

قضیه آخر فرما

علی چراغی

چکیده

در این مقاله سعی می‌شود در مورد پیشنبازها و روند اثبات قضیه آخر فرما^۱ توضیح داده شود. تا آنجا که ممکن بوده، سعی شده خواندن این مقاله نیازی به هیچ پیشنبازی نداشته باشد، ولی با این وجود توضیح بعضی از پیشنبازها (کمی نظریه رسته‌ها و نظریه جبری اعداد) فضای بسیاری را اشغال می‌کند. خواننده برای یادگیری آن‌ها می‌تواند به [۶] و [۵] رجوع کند.

حل کرد.

۱ مقدمه

(۳) سوفی ژرمن^۲ در اوایل قرن ۱۹، راه حلی ایجاد کرد که حداقل برای همه توان‌های اول فرد کمتر از ۱۰۰، حالت اول قضیه فرما را ثابت می‌کرد ($x^n + y^n = z^n \Rightarrow n | xyz$).
 (۴) کومر^۳ با استفاده از نظریه اعداد جبری قضیه را برای حدود ۶۰ درصد (حدسی!) از اعداد اول ثابت کرد.
 (۵) در سال ۱۹۷۷، ترجانیان^۴ حالت اول قضیه را برای همه توان‌های زوج (غیر ۲!) اثبات کرد.
 ولی در سال ۱۹۸۴ بود که فری^۵ یک ارتباط بین این حدس و خمی بیضوی یافت و احساس کرد که غلط بودن قضیه آخر فرما باعث رد حدسی معروف از شیمورا^۶ و تانیاما^۷ می‌شود. دو سال پس از آن، ریبیت^۸ این روند را ادامه داد و با اثبات حدسی از سر

در سال ۱۶۳۷، در ویرایشی از کتاب حساب^۹ فرما ادعای زیر را نوشت (که آن را ترجمه کرده‌ایم!): "غیرممکن است که یک مکعب را به دو مکعب تجزیه کرد، یا یک توان چهارم را به دو توان چهارم، و در حالت کلی هر توان بزرگ‌تر از دو را به دو توان شبیه هم، من یک اثبات شگفت‌انگیز از این پیدا کرده‌ام که این حاشیه کوچک‌تر از آن است که آن را قرار دهم." پس از او ریاضیدان‌های بسیاری برای اثبات این موضوع تلاش کردند و به نتایج جزئی نیز رسیدند. مثلاً:

(۱) فرما در سال ۱۶۴۰، حالت توان چهارم را حل کرد.

(۲) اویلر^{۱۰} بین سال‌های ۱۷۵۸ و ۱۷۷۰ حالت توان سوم را

¹P. Fermat

²Arithmetica

³L. Euler

⁴S. Germain

⁵E. Kummer

⁶G. Terjanian

⁷G. Frey

⁸G. Shimura

⁹Y. Taniyama

¹⁰K. Ribet

¹¹J.P. Serre

¹²Epsilon conjecture

پس این نشان می‌دهد که کافی است مسئله را برای n های اول فرد و $n = 4$ حل کنیم تا برای همه n ها حل شود. حالت $n = 4$ را خود فرما با روش نزول نامتناهی خود ثابت کرده است. پس کافیست قضیه آخر فرما را برای n های اول فرد حل کنیم. همان‌گونه که در مقدمه گفته شد، این قضیه برای اعداد اول بسیاری قبل از اثبات وایلز حل شده بود ولی حالت کلی آن باقی مانده بود.

پس ما از این به بعد یک عدد اول فرد p را فیکس کرده و فرض می‌کنیم $A^p + B^p = C^p$ برای $ABC \neq 0$ به طوری که $\gcd(A, B, C) = 1$ و سعی می‌کنیم تناقضی یافت کنیم!

۳ خم‌های بیضوی

منتظر از یک خم بیضوی روی اعداد گویا، یک خم جبری هموار است به طوری که با معادله‌ی زیر داده شده باشد:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$$

در این صورت هموار بودن به معنی این خواهد بود که چندجمله‌ای $x^3 + ax + b$ ریشه مکرر نداشته باشد (در حالت کلی هموار بودن به این معنی است که در هر نقطه از خم، یک خط مماس بر خم موجود باشد). منظور از تفکیک‌کننده^{۱۹} برای این خم عدد زیر است: $(4a^3 + 27b^2)^{\frac{1}{3}} = -16(4a^3 + 27b^2)$.

تفکیک‌کننده این خاصیت را دارد که ناصفر است اگر و تنها اگر خم هموار باشد. فری خم زیر را برای بررسی پیشنهاد کرد (زیرا این خم دارای تفکیک‌کننده‌ای است که به نظر متناقض با حدسهای اخیر بوده است):

$$F : y^2 = x(x - A^p)(x + B^p)$$

در واقع اگر تفکیک‌کننده مینیمال (مینیمم قدر مطلق تفکیک‌کننده) خم‌های ایزومورف با این خم) این خم بیضوی (همواری از

