مجله‌ی ریاضی شریف
سال اول، شماره نخست

قضیه آخر فرما

علی چراغی

چکیده

در این مقاله سعی می‌شود در مورد پیشنیازها و روند اثبات قضیه آخر فرما[۱] توضیح داده شود. تا آنجا که ممکن بوده، سعی شده خواندن این مقاله نیازی به هیچ پیشنیازی نداشته باشد، ولی با این وجود توضیح بعضی از پیشنیازها (کمی نظریه رسته‌ها و نظریه جبری اعداد) فضای بسیاری را اشغال می‌کند. خواننده برای یادگیری آن‌ها می‌تواند به [۱] و [۲] رجوع کند.

۱ مقدمه

در سال ۱۶۳۷، در ویرایشی از کتاب حساب[۲] 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[۳] بین سال‌های ۱۷۵۸ و ۱۷۷۰ حالت توان سوم را حل کرد.

۳) سوفی ژرمن[۴] در اوایل قرن ۱۹، راه‌حلی ایجاد کرد که حداقل برای همه توان‌های اول فرد کمتر از ۱۰۰، حالت اول قضیه فرما را ثابت می‌کرد ($x^n + y^n = z^n \Rightarrow n \mid xyz$).

۴) کومر[۵] با استفاده از نظریه اعداد جبری قضیه را برای حدود ۶۰ درصد (حدسی!) از اعداد اول ثابت کرد.

۵) در سال ۱۹۷۷، ترجانیان[۶] حالت اول قضیه را برای همه‌ی توان‌های زوج (غیر ۲!) اثبات کرد.

ولی در سال ۱۹۸۴ بود که فری[۷] یک ارتباط بین این حدس و خمی بیضوی یافت و احساس کرد که غلط بودن قضیه آخر فرما باعث رد حدسی معروف از شیمورا[۸] و تانیاما[۹] می‌شود.

[۱] P. Fermat
[۲] Arithmetica
[۳] L. Euler
[۴] S. Germain
[۵] E. Kummer
[۶] G. Terjanian
[۷] G. Frey
[۸] G. Shimura
[۹] Y. Taniyama
[۱۰] K. Ribet
[۱۱] J.P. Serre
[۱۲] Epsilon conjecture

دو سال پس از آن، ریبت[۱۰] این روند را ادامه داد و با اثبات حدسی از سر[۱۱]، به نام حدس اپسیلون[۱۲]، اثبات قضیه آخر فرما را به حدس شیمورا ـ تانیاما کاهش داد. بعد از او، ریاضیدان انگلیسی، اندرو 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 ـ تانیاما 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 انتها، در سال ۱۹۹۵، قضیه آخر فرما به‌طور کامل اثبات شد. همچنین با قوی‌تر کردن ایده‌های وایلز، تعدادی ریاضیدان دیگر، بروی[۱۵] و کنراد[۱۶] و دایموند[۱۷] و تیلور، توانستند حدس شیمورا ـ تانیاما 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. *فرض کنید $n \geq ۳$ عددی صحیح باشد. اگر برای $A, B \in \mathbb{Z}$ داشته باشیم $A^n + B^n = C^n$ آنگاه $ABC = ۰$.*

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

اولاً اگر $d|n$ آنگاه داریم:

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

پس این نشان می‌دهد که کافی است مسئله را برای nهای اول فرد و $n = ۴$ حل کنیم تا برای همه nها حل شود. حالت $n = ۴$ را خود فرما با روش نزول نامتناهی خود ثابت کرده است. پس کافیست قضیه آخر فرما را برای nهای 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 $ABC \neq ۰$ به‌طوری که $\gcd(A, B, C) = ۱$ و سعی می‌کنیم تناقضی یافت کنیم!

۳ خم‌های بیضوی

منظور از یک خم بیضوی روی اعداد گویا، یک خم جبری هموار[۱۸] است به‌طوری که با معادله‌ی زیر داده شده باشد:

$$y^۲ = x^۳ + ax + b, \quad a, b \in \mathbb{Q}$$

در این صورت هموار بودن به معنی این خواهد بود که چندجمله‌ای $x^۳ + ax + b$ 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: $\Delta = -۱۶(۴a^۳ + ۲۷b^۲)$.

