - d \dim M.\end{aligned}$$

令$d_i = \dim H^i(G_{K,S}, M)$，于是

$$d_1 - d_2 = d_0 + dn^2 - \sum_{v \in S_\infty} \dim H^0(G_{K_v}, M).$$

由条件$C(\bar{\rho}) = k$知$d_0 = 1$。我们于是证明了下面的结果。

命题2.19. *令K是$\mathbb{Q}$的d次扩域，令$\bar{\rho} : G_{K,S} \to \mathrm{GL}_n(k)$是一个表示且满足$C(\bar{\rho}) = k$，令$\mathcal{R}$是对应的泛形变环。则有*

$$\mathrm{Krull}\dim(\mathcal{R}/\lambda\mathcal{R}) \geq d_1 - d_2 = 1 + nd^2 - \sum_{v \in S_\infty} \dim H^0(G_{K_v}, M).$$

注意到上面不等式的右边相对来说容易计算：G_{K_v}的阶为1或者2，取决于v是复的或是实的；H^0对应到模的不变子集。下面我们计算两个具体例子。

例2.20 ($n = 1$)**.** 这时$\bar{\rho}$是一个一维表示。由例2.15，我们知道

$$\mathcal{R} = \mathcal{O}[[G_{K,S}^{\mathrm{ab},(p)}]].$$

从而

$$\mathcal{R}/\lambda\mathcal{R} = k[[G_{K,S}^{\mathrm{ab},(p)}]].$$

所以

$$\mathrm{Krull}\dim(\mathcal{R}/\lambda\mathcal{R}) = \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Hom}(G_{K,S}, \mathbb{Z}_p).$$

由命题我们马上得到

$$\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Hom}(G_{K,S}, \mathbb{Z}_p) \geq 1 + r_2.$$

这个不等式从伽罗华理论亦不难得出。值得说明的一点是维数猜想是说上面的不等式实为等式，而这个论断等价于*Leopoldt*猜想。

例2.21 ($K=\mathbb{Q}$, $n=2$)**.** 这时$\{p,\infty\}\subset S$。假设$p\geq 3$。这时对于复共轭c，由于$c^2=1 \pmod p$且$2\nmid p$，$\bar{\rho}(c)$只有下面两种可能

$$\bar{\rho}(c)\sim\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\text{ 或}\bar{\rho}(c)\sim\pm\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

第一种情形，$\det\bar{\rho}(c)=1$，我们称之为偶的；第二种情形，$\det\bar{\rho}(c)=-1$，我们称之为奇的。这时不难看出，在偶的情形下，$d_0=4$；在奇的情形下，$d_0=2$。从而由命题2.19知

1. 若$\bar{\rho}$是偶的，则$\mathrm{Krull}\dim(\mathcal{R}/\lambda\mathcal{R})\geq 1$；
2. 若$\bar{\rho}$是奇的，则$\mathrm{Krull}\dim(\mathcal{R}/\lambda\mathcal{R})\geq 3$；

2.3 伽罗华表示的形变

现在我们将形变理论运用到伽罗华表示上来研究模性猜想。

2.3.1 形变条件

很多时候，我们需要的并不是表示$\bar{\rho}$的所有形变，而是其中满足某些特定条件的形变。哪些条件比较合适，可以得到形变函子的子函子？由函子性，我们给出下面的定义。

定义2.22. 令$\bar{\rho}:\Pi\to\mathrm{GL}_n(k)$是一个表示。一个关于表示$\bar{\rho}$的形变条件是指群$\Pi$在系数环上的$n$-维表示的一个性质$\mathcal{P}$，满足

1. 表示$\bar{\rho}$有性质$\mathcal{P}$；
2. 给定一个形变$\rho:\Pi\to\mathrm{GL}_n(A)$和系数环的一个映射$\alpha:A\to A_1$。若$\rho$有性质$\mathcal{P}$，那么$\alpha\circ\rho$也有性质$\mathcal{P}$；
3. 若在范畴$\mathcal{C}_{\mathcal{O}}^{\circ}$中有纤维积

$$\begin{array}{ccc}A\times_C B & \xrightarrow{q} & B\\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle\beta}\\ A & \xrightarrow{\alpha} & C.\end{array}$$

令$\rho : \Pi \to \mathrm{GL}_n(A \times_C B)$是$\bar{\rho}$的一个形变。则$\rho$有性质$\mathcal{P}$当且仅当$p \circ \rho$和$q \circ \rho$ 都有性质$\mathcal{P}$；

4. 给定一个形变$\rho : \Pi \to \mathrm{GL}_n(A)$和系数环的一个单射$\alpha : A \to A_1$。若$\alpha \circ \rho$有性质$\mathcal{P}$，那么$\rho$也有性质$\mathcal{P}$.

容易验证，如果$\mathcal{P}$是关于表示$\bar{\rho}$的一个形变条件，那么

$$\begin{aligned}\mathbf{D}_{\mathcal{P}} : \mathcal{C}_{\mathcal{O}}^{\circ} &\to \mathrm{Sets}\\ A &\mapsto \{\bar{\rho}\text{在}A\text{上的满足条件}\mathcal{P}\text{的形变}\}.\end{aligned}$$

是形变函子$\mathbf{D}_{\bar{\rho},\mathcal{O}}$的子函子。我们利用连续性可以把$\mathbf{D}_{\mathcal{P}}$延拓到范畴$\mathcal{C}_{\mathcal{O}}$上，定义

$$\mathbf{D}_{\mathcal{P}}(R) = \varprojlim_m \mathbf{D}_{\mathcal{P}}(R/\mathfrak{m}_R^m).$$

命题2.23. *记号如上。函子$\mathbf{D}_{\mathcal{P}}$满足Schlessinger判别法则中的条件H1-H3。若有$C(\bar{\rho}) = k$，则$\mathbf{D}_{\mathcal{P}}$也满足H_4；从而$\mathbf{D}_{\mathcal{P}}$可表，且其对应的泛形变环$\mathcal{R}_{\mathcal{P}}$是泛形变环$\mathcal{R}(\bar{\rho}, \Pi, k)$的一个商环。*

接下来我们给出一些形变条件的例子。

例2.24 (具有给定行列式的形变)**.** 令$\delta : \Pi \to \mathcal{O}^{\times}$是一个连续同态。对任意$\mathcal{O}$-代数$R$，令$\delta_R$是下面的复合映射

$$\delta_R : \Pi \xrightarrow{\delta} \mathcal{O}^{\times} \to R^{\times}.$$

我们称$\bar{\rho}$的一个形变$\rho : \Pi \to \mathrm{GL}_n(R)$有行列式$\delta$，如果$\det \rho = \delta_R$。我们将性质有行列式$\delta$简记为$\det = \delta$，它有下面的性质。

1. 若$\bar{\rho}$的行列式是δ，那么性质$\det = \delta$是一个形变条件。

2. 若$p \nmid n$，则有

$$\mathbf{D}_{\det=\delta}(k[\epsilon]) = H^1(\Pi, \mathrm{Ad}^0(\bar{\rho})) \subset H^1(\Pi, \mathrm{Ad}(\bar{\rho})).$$

3. 若$p \mid n$，则有

$$\mathbf{D}_{\det=\delta}(k[\epsilon]) = \mathrm{Im}(H^1(\Pi, \mathrm{Ad}^0(\bar{\rho})) \to H^1(\Pi, \mathrm{Ad}(\bar{\rho}))).$$

例2.25 (范畴化形变). 令$\mathcal{M}_{\mathcal{O}}$是由长度有限的、具有$\Pi$-作用的$\mathcal{O}$-模组成的范畴，令$\mathbb{P}$是$\mathcal{M}_{\mathcal{O}}$的满子范畴，并假设$\mathbb{P}$在取子对象、商对象、有限直和下都是封闭的。给定$\bar{\rho}$，我们说$\bar{\rho}$ 的一个形变$\rho : \Pi \to \mathrm{GL}_n(R)$是$\mathbb{P}$-型的，如果对任意$m$，表示$\rho_m : \Pi \to \mathrm{GL}_n(R/\mathfrak{m}_R^m)$都对应到$\mathbb{P}$中的一个对象。

假设$\bar{\rho}$是$\mathbb{P}$-型的，那么性质表示是$\mathbb{P}$-型是一个形变条件。这里一类非常重要的例子来自p-进Hodge理论，而在Wiles的证明里，最重要的例子是要求表示是平坦的(定义1.6)。

例2.26 (正规形变). 正规形变最初是Mazur在研究形变理论和Hida的正规p-进模形式理论时提出来的。令R是一个系数环，$I \subset \Pi$是一个子群。令$\rho : \Pi \to \mathrm{GL}_2(R)$是一个表示，并记$M = R \times R$是给出$\rho$的自由$R$-模。我们说$\rho$是$I$-正规的，如果$M^I \subset M$是一个秩为一的$R$-模且是$M$的一个直和项。

假设$\bar{\rho}$是I-正规的，那么性质表示是I-正规的是一个形变条件。对于伽罗华表示，参见定义1.6。

2.3.2 整体伽罗华表示的形变条件

回到我们最感兴趣的情形$\Pi = G_{\mathbb{Q},S}$。令$\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_n(k)$ 是一个表示。一个整体伽罗华形变问题$\mathcal{Q}$是指形变函子$\mathbf{D}_{\bar{\rho}}$的一个子函子，对每一个有限素数$\ell \in S$，局部表示$\bar{\rho}|_{G_{\mathbb{Q}_\ell}}$都给出一个形变条件$\mathcal{Q}_\ell$。

引理2.27. 对于表示$\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_n(k)$，一个整体伽罗华形变问题$\mathcal{Q}$是一个形变条件。