^{۱۲} به نام حدس اپسیلون^{۱۲}، اثبات قضیه آخر فرما را به حدس شیمورا-تانيااما کاهش داد. بعد از او، ریاضیدان انگلیسی، اندری وایلز^{۱۳}، که از زمان کودکی آرزوی حل این مسئله را داشت، ^۶ سال روی این مسئله کار کرد و در نهایت، در سال ۱۹۹۳ موفق به اثبات مقداری از حدس شیمورا-تانيااما شد که برای اثبات قضیه آخر فرما کافی بود. پس از آن اشکالی در اثبات وایلز پیدا شد که باعث شد وایلز و تیلور^{۱۴} (شاگرد قدیمی او) یک سال دیگر تلاش کنند تا آن اشکال را برطرف نمایند. در انتهای، در سال ۱۹۹۵، قضیه آخر فرما بهطور کامل اثبات شد. همچنان با قوی‌تر کردن ایده‌های وایلز، تعدادی ریاضیدان دیگر، بروی^{۱۵} و کنراد^{۱۶} و دایموند^{۱۷} و تیلور، توانستند حدس شیمورا-تانيااما را بهطور کامل اثبات کنند و پس از آن، نام آن تبدیل به قضیه مدولاریتی شد.

در این مقاله ابتدا در مورد خم‌های بیضوی و فرم‌های مدولار کمی توضیح داده می‌شود و سپس روند اثبات قضیه آخر فرما توضیح داده می‌شود. اثبات‌ها به دلیل طولانی بودن، معمولاً ارجاع داده شده‌اند.

۲ صورت قضیه

قضیه آخر فرما، قضیه‌ای با صورت ساده در نظریه اعداد است و از این قرار است:

قضیه ۱. فرض کنید $3 \geq n$ عددی صحیح باشد. اگر برای $A, B \in \mathbb{Z}$ داشته باشیم $A^n + B^n = C^n$ آن‌گاه $ABC = 0$.

حل این مسئله بیش از ۳۵۰ سال زمان برد و با روشی کاملاً غیر مستقیم اثبات شده است.

اولاً اگر $d | n$ آن‌گاه داریم:

$$A^n + B^n = C^n \Leftrightarrow (A^{\frac{n}{d}})^d + (B^{\frac{n}{d}})^d = (C^{\frac{n}{d}})^d$$

¹³ A. Wiles

¹⁴ R. Taylor

¹⁵ C. Breuil

¹⁶ B. Conrad

¹⁷ F. Diamond

¹⁸ Smooth

¹⁹ Discriminant

ناهموار، کاهش ضربی دارد. در واقع فرض کنید داشته باشیم
 $A^p + B^p = C^p$ داریم:

$$\bar{F} : y^2 = x(x)(x + \bar{B}^p)$$

این خم در نقطه‌ی $(0, 0)$ ناهموار است و دقیقاً زمانی در \mathbb{A} کاهش جمعی دارد که $0 = \bar{B}^p$ ، اما این یعنی $B \mid l$ و پس طبق $\gcd(A, B, C) \mid l$ که متناقض با فرض است. پس خم فری در هر نقطه کاهش نیمه‌پایدار دارد (کاهش خوب (که کاهش این خم، هموار باشد) یا کاهش ضربی). تعداد نقاط خم‌های بیضوی روی میدان‌های متناهی (همان کاهش آن‌ها به پیمانه اعداد اول) از اهمیت فوق العاده‌ای برخوردار است. ما اعداد $a_l = l+1 - \#\bar{E}(\mathbb{F}_l)$ را در نظر می‌گیریم. در این صورت داریم $|a_l| \leq 2\sqrt{l}$ (قضیه هسه^{۲۳}) و می‌توان با استفاده از این اعداد، L -تابع^{۲۴} خم‌های بیضوی را تعریف کرد (فرض می‌کنیم خم نیمه‌پایدار باشد):

$$L(E, s) = \prod_{l \nmid \Delta} \frac{1}{1 \pm l^{-s}} \prod_{l \mid \Delta} \frac{1}{1 - a_l l^{-s} + l^{1-2s}}$$

علامت \pm بستگی به یک شرط موضعی دارد (شیب‌های مماس‌های خم بیضوی کاهش یافته در \mathbb{F}_l هستند یا در \mathbb{F}_{l^2}). طبق قضیه هسه این تابع برای $\Re s > \frac{3}{2}$ همگرا است (چرا؟).

۴ فرم‌های مدولار

منظور از یک فرم مدولار روی $SL_2(\mathbb{Z})$ با وزن k ، یک تابع $f : \mathbb{H} \rightarrow \mathbb{C}$ است (\mathbb{H} نیم‌صفحه‌ی بالای \mathbb{C} است)، به طوری که

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad z \in \mathbb{H}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \quad (1)$$

$ABC \neq 0$ بدست آمده است) را حساب کنیم، داریم:

$$\Delta_F = 2^{-8}(ABC)^p$$

این توان p -ام کامل داشتن، یکی از موارد بنظر متناقض با آن حدس اخیر بوده است! آن حدس را بعدتر بیان می‌کنیم. در اینجا عمل گروه روی خم بیضوی را بیان می‌کنیم. برای این کار یک خم بیضوی E با نقطه‌ی گویای $[0 : 1 : 0]$ فیکس کنید (نقاط پروژکتیو آن را در نظر بگیرید که برابر با اجتماع نقاط آفین آن و O است). می‌خواهیم روی $E(\mathbb{Q})$ یک عمل گروه تعريف کنیم. پس دو نقطه $P, Q \in E(\mathbb{Q})$ را در نظر می‌گیریم و جمع آن‌ها را به شکل هندسی نشان داده شده در شکل ۱ تعريف می‌کنیم. همچنین اگر بخواهیم نقطه‌ای را با خودش جمع کنیم، خط گذرنده از آن نقطه و خودش (خط مماس بر خم در آن نقطه) را در نظر می‌گیریم. این عمل خوش‌تعريف است، زیرا می‌توان به سادگی از معادله‌ی خطوط و خم نتیجه گرفت $P + Q \in E(\mathbb{Q})$.