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):

$$F : y^۲ = x(x - A^p)(x + B^p)$$

در واقع اگر تفکیک‌کننده مینیمال (مینیمم قدرمطلق تفکیک‌کننده‌ی خم‌های ایزومورف با این خم) این خم بیضوی

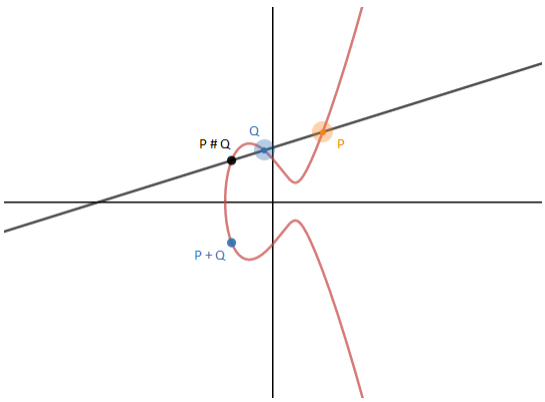
[۱۳] A. Wiles
[۱۴] R. Taylor
[۱۵] C. Breuil
[۱۶] B. Conrad
[۱۷] F. Diamond
[۱۸] Smooth
[۱۹] Discriminant

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

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

این توان pـام 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 $O = [0 : 1 : 0]$ 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 تعریف 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 تعریف 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 خوش‌تعریف است، زیرا می‌توان به سادگی از معادله‌ی خطوط و خم نتیجه گرفت $P + Q \in E(\mathbb{Q})$.



شکل ۱: *عمل گروه روی خم‌های بیضوی*

یک خم بیضوی E تعریف 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 $\bar{E} : y^2 = x^3 + \bar{a}x + \bar{b}$ که $(\bar{.}) : \mathbb{Z} \to \mathbb{Z}/l\mathbb{Z} \cong \mathbb{F}_l$ تابع تصویر است، را برابر با کاهش[۲۰] خم بیضوی به پیمانه l تعریف می‌کنیم. حال اگر $l \mid \Delta$، مشکل این خواهد بود که خم کاهش‌یافته در دقیقاً یک نقطه ناهموار خواهد بود و پس دو حالت داریم:

۱) خم در آن نقطه ناهمواری، دوخط 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 ناهموار، کاهش ضربی دارد. در واقع فرض کنید داشته باشیم $l \mid 2^{-8}(ABC)^p$. پس مثلاً $l \mid A$ و پس داریم:

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

این خم در نقطه‌ی $(0, 0)$ ناهموار است و دقیقاً زمانی در l کاهش جمعی دارد که $\bar{B}^p = 0$، اما این یعنی $l \mid B$ و پس طبق $A^p + B^p = C^p$ داریم $l \mid C$، پس $l \mid \gcd(A, B, C)$ 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 فوق‌العاده‌ای برخوردار است. ما اعداد $a_l = l + 1 - \sharp(\bar{E}(\mathbb{F}_l))$ را در نظر می‌گیریم. در این صورت داریم $|a_l| \leq 2\sqrt{l}$ (قضیه هسه[۲۳]) و می‌توان با استفاده از این اعداد، Lـتوابع[۲۴] خم‌های بیضوی را تعریف کرد (فرض می‌کنیم خم نیمه‌پایدار باشد):

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

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؟).

[۲۰] Reduction
[۲۱] Multiplicative reduction
[۲۲] Additive reduction
[۲۳] H. Hasse
[۲۴] L-functions

۴ فرم‌های مدولار

منظور از یک فرم مدولار روی $SL_۲(\mathbb{Z})$ با وزن k، یک تابع $f : \mathbb{H} \to \mathbb{C}$ است ($\mathbb{H}$ نیم‌صفحه‌ی بالای $\mathbb{C}$ است)، به‌طوری که

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z), z \in \mathbb{H}, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_۲(\mathbb{Z}) \quad (۱)$$

و روی همه‌ی نقاط $\mathbb{H}$ و همچنین در "∞" تحلیلی باشد. شرط آخر به این معنی است که بسط فوریه[۲۵] f (چون داریم $f(z) = f(z+۱)$ از رابطه بالا) در بی‌نهایت از صفر شروع شود:

$$f(q) = \sum_{n \geq ۰} a_n q^n, \quad q = e^{۲\pi i z}, \; a_n \in \mathbb{C}$$

