نظریه اعداد بزرگسالان: کران Hasse-Weil؛ قسمت صفرم

آرین همتی *

چکیده

فرض کنید معادله هم‌نهشتی $P(x_1, x_2, \cdots, x_n) \overset{p}{\equiv} 0$ داده شده باشد که در آن $P \in \mathbb{Z}[X_1, \cdots, X_n]$ یک چندجمله‌ای n متغیره با ضرایب صحیح باشد. بدیهی‌ست که جواب‌های چنین معادله هم‌نهشتی‌ای به پیمانه p تکرار خواهند شد. فرض کنید $N(P)$ تعداد جواب‌های این معادله هم‌نهشتی در $(\mathbb{Z}/p\mathbb{Z})^n$ باشد. (به زبان ساده‌تر، $N(P)$ تعداد n تایی‌های مرتب از اعضای دستگاه کامل مانده‌ها به پیمانه p است که جوابی از معادله هم‌نهشتی فوق را به دست می‌دهند) آیا می‌توان برای هر چندجمله‌ای P، کرانی کارا برای $N(P)$ ارائه داد؟ در وهله اول، احتمالاً این امر برای خواننده غیرمتخصص ناشدنی بنظر می‌رسد. اما قضیه‌ای در نظریه اعداد (که اثبات به غایت دشوار آن، به شدت از ریاضیات پیشرفته شامل قضایای هندسه جبری و هندسه حسابی بهره می‌برد) به نام قضیه Hasse، بیان می‌دارد که خواص هندسی چندجمله‌ای P در واقع کران قدرتمندی از $N(P)$ به دست خواهند داد. قضیه/کران Hasse که قضیه‌ای روی خم‌های بیضوی است. (اگر با تعریف خم بیضوی آشنایی ندارید، احتمالاً تنها نیستید!) این قضیه ابتدا توسط Emil Artin در سال ۱۹۲۴ و در قالب مسئله‌ای در تز دکترای وی[۱] مطرح شد و در سال ۱۹۳۳ توسط ریاضی‌دان آلمانی Helmut Hasse به اثبات رسید.[۲] در سال ۱۹۴۹، ریاضی‌دان نامی فرانسوی André Weil مجموعه‌ای از حدسیات تاثیرگذار خود در نظریه اعداد را در قالب یک برنامه ریاضیاتی ارائه داد.[۳] یکی از نتایج حدسیات Weil، بدست آوردن کرانی مشابه کران Hasse برای خم‌های دلخواه (و نه لزوماً بیضوی) بود و در نتیجه کران Hasse را به مجموعه بسیار بزرگتری از معادلات هم‌نهشتی گسترش می‌داد. حدسیات Weil در حالت یک‌بعدی (خم) توسط خود Weil به اثبات رسید.[۱] اثبات این قضیه منجر به تعمیم کران Hasse به خم‌های جبری دلخواه شد و از آن با نام کران Hasse-Weil یاد می‌شود. در ادامه، در سال ۱۹۵۴، Weil به همراه Serge Lang سعی کردند در مقاله مشهور خود، با استفاده از حدس ریمان روی خم‌های مسطح، حدسیات Weil را در ابعاد بالاتر به اثبات برسانند.[۴] یکی از نتایج این تلاش، کران Lang-Weil است که تعمیم نتیجه Hasse-Weil به واریته‌های کلی‌تر است. (مجدداً اگر با تعریف واریته آشنا نیستید، تنها نخواهید بود) در این سلسله نوشتار، قصد داریم در ابتدا از نتایجی مقدماتی از سیر نتایج بیان شده آغاز کرده و در نهایت با توضیحاتی درباره کران Lang-Weil، شما را با این قضیه عمیق در ریاضیات آشناتر کنیم. تلاش بر این خواهد بود که نوشتارهای این سلسله تا حد ممکن مقدماتی باشند اما طبیعتاً با توجه به ذات موضوعات مورد بحث، تلاش ما از جایی به بعد واهی خواهد بود! اما تا اطلاع ثانوی، دانش مقدماتی نظریه اعداد برای دنبال کردن نوشتار کفایت می‌کند.

در این نوشتار، اثباتی مقدماتی از حالت ضعیف قضیه Hasse-Weil را درباره خم‌های Hyperelliptic ارائه می‌دهیم. گزاره دقیق چنین است:

قضیه ۱. فرض کنید $n \leq 3$ عددی فرد باشد و چندجمله‌ای $P \in \mathbb{Z}[X]$ چندجمله‌ای تکینی از درجه n باشد. عدد اول $9n^2 < p$ داده شده است. معادله هم‌نهشتی $y^2 \overset{p}{\equiv} P(x)$ را در نظر بگیرید و تعداد جواب‌های آن (در دستگاه کامل مانده‌ها به پیمانه p) را N بنامید. آنگاه:

$$|N - p| \leq n\sqrt{3np} < pn$$

ابتدا دقت کنید حل معادله هم‌نهشتی داده شده معادل پیدا کردن مقادیر صحیحی از x در دستگاه کامل مانده‌ها به پیمانه p است که به ازای آنها، $P(x)$ یک مانده درجه دوم به پیمانه p باشد. از این رو، اعضای دستگاه کامل مانده‌ها به پیمانه p را می‌توان به سه دسته تقسیم کرد:

۱. اعضای $x_0 \in \mathbb{Z}/p\mathbb{Z}$ که $P(x)$ مانده درجه دوم به پیمانه p باشد. به نوشتار نماد لژاندر: $\left(\frac{P(x_0)}{p}\right) = 1$. طبق محک اویلر $P(x_0)^{\frac{p-1}{2}} \overset{p}{\equiv} 1$

۲. اعضای $x_0 \in \mathbb{Z}/p\mathbb{Z}$ که $P(x_0)$ نامانده درجه دوم به پیمانه p باشد. به نوشتار نماد لژاندر: $\left(\frac{P(x_0)}{p}\right) = -1$. طبق محک اویلر $P(x_0)^{\frac{p-1}{2}} \overset{p}{\equiv} -1$

۳. اعضای $x_0 \in \mathbb{Z}/p\mathbb{Z}$ که $P(x_0) \overset{p}{\equiv} 0$. به نوشتار نماد لژاندر: $\left(\frac{P(x_0)}{p}\right) = 0$

مجموعه اعضای دسته اول، دوم و سوم را به ترتیب با N_1, N_{-1}, N_0 نمایش می‌دهیم. بدیهی‌ست که $|N_1| + |N_{-1}| + |N_0| = p$. همچنین واضح است که هر مقدار x از دسته اول، دوم و سوم، به ترتیب دو، صفر و یک جواب از معادله هم‌نهشتی داده شده به دست خواهند داد. در نتیجه $N = |N_0| + 2|N_1|$. برای به دست آوردن یک کران از N، می‌توانیم ابتدا کران‌هایی از $|N_1|, |N_{-1}|, |N_0|$ به دست آوریم. از نظریه اعداد مقدماتی می‌دانیم به ازای هر چندجمله‌ای P با ضرایب صحیح، در صورتی که تمام ضرایب Q بر عدد اول p بخش‌پذیر نباشند، معادله هم‌نهشتی $Q(x) \overset{p}{\equiv} 0$ حداکثر d ریشه در دستگاه کامل مانده‌ها به پیمانه p دارد که d، باقی‌مانده $\deg(Q)$ در تقسیم بر p می‌باشد. در نتیجه $|N_0|$ که تعداد ریشه‌های معادله هم‌نهشتی $P(x) \overset{p}{\equiv} 0$ در دستگاه کامل مانده‌ها به پیمانه p می‌باشد، حداکثر برابر با n است. (حالتی که تمام ضرایب P بر p بخش‌پذیر باشند، بدیهی‌ست) در نتیجه کافی‌ست کران‌هایی برای $|N_1|, |N_{-1}|$ به دست آوریم. برای حصول این نتیجه از لم مهم زیر استفاده می‌کنیم:

---

*aryanhemmati1382@gmail.com

[۱] در سال‌های آتی، Grothendieck به کمک Artin, Verdier, Dwork سه تا از چهار حدس Weil را اثبات کردند و تنها حدس سوم که به حدس ریمان معروف بود (متفاوت از حدس حل‌نشده ریمان) لاینحل باقی ماند. در سال‌های ۱۹۷۴ و ۱۹۸۰، Pierre Deligne با ارائه دو اثبات مختلف از حدس سوم Weil، اثبات این حدسیات را به پایان رساند.

لم ۱. برای هر مقدار طبیعی $m \leq \sqrt{\frac{p}{3n}}$، چندجمله‌ای $R \in \mathbb{Z}[X]$ موجود است به طوری که تمام ضرایب آن بر p بخش‌پذیر نباشند، تمام اعضای N_{-1} را به عنوان ریشه‌هایی (به پیمانه p) با تکرر حداقل $2m$ دارا باشد و همچنین $\deg(R) \leq \frac{p-1}{2}n+(m-1)p+(n-1)m^2+n$.

برای اثبات، نشان می‌دهیم می‌توان ضرایب $r_1, \cdots, r_m, t_1, \cdots, t_m \in \mathbb{Z}[X]$ را طوری انتخاب کرد که چندجمله‌ای زیر مطلوب باشد:

$$R(x) = \left(1 + P(x)^{\frac{p-1}{2}}\right) \sum_{i=1}^{m} r_i(x)(x^p - x)^{i-1} + \sum_{i=1}^{m} t_i(x)(x^p - x)^i$$

گام ۱. ابتدا شرایط لازم برای انتخاب ضرایب را می‌یابیم تا هر عضو N_{-1} با تکرر حداقل $2m$ ریشه‌ای از R باشد. دقت کنید تمام اعضای دستگاه کامل مانده‌ها به پیمانه p در رابطه $x^p - x \overset{p}{\equiv} 0$ صدق می‌کنند. در نتیجه $R(x) \overset{p}{\equiv} 1 + P(x)^{\frac{p-1}{2}}$. از طرفی تمام اعضای $x_0 \in N_{-1}$ در رابطه $1 + P(x_0)^{\frac{p-1}{2}}$ صادقند. (مطابق محک اویلر) در نتیجه، اعضای مجموعه N_{-1} دقیقاً همان ریشه‌های صحیح R هستند.