یک خم بیضوی E تعريف شده روی اعداد صحیح $(a, b \in \mathbb{Z})$ را می‌توان به پیمانه یک عدد اول l در نظر گرفت و اگر $l \nmid \Delta_E$ خم بیضوی جدیدی را پیدا کرد. در واقع خم بیضوی جدید $\bar{E} : \mathbb{Z} \rightarrow \mathbb{Z}/l\mathbb{Z} \cong \mathbb{F}_l$ که $y^2 = x^3 + \bar{a}x + \bar{b}$ تصویر است، را برابر با کاهش^{۲۰} خم بیضوی به پیمانه l تعريف می‌کنیم. حال اگر $\Delta \mid l$ ، مشکل این خواهد بود که خم کاهش یافته در دقیقاً یک نقطه ناهموار خواهد بود و پس دو حالت داریم:

۱) خم در آن نقطه ناهمواری، دو خط مماس متفاوت دارد که در این صورت به آن کاهش ضربی^{۲۱} گوییم.

۲) خم در آن نقطه ناهمواری، یک خط مماس (مکرر) دارد که در این صورت به آن کاهش جمعی^{۲۲} گوییم.

اصطلاحات "ضربی" و "جمعی" تفسیر ساده‌ای دارند که البته اهمیتی در بحث ما ندارند و پس آن را بیان نمی‌کنیم. حال خم فری F ، این خاصیت را دارد که در همه‌ی کاهش‌های

²⁰Reduction

²¹Multiplicative reduction

²²Additive reduction

²³H. Hasse

²⁴L-functions

²⁵Fourier expansion

کاسپ‌های Γ گوییم. فضای همه‌ی فرم‌های کاسپ از وزن k روی Γ را با $S_k(\Gamma)$ نمایش می‌دهیم. همچنین منظور از یک فرم مدولار (فرم کاسپ) در $(S_k(\Gamma_0(N))) M_k(\Gamma_0(N))$ است.

حال عملگرهای هکه^{۲۹} را مختصرًا توضیح می‌دهیم. برای سادگی فرض کنید $\Gamma = SL_2(\mathbb{Z})$. اولاً دقت کنید که هر کدام از نقاط بالای صفحه را می‌توان با یک شبکه در \mathbb{C} نمایش داد:

$$\begin{aligned} \mathbb{H} &\rightarrow \mathcal{L} \\ \alpha &\mapsto <\alpha, 1> \end{aligned}$$

که \mathcal{L} ، مجموعه‌ی همه‌ی شبکه‌هایست و همچنین اگر شبکه‌ها را در حد هموتونی^{۳۰} (ضرب در یک عدد مختلط) در نظر بگیریم، تابع بالا یک دوسویی خواهد داد:

$$\mathbb{H} \rightarrow \mathcal{L}/\text{homothety}$$

پس فرم‌های مدولار را می‌توان روی شبکه‌ها نیز تعریف کرد. پس یک فرم مدولار از وزن k مثل f فیکس کنید. در این صورت قرار می‌دهیم:

$$f(<\omega_1, \omega_2>) = (\omega_2)^{-k} f(\omega_1/\omega_2)$$

حال مثلاً یک شبکه L در نظر بگیرید و جمع صوری زیر را در نظر بگیرید: $(n \in \mathbb{N})$

$$T_n L := \sum_{[L:L']=n} L'$$

و برای $f \in M_k(SL_2(\mathbb{Z}))$ قرار دهید:

$$T_n f(L) = n^{k-1} \sum_{[L:L']=n} f(L')$$

در این صورت T_n ‌ها عملگرهایی روی $M_k(SL_2(\mathbb{Z}))$ و $S_k(SL_2(\mathbb{Z}))$ خواهند بود. همچنین برای $\mathbb{C}^* \ni \lambda, [\lambda] \in \mathbb{C}^*$ را برابر با $L \mapsto \lambda L$ تعریف کنید و برای $f \in M_k(SL_2(\mathbb{Z}))$ قرار دهید:

$$([\lambda]f)(L) = f(\lambda L)$$

و روی همه‌ی نقاط \mathbb{H} و همچنین در " ∞ " تحلیلی باشد. شرط آخر به این معنی است که بسط فوریه^{۲۵} f (چون داریم $f(z) = f(z+1)$ از رابطه بالا) در بینهایت از صفر شروع شود:

$$f(q) = \sum_{n \geq 0} a_n q^n, \quad q = e^{2\pi i z}, \quad a_n \in \mathbb{C}$$