在可表的情况下，我们想要了解满足性质$\mathcal{Q}$的所有的形变，只需要了解其对应的泛形变环$\mathcal{R}_{\mathcal{Q}}$；而要了解泛形变环$\mathcal{R}_{\mathcal{Q}}$，第一步便是了解函子$\mathbf{D}_{\mathcal{Q}}$的切空间维数，因为这个维数告诉我们环$\mathcal{R}_{\mathcal{Q}}$可以由多少个元素生成。令$H^1_{\mathcal{Q}}(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho})) \subset H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))$对应到函子$\mathbf{D}_{\mathcal{Q}}$的切空间，我们有如下结果。

定理2.28. 记号如上，我们有交换图

$$\begin{array}{ccc} H^1_{\mathcal{Q}}(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho})) & \longrightarrow & H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho})) \\ \downarrow & & \downarrow \\ \oplus_{\ell \in S} H^1_{\mathcal{Q}_\ell}(G_{\mathbb{Q}_\ell}, \mathrm{Ad}(\bar{\rho})) & \longrightarrow & \oplus_{\ell \in S} H^1(G_{\mathbb{Q}_\ell}, \mathrm{Ad}(\bar{\rho})). \end{array}$$

这里水平箭头都是包含关系。更进一步，这个图是*Cartesian*的。

2.3.3 模性形变

假设$f \in S_k(\Gamma_1(N), \mathbb{Z}_p)$，令$\bar{\rho} := \bar{\rho}_f$。任意一个特征形式$f$对应到一个同态$\mathbb{T}(\Gamma_1(N), k) \to \mathbb{Z}_p$，模$p$之后得到同态

$$\mathbb{T}(\Gamma_1(N), k) \to \mathbb{F}_p.$$

这个同态的核是Hecke代数的一个极大理想$\mathfrak{m}$。令$\mathbb{T}(\bar{\rho})$是$\mathbb{T}(\Gamma_1(N), k)$在$\mathfrak{m}$处的完备化。由伽罗华表示模性的定义，我们知道$\mathbb{T}(\bar{\rho})$给出所有的$\bar{\rho}$的从权重$k$、水平$\Gamma_1(N)$模形式得到的形变。从而我们有满射

$$\mathcal{R}(\bar{\rho}) \twoheadrightarrow \mathbb{T}(\bar{\rho}).$$

如果这个满射是同构，即是说$\bar{\rho}$的所有形变都是模性的，这与事实不符。另一方面，我们可以从模性形变的性质出发，找出形变条件$\mathcal{Q}$，并得到满射

$$\mathcal{R}_{\mathcal{Q}}(\bar{\rho}) \twoheadrightarrow \mathbb{T}(\bar{\rho}).$$

Wiles的证明中一个很重要的工作是找到了精准的形变条件$\mathcal{Q}$，使得上面的满射是同构。我们在下面会详细介绍这个条件。

2.4 定理1.18的证明

回到定理1.18，我们要证明半稳定的椭圆曲线$E/\mathbb{Q}$是模性的，由定理1.17，即要证明对某个p，伽罗华表示$\rho_{E,p}$是模性的。注意到$\rho_{E,p}$ 是$\bar{\rho}_{E,p}$的满足若干条件的形变(定理1.7)，Wiles的思路即是证明满足这些条件的所有的$\bar{\rho}_{E,p}$的形变都是模性的，从而$\rho_{E,p}$必定是模性的。

令$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$是一个伽罗华表示。假设$\bar{\rho}$满足下列条件：

1. $\bar{\rho}|_{G_L}$是绝对不可约的，这里$L = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$；
2. $\det \bar{\rho} = \bar{\chi}_p$；
3. $\bar{\rho}$是模性的；

4. $\bar{\rho}$是半稳定的。

令$S = \{\ell \neq p \mid \bar{\rho}$在$\ell$处分歧$\}$，$\Sigma$是有限个素数组成的集合且$\Sigma \cap S = \emptyset$。考虑$\bar{\rho}$的整体形变问题$\mathcal{D}_\Sigma$:

- $\det \rho = \chi_p$;
- ρ在$S \cup \Sigma$外非分歧;
- ρ在Σ外是半稳定的;
- 若$p \notin \Sigma$且$\bar{\rho}$在p处是平坦的，则ρ在p处是平坦的。

这个整体形变问题给我们一个泛形变环$\mathcal{R}_{\mathcal{D}_\Sigma}$。方便起见，若$X$是一个由有限个素数组成的集合，我们用同一个字母$X$表示集合中素数的乘积。令$\mathbb{T}_\Sigma$是完备化的Hecke代数，且给出所有的由权重为2、水平为$\Gamma_0(S\Sigma)$ 的模形式构造出来的形变。由定理1.15，我们有满射

$$\mathcal{R}_{\mathcal{D}_\Sigma} \to \mathbb{T}_\Sigma.$$

Wiles证明了如下结果。

定理2.29. *满射$\mathcal{R}_{\mathcal{D}_\Sigma} \to \mathbb{T}_\Sigma$是一个同构。*

这样的结果称之为$R = T$定理。我们将在下一节介绍这个定理的证明，下面我们从这个定理出发，完成定理1.18的证明。首先由定理2.29，我们有下面的推论。

推论2.30. *令E是定义在$\mathbb{Q}$上的椭圆曲线。假设对某一个$p \geq 3$，$\bar{\rho}_{E,p}$是模性的、绝对不可约的，那么E是模性的。*

注2.31. 当E是半稳定的，Serre的一个结果[46, Prop. 21]告诉我们：对所有$p \geq 3$，$\bar{\rho}_{E,p}$要么是满的，要么是可约的；从而这时$\bar{\rho}_{E,p}$不可约等价于$\bar{\rho}_{E,p}$绝对不可约。更进一步，若$p = 3$，$\bar{\rho}_{E,p}$绝对不可约等价于$\bar{\rho}|_{G_{\mathbb{Q}(\sqrt{-3})}}$绝对不可约。所以$p = 3$时，推论2.30的条件可以放松为：$\bar{\rho}_{E,3}$是模性的、不可约的。

Langlands-Tunnell(参见[36, 57])对模3的伽罗华表示证明了如下的结果。

定理2.32. *若$\bar{\rho}_{E,3}$是不可约的，那么$\bar{\rho}_{E,3}$是模性的。*

注2.33. 上面的定理是Langlands-Tunnell结果的一个特殊情况，他们的主要工具是迹公式和Base change的技巧，属于自守表示的范畴。我们简单解释其内容：

1. 连续表示$\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$的像必定是有限的，其在$\mathrm{PGL}_2(\mathbb{C})$中的像只可能是$\mathbb{R}^3$中某个正多面体的对称群[47, Section 13]。从而若σ是不可约的，那么其在$\mathrm{PGL}_2(\mathbb{C})$中的像只有如下几种可能：$A_5$(十二面体)，$S_4$(八面体)，$A_4$(四面体)，$D_{2n}$(二面体)。Langlands-Tunnell证明了：*若σ 是奇的、不可约的，且在$\mathrm{PGL}_2(\mathbb{C})$中的像是可解的，那么$\sigma$是模性的。*在二面体情形时，$\sigma$的模性已由Hecke和Maass证明；Langlands和Tunnell 证明了八面体群和四面体群的情形。

2. Langlands和Tunnell证明了从σ可以构造出$\mathrm{GL}_2/\mathbb{Q}$的一个自守表示。而在$\sigma(c) = -1$时，从他们构造出的自守表示可以构造出一个新形式f，使得$\sigma \cong \rho_f$，从而σ是模性的。

3. 我们关注的表示是模3的表示，但是这样的表示可以通过下面的同态提升为一个定义在$\mathbb{C}$上的表示

$$\Psi : \mathrm{GL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \subset \mathrm{GL}_2(\mathbb{C})$$
$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{pmatrix}$$

   注意到$\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$是可解的，我们便得到了$\bar{\rho}_{E,3}$的模性。

现在还有一个问题：$\bar{\rho}_{E,3}$有可能是可约的。这时候没有办法运用上面的结果。Wiles从Mazur的一个结果出发(参见[42])，利用所谓的*3-5*变换技巧解决了这个困难。

定理2.34. 设E是一条定义在$\mathbb{Q}$上的半稳定的椭圆曲线，那么$\bar{\rho}_{E,3}$和$\bar{\rho}_{E,5}$中至少有一个是不可约的。

注2.35. 假设$\bar{\rho}_{E,3}$和$\bar{\rho}_{E,5}$都是可约的，那么$E[15]$有一个15阶子群C在伽罗华作用下不变，于是(E,C)对应到模曲线$X_0(15)(\mathbb{Q})$中的一个点。然而集合$X_0(15)(\mathbb{Q})$是一个有限集，其对应的椭圆曲线在5处都不是半稳定的。参见[42, Lemma 9]。

定理2.36. 设E是一条定义在$\mathbb{Q}$上的半稳定的椭圆曲线且$\bar{\rho}_{E,5}$是不可约，那么存在另外一条半稳定的定义在$\mathbb{Q}$上的椭圆曲线E'，满足：

1. $\bar{\rho}_{E',3}$是不可约的；
2. $\bar{\rho}_{E',5} \cong \bar{\rho}_{E,5}$.