گام ۲. می‌دانیم برای هر چندجمله‌ای $Q \in \mathbb{Z}[X]$ با ضرایب صحیح، مقدار صحیح $a \in \mathbb{Z}$ ریشه‌ای (به پیمانه p) از تکرر حداقل k است اگر و فقط اگر $Q^{(i)}(a) \overset{p}{\equiv} 0, \ \forall 0 \leq i < k$ که در آن، $Q^{(i)}$ مشتق از مرتبه iـ‌اُم می‌باشد. (اگر تا به حال به این قضیه برخورد نکرده‌اید، آن را ثابت کنید) در نتیجه برای بررسی تکرر هر عضو مجموعه N_{-1} در چندجمله‌ای R، نیاز است مشتقات R را محاسبه کنیم:

$$R^{(1)}(x) = \left(1 + P(x)^{\frac{p-1}{2}}\right) \left(\sum_{i=1}^{m} {r_i}'(x)(x^p - x)^{i-1} + \sum_{i=2}^{m} r_i(x)(i-1)(x^p - x)^{i-2}(px^{p-1} - 1)\right)$$

$$+\frac{p-1}{2} P(x)^{\frac{p-3}{2}} P'(x) \sum_{i=1}^{m} r_i(x)(x^p - x)^{i-1} + \sum_{i=1}^{m} {t_i}'(x)(x^p - x)^i + \sum_{i=1}^{m} t_i(x) i (x^p - x)^{i-1}(px^{p-1} - 1)$$

برای راحتی محاسبات به پیمانه p، نیاز است این عبارت در ۲ ضرب شود تا ضریب $\frac{p-1}{2}$ از بین برود. برای این امر، اپراتور $D = \frac{2d}{dx}$ را معرفی می‌کنیم. توجه کنید $D^i R(x) = 2^i R^{(i)}(x)$. در نتیجه این تغییر اپراتور، تغییری در روند استفاده از محک تکرر ایجاد نمی‌کند.

$$\implies DR(x) = 2R^{(1)}(x) \overset{p}{\equiv} \left(1 + P(x)^{\frac{p-1}{2}}\right) \left(\sum_{i=1}^{m} Dr_i(x)(x^p - x)^{i-1} - 2\sum_{i=2}^{m} r_i(x)(i-1)(x^p - x)^{i-2}\right)$$

$$-P(x)^{\frac{p-3}{2}} P'(x) \sum_{i=1}^{m} r_i(x)(x^p - x)^{i-1} + \sum_{i=1}^{m} Dt_i(x)(x^p - x)^i - 2\sum_{i=1}^{m} t_i(x) i (x^p - x)^{i-1}$$

$$= \left(1 + P(x)^{\frac{p-1}{2}}\right) \left(\sum_{i=1}^{m} Dr_i(x)(x^p - x)^{i-1} - 2\sum_{i=2}^{m} r_i(x)(i-1)(x^p - x)^{i-2}\right)$$

$$-P(x)^{\frac{p-1}{2}} \frac{P'(x)}{P(x)} \sum_{i=1}^{m} r_i(x)(x^p - x)^{i-1} + \sum_{i=1}^{m} Dt_i(x)(x^p - x)^i - 2\sum_{i=1}^{m} t_i(x) i (x^p - x)^{i-1}$$

$$= \left(1 + P(x)^{\frac{p-1}{2}}\right) \left(\sum_{i=1}^{m} Dr_i(x)(x^p - x)^{i-1} - 2\sum_{i=2}^{m} r_i(x)(i-1)(x^p - x)^{i-2} - \frac{P'(x)}{P(x)} \sum_{i=1}^{m} r_i(x)(x^p - x)^{i-1}\right)$$

$$+\frac{P'(x)}{P(x)} \sum_{i=1}^{m} r_i(x)(x^p - x)^{i-1} + \sum_{i=1}^{m} Dt_i(x)(x^p - x)^i - 2\sum_{i=1}^{m} t_i(x) i (x^p - x)^{i-1}$$

$$= \left(1 + P(x)^{\frac{p-1}{2}}\right) \left(\sum_{i=1}^{m-1} \left(Dr_i(x) - 2ir_i(x) - \frac{P'(x)}{P(x)} r_i(x)\right)(x^p - x)^{i-1} + \left(Dr_m(x) - \frac{P'(x)}{P(x)} r_m(x)\right)(x^p - x)^{m-1}\right)$$

$$+\sum_{i=1}^{m-1}\left(Dt_i(x)-2(i+1)t_{i+1}(x)+\frac{P'(x)}{P(x)}r_{i+1}(x)\right)(x^p-x)^i+Dt_m(x)(x^p-x)^m+\left(\frac{P'(x)}{P(x)}r_1(x)-2t_1(x)\right)$$

که به جز جمله آخر، یک فرم بازگشتی را نشان می‌دهد. برای از بین بردن جمله آخر قرار می‌دهیم $t_1(x)=\frac{P'(x)}{2P(x)}r_1(x)$. برای هر $1\le j\le m$، دنباله $r_{i,j},\ t_{i,j}$ را برای هر $0\le i<2m$ تعریف می‌کنیم، به طوری که فرم بازگشتی مربوط به چندجمله‌ای $D^kR(x)=2^kR^{(k)}(x)$ را نمایش دهد. (تعریف می‌کنیم $r_{0,i}:=r_i,\ t_{0,i}:=t_i$) در این صورت باید داشته باشیم:

$$DR(x)=2R^{(1)}(x)=\left(1+P(x)^{\frac{p-1}{2}}\right)\sum_{i=1}^{m}r_{1,i}(x)(x^p-x)^{i-1}+\sum_{i=1}^{m}t_{1,i}(x)(x^p-x)^i$$

$$r_{1,i}(x)=Dr_{0,i}(x)-2ir_{0,i+1}(x)-\frac{P'(x)}{P(x)}r_{0,i}(x),\ \forall 1\le i<m,\quad r_{1,m}=Dr_{0,m}(x)-\frac{P'(x)}{P(x)}r_{0,m}(x)$$

$$t_{1,i}(x)=Dt_{0,i}(x)-2(i+1)t_{0,i+1}(x)+\frac{P'(x)}{P(x)}r_{0,i+1}(x),\ \forall 1\le i<m,\quad t_{1,m}(x)=Dt_{0,m}(x)$$