همه‌ی فرم‌های مدولار از وزن k روی $SL_2(\mathbb{Z})$ را با $M_k(SL_2(\mathbb{Z}))$ نمایش می‌دهیم. همچنین واضح است که این تعریف را می‌توان زیرگروه‌هایی از $SL_2(\mathbb{Z})$ مثل Γ تعمیم داد به این شکل که در شرط (۱) به جای $SL_2(\mathbb{Z})$ داشته باشیم $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. فرض می‌کنیم Γ خیلی کوچک نباشد یعنی $\Gamma(N) \subseteq \Gamma$ برای N ی که

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$$

همچنین قرار می‌دهیم:

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

در این صورت $\Gamma(N)$ از اندیس متناهی در $SL_2(\mathbb{Z})$ است (چرا؟) و پس Γ و $\Gamma_0(N)$ نیز از اندیس متناهی هستند. به چنین زیرگروه‌هایی از $SL_2(\mathbb{Z})$ زیرگروه‌های همنهشتی^{۲۶} گوییم. پس مانند قبل، فرم‌های مدولار در این فضای را با $M_k(\Gamma)$ نمایش می‌دهیم. فرم‌های مدولار این خاصیت مهم را دارند که هر کدام از $M_k(\Gamma)$ ‌ها متناهی بعد هستند (پس مثلاً اگر یک فرم مدولار داشته باشیم، می‌توانیم آن را بحسب پایه‌ای در این فضای بنویسیم و ضرایب فوریه آن فرم مدولار را بهتر بشناسیم).

منظور از یک فرم کاسپ^{۲۷} از وزن k روی Γ ، یک فرم مدولار با وزن k روی Γ است به طوری که در همه‌ی "کاسپ"‌های Γ صفر شود: اگر Γ یک زیرگروه همنهشتی باشد، می‌توان فضای \mathbb{H}/Γ را در نظر گرفت. در این صورت این یک رویه ریمانی باز است به طوری که فشرده‌سازی^{۲۸} آن به متناهی نقطه نیاز دارد. به این متناهی نقطه،

²⁶Congruence subgroups

²⁷Cusp form

²⁸Compactification

²⁹E. Hecke

³⁰Homothety

بسط فوریه‌ی $\tau(n)q^n = \sum_{n \geq 1} \tau(n)q^n$ را دارد که $\tau(n)$ تابع رامانوجان است. رامانوجان حدس زده بود که

۱) تابع τ ضربی است.

۲) برای l اول و $n \in \mathbb{N}$ داریم:

$$\begin{aligned} \tau(l^{n+1}) &= \tau(l)\tau(l^n) - l^{11}\tau(l^{n-1}) \\ |\tau(l)| &\leq 2l^{11/2} \end{aligned} \quad (3)$$

حال می‌توان دید که فضای $S_{12}(SL_2(\mathbb{Z}))$ یک بعدی است و $\langle \Delta \rangle = S_{12}(SL_2(\mathbb{Z}))$. پس η باید بردار ویژه‌ی همه‌ی T_n را به فرم τ خاصیت ۵ باید داشته باشیم:

$$a_1(T_n\Delta) = a_n(\Delta) = \tau(n)$$

و از آنجا که $a_1(\Delta) = 1$ ، پس باید مقدار ویژه‌ی متناظر آن $\tau(n)$ باشد و پس از خاصیت ۴ با عمل کردن به روی Δ قسمت دوم حدس بدست می‌آید. همچنین از خاصیت ۳ نیز با همین روند قسمت اول حدس بدست می‌آید. قسمت سوم حدس سخت‌تر است و از اثبات حدهای وی ^{۳۳} بدست می‌آید.

یک فرم کاسپ $f \in S_k(\Gamma_0(N))$ در نظر بگیرید به طوری که فرم ویژه‌ی همه‌ی T_n را η باشد. در این صورت خواص ۳ و ۴ عملگرهای هکه پیشنهاد می‌کنند که ما L -تابع ضرایب بسط فوریه‌ی آن را در نظر بگیریم:

اگر $f = \sum_{n \geq 1} a_n q^n$ قرار دهد:

$$L(f, s) = \sum_{p \nmid N} \frac{a_n}{n^s}$$

و پس از ۳ و ۴ و بسط تیلور داریم که این تابع حاصلضرب اویلری زیر را دارد:

$$L(f, s) := \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

این حاصلضرب اویلری ما را یاد L -تابع خم‌های بیضوی می‌اندازد. پس احتمالاً رابطه‌ای بین فرم‌های ویژه و خم‌های بیضوی وجود دارد.

[λ] نیز عملگری از فضاهای فرم‌های مدولار و فرم‌های کاسپ خواهد بود.