注2.37. 在[42, Section 4]中，Rubin构造了一组椭圆曲线$E'/\mathbb{Q}$满足定理2.36的两个条件，所有曲线在5之外都是半稳定的。在这组曲线里取一条在5-进意义下非常靠近E 的曲线，这条曲线即满足定理2.36中的所有条件。

当我们考虑$\bar{\rho}_{E,5}$的时候，需要了解$\bar{\rho}_{E,5}|_{G_{\mathbb{Q}(\sqrt{5})}}$的性质，对此，我们有下面的结果(参见[42, Proposition 7])。

命题2.38. 令$E/\mathbb{Q}$是一条椭圆曲线，E在5处半稳定，且$\bar{\rho}_{E,5}$不可约，那么$\bar{\rho}_{E,5}|_{G_{\mathbb{Q}(\sqrt{5})}}$绝对不可约。

现在，利用上面的结果，我们可以证明定理1.18。

定理1.18的证明. 令$E/\mathbb{Q}$是一条半稳定的椭圆曲线。若$\bar{\rho}_{E,3}$是不可约的，那么由定理2.32可知E是模性的。若$\bar{\rho}_{E,3}$是可约的，那么$\bar{\rho}_{E,5}$是不可约的；存在半稳定的椭圆曲线$E'/\mathbb{Q}$满足定理2.36中的两个条件；将定理2.32运用到$\bar{\rho}_{E',3}$上，我们知道$\bar{\rho}_{E',3}$是模性的，从而$\bar{\rho}_{E',5} \cong \bar{\rho}_{E,5}$是模性的；最后将推论2.30运用到$\bar{\rho}_{E,5}$上，得到$E$是模性的。 □

3 $R = T$

在这一节里，我们通过构造所谓的Diamond-Taylor-Wiles系统来证明定理2.29。这里我们不采用Wiles最初的证明，而是采用Faltings、Diamond、Fujiwara等简化后证明(参见[16, 24])。两个方法的思路基本一致，只是细节稍有区别。在了解了更多内容后，我们将在节4.2.3中解释它们的区别。

定理2.29的证明分为两个部分。第一个部分是$\Sigma = \emptyset$的情形，即所谓的极小情形，这里我们的工具是定理3.1。第二个部分是一般情形，简单地说，我们利用定理3.3，对Σ中的元素个数做归纳法。

3.1 自由性的判别方法

3.1.1 Patching

这里我们给出一个判别特定模的自由性的交换代数结果，这个结果最开始由Wiles和Taylor-Wiles提出，然后由Faltings和Diamond简化(参见[56, 60, 16, 24])。

给定正整数r。令$A = k[[S_1, \dots, S_r]]$，$B = k[[X_1, \dots, X_r]]$，令$\mathfrak{n}$是A的极大理想。

定理3.1. *令R是一个k-代数，H是一个非零R-模且在k-上是有限维的。若对任意的正整数n，都存在k-代数映射$\varphi_n : A \to B$和$\psi_n : B \to R$，B-模H_n，B-线性映射$\pi_n : H_n \to H$，并且这些对象满足：*

1. *ψ_n是满射且$\psi_n\varphi_n(\mathfrak{n}) = 0$；*
2. *π_n诱导了一个同构$H_n/\mathfrak{n}H_n \to H$；*
3. *$\operatorname{Ann}_A H_n = \mathfrak{n}^n$且$H_n$是自由$A/\mathfrak{n}^n$-模。*

那么R是维数为零的完备交，且H是一个自由R-模。

证明. 令$d = \dim_k H$并取定H的一组基$x_1, \dots, x_d$。对每一个$n \geq 1$和$i = 1, \dots, d$，选取$x_{i,n} \in H_n$使得$\pi_n(x_{i,n}) = x_i$。由Nakayama引理，$x_{1,n}, \dots, x_{d,n}$构

成H_n的一组$(A/\mathfrak{n}^n A)$-基。利用$H_n \cong (A/\mathfrak{n}^n A)^d$，$H_n$的$B$-模结构给我们一个$A$-代数同态

$$\mu_n : B \to M_d(A/\mathfrak{n}^n A).$$

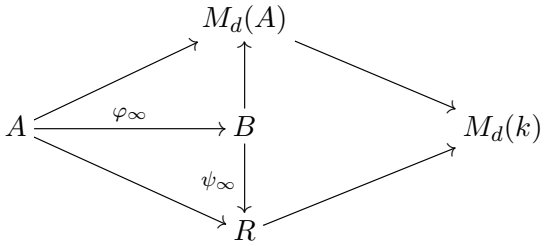
对每一个$n \geq 1$和$j = 1, \ldots, r$，选取$\mu_n(X_j) \in M_d(A/\mathfrak{n}^n A)$ 的提升$\nu_n(X_j) \in M_d(A)$。注意到$B^r \times R^r \times M_d(A)^r$是紧的，序列

$$(\varphi_n(S_1), \ldots, \varphi_n(S_r), \psi_n(X_1), \ldots, \psi_n(X_r), \nu_n(X_1), \ldots, \nu_n(X_r))$$

有一个收敛子列。选取一个极限点

$$(\varphi_\infty(S_1), \ldots, \varphi_\infty(S_r), \psi_\infty(X_1), \ldots, \psi_\infty(X_r), \nu_\infty(X_1), \ldots, \nu_\infty(X_r))$$

容易验证，φ_∞、ψ_∞、ν_∞都可延拓为k-代数同态。另一方面，我们有交换图



这里$A \to M_d(A)$和$M_d(A) \to M_d(k)$为自然映射，$A \to R$通过k分解，$R \to M_d(k)$由R在H上的作用给出。上面的构造同时也给了我们一个A上的秩为d的自由A-模，记为H_∞。同时我们有

- ψ_∞是满的
- $\psi_\infty \varphi_\infty(\mathfrak{n}) = 0$
- 作为B-模，有同构$H_\infty/\mathfrak{n}H_\infty \cong H$

注意到$\varphi_\infty(S_1), \ldots, \varphi_\infty(S_r)$是一个$H_\infty$-正则序列，所以

$$\operatorname{depth}_B H_\infty = r.$$

由Auslander-Buchsbaum-Serre定理(参见[7, Theorem 2.2.7])，H_∞作为B-模的投射维数是有限的。由Auslander-Buchsbaum公式(参见[7, Theorem 1.3.3])，我们有

$$\operatorname{depth}_B H_\infty + \operatorname{proj\,dim}_B H_\infty = \operatorname{depth} B.$$

从而$\operatorname{proj\,dim}_B H_\infty = 0$，即$H_\infty$是一个自由$B$-模。故$H$是一个自由$(B/\varphi_\infty(\mathfrak{n})B)$-模，且$\psi_\infty$诱导了同构

$$B/\varphi_\infty(\mathfrak{n})B \to R.$$

从而定理结论成立。 □

3.1.2 数值判别法

在这一节里，$\mathcal{O}$是一个完备的离散赋值环，λ和k分别是$\mathcal{O}$的素元和剩余类域。选定一个系数环$R \in \mathcal{C}_\mathcal{O}$以及一个$\mathcal{O}$-同态$\pi : R \to \mathcal{O}$。令$\mathfrak{p} = \operatorname{Ker}(\pi)$和$I = \operatorname{Ann}_R \mathfrak{p}$。

定理3.2. *令T是一个局部的、诺特的$\mathcal{O}$-代数，并且作为$\mathcal{O}$-模，T是有限自由的。令$\phi : R \to T$是一个$\mathcal{O}$-代数满射且$\operatorname{Ker}\phi \subset \mathfrak{p}$。令$\pi_T : T \to \mathcal{O}$满足$\pi_T \circ \phi = \pi$，令$\mathfrak{p}_T = \operatorname{Ker}(\pi_T)$，$I_T = \operatorname{Ann}_T \mathfrak{p}_T$。若$\pi_T(I_T)$非零，则下列条件等价：*

1. *$\pi_T(I_T) \subset \operatorname{Fitt}_\mathcal{O}(\mathfrak{p}/\mathfrak{p}^2)$;*
2. *$\pi_T(I_T) = \operatorname{Fitt}_\mathcal{O}(\mathfrak{p}/\mathfrak{p}^2)$;*
3. *R是一个完备交且ϕ是一个同构。*

当T是Gorenstein时，这个结果最初由Wiles证明；一般情形由Lenstra证明。Diamond从这个结果出发，给出了下面的数值判别法(参见[16])。

定理3.3. *令H是一个R-模，作为$\mathcal{O}$-模是有限自由的，且$H_\mathfrak{p} \neq \{0\}$。令$\Omega = H/(H[\mathfrak{p}_T]+H[I_T])$，这里$T = R/\operatorname{Ann}_R H$。令$d = \operatorname{rank}_\mathcal{O} H[\mathfrak{p}]$。若$\operatorname{length}_\mathcal{O}\Omega < \infty$，则下列条件等价：*

1. *$\operatorname{rank}_\mathcal{O} H \leq d \cdot \operatorname{rank}_\mathcal{O} T$，且$\operatorname{length}_\mathcal{O}\Omega \geq d \cdot \operatorname{length}_\mathcal{O}(\mathfrak{p}/\mathfrak{p}^2)$;*

2. $\operatorname{rank}_{\mathcal{O}} H = d \cdot \operatorname{rank}_{\mathcal{O}} T$，且$\Omega \cong (\mathcal{O}/\operatorname{Fitt}_{\mathcal{O}}(\mathfrak{p}/\mathfrak{p}^2))^d$；

3. R是一个完备交，且H是一个秩为d的自由R-模。

证明. “2⇒1”是显然的。

“3⇒2”：由假设条件知R是有限自由$\mathcal{O}$-代数。由于R是Gorenstein，$\mathcal{O}$-模$R[\mathfrak{p}] = I$的秩为一。另一方面，我们有$R[I] = \mathfrak{p}$，从而$\pi(I) = \operatorname{Fitt}_{\mathcal{O}}(\mathfrak{p}/\mathfrak{p}^2)$。故条件2成立。

“1⇒3”：首先注意到作为$\mathcal{O}$-模，$H[\mathfrak{p}_T] = H[\mathfrak{p}]$的秩为$d$。由于$H/H[I_T]$是自由$\mathcal{O}$-模且秩至多为$d$，从而作为$\mathcal{O}$-模，$\Omega$可以由$d$ 个元素生成。故$H/H[I_T]$的秩为d。同时我们也有$H[\mathfrak{p}_T] \cap H[I_T] = \{0\}$且

$$\operatorname{Fitt}_{\mathcal{O}}(\mathfrak{p}/\mathfrak{p}^2) \supset \operatorname{Ann}_{\mathcal{O}}(H/H[\mathfrak{p}_T] \oplus H[I_T]) \supset \pi_T(I_T).$$