همه‌ی فرم‌های مدولار از وزن k روی $SL_۲(\mathbb{Z})$ را با $M_k(SL_۲(\mathbb{Z}))$ نمایش می‌دهیم. همچنین واضح است که این تعریف را می‌توان زیرگروه‌هایی از $SL_۲(\mathbb{Z})$ مثل Γ تعمیم داد به این شکل که در شرط (۱) به جای $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_۲(\mathbb{Z})$ داشته باشیم $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. فرض می‌کنیم Γ خیلی کوچک نباشد یعنی $\Gamma(N) \subseteq \Gamma$ برای Nی که

$$\Gamma(N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_۲(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix} \mod N \}$$

هم‌چنین قرار می‌دهیم:

$$\Gamma_۰(N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_۲(\mathbb{Z}) \mid c \equiv ۰ \mod N \}$$

در این صورت $\Gamma(N)$ از اندیس متناهی در $SL_۲(\mathbb{Z})$ است (چرا؟) و پس Γ و $\Gamma_۰(N)$ نیز از اندیس متناهی هستند. به چنین زیرگروه‌هایی از $SL_۲(\mathbb{Z})$ زیرگروه‌های هم‌نهشتی[۲۶] گوییم. پس مانند قبل، فرم‌های مدولار در این فضا را با $M_k(\Gamma)$ نمایش می‌دهیم. فرم‌های مدولار این خاصیت مهم را دارند که هر کدام از $M_k(\Gamma)$ها متناهی‌بعد هستند (پس مثلاً اگر یک فرم مدولار داشته باشیم، می‌توانیم آن را برحسب پایه‌ای در این فضا 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 به‌طوری که در همه‌ی "کاسپ"های Γ صفر شود: اگر Γ یک زیرگروه هم‌نهشتی باشد، می‌توان فضای $\mathbb{H}/\Gamma$ را در نظر گرفت. در این صورت این یک رویه ریمانی باز است بطوری که فشرده‌سازی[۲۸] آن به متناهی نقطه نیاز دارد. به این متناهی نقطه، 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) از وزن k و مرحله‌ی n، یک فرم مدولار (فرم کاسپ) در $M_k(\Gamma_۰(N))$ $(S_k(\Gamma_۰(N)))$ است.

حال عملگرهای هکه[۲۹] را مختصراً توضیح می‌دهیم. برای سادگی فرض کنید $\Gamma = SL_۲(\mathbb{Z})$. اولاً دقت کنید که هر کدام از نقاط بالای صفحه را می‌توان با یک شبکه در $\mathbb{C}$ نمایش داد:

$$\mathbb{H} \to \mathcal{L}$$
$$\alpha \mapsto < \alpha, ۱ >$$

که $\mathcal{L}$، مجموعه‌ی همه‌ی شبکه‌هاست و همچنین اگر شبکه‌ها را در حد هموتتی[۳۰] (ضرب در یک عدد مختلط) در نظر بگیریم، تابع بالا یک دوسویی خواهد داد:

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

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

[۲۵] Fourier expansion
[۲۶] Congruence subgroups
[۲۷] Cusp form
[۲۸] Compactification
[۲۹] E. Hecke
[۳۰] Homothety

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 ($n\in\mathbb{N}$):

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

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

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

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

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

$[\lambda]$ نیز عملگری از فضاهای فرم‌های مدولار و فرم‌های کاسپ خواهد بود.

حال می‌توان به‌سادگی چک کرد که T_nها و $[\lambda]$ها با یکدیگر جابجا می‌شوند و T_nها نسبت به ضرب داخلی پترسون:

$$(f,g):=\int_{\mathbb{H}/SL_2(\mathbb{Z})}f(\tau)\bar{g}(\tau)(\mathrm{Im}\,\tau)^k d\nu(\tau),$$
$$\nu(\tau)=y^{-2}dxdy,\ f,g\in S_k(SL_2(\mathbb{Z}))$$

خودالحاق هستند. پس می‌توان فضای فرم‌های کاسپ از وزن k روی $SL_2(\mathbb{Z})$ را به فرم‌های ویژه همه‌ی T_nها 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:

۱) $[\lambda][\mu]=[\mu][\lambda]$ برای $\lambda,\mu\in\mathbb{C}^*$.

۲) $[\lambda]T_n=T_n[\lambda]$ برای $\lambda\in\mathbb{C}^*$ و $n\in\mathbb{N}$.

۳) $T_nT_m=T_{nm}$ اگر m,n نسبت به هم اول باشند.

۴) $T_{l^n}T_l=T_{l^{n+1}}+lT_{l^{n-1}}[l]$ برای l اول و $n\in\mathbb{N}$.