حال می‌توان به سادگی چک کرد که T_n ها و [λ] ها با یکدیگر

جابجا می‌شوند و T_n ها نسبت به ضرب داخلی پتروسون:

$$(f, g) := \int_{\mathbb{H}/SL_2(\mathbb{Z})} f(\tau) \bar{g}(\tau) (\text{Im } \tau)^k d\nu(\tau),$$

$$\nu(\tau) = y^{-2} dx dy, f, g \in S_k(SL_2(\mathbb{Z}))$$

خودالحق هستند. پس می‌توان فضای فرم‌های کاسپ از وزن k روی $SL_2(\mathbb{Z})$ را به فرم‌های ویژه‌ی T_n ها تجزیه کرد (که یکه و عمود هستند). این فرم‌های ویژه را می‌توان صریحاً پیدا کرد و برابر با سری‌های آیزنشتاین ^{۳۱} می‌شوند. خواص مهمی که عملگرهای هکه دارند عبارتند از:

$$\lambda, \mu \in \mathbb{C}^* \text{ برای } [\lambda][\mu] = [\mu][\lambda] \quad (1)$$

$$n \in \mathbb{N} \text{ برای } [\lambda]T_n = T_n[\lambda] \quad (2)$$

$$m, n \text{ اگر } T_n T_m = T_{nm} \text{ نسبت به هم اول باشند.} \quad (3)$$

$$n \in \mathbb{N} \text{ برای } T_l^n T_l = T_{l^{n+1}} + l T_{l^{n-1}}[l] \quad (4)$$

$a_1(T_n f) = a_n(f)$ که منظور از $a_n(f)$ ضریب n -ام فوریه‌ی f در بی‌نهایت است.

همچنین در حالت کلی‌تر، می‌توان این عملگرهای هکه را تعریف کرد که توابعی خطی از $M_k(\Gamma_1)$ ($S_k(\Gamma_1)$ به $M_k(\Gamma_2)$) $(S_k(\Gamma_2))$ خواهد بود. چیزی که برای ما مهم است، فقط عملگرهای هکه روی $S_k(\Gamma_0(N))$ هست که تعریف آن روش‌کننده نیست و تعمیمی از حالت قبل خواهد بود (می‌توان به سادگی روی بسط‌های فوریه‌ی آن‌ها را تعریف کرد). همچنین خواصی که این عملگرهای هکه کلی‌تر روی $S_k(\Gamma_0(N))$ دارند، مشابه خواص بالا است (برای $N | l$ باید حواسمن را بیشتر جمع کنیم).

مثلاً یکی از کاربردهای این عملگرهای از حدهای رامانوجان ^{۳۲} بوده است. در واقع تابع

$$\Delta(q) = q(1 - q^n)^{24}, \quad q = e^{2\pi iz}$$

³¹Eisenstein series

³²S. Ramanujan

³³Weil conjectures

تعريف می‌شود: یک عدد اول l را فیکس کنید و قرار دهید

$$\chi_l : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_l^*$$

بهطوری که

$$\sigma : \zeta_{l^n} \mapsto \zeta_{l^n}^{\chi_l(\sigma)} \quad n \in \mathbb{N}$$

همچنین، نمایش‌های شاخه‌ای^{۳۵} و غیرشاخه‌ای^{۳۶} به معنی زیر هستند:

تعريف ۱. به نمایش m در عدد اول l غیرشاخه‌ای گویند هرگاه $\rho(I_l) = \{1\}$ که I_l یک گروه سکون^{۳۷} در l است و در غیر این صورت به آن شاخه‌ای در l گویند.

نمایش‌های گالوا روی خم‌های بیضوی.

یک خم بیضوی E/\mathbb{Q} را در نظر بگیرید. دیدیم که عمل گروه روی E داریم و پس می‌توان نقاط تابی^{۳۸} روی آن را در نظر گرفت:

$$E[n] = \{p \in E(\bar{\mathbb{Q}}) \mid [n]p = O\}$$

در این صورت داریم:

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

حال مدول تیت^{۳۹} را به شکل زیر تعريف می‌کنیم:

$$T_l(E) := \lim_{\leftarrow} E[l^n] \cong \mathbb{Z}_l \times \mathbb{Z}_l$$

که \mathbb{Z}_l گروه اعداد l -تابی^{۴۰} هاست.

با استفاده از مدول تیت می‌توان یک نمایش گالوا معرفی کرد، در واقع برای هر نقطه‌ی $(x, y) \in E[l^n]$ می‌توان $P = P^\sigma = (\sigma(x), \sigma(y))$ را بدست آورد که از آنجا که عمل گروه، به شکل توابع گویا تعريف شده است، P^σ باید در $E[l^n]$ باشد. پس می‌توان نمایشی به شکل $G_{\mathbb{Q}} \rightarrow GL(E[l^n]) = GL_2(\mathbb{Z}/l^n\mathbb{Z})$ تعريف کرد که این‌ها

حال می‌توان یک بیان ساده از قضیه مدولاریتی (همان "حدس اخیر"^{۴۱} که وعده داده بودیم!) را گفت:

قضیه ۲. فرض کنید E/\mathbb{Q} یک خم بیضوی باشد. فرض کنید l یک عدد اول باشد. در این صورت قرار دهید $a_l = l+1 - \bar{E}(\mathbb{F}_l)$ (برای p های با کاهش خوب) در این صورت ($f \in S_2(\Gamma_0(N))$) وجود دارد که نرمال $(a_l(f) = 1)$ و "جدید" و فرم ویژه‌ی همه‌ی عملگرهای هنکه باشد و $a_l(f) = a_l$ برای همه بجز متناهی l .