استدلالی مشابه قبل نشان می‌دهد که $DR(x)\overset{p}{\equiv}0,\ \forall x\in N_{-1}$ و در نتیجه، $DR(x)\overset{p}{\equiv}(1+P(x)^{\frac{p-1}{2}})r_{1,1}(x),\ \forall x\in\mathbb{Z}$ برای ادامه این فرایند و به دست آوردن یک رابطه بازگشتی، نیاز است در هر مرحله شرط $t_{i,1}(x)=\frac{P'(x)}{P(x)}r_{i,1}(x)$ برای هر $0\le i<2m$ برقرار باشد. در این صورت می‌توان به استقرا ثابت کرد که برای هر $i\in\mathbb{N}$ داریم:

$$D^iR(x)=2^iR^{(i)}(x)=\left(1+P(x)^{\frac{p-1}{2}}\right)\sum_{j=1}^{m}r_{i,j}(x)(x^p-x)^{j-1}+\sum_{j=1}^{m}t_{i,j}(x)(x^p-x)^j$$

$$r_{i,j}(x)=Dr_{i-1,j}(x)-2jr_{i-1,j+1}(x)-\frac{P'(x)}{P(x)}r_{i-1,j}(x),\ \forall 1\le j<m,\quad r_{i,m}=Dr_{i-1,m}(x)-\frac{P'(x)}{P(x)}r_{i-1,m}(x)$$

$$t_{i,j}(x)=Dt_{i-1,j}(x)-2(j+1)t_{i-1,j+1}(x)+\frac{P'(x)}{P(x)}r_{i-1,j+1}(x),\ \forall 1\le j<m,\quad t_{i,m}(x)=Dt_{i-1,m}(x)$$

با روندی مشابه، $D^iR(x)=2^iR^{(i)}(x)\overset{p}{\equiv}0,\ \forall 0\le i<2m\iff R^{(i)}(x)\overset{p}{\equiv}0$ که تکرر حداقل $2m$ را نتیجه می‌دهد.

نکته ۱. تنها مانع تکمیل اثبات لم ۱، برقراری روابط $t_{i,1}(x)=\frac{P'(x)}{P(x)}r_{i,1}(x)$ است. با اینکه انتخاب چندجمله‌ای‌های مناسب برای برقرار کردن رابطه $t_{0,1}(x)=\frac{P'(x)}{P(x)}r_{0,1}(x)$ به علت وجود دو درجه آزادی (انتخاب $r_{0,i},\ t_{0,i},\ \forall 1\le i\le m$ آزاد است) بلافاصله قابل انجام است، اثبات امکان انتخاب مناسب چندجمله‌ای‌های $r_{0,i},\ t_{0,i}$ به نحوی که چندجمله‌ای‌های ثانویه $r_{i,0},\ t_{i,0}$ در رابطه مذکور صدق کنند، به این میزان بدیهی نیست. در باقی اثبات، نشان می‌دهیم این انتخاب امکان‌پذیر است.

زیر لم ۱. برای هر مقدار $0\le i<2m,\ 1\le j\le m$، چندجمله‌ای $2^jj!t_{i,j}(x)\in\mathbb{Z}[X]$ به صورت یک فرم خطی از چندجمله‌ای‌های $r_{i,1},\cdots,r_{i,j}$ با ضرایبی در $Z(X)$ قابل نمایش است. به بیان دیگر، توابع گویای $F_{k,l}\in\mathbb{Z}(X)$ موجودند (یک تابع گویا، تابعی به فرم $\frac{P(x)}{Q(x)}$ است که در آن $P,\ Q$ چندجمله‌ای هستند و $Q\not\equiv 0$. به طور خاص، $\mathbb{Z}(X)$ مجموعه شامل تمام توابع گویایی‌ست که حاصل تقسیم یک چندجمله‌ای با ضرایب صحیح بر یک چندجمله‌ای ناصفر با ضرایب صحیح باشند) به نحوی که رابطه زیر برقرار باشد:

$$\forall 0\le i<2m,\ 1\le j\le m: 2^jj!t_{i,j}(x)=F_{j,1}(x)r_{i,1}(x)+\cdots+F_{j,j}(x)r_{i,j}(x)$$