由于$\mathfrak{p}/\mathfrak{p}^2$长度有限，所以$\pi_T(I_T)$的长度有限。由定理3.2，$\phi$是一个同构且$R$是一个完备交，$R$是一个有限自由$\mathcal{O}$-代数。

上面的讨论告诉我们$\operatorname{rank}_{\mathcal{O}} H \leq d \cdot \operatorname{rank}_{\mathcal{O}} R$且$\Omega \cong (\mathcal{O}/\pi(I))^d$。由于$HI \subset H[\mathfrak{p}]$，$\mathcal{O}$-模$\Omega$是$H/(H[I] + IH)$的商模，从而可以由$d$ 个元素生成且被$\pi(I)$零化。故$IH = H[\mathfrak{p}]$是秩为d的自由$\mathcal{O}$-模。

令$\bar{R} = R \otimes_{\mathcal{O}} k$，$\mathfrak{m}$是$\bar{R}$的极大理想，$\bar{H} = H \otimes_{\mathcal{O}} k$。由于$\bar{R}$是Gorenstein，我们知道$\bar{R}[\mathfrak{m}] = I\bar{R}$是一维的$k$-空间。由于$H/IH$ 是无扰的，$I\bar{H}$是d-维的k-向量空间。取$x_1, \ldots, x_d \in \bar{H}$使得$I\bar{H} = \oplus_i I x_i$，定义映射

$$\alpha : \bar{R}^d \to \bar{H}$$
$$(r_1, \ldots, r_d) \mapsto \sum r_i x_i.$$

令$V = \operatorname{Ker}(\alpha)$。由于$V \cap I\bar{R}^d = 0$，故$V[\mathfrak{m}] = 0$，进而得到$V = 0$，$\alpha$是单射。由于$\alpha$两边的对象的维数相等，故$\alpha$是同构，从而$H$是$R$上秩为$d$的自由模。 □

3.2 系统的构造

现在我们回到节2.4给出的$\bar{\rho}$和形变问题，并为之构造一个Diamond-Taylor-Wiles系统。

3.2.1 辅助素数的存在性

令$W = \mathrm{Ad}^0(\bar{\rho})$，令

$$W^* = \mathrm{Hom}(W, \mu_p) \cong W(1) \cong \mathrm{Symm}^2(\bar{\rho}).$$

局部形变条件给出了有限奇异结构

$$0 \to L_\ell \to H^1(G_\ell, W) \to H^1(G_\ell, W)/L_\ell \to 0.$$

定义Selmer群

$$H^1_{\mathcal{D}_\Sigma}(\mathbb{Q}, W) = \mathrm{Ker}(H^1(G_{\Sigma\cup S}, W) \to \prod_{v\in S\cup\Sigma} H^1(G_v, W)/L_v).$$

由形变理论，我们知道

$$H^1_{\mathcal{D}_\Sigma}(\mathbb{Q}, W) \cong \mathrm{Hom}(\mathfrak{m}_{\mathcal{R}_\Sigma}/(\pi, \mathcal{R}_\Sigma^2), k).$$

即作为$\mathcal{O}$-代数，$\mathcal{R}_\Sigma$可以由$r(\Sigma) = \dim H^1_{\mathcal{D}_\Sigma}(\mathbb{Q}, W)$个元素生成。

定义对偶Selmer群

$$H^1_{\mathcal{D}^*_\Sigma}(\mathbb{Q}, W^*) = \mathrm{Ker}(H^1(G_{\Sigma\cup S}, W^*) \to \prod_{v\in S\cup\Sigma} H^1(G_v, W^*)/L_v^*).$$

尽管Selmer群和对偶Selmer群自身的大小很难计算，它们之间的关系并不复杂。由Tate-Poitou正合列(参见[59])，我们有下面的定理。

定理3.4. *记号如上，我们有*

$$\frac{\sharp H^1_{\mathcal{D}_\Sigma}(\mathbb{Q}, W)}{\sharp H^1_{\mathcal{D}^*_\Sigma}(\mathbb{Q}, W^*)} = \frac{\sharp H^0(\mathbb{Q}, W)}{\sharp H^0(\mathbb{Q}, W^*)} \prod_{v|\infty} \frac{\sharp L_v}{\sharp H^0(G_v, W)}.$$

在我们考虑的情形下，直接计算可以得到

$$r(\Sigma) = \dim_k H^1_{\mathcal{D}_\Sigma}(\mathbb{Q}, W) = \dim_k H^1_{\mathcal{D}^*_\Sigma}(\mathbb{Q}, W^*) + \sharp\Sigma.$$

Wiles的一个重要发现是我们可以选取特别的Σ，使得$H^1_{\mathcal{D}^*_\Sigma}(\mathbb{Q}, W^*) = \{0\}$，从而很好地控制$r(\Sigma)$。具体地说，我们有下面的结果(参见[48, 60])。

命题3.5. 存在一个正整数r，使得对任意正整数n，都存在一个素数组成的集合Q，满足

1. Q中有r个元素且$Q \cap S = \emptyset$；
2. 对任意$q \in Q$，有$q \equiv 1 \pmod{p^n}$；
3. 对任意$q \in Q$，$\bar{\rho}(\mathrm{Frob}_q)$的两个特征值不相等且都属于$k$；
4. $H^1_{\mathcal{D}^*_Q}(\mathbb{Q}, W^*) = \{0\}$，从而$\mathcal{R}_Q$作为$\mathcal{O}$-代数，可以由$r$个元素生成。

证明. 注意到

$$H^1_{\mathcal{D}^*_Q}(\mathbb{Q}, W^*) = \mathrm{Ker}(H^1_{\mathcal{D}^*}(Q, W^*) \to \prod_{q \in Q} H^1(G_q/I_q, W^*)).$$

我们只要证明对任意的$0 \neq [\varphi] \in H^1_{\mathcal{D}^*_Q}(\mathbb{Q}, W^*)$，都存在无穷多$q \notin S$，满足

1. $q \equiv 1 \pmod{p^n}$；
2. $\bar{\rho}(\mathrm{Frob}_q)$有两个不等的特征值；
3. $\mathrm{res}_q([\varphi]) \neq 0$.

然后我们可以一步步把$H^1_{\mathcal{D}^*_Q}(\mathbb{Q}, W^*)$的维数减少一，直到$H^1_{\mathcal{D}^*_Q}(\mathbb{Q}, W^*) = \{0\}$。由Cebotarev密度定理，我们只要证明存在$\sigma \in G_{\mathbb{Q}}$满足

1. $\sigma|_{\mathbb{Q}(\zeta_{p^n})} = 1$;
2. $\bar{\rho}(\sigma)$的特征值不等；
3. $\varphi_\sigma \notin (\sigma - 1)W^*$.

事实上，若我们找到了这样一个σ，令q是一个素数满足$\sigma|_L = \left(\frac{L/\mathbb{Q}}{\mathfrak{q}}\right)$，这里$L$是$\mathbb{Q}$的一个有限扩张，且包含$\mathbb{Q}(\zeta_{p^n})$和$\bar{\rho}$及$\varphi$的分裂域；$\mathfrak{q}$是$L$的一个素理想且$\mathfrak{q} \mid q$。这个$q$便满足所需条件。

令F是$\mathrm{Ker}(\bar{\rho})$对应的$\mathbb{Q}(\zeta_{p^n})$的扩张，K是$\mathrm{Ker}(\mathrm{Ad}^0\,\bar{\rho})$对应的$\mathbb{Q}(\zeta_{p^n})$ 的扩张，$H = \mathrm{Gal}(K/\mathbb{Q}(\zeta_{p^n}))$，$\tilde{H} = \mathrm{Gal}(F/\mathbb{Q}(\zeta_{p^n})) \subset \tilde{G} = \mathrm{Im}(\bar{\rho})$。又$\mathrm{Ker}(\mathrm{Im}(\bar{\rho}) \to \mathrm{Im}(\mathrm{Ad}^0\,\bar{\rho}))$对应到$\mathrm{Im}\,\bar{\rho}$中的数乘矩阵，我们有

$$H = \tilde{H}k^\times/k^\times \subset G = \mathrm{Im}(\mathrm{Ad}^0\,\bar{\rho}) \subset \mathrm{PGL}_2(k).$$

由[48, Lemma 19]，$H^1(K/\mathbb{Q}, W^*) = 0$。于是

$$0 \neq \varphi|_{G_K} \in \mathrm{Hom}(G_K, W^*)^{\mathrm{Gal}(K/\mathbb{Q})}.$$

由于$\bar{\rho}|_{G_L}$不可约，从而W^*不可约。又由于$\varphi(G_K)$是W^*的不变子空间，从而必有$\varphi(G_K) = W^*$。

假设对任意的$\sigma \in G_{\mathbb{Q}(\zeta_{p^n})}$，$\bar{\rho}(\sigma)$的两个特征值都相等，从而可以选定一组基，使得$\bar{\rho}(G_{\mathbb{Q}(\zeta_{p^n})})$包含在上三角矩阵中。这会与$\bar{\rho}$ 的不可约假设条件矛盾。所以我们选取$\sigma_0 \in G_{\mathbb{Q}(\zeta_{p^n})}$，使得$\bar{\rho}(\sigma_0)$的两个特征值不相等，记它们为$\alpha$，$\beta$。

作用在W上，σ_0的特征值为α/β，1，β/α。由于σ_0作用在单位根ζ_p上是平凡的，作用在W^* 上，σ_0的特征值也为α/β，1，β/α。从而$(\sigma_0 - 1)W^* \neq W^*$，故$\varphi(G_K) \not\subset (\sigma_0 - 1)W^*$。