"جدید" یعنی این‌که f از $S_2(\Gamma_0(d) \mid N)$ نیامده باشد: در واقع، اگر $g \in S_2(\Gamma_0(d))$ باشد، آن‌گاه $h : z \mapsto g(\frac{N}{d}z)$ یک فرم کاسپ در $S_2(\Gamma_0(N))$ هست و منظور از جدید یعنی f ترکیب خطی تعدادی از این خم‌های $S_2(\Gamma_0(d))$ برای d های کمتر نباشد.

با فرض این قضیه خواهیم داشت:

$$L(E, s) = L(f, s)$$

(روی متناهی عدد اول کنار گذاشته شده می‌توان این توابع را جوری تعريف کرد که رابطه بالا درست باشد) و پس خواص خوب (معادله تابعی و گسترش تحلیلی و ...) که برای L -تابع فرم‌های کاسپ ساده است به L -تابع خم‌های بیضوی می‌رسد.

۵ نمایش‌های گالوا

در این‌جا نمایش‌های گالوا روی خم‌های بیضوی و فرم‌های مدولار را توضیح می‌دهیم (مساوی بودن نمایش‌های گالوا نیز صورتی دیگر از قضیه مدولاریتی خواهد بود). منظور از یک نمایش گالوا یک همومورفیسم ($G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_n(A)$ است که) است. یک مثال از نمایش‌های گالوا نمایش دایره‌بر^{۴۲} است. این نمایش یک‌بعدی به شکل زیر

³⁴Cyclotomic

³⁵Ramified

³⁶Unramified

³⁷Inertia group

³⁸Torsion points

³⁹Tate module

⁴⁰ l -adic numbers

۶ حدس اپسیلون (قضیه ریبت)

این حدس را اولین بار سر مطرح کرد و ریبت آن را اثبات کرد و اثبات قضیه آخر فرما را به حدس شیمورا-تانياما کاهش داد. این قضیه در مورد کاهش دادن مرحله‌ی یک فرم کاسپ حرف می‌زند:

قضیه ۴. (قضیه ریبت) فرض کنید q عدد اولی باشد و f در $S_2(\Gamma_0(lN))$ یک فرم کاسپ جدید نرمال ($a_1(f) = 1$) و فرم‌ویژه همه‌ی عملگرهای هکه باشد به‌طوری که دارای نمایش‌های "مطلقًا تحویل ناپذیر"^{۴۱} $\rho_{f,q}$ باشد و این نمایش درا غیرشاخه‌ای ("متناهی" و "صف" ^{۴۲}) باشد اگر $q \neq l$. آن‌گاه $\rho_{f,q} \in S_2(\Gamma_0(N))$ نرمال و جدید وجود دارد که داریم:

$$\rho_{f,q} \sim \rho_{g,q}$$

اثبات. رجوع شود به [۳].

متناهی و صاف معانی جزئی دارند که توضیح آنها از سطح این مقاله بالاتر است. مطلقًا تحویل ناپذیر یعنی به عنوان نمایش‌های به $GL_2(\bar{\mathbb{F}}_p)$ تحویل ناپذیر باشند. نحوی استفاده از این قضیه را در بخش آخر توضیح می‌دهیم.

۷ دگردیسی‌های نمایش‌های گالوا

فرض کنید یک خم بیضوی روی اعداد گویا داریم و می‌خواهیم نمایش‌های گالوا روی آن را بررسی کنیم. در این صورت اگر نمایش روی کل مدول تیت را در نظر بگیریم، بررسی آن به نظر کار بسیار سختی است. پس ما ابتدا نمایش روی نقاط \mathcal{A} -تابی را بررسی می‌کنیم و سعی می‌کنیم با ایده‌ای با بررسی این نمایش، کار را تمام کنیم!

در این قسمت نمایش‌های گالوا را کلی تر می‌نویسیم و سعی می‌کنیم شرط‌های محدودکننده‌ای روی آن قرار دهیم (شرط‌هایی که مطمئن باشیم برای نمایش‌های گالوا روی خم‌های نیمه‌پایدار درست باشند) و مدولاریتی آن‌ها را اثبات کنیم.

با سیستم وارون سازگارند و پس نمایش گالوا روی مدول تیت پیدا می‌کنیم:

$$\rho_{E,l} : G_{\mathbb{Q}} \rightarrow GL(T_l(E)) \cong GL_2(\mathbb{Z}_l)$$

نمایش‌های گالوا روی فرم‌های مدولار

تعريف این کمی دشوارتر از حالت قبل است و قسمت اصلی ساخت آن را ارجاع می‌دهیم. در واقع برای ساخت آن ابتدا باید یک خم بیضوی (واریته آبلی در حالت کلی) بسازیم و سپس نمایش گالوا روی آن را مساوی با نمایش این فرم مدولار تعریف کنیم. پس فرض کنید $f \in S_2(\Gamma_0(N))$ طوری باشد که همه‌ی ضرایب بسط فوریه‌ی آن گویا هستند. در این صورت با استفاده از آن می‌توان یک خم بیضوی E_f ساخت به‌طوری که مدولار باشد (به معنی صورت قضیه مدولاریتی بالا) و سپس قرار می‌دهیم:

$$\rho_{f,l} := \rho_{E_f,l}$$

برای دیدن نحوه ساخت آن خم بیضوی می‌توانید به بخش ۵.۲ از [۲] رجوع کنید.