اثبات. حکم را برای $j\ne m$ به استقرا روی j اثبات می‌کنیم. پایه استقرا از رابطه فوق روی $t_{1,0},\ r_{1,0}$ ($2t_{i,1}=\frac{P'(x)}{P(x)}r_{i,1}(x)$) نتیجه می‌شود. بنابراین $F_{1,1}(x)=\frac{P'(x)}{P(x)}$. برای اثبات گام استقرایی، فرض کنید حکم برای مقادیر طبیعی $j<j_0$ صادق باشد. از رابطه بازگشتی $t_{i,j}$ داریم: $t_{i+1,j_0-1}(x)=Dt_{i,j_0-1}(x)-2j_0t_{i,j_0}(x)+\frac{P'(x)}{P(x)}r_{i,j_0}(x)$. معادلاً:

$$2^{j_0-1}(j_0-1)!t_{i+1,j_0-1}(x)=2^{j_0-1}(j_0-1)!Dt_{i,j_0-1}(x)-2^{j_0}j_0!t_{i,j_0}(x)+2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,j_0}(x)$$

$$\iff 2^{j_0}j_0!t_{i,\,j_0}(x) = 2^{j_0-1}(j_0-1)!Dt_{i,\,j_0-1}(x) - 2^{j_0-1}(j_0-1)!t_{i+1,\,j_0-1}(x) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,\,j_0}(x)$$

اما با استفاده از فرض استقرا داریم:

$$2^{j_0}j_0!t_{i,\,j_0}(x) = D(2^{j_0-1}(j_0-1)!t_{i,\,j_0-1}(x)) - 2^{j_0-1}(j_0-1)!t_{i+1,\,j_0-1}(x) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,\,j_0}(x)$$

$$= D\left(\sum_{k=1}^{j_0-1} F_{j_0-1,\,k}(x)r_{i,\,k}(x)\right) - \sum_{k=1}^{j_0-1} F_{j_0-1,\,k}(x)r_{i+1,\,k}(x) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,\,j_0}(x)$$

$$= \sum_{k=1}^{j_0-1} DF_{j_0-1,\,k}(x)r_{i,\,k}(x) + \sum_{k=1}^{j_0-1} F_{j_0-1,\,k}(x)Dr_{i,\,k}(x) - \sum_{k=1}^{j_0-1} F_{j_0-1,\,k}(x)r_{i+1,\,k}(x) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,\,j_0}(x)$$

$$= \sum_{k=1}^{j_0-1} DF_{j_0-1,\,k}(x)r_{i,\,k}(x) + \sum_{k=1}^{j_0-1} F_{j_0-1,\,k}(x)\left(Dr_{i,\,k}(x) - r_{i+1,\,k}(x)\right) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,\,j_0}(x)$$

از روابط به دست آمده در طی محاسبات گام 2 داریم: $r_{i+1,\,k}(x) = Dr_{i,\,k}(x) - 2kr_{i,\,k+1}(x) - \frac{P'(x)}{P(x)}r_{i,\,k}(x),\ \forall 1 \le k < m$ **و معادلاً** $Dr_{i,\,k}(x) - r_{i+1,\,k}(x) = 2kr_{i,\,k+1}(x) + \frac{P'(x)}{P(x)}r_{i,\,k}(x),\ \forall 1 \le k \le m$**. با جاگذاری این تساوی داریم:**

$$= \sum_{k=1}^{j_0-1} DF_{j_0-1,\,k}(x)r_{i,\,k}(x) + \sum_{k=1}^{j_0-1} F_{j_0-1,\,k}(x)\left(2kr_{i,\,k+1}(x) + \frac{P'(x)}{P(x)}r_{i,\,k}(x)\right) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}r_{i,\,j_0}(x)$$

$$= \sum_{k=1}^{j_0-1}\left(DF_{j_0-1,\,k}(x) + 2(k-1)F_{j_0-1,\,k-1}(x) + \frac{P'(x)}{P(x)}F_{j_0-1,\,k}(x)\right)r_{i,\,k}(x)$$
$$+ \left(2(j_0-1)F_{j_0-1,\,j_0-1}(x) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}\right)r_{i,\,j_0}(x)$$

در نتیجه مقادیر $F_{j_0,\,k}(x),\ \forall j_0 < m,\ 1 \le k \le j_0$ **مطابق زیر داده می‌شوند:**

$$F_{j_0,\,k}(x) = DF_{j_0-1,\,k}(x) + 2(k-1)F_{j_0-1,\,k-1}(x) + \frac{P'(x)}{P(x)}F_{j_0-1,\,k}(x),\ \forall 1 \le k < j_0$$

$$F_{j_0,\,j_0}(x) = 2(j_0-1)F_{j_0-1,\,j_0-1}(x) + 2^{j_0-1}(j_0-1)!\frac{P'(x)}{P(x)}$$

دقت کنید این روابط بازگشتی مستقل از i هستند و در نتیجه اثبات در حالت $j < m$ کامل خواهد بود. □

تمرین ۱. **به استقرای ریاضی اثبات کنید** $F_{i,\,i}(x) = 2^{i-1}i!F_{1,\,1}(x) = 2^{i-1}i!\frac{P'(x)}{P(x)},\ \forall 1 \le i \le m$.