现在令$\tau \in G_K$并考虑$\sigma = \tau\sigma_0$。注意到τ在W和W^*上的作用都是平凡的。由于$\bar{\rho}(\tau)$是数乘矩阵，$\bar{\rho}(\sigma)$的两个特征值是不同的，且$\sigma(\zeta_{p^n}) = \zeta_{p^n}$。现在

$$\varphi_\sigma = \tau\varphi_{\sigma_0} + \varphi_\tau = \varphi_{\sigma_0} + \psi_\tau.$$

我们总是可以选取τ，使得$\varphi_\sigma \notin (\sigma - 1)W^* = (\sigma_0 - 1)W^*$，从而命题得证。

□

3.2.2 泛形变环$\mathcal{R}_Q$

选取素数的集合Q，满足

1. 对任意$q \in Q$，有$q \equiv 1 \pmod{p^n}$；
2. 对任意$q \in Q$，$\bar{\rho}(\mathrm{Frob}_q)$的两个不同的特征值$\alpha_q$和$\beta_q$，且都属于$k$；

若$q \in Q$，令Δ_q是$(\mathbb{Z}/q\mathbb{Z})^\times$的极大的阶为$p$的幂次的商群。记$\Delta_Q = \prod_{q\in Q} \Delta_q$。定义

$$\Gamma_Q = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(NQ) \mid a^{-1}d = 1 \in \Delta_Q\}.$$

考虑模曲线$X_0(NQ)$和$X(\Gamma_Q)$及其上同调群$H^1_{\mathrm{et}}(X_0(NQ)\otimes\bar{\mathbb{Q}}, \mathbb{Z}_p)$和$H^1_{\mathrm{et}}(X(\Gamma_Q)\otimes\bar{\mathbb{Q}}, \mathbb{Z}_p)$。令$\mathbb{T}(NQ, \mathcal{O})$和$\mathbb{T}(\Gamma_Q, \mathcal{O})$分别是对应的Hecke代数。令$\mathfrak{m}_Q$是由下面

映射的核给出的Hecke代数的极大理想

$$\begin{aligned}\mathbb{T}(NQ,\mathbb{Z}_p)\text{或}\mathbb{T}(\Gamma_Q,\mathbb{Z}_p)&\to k\\ T_x&\mapsto \mathrm{Tr}(\bar\rho(\mathrm{Frob}_x))\quad (x\nmid pNQ)\end{aligned}$$

引理3.6. 记号如上，我们有

1. 若$q\in Q$，则$\rho_Q^u|_{G_q}\sim\chi_{\alpha,q}\oplus\chi_{\beta,q}$。这里$\chi_{\alpha,q}\pmod{\mathfrak{m}_{\mathcal{R}_Q}}$和$\chi_{\beta,q}\pmod{\mathfrak{m}_{\mathcal{R}_Q}}$是非分歧特征，并且把$\mathrm{Frob}_q$分别映射到$\alpha_q$和$\beta_q$。

2. 特征$\chi_{\alpha,q}\circ\mathrm{Art}|_{\mathbb{Z}_q^\times}:\mathbb{Z}_q^\times\to\mathcal{R}_Q^\times$分解通过$\mathbb{Z}_q^\times\to(\mathbb{Z}_q/z\mathbb{Z}_q)^\times\to\Delta_q$。从而我们可以将$\mathcal{R}_Q$视为$\mathcal{O}[\Delta_Q]$-模。

3. 泛形变性质诱导出一个满射

$$\mathcal{R}_Q\to\mathbb{T}(\Gamma_Q,\mathcal{O})_{\mathfrak{m}_Q}.$$

为方便起见，记$H^1(K)=H^1_{\text{ét}}(X(K)\otimes\bar{\mathbb{Q}},\mathbb{Z}_p)$。我们有下列结果。

引理3.7. 1. 对任意$q\in Q$，映射

$$\begin{aligned}\eta:H^1(\Gamma_0(NQ/q)_{\mathfrak{m}_{Q/q}}&\to H^1(\Gamma_0(NQ))_{\mathfrak{m}_Q}\\ f&\mapsto A_q1_*f-\begin{pmatrix}1&0\\0&q\end{pmatrix}_*f\end{aligned}$$

是一个同构。这里$A_q\in\mathbb{T}(NQ,\mathbb{Z}_p)$是$\alpha_q$的提升。

2. $H^1(\Gamma_Q)$是一个自由的$\mathcal{O}[\Delta_Q]$-模。

3. $(H^1(\Gamma_Q)_{\Delta_Q})_{\mathfrak{m}}\cong H^1(\Gamma_0(N))_{\mathfrak{m}}$，且这个同构与*Hecke*算子的作用相容。

3.3 定理2.29的证明

3.3.1 极小情形

对任意正整数m，取素数集Q_n满足

1. $\sharp Q_n=\dim H^1(G_F,\mathrm{Ad}^0\,\bar\rho(1))$;

2. 任意$q \in Q_n$，有$q \equiv 1 \pmod{p^n}$；

3. $\bar{\rho}(\mathrm{Frob}_q)$的两个特征值不相等。

由Q_n的选取，泛形变环$\mathcal{R}_{Q_n}$可以由$r = \dim H^1(G_F, \mathrm{Ad}^0\,\bar{\rho}(1))$个元素生成。令$\mathcal{R}_n = \mathcal{R}_{Q_n}/\lambda\mathcal{R}_{Q_n}$，则$\mathcal{R}_n$也可以由$r$个元素生成。由此我们定义映射$\theta_n : B \to \mathcal{R}_n$。另一方面，由引理3.6，我们知道$\mathcal{R}_n$是一个$k[\Delta_{Q_n}]$-代数，我们有自然的映射$k[\Delta_{Q_n}] \to \mathcal{R}_n$，并且由构造知$k[\Delta_{Q_n}]$的极大理想的像是平凡的。由$\Delta_{Q_n}$的定义，我们可以选取$k$-代数的满射$A \to k[\Delta_{Q_n}]$。

定义$\varphi_n : A \to B$，使得下面的图表交换

$$\begin{array}{ccc} A & \xrightarrow{\varphi_n} & B \\ \downarrow & & \downarrow{\scriptstyle \theta_n} \\ k[\Delta_{Q_n}] & \longrightarrow & \mathcal{R}_n. \end{array}$$

定义$\psi_n : B \to \mathcal{R}$是复合映射$B \xrightarrow{\theta_n} \mathcal{R}_n \to \mathcal{R}$。令$H_n = H^1_{\mathrm{et}}(X(\Gamma_{Q_n}) \otimes \bar{\mathbb{Q}}, k)_{\mathfrak{m}_Q}$，由上节的结果，这些对象满足定理3.1中的条件，所以得到

- $\mathcal{R}/\lambda\mathcal{R} = \mathbb{T}(N, k)_{\mathfrak{m}}$
- $H = H^1_{\mathrm{et}}(X_0(N) \otimes \bar{\mathbb{Q}}, k)_{\mathfrak{m}}$是秩为2的自由$\mathcal{R}$-模。

3.3.2 一般情形

令π_Σ是复合映射$\mathcal{R}_\Sigma \to \mathcal{R}_\emptyset \to \mathbb{T}_\emptyset \to \mathcal{O}$，令$H_\Sigma = H^1_{\mathrm{et}}(X_0(N\Sigma) \otimes \bar{\mathbb{Q}}, \mathcal{O})_{\mathfrak{m}_\Sigma}$，并通过$\phi_\Sigma : \mathcal{R}_\Sigma \to \mathbb{T}_\Sigma$视$H_\Sigma$为$\mathcal{R}_\Sigma$-模。我们验证$(\mathcal{R}_\Sigma, H_\Sigma)$满足定理3.3中的第一个条件。首先注意到$(H_\Sigma)_{\mathfrak{p}_\Sigma} \neq 0$，这里$\mathfrak{p}_\Sigma = \mathrm{Ker}(\pi_\Sigma)$；并且

$$\mathrm{rank}_{\mathcal{O}} H_\Sigma = d \cdot \mathrm{rank}\, \mathbb{T}_\Sigma.$$

这里$d = \mathrm{rank}_{\mathcal{O}} H_\Sigma[\mathfrak{p}_\Sigma] = 2$。所以我们需要验证，对$\Omega_\Sigma = H_\Sigma/(H_\Sigma[\mathfrak{p}_{\mathbb{T}_\Sigma}] + H_\Sigma[I_{\mathbb{T}_\Sigma}])$,

$$\mathrm{length}_{\mathcal{O}} \Omega_\Sigma \geq 2 \cdot \mathrm{length}_{\mathcal{O}} \mathfrak{p}_\Sigma/\mathfrak{p}_\Sigma^2.$$

注意到由极小情形，上面的不等式对$\Sigma = \emptyset$是成立的。另一方面，我们可以利用伽罗华上同调来描述$\mathfrak{p}_\Sigma/\mathfrak{p}_\Sigma^2$，从而容易得到

$$\mathrm{length}_{\mathcal{O}} \mathfrak{p}_\Sigma/\mathfrak{p}_\Sigma^2 \leq \mathrm{length}_{\mathcal{O}} \mathfrak{p}_\emptyset/\mathfrak{p}_\emptyset^2 + \sum_{q\in\Sigma} v_\lambda((q-1)(\theta(T_q)^2 - (q+1)^2)).$$

于是我们只需要证明

$$\mathrm{length}_{\mathcal{O}} \Omega_\Sigma \geq \mathrm{length}_{\mathcal{O}} \Omega_\emptyset + 2\sum_{q\in\Sigma} v_\lambda((q-1)(\theta(T_q)^2 - (q+1)^2)).$$

再简化，我们只需要证明

$$\mathrm{length}_{\mathcal{O}} \Omega_\Sigma \geq \mathrm{length}_{\mathcal{O}} \Omega_{\Sigma-q} + 2v_\lambda((q-1)(\theta(T_q)^2 - (q+1)^2)).$$