حال صورت دومی از قضیه مدولاریتی را بیان می‌کنیم:

قضیه ۳. فرض کنید E یک خم بیضوی روی \mathbb{Q} باشد. در این صورت $(S_2(\Gamma_0(N)) \cap f)$ (که f جدید و فرم‌ویژه همه‌ی عملگرهای هکه و دارای ضرایب فوریه گویا) وجود دارد که برای همه اهای اول:

$$\rho_{f,l} \sim \rho_{E,l}$$

علامت \sim به معنی مزدوج است.

رونندی که وایلز برای اثبات قضیه آخر فرما در پیش گرفت همین صورت از قضیه مدولاریتی بود و کاری که او کرد این بود که قضیه مدولاریتی را برای همه‌ی خم‌های بیضوی نیمه‌پایدار (از جمله خم فری) اثبات کرد که برای اثبات قضیه آخر فرما کافی بود.

⁴¹Absolutely irreducible

⁴²flat

تعريف ۴. دگردیسی ρ را از نوع D_{Σ} گوییم هرگاه:
 ۱) ρ بیرون از $\{p\} \cup S \cup \Sigma$ غیرشاخه‌ای باشد.

$$\det \rho = \chi_p \quad (2)$$

۲) برای هر S ,

$$\rho|_{I_l} \sim \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$$

این شرط نیمه‌پایداری در ρ است.

۳) تحدید $\rho|_{D_p}$ یا "صف" باشد یا "معمولی"^{۴۷}. این‌ها دو شرط موضعی هستند تعریف آن‌ها از سطح این مقاله بالاتر است.
 همچنین به دگردیسی‌ای، مجاز ^{۴۸} گوییم هرگاه برای Σ
 D_{Σ} باشد. حال مجموعه‌های همه‌ی دگردیسی‌های از نوع D_{Σ}
 و دگردیسی‌های مدلار از نوع D_{Σ} را به ترتیب با (A) و $DA_{\Sigma}(A)$ که
 این‌ها دو مجموعه‌ی متناهی هستند و اگر به آن‌ها به عنوان فانکتور
 نگاه کنیم:^{۴۹}

$$DM_{\Sigma} \subseteq DA_{\Sigma} : \mathcal{C}_O \rightarrow \text{FiniteSets}$$

نمایش‌پذیر^{۵۰} خواهد بود. پس دو عضو از \mathcal{C}_O وجود دارند مثل
 R_{Σ} و \mathbb{T}_{Σ} به‌طوری که

$$DM_{\Sigma}(A) = \text{Hom}(\mathbb{T}_{\Sigma}, A) \subseteq DA_{\Sigma}(A) = \text{Hom}(R_{\Sigma}, A)$$

حال با قرار دادن $A = \mathbb{T}_{\Sigma}$ یک تابع کانونی $\phi_{\Sigma} : R_{\Sigma} \rightarrow \mathbb{T}_{\Sigma}$ پیدا
 می‌کنیم. حال می‌توانیم نمایش‌های زیر را پیدا می‌کنیم:

$$\rho_{\Sigma}^{\text{univ}} : G_{\mathbb{Q}} \rightarrow GL_2(R_{\Sigma})$$

$$\rho_{\Sigma}^{\text{univ.mod}} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{T}_{\Sigma})$$

به‌طوری که با ϕ_{Σ} به هم مربوط می‌شوند. کاری که وایلز برای اثبات
 این قضیه می‌کند، اثبات قضیه زیر است:

قضیه ۵. (قضیه اصلی) ϕ_{Σ} ایزومورفیسم در رسته \mathcal{C}_O است.

تعريف ۲. فرض کنید K یک توسعه متناهی^{۴۱} باشد و O حلقه‌ی
 اعداد صحیح K باشد. رسته \mathcal{C}_O را تعریف کنید: اشیا از همه
 O -جبرهای نوتری موضعی A (با ایدآل ماسکیمال

) به همراه نگاشتی پوشان (نگاشت تشدید^{۴۲} $\pi : A \rightarrow O$)

تعریف کنید به‌طوری که $A/\mathfrak{m}_A \cong O/\mathfrak{m}_O = \mathbb{F}_q$ و نگاشتهای
 بین این اشیا را برابر O -جبر همومورفیسم‌های روی O تعریف کنید
 (نمودار زیر جابجا شود):

$$\begin{array}{ccc} A & \longrightarrow & A' \\ \pi_A \downarrow & & \downarrow \pi_{A'} \\ O & \xrightarrow{\mathbb{1}_O} & O \end{array}$$

حال یک شیء از رسته بالا مثل A را فیکس کنید. می‌خواهیم
 دگردیسی^{۴۴} نمایش‌های گالوا را تعریف می‌کنیم:

تعريف ۳. ۱) یک نمایش گالوا^{۴۵} $\rho_0 : G_{\mathbb{Q}} \rightarrow GL_m(\mathbb{F}_q)$ فیکس
 کنید. منظور از یک بالابری^{۴۶} ρ از این نمایش گالوا یک نمایش
 $\rho_0 : G_{\mathbb{Q}} \rightarrow GL_m(A)$ است به‌طوری که ρ به پیمانه‌ی \mathfrak{m}_A برابر شود.