تمرین ۲. **حکم را در حالت $j = m$ اثبات کنید.**

گام ۳. **در حالت $j = m$، گزاره زیر لم 1 به صورت** $2^m m!t_{i,\,m}(x) = F_{m,\,1}(x)r_{i,\,1}(x) + \cdots + F_{m,\,m}(x)r_{i,\,m}(x)$ **نوشته می‌شود. اما از روابط گام 2 می‌دانیم:** $t_{i,\,m}(x) = Dt_{i-1,\,m}(x),\ \forall 0 < i < 2m$**. در نتیجه خواهیم داشت:**

$$\sum_{k=1}^{m} F_{m,\,k}(x)r_{i,\,k}(x) = 2^m m!t_{i,\,m}(x) = 2^m m!Dt_{i-1,\,m}(x) = D(2^m m!t_{i-1,\,m}(x)) = D\left(\sum_{k=1}^{m} F_{m,\,k}(x)r_{i-1,\,k}(x)\right)$$

$$\Longrightarrow \sum_{k=1}^{m-1} F_{m,\,k}(x)\left(Dr_{i-1,\,k}(x) - 2kr_{i-1,\,k+1}(x) - \frac{P'(x)}{P(x)}r_{i-1,\,k}(x)\right) + F_{m,\,m}(x)\left(Dr_{i-1,\,m}(x) - \frac{P'(x)}{P(x)}r_{i-1,\,m}(x)\right)$$

$$= \sum_{k=1}^{m} DF_{m,\,k}(x)r_{i-1,\,k}(x) + \sum_{k=1}^{m} F_{m,\,k}(x)Dr_{i-1,\,k}(x)$$

$$\Longrightarrow -\sum_{k=1}^{m-1} F_{m,\,k}(x)\left(2kr_{i-1,\,k+1}(x) + \frac{P'(x)}{P(x)}r_{i-1,\,k}(x)\right) - F_{m,\,m}(x)\frac{P'(x)}{P(x)}r_{i-1,\,m}(x) = \sum_{k=1}^{m} DF_{m,\,k}(x)r_{i-1,\,k}(x)$$

$$\Longrightarrow \sum_{k=1}^{m} r_{i-1,\,k}(x)\left(DF_{m,\,k}(x) + 2(k-1)F_{m,\,k-1}(x) + \frac{P'(x)}{P(x)}F_{m,\,k}(x)\right) = 0$$

با توجه به شباهت عبارت فوق به رابطه بازگشتی مربوط به $F_{j,\,k}(x),\ \forall j < m,\ 1 \le k \le j$، تعریف می‌کنیم:

$$F_{m+1,\,k}(x) := DF_{m,\,k} + 2(k-1)F_{m,\,k-1}(x) + \frac{P'(x)}{P(x)}F_{m,\,k}(x),\ \forall 1 \le k \le m \implies \sum_{k=1}^{m} F_{m+1,\,k}(x)r_{i-1,\,k}(x) = 0$$

تمرین ۳. ثابت کنید $\sum_{k=1}^{m} F_{m+i+1,\,k}(x)r_{0,\,k}(x) = 0$ که در آن:

$$F_{m+i+1,\,k}(x) := DF_{m+i,\,k} + 2(k-1)F_{m+i,\,k-1}(x) + \frac{P'(x)}{P(x)}F_{m+i,\,k}(x),\ \forall 0 \le i < m-1,\ 1 \le k \le m$$

نکته ۲. طبق محاسبات اخیر، واضح است وجود مجموعه چندجمله‌ای‌های $\{r_{i,\,j}\},\ \{t_{i,\,j}\}$ به طوری که روابط $t_{i,\,1}(x) = \frac{P'(x)}{P(x)}r_{i,\,1}(x),\ \forall 1 \le i < 2m$ برقرار باشند، وجود $\{r_{i,\,j}\},\ \{F_{k,\,l}\}$ که در روابط تمرین 3 و زیر لم 1 صدق کنند را نتیجه می‌دهد. ثابت کنید عکس این گزاره نیز صحیح است و کافیست به اثبات وجود چندجمله‌ای‌های $\{r_{i,\,j}\},\ \{F_{k,\,l}\}$ بپردازیم.

برای سادگی نوشتار روابط $\sum_{k=1}^{m} F_{m+i+1,\,k}(x)r_{i-1,\,k}(x) = 0,\ \forall 0 \le i < m-1$ از معادله ماتریسی زیر استفاده می‌کنیم:

$$\begin{bmatrix} F_{m+1,\,1}(x) & F_{m+1,\,2}(x) & \dots & F_{m+1,\,m}(x) \\ F_{m+2,\,1}(x) & F_{m+2,\,2}(x) & \dots & F_{m+2,\,m}(x) \\ \vdots & \vdots & \ddots & \vdots \\ F_{2m-1,\,1}(x) & F_{2m-1,\,2}(x) & \dots & F_{2m-1,\,m}(x) \end{bmatrix} \begin{bmatrix} r_{0,\,1}(x) \\ r_{0,\,2}(x) \\ \vdots \\ r_{0,\,m}(x) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

تمرین ۴. به استقرا ثابت کنید برای هر $1 \le i < 2m,\ 1 \le j \le m,\ j \le i$، تابع گویای $F_{i,\,j}(x)$ به صورت $\frac{Q_{i,\,j}(x)}{P(x)^{i-j+1}}$ قابل نمایش است که در آن $Q(x) \in \mathbb{Z}[X]$ یک چندجمله‌ای از درجه حداکثر $(i-j+1)(n-1)$ می‌باشد.