而这个是Ihara引理的推论(参见[60, 54])。从而我们完成了定理的证明。

4 意义和发展

4.1 模性猜想与相关猜想

4.1.1 BSD猜想

Birch和Swinnerton-Dyer猜想(下面简称BSD猜想)将椭圆曲线的L-函数和它的许多算术不变量联系起来。为简单起见，我们假定椭圆曲线定义在有理数域$\mathbb{Q}$上。令$E/\mathbb{Q}$是一条椭圆曲线，令ω是由E的一个极小Wieerstrass方程给出的不变微分。定义

$$\Omega_\infty = \int_{E(\mathbb{R})} |\omega|.$$

对每一个素数p，定义

$$\Omega_p = \sharp E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p).$$

这里$E_0(\mathbb{Q}_p) = \{P \in E_0(\mathbb{Q}_p) \mid P \pmod p$是光滑的$\}$。注意到若$E$在$p$处有好的约化，那么$\Omega_p = 1$，从而$\prod_p \Omega_p$有意义。

猜想4.1 (BSD猜想). *令$E/\mathbb{Q}$是一条椭圆曲线。则*

1. $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = \operatorname{rank} E(\mathbb{Q})$;

2. 令$r = \operatorname{rank} E(\mathbb{Q})$，有

$$\lim_{s\to 1} \frac{L(E/\mathbb{Q}, s)}{(s-1)^r} = \Omega_\infty \prod_p \Omega_p \frac{R(E/\mathbb{Q}) \cdot \sharp Ш(E/\mathbb{Q})}{(\sharp E(\mathbb{Q})_{tors})^2}.$$

这里，$R(E/\mathbb{Q})$是E的*regulator*，$Ш(E/\mathbb{Q})$是指E的*Tate-Shafarevich*群。

BSD猜想是七个千禧年问题之一，其在数学上的重要性不言而喻，在Clay Mathematics Institute的官方网页上可以查阅到更多信息。模性猜想与BSD猜想也有紧密联系：在BSD猜想最开始提出来的时候，数学家并不能证明对一般的椭圆曲线，$L(E/\mathbb{Q}, s)$ 可以延拓到整个复平面$\mathbb{C}$上；到目前为止，我们也不能证明$Ш(E/\mathbb{Q})$总是有限的。正如Tate在1974年提到："this remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite!"

Eichler-Shimura证明了若椭圆曲线$E/\mathbb{Q}$是模性的，那么$L(E/\mathbb{Q}, s) = L(f, s)$，这里$f$是某个新形式，故是可以延拓的；从而模性猜想的证明告诉我们$L(E/\mathbb{Q}, s)$总是可以延拓的。所以BSD猜想第一个等式的左右两项都是有意义的。文献[49, Section C16]对这个猜想作了更详细的介绍，并提供了更完整地文献资料。

4.1.2 Sato-Tate猜想

Sato-Tate猜想是关于模形式系数分布的猜想。令$f \in S_k(\Gamma_0(N))$是一个权重为k、水平为$\Gamma_0(N)$的(规范)新形式。设f的Fourier展式为

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

*Ramanujan*猜想指出：若$p \nmid N$，则$|a_p| \leq 2p^{(k-1)/2}$。这个猜想已经被完整证明：$k = 1$时由Deligne-Serre证明；$k = 2$时由Eichler-Shimura证明；$k \geq 3$时由Deligne证明。

$p \nmid N$，由$L(f,s)$在p处的Euler乘积项，我们给出等式

$$1 - a_p p^{-s} + p^{k-1} p^{-2s} = (1 - \alpha_p p^{-s})(1 - \beta_p p^{-s}).$$

于是

$$|a_p| \leq 2p^{(k-1)/2} \Leftrightarrow |\alpha_p| = |\beta_p| = p^{(k-1)/2}.$$

从而我们可以将α_p和β_p表示为$\alpha_p = p^{(k-1)/2} e^{i\theta_p}$，$\beta_p = p^{(k-1)/2} e^{-i\theta_p}$。这里$\theta_p \in [0, \pi]$。

我们的问题是：θ_p在$[0,\pi]$区间是怎么分布的？换一种说法，令

$$r_p = \frac{\alpha_p + \beta_p}{p^{(k-1)/2}} = 2\cos\theta_p \in [-2, 2].$$

r_p在区间$[-2,2]$是怎么分布的？Sato-Tate猜想描述了这个分布。

猜想4.2 (Sato-Tate猜想). *记号如上，假设f没有复乘，即$L(f,s)$不是由虚二次域的特征给出。那么r_p在$[-2,2]$上的分布遵循Sato-Tate测度*

$$\mu_{st} = \frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}\,\mathrm{d}\,x.$$

即对任意区间$[a,b] \subset [-2,2]$，

$$\lim_{x\to\infty} \frac{\sharp\{p \leq x \mid r_p \in [a,b]\}}{\sharp\{p \leq x\}} = \int_a^b \mu_{st}.$$

Sato-Tate猜想最初是关于椭圆曲线$E/\mathbb{Q}$的，但是模性猜想告诉我们，定义在有理数域上的椭圆曲线对应到权重为2的新形式，所以我们在上面直接给出了关于模形式的Sato-Tate猜想。这个猜想在一般全实域上也有推广，在某些情况已经被证明。对于猜想的推广和被证明的情形，参见文献[1, 2, 55]；对于猜想的一个更具体形式——Lang-Trotter猜想，参见[49, Conjecture 4.8]。

4.1.3 Fontaine-Mazur猜想

定义4.3. 令$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{Q}}_l)$是一个$l$-进的伽罗华表示。我们称$\rho$ 是几何的，若ρ满足

- ρ在有限个素数外都是非分歧的；
- $\rho|_{G_{\mathbb{Q}_l}}$是预半稳定的(potentially semi-stable)。

猜想4.4 (Fontaine-Mazur猜想). *令ρ是一个不可约的、几何的表示，那么存在一个光滑的、投射的代数簇$X/\mathbb{Q}$，和整数i、j，使得ρ同构于$H^j_{\text{et}}(X \otimes \bar{\mathbb{Q}}, \bar{\mathbb{Q}}_l(i))$的一部分。*

一维的Fontaine-Mazur猜想基本等价于类域论。二维Fontaine-Mazur猜想的一部分等价于：若ρ 是单的、不可约的、几何的表示，那么ρ是模性的。这个情形被Emerton、Kisin、Colmez等证明，参见文献[19, 34]。

4.2 模性猜想的发展和若干推广

最后我们对模性猜想的证明和1995年之后相关研究的发展做一些注解，部分资料来自文献[8]。

4.2.1 Wiles的结果：半稳定条件

Wiles的结果定理1.18并没有证明完整的模性猜想，而是证明了半稳定的椭圆曲线是模性的。为什么有半稳定这个条件？回到Wiles的证明：从一个模性的表示$\bar{\rho}$ 出发，考虑$\bar{\rho}$的满足条件$\mathcal{Q}$的所有形变，得到泛形变环$\mathcal{R}_{\mathcal{Q}}$，考虑所有的模性形变得到泛形变环$\mathbb{T}(\bar{\rho})$。这里我们选取$\mathcal{Q}$p使得所有的模性形变满足条件$\mathcal{Q}$，从而得到满射$\mathcal{R}_{\mathcal{Q}} \to \mathbb{T}(\bar{\rho})$。最后证明这个满射是个同构。

在这个证明里，我们需要选取一个好的形变条件$\mathcal{Q}$，节2.4中的条件满足了这个要求：半稳定的椭圆曲线对应到半稳定的伽罗华表示。如果我们要放松半稳定的条件，那么我们需要选择一个形变条件，这个形变条件要足够强，从而我们得到泛形变环的维数合适；这个形变条件要足够弱，至少要包含半稳定这个条件。在$q \neq p$的情形下，这个问题被Diamond解决(参见[15])。Diamond的主要结果是说：若$E/\mathbb{Q}$在3和5处都是半稳定的，那么E是模性的。这个条件弱于定理1.18的条件，而这个条件的存在当然还是因为我们需要运用3-5变换技巧。

在1990年代，要证明模性猜想，总绕不开3-5变换技巧。注意到半稳定条件是指椭圆曲线有好的约化或者乘法约化。若$E/\mathbb{Q}$在3处有非常坏

的加法约化，(比如其导子被3的很高幂次整除，)这将在$E[5]$中体现出来，其导子也会被3的很高幂次整除，从而对其它的$A[5] \cong E[5]$，在3处也不好控制。这时如上所说，我们需要一个好的形变条件，它足够弱，包含了$E[p]$和$T_p(E)$在p处很坏的情形；它足够强，使得对应泛形变环的维数足够小，从而Taylor-Wiles的方法可以用上。从这个角度来说，我们需要推广平坦这个条件。但是在Wiles年代，p-进Hodge理论还不够完善，没有足够成熟的工具供当时的数学家使用。

4.2.2 模性猜想的完整证明

在上一节我们提到，要证明完整地模性猜想，我们需要运用Langlands-Tunnell的结果，从而必须考虑$p = 3$的情形。所以我们考虑的椭圆曲线必须在3处有可以控制的约化情况。

我们将这一情形一般化。考虑不可约的、模p的局部伽罗华表示$\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}) \to \mathrm{GL}_2(k)$，这个表示给了我们泛形变环$\mathcal{R}^u \cong W(k)[[X_1, \ldots, X_d]]$，这个环太大导致我们不能使用Taylor-Wiles方法。于是我们考虑$\bar{\rho}$的有限平坦形变，得到泛形变环$\mathcal{R}^f$，而这个环正好满足了Taylor-Wiles方法的条件。