۵) $a_1(T_nf)=a_n(f)$ که منظور از $a_n(f)$ ضریب nـام 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 $M_k(\Gamma_2)$ $(S_k(\Gamma_2))$ خواهند بود. چیزی که برای ما مهم است، فقط عملگرهای هکه روی $S_k(\Gamma_0(N))$ هست که تعریف آن روشن‌کننده نیست و تعمیمی از حالت قبل خواهد بود (می‌توان به سادگی روی بسط‌های فوریه آن‌ها را تعریف کرد). همچنین خواصی که این عملگرهای هکه کلی‌تر روی $S_k(\Gamma_0(N))$ دارند، مشابه خواص بالا است (برای $l\mid N$ باید حواسمان را بیشتر جمع کنیم).

مثلاً یکی از کاربردهای این عملگرها قسمت‌هایی از حدس رامانوجان[۳۲] بوده است. در واقع تابع

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

بسط فوریه‌ی $\eta(q)=\sum_{n\geq1}\tau(n)q^n$ 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:

$$\tau(l^{n+1})=\tau(l)\tau(l^n)-l^{11}\tau(l^{n-1})$$

۳) $|\tau(l)|\leq2l^{11/2}$.

حال می توان دید که فضای $S_{12}(SL_2(\mathbb{Z}))$ یک بعدی است و $S_{12}(SL_2(\mathbb{Z}))=<\Delta>$. پس η باید بردار ویژه‌ی همه‌ی T_nها باشد. پس طبق 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 مقدارویژه‌ی 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

[۳۱] Eisenstein series
[۳۲] S. Ramanujan

است و از اثبات حدس‌های وی[۳۳] بدست می‌آید.

یک فرم کاسپ $f \in S_k(\Gamma_0(N))$ در نظر بگیرید به‌طوری که فرم ویژه‌ی همه‌ی T_nها ($n \nmid N$) باشد. در این صورت خواص ۳ و ۴ عملگرهای هکه پیشنهاد می‌کنند که ما Lـتابع ضرایب بسط فوریه‌ی آن را در نظر بگیریم:

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

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

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 Lـتابع خم‌های بیضوی می‌اندازد. پس احتمالاً رابطه‌ای بین فرم‌های ویژه و خم‌های بیضوی وجود دارد.

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

قضیه. *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 pهای با کاهش خوب) در این صورت $f \in S_2(\Gamma_0(N))$ وجود دارد که نرمال ($a_1(f) = 1$) و "جدید" و فرم ویژه‌ی همه‌ی عملگرهای هکه باشد و $a_l(f) = a_l$ برای همه بجز متناهی l.*

"جدید" یعنی این‌که f از $S_2(\Gamma_0(d))$ $(d \mid N)$ 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 dهای 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 تعریف کرد که رابطه بالا درست باشد) و پس خواص خوب (معادله تابعی و گسترش تحلیلی و ...) که برای Lـتوابع فرم‌های کاسپ ساده است به Lـتوابع 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 هومومورفیسم $\rho : G_{\mathbb{Q}} \to GL_n(A)$ است که $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ و A یک حلقه‌ی جابجایی و یکدار است. یک مثال از نمایش‌های گالوا نمایش دایره‌بر[۳۴] است. این نمایش یک‌بعدی به شکل زیر تعریف می‌شود: یک عدد اول l را فیکس کنید و قرار دهید

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

به‌طوری که

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

همچنین، نمایش‌های شاخه‌ای[۳۵] و غیرشاخه‌ای[۳۶] به معنی زیر هستند:

تعریف. *به نمایش ρ 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

[۳۳] Weil conjectures
[۳۴] Cyclotomic
[۳۵] Ramified
[۳۶] Unramified
[۳۷] Inertia group
[۳۸] Torsion points

روی E داریم و پس می‌توان نقاط تابی[۳۸] روی آن را در نظر گرفت:

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

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 تعریف می‌کنیم:

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

که $\mathbb{Z}_l$ گروه اعداد lـ تایی[۴۰] هاست.