بنابراین سیستم معادلات اخیر به شکل زیر قابل بازنویسی‌ست:

$$\begin{bmatrix} \frac{Q_{m+1,\,1}(x)}{P(x)^{m+1}} & \frac{Q_{m+1,\,2}(x)}{P(x)^{m}} & \dots & \frac{Q_{m+1,\,m}(x)}{P(x)^{2}} \\ \frac{Q_{m+2,\,1}(x)}{P(x)^{m+2}} & \frac{Q_{m+2,\,2}(x)}{P(x)^{m+1}} & \dots & \frac{Q_{m+2,\,m}(x)}{P(x)^{3}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{Q_{2m-1,\,1}(x)}{P(x)^{2m-1}} & \frac{Q_{2m-1,\,2}(x)}{P(x)^{2m-2}} & \dots & \frac{Q_{2m-1,\,m}(x)}{P(x)^{m}} \end{bmatrix} \begin{bmatrix} r_{0,\,1}(x) \\ r_{0,\,2}(x) \\ \vdots \\ r_{0,\,m}(x) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \iff \begin{bmatrix} Q_{m+1,\,1}(x) & Q_{m+1,\,2}(x) & \dots & Q_{m+1,\,m}(x) \\ Q_{m+2,\,1}(x) & Q_{m+2,\,2}(x) & \dots & Q_{m+2,\,m}(x) \\ \vdots & \vdots & \ddots & \vdots \\ Q_{2m-1,\,1}(x) & Q_{2m-1,\,2}(x) & \dots & Q_{2m-1,\,m}(x) \end{bmatrix} \begin{bmatrix} \frac{r_{0,\,1}(x)}{P(x)^{m}} \\ \frac{r_{0,\,2}(x)}{P(x)^{m-1}} \\ \vdots \\ \frac{r_{0,\,m}(x)}{P(x)^{1}} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

نکته ۳. واضح است که وجود $r_{i,\,j},\ F_{i,\,j}$ های وجود چندجمله‌ای‌های (صادق در روابط تمرین 3 و زیر لم 1) دقیقاً معادل وجود چندجمله‌ای‌های $Q_{i,\,j}(x)$ و توابع گویای $\frac{r_{0,\,i}(x)}{P(x)^{m-i+1}}$ است که در دستگاه معادلات فوق صادق باشند.

فرض کنید چندجمله‌ای $Q_{i,\,j}(x)$ به صورت $\sum_{k=1}^{(i-j+1)(n-1)} a_{i,\,j;k}x^k$ داده شده باشد. ثابت می‌کنیم می‌توان توابع گویای $\frac{r_{0,\,i}(x)}{P(x)^{m-i+1}}$ را به صورت چندجمله‌ای‌هایی به فرم $\sum_{k=1}^{(m^2-m+i)(n-1)} b_{0,\,i;k}x^k$ از درجه حداکثر $(m^2-m+i)(n-1)$ اتخاذ کرد به نحوی که در دستگاه معادلات فوق صادق باشند. مطابق نکته 2 و نکته 3، این گزاره اثبات وجود چندجمله‌ای R را تکمیل خواهد کرد.

با بسط‌های ارائه شده، دستگاه معادلات اخیر به صورت زیر قابل بازنویسی‌ست:

$$\sum_{l=0}^{(i-j+1)(n-1)+(m^2-m+j)(n-1)} \left(\sum_{j=1}^{m}\sum_{u+v=l} a_{i,\,j;u}b_{0,\,j;v}\right)x^l = 0$$

$$\implies \sum_{j=1}^{m}\sum_{u+v=l} a_{i,\,j;u}b_{0,\,j;v} = 0,\ \forall 0 \le l \le (i-j+1)(n-1)+(m^2-m+j)(n-1),\ m < i \le 2m$$

تمرین ۵. (نیازمند دانش مقدماتی جبرخطی) ثابت کنید دستگاه معادلات فوق در میدان $\mathbb{Z}/p\mathbb{Z}$ دارای جواب نابدیهی‌ست.

تمرین ۶. اثبات کنید درجه چندجمله‌ای R حاصل از جواب فوق، از $\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n$ تجاوز نمی‌کند.

گام ۴. در آخر تنها کافی‌ست ثابت کنیم تمام ضرایب چندجمله‌ای حاصل شده $R(x)$ بر p بخش‌پذیر نیستند. دقت کنید از طریق نتیجه تمرین 5 می‌دانیم حداقل یکی از $r_{i,\,j},\, t_{i,\,j}$ ها به پیمانه p هم‌نهشت با چندجمله‌ای متحد صفر نیستند. با استفاده از مفروضات اولیه قضیه 1 $(9n^2 < p,\ m \le \sqrt{\frac{p}{3n}})$ ثابت کنید این برای تکمیل اثبات ناصفر بودن R به پیمانه p کافی‌ست.

در نتیجه اثبات لم 1 به پایان می‌رسد. به طریق کاملاً مشابه می‌توان قضیه مشابه زیر را اثبات کرد. (اثبات به خواننده واگذار می‌شود)

لم ۲. برای هر مقدار طبیعی $m \le \sqrt{\frac{p}{3n}}$، چندجمله‌ای $S \in \mathbb{Z}[X]$ موجود است به طوری که تمام ضرایب آن بر p بخش‌پذیر نباشند، تمام اعضای N_1 را به عنوان ریشه‌هایی (به پیمانه p) با تکرر حداقل $2m$ دارا باشد و همچنین $\deg(R) \le \frac{p-1}{2}n+(m-1)p+(n-1)m^2+n$.