形变条件的定义中，第一条便是$\bar{\rho}$要满足这个条件，这样便要求$E[3]$或者$E[5]$满足这个条件：E在3和5处不能“太坏”。在推广这个方法的过程中，我们考虑预有限平坦这个条件：即表示$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}(R)$在限制到子群$\rho|_{\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)}$上是有限平坦的，这里$K$是$\mathbb{Q}_p$的一个有限扩张。这个时候，我们需要对$K$上的有限平坦群概型有一个很好地分类结果来计算相应的形变环的维数。而在$K/\mathbb{Q}_p$是野分歧时，这样的分类结果在1995年前后是不存在的。

为了解决上面提到的困难，Conrad-Diamond-Taylor [13]提出了一个新的想法。我们不去考虑由形变条件给出来的泛形变环，而是考虑有类似泛性质的环：首先我们考虑形变$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(O)$，这里$O$是$\mathbb{Q}_p$的有限扩张的整数环。这样我们可以考虑$\rho$的$p$-进Hodge性质，如：Hodge-Tate，de Rham，potentially semi-stable，crystalline等等。这些性质对一般的形变$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(A)$而言是没有意义的。更进一步，若$\rho$是potentially semi-stable，那么其对应的Fontaine模$D_{\mathrm{pst}}(\rho)$是一个两维的线性空间，在

其上有一个I_p的作用，这样得到一个表示$\tau : I_p \to \mathrm{GL}_2(\mathbb{Q}_p)$，我们称之为型(type)。所以我们可以固定一个型τ，考虑所有的potentially semi-stable、型为τ的形变$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(O)$。

这样我们得到的并不是一个形变条件，从而也不会得到泛形变环。但是我们会得到一个具有类似泛性质的环。考虑$\bar{\rho}$的泛形变环$\mathcal{R}$，考虑所有映射$s : \mathcal{R} \to O$，O如上。从泛形变$\rho^u : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathcal{R})$复合上$s$我们得到形变$\rho_s : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(O)$。我们称$\mathrm{Ker}(s)$是$\tau$-型的，若$\rho_s$是potentially semi-stable、τ-型的。这里我们还可以加上其它条件：如potentially Barsotti-Tate，或者$\det \rho_s = \chi$等等。

定义$\mathcal{R}_\tau := \mathcal{R}/\cup_s \mathrm{Ker}(s)$，这里$s$遍历所有$\tau$-型的理想。从几何上看，在泛形变空间$\mathrm{Spec}(\mathcal{R})$中，我们考虑包含所有$\tau$-型素理想的闭子概型。$\mathcal{R}_\tau$并不是一个泛形变环，但是当我们考虑如上形变问题的时候，是一个很自然的研究对象。

这里有一个问题，就是所有的τ-型点是否组成一个闭集？令S是所有τ-型点组成的集合，$\bar{S}$是其在形变空间中的闭包。$\bar{S} - S$中的点同样给我们伽罗华表示，这样的表示我们称之为*弱*τ-型的。在[43]中，Savitt证明了弱τ-型和τ-型是等价的条件。

回到模性猜想的证明，利用环$\mathcal{R}_\tau$，经过计算$\mathcal{R}_\tau$的维数，Conrad-Diamond-Taylor证明了如下结果(参见[13])。

定理4.5 (Conrad-Diamond-Taylor). *令$E/\mathbb{Q}$是一条椭圆曲线，且在3处一个顺分歧扩张后有半稳定约化，那么E是模性的。*

在几乎同一时间，Christophe Breuil [3]对定义在任意p-进域上的有限平坦群概型作出了完整地分类，这个结果和上面CDT的想法结合在一起，最终导致了模性猜想的完整证明(定理1.19)。

4.2.3 Kisin的结果

首先我们简单讲讲patching这个过程的发展。在Wiles最开始的证明中，所谓的patching的对象是形变环和Hecke代数，从而在其证明中，我们需要先知道对应的模是有限自由的，并且需要知道泛形变环是Gorenstein(参见[48, 60])。在这篇文章里，我们采用的是Diamond改进后的方法，patching的

对象是模，而有限自由的结构作为一个副产品在证明$R = T$的过程中得到了(参见定理3.1)。

在Kisin [33]之前，这已经是最佳的证明模性问题的方法。在上一节我们也看到，在这个方法里，我们需要计算环$\mathcal{R}_\tau$，这个环很难控制，并且在实际操作中并不会给出我们需要的维数。BCDT的证明能成立在于我们只考虑3处的形变，这个时候所有相关的环都可以明确写出来。事实上，正是由于这些计算，Breuil-Mézard [6]给出了一个猜想，描述了$\mathcal{R}_\tau$的模p的Hilbert-Samuel重数和对应的表示论不变量之间的关系。

文章[33]虽然直到2009年才发表，但是2004年左右就已经发布了。Kisin的新想法是说：与其对$\mathbb{Z}_p$-代数来考虑我们的问题，这时需要了解$\mathcal{R}_\tau$的性质，不如直接考虑$\mathcal{R}_\tau$-代数。这时的patching过程中，我们不需要证明$\mathcal{R}_\tau$的切空间是一维的，只需要知道$\mathcal{R}_\tau$是一个Krull维数为2的整环。更进一步，如果我们知道所考虑的形变都在同一个分支上，我们可以只选取Spec$(\mathcal{R}_\tau[1/p])$的一个不可约分支。

当然，若Spec$(\mathcal{R}_\tau[1/p])$是不可约的，Kisin的方法不会有任何问题。如果Spec$(\mathcal{R}_\tau[1/p])$有多个不可约分支，在某些特殊情况下，Kisin采用了所谓的"component-hopping"技巧。在[33]中，Kisin证明了如下的模性定理。

定理4.6. *令$p \geq 3$是素数，ρ是$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$的2维表示且在有限个素数外非分歧。令$\bar{\rho}$是$\rho$的约化，假设$\bar{\rho}$是模性的，$\bar{\rho}|_{\mathrm{Gal}(\bar{\mathbb{Q}}/L)}$是绝对不可约的($L = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$)。若$\rho$是potentially Barsotti-Tate的，并且$\det\rho$是分圆特征和一个有限特征的乘积，那么ρ是模性的。*

注意到这里我们并没有对ρ的型做任何要求，这正是这个定理强大的地方。这个方法最终导致了Breuil-Mézard猜想的证明(参见[35, 26])。另一方面，由于缺乏对形变环的足够了解，Kisin的patching方法不能得到$R = T$的结果，而是得到$R[1/p] = T[1/p]$的结果。

4.2.4 全实域上的推广

到目前为止我们只考虑了关于$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$的表示的模性提升。事实上，数学家们早就意识到全实域上的模性定理在数论上也有重要意义，这时我们可以采用基变换的技巧[36]而得到有理数域$\mathbb{Q}$上的信息。早期Carayol的一

个结果[10, Section 0.8]证明了一个定义在$\mathbb{Q}$上的模性的椭圆曲线的导子等于对应的新形式的水平。尽管这是关于$\mathbb{Q}$的一个结论，但是证明中运用了全实域上的Hilbert模形式。

我们简单介绍一下全实域上的Serre模性猜想。令F是一个全实域，$F \neq \mathbb{Q}$，$\bar{\rho} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$是一个二维的连续表示。我们称$\bar{\rho}$是全奇的，若对任意的复共轭$c$，都有$\det \bar{\rho}(c) = -1$。

猜想4.7. *若$\bar{\rho} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$是不可约的、全奇的、连续的表示，那么$\bar{\rho}$是模性的。即存在一个Hilbert模形式$f$，使得$\bar{\rho} \cong \bar{\rho}_f$，这里$\bar{\rho}_f$是由$f$构造的伽罗华表示。*

由于这个猜想与猜想1.22类似，所以尽管这个猜想不是Serre提出来的，也被称为Serre模性猜想。如果我们能证明这个猜想，那么就能得到全实域上的椭圆曲线的模性。关于这个猜想的更多细节，以及这个猜想和模p的Langlands对应的联系，可以参考文献[9, 25]；关于全实域上的椭圆曲线的模性，就作者了解到的情况而言，比较完整的结果是[21]中，Freitas-Le Hung-Siksek证明了实二次域上的椭圆曲线都是模性的。

定理4.8 (Freitas-Le Hung-Siksek 2015)**.** *实二次域上的椭圆曲线都是模性的。*

Freitas-Le Hung-Siksek的证明运用到了很强的模性提升定理，同时也推广了3-5变换技巧，我们概括一下这个证明的主要步骤。令$F \neq \mathbb{Q}$是一个全实域，E/F是一条椭圆曲线，$\bar{\rho} := \bar{\rho}_{E,p} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\mathbb{F}_p)$是由$E[p]$给出的伽罗华表示。令$L = F(\zeta_p)$。

Step 1 综合[33, 25, 5]的结果，Freitas-Le Hung-Siksek证明了：若$\bar{\rho}$是模性的，且$\bar{\rho}|_{\mathrm{Gal}(\bar{F}/L)}$是绝对不可约的，那么$E$是模性的。

Step 2 令$p = 3$或者5，若$\bar{\rho}|_{\mathrm{Gal}(\bar{F}/L)}$是绝对不可约的，那么$E$是模性的。

注意到模曲线$X_0(15)$有无穷多的实二次点，考虑3-5变换不足以证明实二次域上的模性猜想，对此我们需要更进一步。

Step 3 令$p = 7$，若$\bar{\rho}|_{\mathrm{Gal}(\bar{F}/L)}$是绝对不可约的，那么$E$ 是模性的。

Step 4 找出所有的定义在实二次域上的，使得对$p = 3, 5, 7$，$\bar{\rho}|_{\mathrm{Gal}(\bar{F}/L)}$都绝对可约的椭圆曲线。这样的曲线对应到27条模曲线上某一点。Freitas-Le Hung-Siksek一一证明了这些例外曲线的模性，从而完成了整个证明。

若我们考虑椭圆曲线的预模性，则有如下的完整结果。

定理4.9. *令E是定义在全实域F上的椭圆曲线。存在全实域F'/F，使得$E \times_F F'$是模性的。特别地，我们知道$L(E, s)$可以亚纯延拓到整个复平面上。*

在Kisin的patching方法出现后，Taylor就意识到上面的结果是可证的，不过当时Taylor将精力集中在Sato-Tate猜想上。尽管在2005年左右，证明定理4.9的工具已被大家掌握，第一个发表的证明由Wintenberger在[39]的附录中给出。定理4.9在高维的推广可参见文献[2]。

参考文献

[1] T. Barnet-Lamb; T. Gee; D. Geraghty; R. Taylor: *Potential automorphy and change of weight.* Annals of Math 179 (2014), 501-609.