با استفاده از مدول تیت می‌توان یک نمایش گالوا معرفی کرد، در واقع برای هر نقطه‌ی $P = (x, y) \in E[l^n]$ می‌توان $\sigma \in G_{\mathbb{Q}}$ را روی آن اثر داد و $P^\sigma = (\sigma(x), \sigma(y))$ را بدست آورد که از آنجا که عمل گروه، به شکل توابع گویا تعریف شده است، P^σ باید در $E[l^n]$ باشد. پس می‌توان نمایشی به شکل $\rho : G_{\mathbb{Q}} \to GL(E[l^n]) = GL_2(\mathbb{Z}/l^n\mathbb{Z})$ تعریف کرد که این‌ها با سیستم وارون سازگارند و پس نمایش گالوا روی مدول تیت پیدا می‌کنیم:

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

نمایش‌های گالوا روی فرم‌های مدولار.

تعریف 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 ۲,۵ از [۳] رجوع کنید.

حال صورت دومی از قضیه مدولاریتی را بیان می‌کنیم:

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

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

علامت $\sim$ به معنی مزدوج است.

روندی 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.

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 ـ تانیاما کاهش داد. این قضیه در مورد کاهش دادن مرحله‌ی یک فرم کاسپ حرف می‌زند:

قضیه. (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 "مطلقاً تحویل‌ناپذیر"[۴۱] $\rho_{f,q}$ باشد و این نمایش در l غیرشاخه‌ای ("متناهی" و "صاف"[۴۲]) باشد اگر $l \neq q$ $(l = q)$. آن‌گاه $g \in S_2(\Gamma_0(N))$ نرمال و جدید وجود دارد که*

[۳۹] Tate module
[۴۰] l-adic numbers
[۴۱] Absolutely irreducible
[۴۲] flat

داریم:

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

اثبات. رجوع شود به [۴].

متناهی و صاف معانی جزئی دارند که توضیح آنها از سطح این مقاله بالاتر است. مطلقاً تحویل‌ناپذیر یعنی به عنوان نمایش‌های به $GL_۲(\bar{\mathbb{F}}_p)$ تحویل‌ناپذیر باشند. نحوه‌ی 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 lـ تابی را بررسی می‌کنیم و سعی می‌کنیم با ایده‌ای با بررسی این نمایش، کار را تمام کنیم!

در این قسمت نمایش‌های گالوا را کلی‌تر 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.

تعریف. *فرض کنید K یک توسیع متناهی $\mathbb{Q}_l$ باشد و O حلقه‌ی اعداد صحیح K باشد. رسته $\mathcal{C}_O$ را تعریف کنید: اشیا از همه Oـ جبرهای نوتری موضعی A (با ایدآل ماکسیمال $\mathfrak{m}_A$) به همراه نگاشتی پوشا (نگاشت تشدید[۴۳]) $\pi : A \to O$ تعریف کنید به‌طوری که $A/\mathfrak{m}_A \cong O/\mathfrak{m}_O = \mathbb{F}_q$ و نگاشت‌های بین این اشیا را برابر Oـ جبر هوموموفیسم‌های روی O تعریف کنید (نمودار زیر جابجا شود):*

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

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

تعریف. ۱) *یک نمایش گالوا $\rho_۰ : G_{\mathbb{Q}} \to GL_m(\mathbb{F}_q)$ فیکس کنید. منظور از یک بالابری[۴۵] ρ از این نمایش گالوا یک نمایش $\rho : G_{\mathbb{Q}} \to GL_m(A)$ است به‌طوری که ρ به پیمانه‌ی $\mathfrak{m}_A$ برابر $\rho_۰$ شود.*

۲) *دو بالابری ρ, ρ' از $\rho_۰$ را اکیداً معادل[۴۶] گوییم هرگاه یک ماتریس C وجود داشته باشد که به پیمانه‌ی $\mathfrak{m}_A$ همانی شود و داشته باشیم:*

$$\rho(g) = C^{-۱}\rho'(g)C,\ g \in G_{\mathbb{Q}}$$

۳) *منظور از یک دگردیسی $\rho_۰$ یک مولفه‌ی هم‌ارزی از رابطه‌ی هم‌ارزی بالا است.*

حال شرط‌هایی که گفتیم را باید روی دگردیسی‌های نمایش‌های گالوا قرار دهیم: پس یک نمایش گالوا $\rho_۰ : G_{\mathbb{Q}} \to GL_m(\mathbb{F}_q)$ فیکس کنید و S را مجموعه‌ی اعداد اولی قرار دهید که $\rho_۰$ در آن‌ها شاخه‌ای است. این یک مجموعه‌ی متناهی است (چرا؟). حال فرض کنید Σ یک مجموعه‌ی متناهی از اعداد اول باشد.