۲) دو بالابری ρ, ρ' از ρ_0 را اکیداً معادل^{۴۷} گوییم هرگاه یک
 ماتریس C وجود داشته باشد که به پیمانه‌ی \mathfrak{m}_A همانی شود و داشته
 باشیم:

$$\rho(g) = C^{-1} \rho'(g) C, \quad g \in G_{\mathbb{Q}}$$

۳) منظور از یک دگردیسی^{۴۸} ρ_0 یک مولفه‌ی هم‌ارزی از رابطه‌ی
 هم‌ارزی بالا است.

حال شرط‌هایی که گفتیم را باید روی دگردیسی‌های نمایش‌های
 گالوا قرار دهیم: پس یک نمایش گالوا^{۴۹} $\rho_0 : G_{\mathbb{Q}} \rightarrow GL_m(\mathbb{F}_q)$
 فیکس کنید و S را مجموعه‌ی اعداد اولی قرار دهید که ρ_0 در آن‌ها
 شاخه‌ای است. این یک مجموعه‌ی متناهی است (چرا؟). حال
 فرض کنید Σ یک مجموعه‌ی متناهی از اعداد اول باشد.

⁴³Augmentation

⁴⁴Deformation

⁴⁵Lift

⁴⁶Strictly equivalent

⁴⁷Ordinary

⁴⁸Admissible

⁴⁹Functor

⁵⁰Representable

ریست بدست می‌آید که آن را بیان نکردیم. می‌توانید این را در [۴] پیدا کنید). حال با استفاده از تفکیک‌کننده یک خم می‌توان شرطی روی نمایش‌های گالوای بدست آمده از نقاط ۱–تابی قرار داد. اگر این کار را برای خم فری انجام دهیم نتیجه می‌شود که همه‌ی اعداد اولی که ABC را عاد می‌کنند در شرط قضیه‌ی ریست صدق می‌کنند (به عنوان q در قضیه). پس طبق قضیه ریست می‌توان فرم کاسپی نرمال در $(\Gamma_0(2))S_2$ پیدا کرد. اما داریم $\{0\} = S_2(\Gamma_0(2))$ (این بهسادگی از این‌که فشرده‌سازی $(\Gamma_0(2))\mathbb{H}$ گونه^{۵۲} صفر دارد بدست می‌آید) و پس فرم مدولار نرمالی در آن وجود ندارد. این همان تناظری بود که دنبالش بودیم!

مراجع

- [1] Wiles A. Modular elliptic curves and Fermat's Last Theorem. 1995.
- [2] Darmon H. Rational points on modular elliptic curves. 2003.
- [3] Ribet K. From the Taniyama-Shimura conjecture to Fermat's last theorem. 1990.
- [4] Panchishkin Alexei A. Manin, Yu. I. Introduction to Modern Number Theory. 2005.
- [5] P. Samuel. Algebraic Theory of Numbers. 1970.
- [6] Hungerford T. W. Algebra. Springer, 1974.

این قضیه کار را تمام می‌کند، زیرا نشان می‌دهد که تعداد اعضای مجموعه‌های $DA_{\Sigma}(A)$ و $DM_{\Sigma}(A)$ برای همه‌ی A ها یکی است و پس همه‌ی دگردیسی‌های مجاز، مدولار هستند و پس قضیه مدولاریتی خم‌های نیمه‌پایدار به اتمام می‌رسد. نحوه‌ی اثبات وایلز به این شکل است که او روی تعداد اعضای Σ استقرا می‌زند و R_{Σ} و T_{Σ} را به‌طور صریح می‌سازد و انتخاب هوشمندانه‌ای برای توابع تشدید آن‌ها می‌کند و سپس با تکنیک‌های جبر این مسئله را به یک نامساوی درباره تعداد اعضای یک ناوردا در این حلقه‌ها تبدیل می‌کند و آن را اثبات می‌کند. شکافی که در اثبات ابتدایی وایلز وجود داشت این بود که اثبات پایه استقرا ($\emptyset = \Sigma$) کامل نبود و او و تیلور مجبور شدند یک سال دیگر روی آن زمان بگذارند تا آنرا اثبات کنند. این کار را باز با استفاده از تکنیک‌های جبری مشابه حالت گام استقرا اثبات کردند. برای خواندن اثبات دقیق آن می‌توانید به مقاله وایلز [۱] رجوع کنید.

۸ اتمام اثبات

پس فرض کردیم که معادله‌ی فرما یک جواب نابدیهی دارد: $A^p + B^p = C^p$ حال خم فری را به شکل زیر تعریف کردیم: $F : y^2 = x(x - A^p)(x + B^p)$ و نمایش‌های گالوای روی آن را در نظر گرفتیم. می‌توان دید که این نمایش‌ها مجاز هستند و پس از قضیه اصلی وایلز، مدولار هستند و پس یک فرم مدولار نرمال در $(\Gamma_0(N))S_2$ برای N پیدا می‌کنیم که N عددی خالی از مربع خواهد بود که $N \mid 2ABC$ (این از ترکیب قضیه‌ای از میزرا^{۵۱} و

^{۵۱}B. Mazur

^{۵۲}Genus