[2] T. Barnet-Lamb; D. Geraghty; M. Harris; R. Taylor: *A family of Calabi-Yau varieties and potential automorphy 2.* P.R.I.M.S. 47 (2011), 29-98.

[3] C. Breuil: *Groupes p-divisibles, groupes finis et modules filtrés.* Ann. of Math. (2) 152 (2000), 489-549.

[4] C. Breuil; B. Conrad; F. Diamond; R. Taylor: *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), 843-939.

[5] C. Breuil; F. Diamond: *Hilbert modular forms modulo p and values of extensions between Galois characters.* Ann. Sci. Éc. Norm. Supér. (4) 47 (2014), no. 5, 905-974.

[6] C. Breuil; A. Mézard: *Multiplicités modulaires et repreésentations de* $\mathrm{GL}_2(\mathbb{Z}_p)$ *et de* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ *en* $l = p$. Duke Math. J. 115 (2002), 205-310.

[7] W. Bruns, J. Herzog: *Cohen-Macaulary rings.* Cambridge Studies in Adv. Math. 39, Cambridge University Press, Cambridge (1986).

[8] K. Buzzard: *Potential modularity–a survey.* In *Non-abelian fundamental groups and Iwasawa theory*, 188–211, London Math. Soc. Lecture Note Ser., 393, Cambridge Univ. Press, Cambridge, 2012.

[9] K. Buzzard; F. Diamond; F. Jarvis: *On Serre's conjecture for mod* ℓ *Galois representations over totally real fields.* Duke Math. J. Vol. 155, no. 1, 2010, 105-161.

[10] H. Carayol: *Sur les représentations l-adiques attachées aux formes modulaires de Hilbert.* C. R. Acad. Sci. Paris Sér. I Math. 296 (1983), no. 15, 629–632.

[11] L. Clozel; M. Harris; R. Taylor: *Automorphy for some l-adic lifts of automorphic mod l representations.* Pub. Math. IHES 108 (2008), 1-181.

[12] G. Cornell; J. H. Silverman; G. Stevens: *Modular forms and Fermat's Last Theorem.* Springer 1997.

[13] B. Conrad; F. Diamond; R. Taylor: *Modularity of certain potentially Barsotti-Tate Galois representations.* J. Amer. Math. Soc. 12 (1999), no. 2, 521–567.

[14] H. Darmon; F. Diamond; R. Taylor: *Fermat's last theorem.* In *Elliptic curves, modular forms and Fermat's last theorem* (Hong Kong, 1993), 2-140, Int. Press, Cambridge, MA, 1997.

[15] F. Diamond: *On deformation rings and Hecke rings.* Ann. of Math. (2) 144 (1996), no. 1, 137–166.

[16] F. Diamond: *The Taylor-Wiles construction and multiplicity one.* Invent. Math. 128 (1997). no. 2, 379–391.

[17] F. Diamond; J. Shurman: *A first course in modular forms.* Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp. ISBN: 0-387-23229-X.

[18] M. Dickinson: *On the modularity of certain 2-adic Galois representations.* Duke Math. J. 109 (2001), no. 2, 319-382.

[19] M. Emerton: *Local-global compatiblity in the p-adic Langlands program fro* GL_2. http://www.math.uchicago.edu/~emerton/pdffiles/lg.pdf

[20] J-M. Fontaine; G. Laffaille: *Construction de représentations p-adiques.* Ann. Sci. école Norm. Sup. (4) 15 (1982), no. 4, 547-608 (1983).

[21] N. Freitas; B. V. Le Hung; S. Siksek: *Elliptic curves over real quadratic fields are modular.* Inventiones Mathematicae, 201 (1): 159-206.

[22] G. Frey: *Links between solutions of* $A - B = C$ *and elliptic curves.* In *Number Theory, proceedings of the Journees arithmetiques, held in Ulm, 1987,* H. P. Schlichewei, E. Wirsing, editors. Lecture Notes in Mathematics 1380. Springer-Verlag, Berlin, New York, 1989.

[23] G. Frey: *Links between stabel elliptic curves and certain Diophantine equations.* Ann. Univ. Saraviensis, Ser. Math. 1 (1986), 1-40.

[24] K. Fujiwara: *Deformation rings and Hecke algebras in the totally real case.* arxiv.org/abs/math/0602606

[25] T. Gee: *Automorphic lifts of prescribed types.* , Mathematische Annalen 350 (2011), 107-144.

[26] T. Gee; M. Kisin: *The Breuil-Mézard conjecture for potentially Barsotti-Tate representations.* Forum of Mathematics Pi, 2 (2014), e1, 56 pp.

[27] F. Q. Gouvêa: *Deformations of Galois representations.* IAS/Park City Mathematics Series, Vol. 9, 2001.

[28] A. Granville; T. J. Tucker: *It's as easy as abc.* Notices of the American Mathematical Society, 2009, 49 (10): 1224-1231.

[29] A. Grothendieck: *Technique de descente et théorèmes d'existence en géomérie algébrique. II. Le théorème d'existence en théorie formelle des modules* Séminaire Bourbaki, Vol. 5 (Paris), Soc. Math. France, 1995, Exp. No. 195, 369-390.

[30] C. Khare: *Serre's modularity conjecture: a survey of the level one case.* in *L-functions and Galois representations*, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, 270-299.

[31] C. Khare; J-P. Wintenberger: *Serre's modularity conjecture. 1* Invent. Math. 178 (2009), no. 3, 485-504.

[32] C. Khare; J-P. Wintenberger: *Serre's modularity conjecture. 2* Invent. Math. 178 (2009), no. 3, 505-586.

[33] M. Kisin: *Moduli of finite flat group schemes, and modularity.* Ann. of Math. (2) 170 (2009), no. 3, 1085-1180.

[34] M. Kisin: *The Fontaine-Mazur conjecture for GL_2.* J.A.M.S. 22(3) (2009) 641-690.

[35] M. Kisin: *The structure of potentially semi-stable deformation rings.* Proceedings of ICM 2010, Vol. II, 294-311.

[36] R. P. Langlands: *Base change for GL_2.* Annales of Math. Studies, vol. 96, Princeton University Press, Princeton, N. J., 1980.

[37] B. Mazur: *Modular curves and the Eisenstein ideal.* Publ. Math. IHES 47, 33-186(1977).

[38] B. Mazur: *An introduction to the deformation theory of Galois representations.* in *Modular forms and Fermat's last theorem* G. Cornell, J. H. Silverman, G. Stevens, Springer.

[39] J. Nekovář: *On the parity of ranks of Selmer groups.* Compos. Math. 145 (2009), no. 6, 1351-1359.

[40] P. Ribenboim: *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York and Heidelberg, 1979.

[41] K. Ribet: *On modular representations of $Gal(\bar{Q}/Q)$ arising from modular forms.* Invent. Math. 100 (1990), no. 2, 431-476.

[42] K. Rubin: *Modularity of mod 5 Galois representations.* in *Modular forms and Fermat's last theorem* G. Cornell, J. H. Silverman, G. Stevens, Springer.

[43] D. Savitt: *On a conjecture of Conrad, Diamond, and Taylor.* Duke Math. J. 128 (2005), no. 1, 141-197.

[44] M. Schlessinger: *Functors of Artin rings.* Trans. A. M. S. 130 (1968), 208-222.

[45] J.-P. Serre: *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematical Journal, 1987, 259-331.

[46] J.-P. Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. 15 (1972), 1987, 54 (1), 179-230.

[47] I. Shafarevich: *Algebra I.* Encyclopaedia of Mathematical Sciences, vol. 11, Springer-Verlag, 1990.

[48] E. de. Shalit: *Hecke rings and universal deformation rings.* in *Modular forms and Fermat's last theorem* G. Cornell, J. H. Silverman, G. Stevens, Springer.

[49] J. H. Silverman: *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer.

[50] J. H. Silverman: *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics 151, Springer.

[51] S. Singh: *Fermat's Last Theorem.* ISBN 978-1857025217 (1997).

[52] G. Stevens: *An overview of the proof of Fermat's Last Theorem.* in *Modular forms and Fermat's last theorem* G. Cornell, J. H. Silverman, G. Stevens, Springer.

[53] R. Taylor: *Remarks on a cojecture of Fontaine and Mazur.* J. Inst. Math. Jussieu 1 (2002), no. 1, 125-143.

[54] R. Taylor: *On the meromorphic continuation of degree two L-functions.* Doc. Math. 2006, Extra Vol., 729-779 (electronic).

[55] R. Taylor: *Automorphy for some l-adic lifts of automorphic mod l Galois representations. II.* Publ. Math. Inst. Hautes Études Sci. 108: 183-239.

[56] R. Taylor; A. Wiles: *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553-572.

[57] J. Tunnell: *Artin's conjecture for representations of octahedral type.* Bull. Amer. Math. Soc. 5 (1981), no. 2, 173-175.

[58] P. Vojta: *Diophantine approximations and value distribution theory.* Lect. Notes in Math. 1239, (1987).

[59] L. C. Washington: *Galois Cohomology.* in *Modular forms and Fermat's last theorem* G. Cornell, J. H. Silverman, G. Stevens, Springer.

[60] A. Wiles: *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443-551.