تعریف. *دگردیسی ρ را از نوع D_Σ گوییم هرگاه:*

۱) *ρ بیرون از $\Sigma \cup S \cup \{p\}$ غیرشاخه‌ای باشد.*

۲) $\det \rho = \chi_p$.

۳) *برای هر $l \in S$،*

$$\rho|_{I_l} \sim \begin{bmatrix} ۱ & * \\ ۰ & ۱ \end{bmatrix}$$

این شرط نیمه‌پایداری در l است.

۴) *تحدید $\rho|_{D_p}$ یا "صاف" باشد یا "معمولی"[۴۷]. این‌ها دو شرط موضعی هستند تعریف آن‌ها از سطح این مقاله بالاتر است.*

[۴۳] Augmentation
[۴۴] Deformation
[۴۵] Lift
[۴۶] Strictly equivalent
[۴۷] Ordinary
[۴۸] Admissible

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 [۵] 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 $S_2(\Gamma_0(N))$ برای Nی پیدا می‌کنیم که N عددی خالی از مربع خواهد بود که $N \mid 2ABC$ (این از ترکیب قضیه‌ای از میزر[۵۱] و ریبت بدست می‌آید که آن را بیان نکردیم. می‌توانید این را در [۶] پیدا کنید). حال با استفاده از تفکیک‌کننده یک خم می‌توان شرطی روی نمایش‌های گالوای بدست آمده از نقاط lـ تابی قرار داد. اگر این کار را برای خم فری انجام دهیم نتیجه می‌شود که همه‌ی اعداد اولی که ABC را عاد می‌کنند در شروط قضیه‌ی ریبت صدق می‌کنند (به عنوان q در قضیه). پس طبق قضیه ریبت می‌توان فرم کاسپی نرمال در $S_2(\Gamma_0(2))$ پیدا کرد. اما داریم $S_2(\Gamma_0(2)) = \{0\}$ (این به‌سادگی از این‌که فشرده‌سازی $\mathbb{H}/\Gamma_0(2)$ گونه[۵۲] صفر دارد بدست می‌آید) و پس فرم مدولار نرمالی در آن وجود ندارد. این همان تناقضی بود که دنبالش بودیم!

همچنین به دگردیسی‌ای، مجاز[۴۸] گوییم هرگاه برای Σیی D_Σ باشد. حال مجموعه‌های همه‌ی دگردیسی‌های از نوع D_Σ و دگردیسی‌های مدولار از نوع D_Σ را به ترتیب با $DA_\Sigma(A)$ و $DM_\Sigma(A)$ نشان می‌دهیم. در این صورت می‌توان ثابت کرد که این‌ها دو مجموعه‌ی متناهی هستند و اگر به آن‌ها به عنوان فانکتور[۴۹] نگاه کنیم:

$$DM_\Sigma \subseteq DA_\Sigma : \mathcal{C}_O \to \mathbf{FiniteSets}$$

نمایش‌پذیر[۵۰] خواهند بود. پس دو عضو از $\mathcal{C}_O$ وجود دارند مثل R_Σ و $\mathbb{T}_\Sigma$ به‌طوری که

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

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

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

به‌طوری که با ϕ_Σ به هم مربوط می‌شوند. کاری که وایلز برای اثبات این قضیه می‌کند، اثبات قضیه زیر است:

قضیه. (*قضیه اصلی*) *ϕ_Σ ایزومورفیسم در رسته $\mathcal{C}_O$ است.*

این قضیه کار را تمام می‌کند، زیرا نشان می‌دهد که تعداد اعضای مجموعه‌های $DM_\Sigma(A)$ و $DA_\Sigma(A)$ برای همه‌ی Aها 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 ($\Sigma = \emptyset$) کامل نبود و او و تیلور مجبور

[۴۹] Functor
[۵۰] Representable
[۵۱] B. Mazur
[۵۲] Genus

مراجع

[1] Hungerford T. W., *Algebra*, Springer, 1974.

[2] P. Samuel, *Algebraic Theory of Numbers*, Translated from French by Allan J. Silberger, 1970.

[3] Darmon H., *Rational Points on Modular Elliptic Curves*, 2003.

[4] Ribet K., *From the Taniyama-Shimura conjecture to Fermat's last theorem* , 1990.

[5] Wiles A., *Modular elliptic curves and Fermat's Last Theorem*, 1995.

[6] Manin, Yu. I., Panchishkin, Alexei A., *Introduction to Modern Number Theory*, 2005.