راهنمایی ۱. روند اثبات لم 2 را به طور کاملاً مشابه طی کنید و تلاش کنید چندجمله‌ای S را از فرم زیر بیابید:

$$S(x) = \left(1-P(x)^{\frac{p-1}{2}}\right)\sum_{i=1}^{m} r_i(x)(x^p-x)^{i-1} + \sum_{i=1}^{m} t_i(x)(x^p-x)^i$$

در نهایت به اثبات قضیه 1 نائل می‌آییم. از لم 1 می‌دانیم:

$$2m(p-\frac{N+|N_0|}{2}) = 2m(p-|N_1|-|N_0|) = 2m|N_{-1}| \le \frac{p-1}{2}n+(m-1)p+(n-1)m^2+n, \quad |N_0| \le n$$

$$\implies 2m(p-\frac{N+n}{2}) \le 2m(p-\frac{N+|N_0|}{2}) \le \frac{p-1}{2}n+(m-1)p+(n-1)m^2+n$$

$$\implies 2mp-mN-mn \le \frac{p-1}{2}n+(m-1)p+(n-1)m^2+n \implies p-n-\frac{(p+1)n}{2m}+\frac{p}{m}-(n-1)m \le N$$

به طور مشابه، از لم 2 می‌توان نتیجه گرفت: $N \le p+n+\frac{(p+1)n}{2m}-\frac{p}{m}+(n-1)m$. در نتیجه:

$$p-n-\frac{(p+1)n}{2m}+\frac{p}{m}-(n-1)m \le N \le p+n+\frac{(p+1)n}{2m}-\frac{p}{m}+(n-1)m \xrightarrow{\lfloor\sqrt{\frac{p}{3n}}\rfloor \mapsto m} p-n\sqrt{3np} \le N \le p+n\sqrt{3np}$$

که اثبات را به پایان می‌رساند. $\square$

پروژه با جایزه فوق‌نفیس ۱. حکم قضیه 1 را در حالتی که ضریب پیشرو P برابر با -1 باشد اثبات کنید. آیا همواره در حالتی که چندجمله‌ای P تکین نباشد، می‌توان نتیجه‌ای مشابه با قضیه 1 به دست آورد؟

پروژه با جایزه فوق‌نفیس ۲. (نیازمند دانش نظریه گالوا) مشابه قضیه 1، فرض کنید $n \leq 3$ عددی فرد باشد و $P \in \mathbb{Z}[X]$ چندجمله‌ای تکینی از درجه n باشد. عدد اول $p > 9n^2$ داده شده است. فرض کنید k_{p^r} میدان گالوا با p^r عضو باشد. معادله $y^2 = P(x)$ را در میدان k_{p^r} در نظر گرفته و تعداد جواب‌های آن را N بنامید. ثابت کنید:

$$|N - p^r| \leq n\sqrt{3np^r}$$

برای تمرین و دیدن کاربردهایی از این حالت ضعیف از کران Hasse-Weil، خوب است روی مسائل زیر فکر کنید. همچنین تمرین بسیار خوبی‌ست که پیش از آن، سعی کنید بدون استفاده از این قضیه این مسائل را حل کنید!

مسئله ۱. ثابت کنید برای هر عدد اول p، مجموعه $\{x^2 - y^3 \mid x, y \in \mathbb{Z}\}$ تمام دستگاه کامل مانده‌ها به پیمانه p را تولید می‌کند. سپس ثابت کنید برای هر عدد اول p، مجموعه $\{x^2 + y^3 \mid x, y \in \mathbb{Z}\}$ نیز تمام دستگاه کامل مانده‌ها به پیمانه p را تولید می‌کند.

مسئله ۲. (IMO SL 2012 N8) برای هر $p > 100$ و هر مقدار صحیح r، ثابت کنید اعداد صحیح a, b موجودند به نحوی که $p \mid a^2 + b^5 - r$.

مسئله ۳. آیا مقدار $k \in \mathbb{N}$ وجود دارد به نحوی که $p = 6k + 1$ عددی اول باشد و همچنین $\binom{3k}{k} \overset{p}{\equiv} 1$؟

مسئله ۴. فرض کنید p عددی اول و $\mathbb{F}_p$ دستگاه کامل مانده‌ها به پیمانه p باشد. همچنین فرض کنید $\mathbb{F}_p[X]$ مجموعه تمام چندجمله‌ای‌های با ضرایب در $\mathbb{F}_p$ باشد. تمام مقادیر ممکن p را بیابید به نحوی که چندجمله‌ای $P \in \mathbb{F}_p[X]$ از درجه چهار وجود داشته باشد و برای هر عدد صحیح $k \in \mathbb{Z}$، مقدار صحیح $l \in \mathbb{Z}$ موجود باشد به طوری که $P(l) \overset{p}{\equiv} k$.

مراجع

[1] E. Artin, “Quadratische körper im gebiete der höheren kongruenzen. ii,” *Mathematische Zeitschrift*, vol. 19, 1924.

[2] H. Hasse, “Zur theorie der abstrakten elliptischen funktionenkörper iii,” *Journal für die reine und angewandte Mathematik*, 1936.

[3] A. Weil, “Numbers of solutions of equations in finite fields,” *Bulletin of the American Mathematical Society*, vol. 55, no. 5, pp. 497–508, 1949.

[4] S. Lang and A. Weil, “Number of points of varieties in finite fields,” *American Journal of Mathematics*, vol. 76, no. 4, pp. 819–827, 1954.

[5] Y. I. Manin, “On cubic congruences to a prime modulus,” *Izv. Math.*, 1956.

[6] A. Weil, *Sur les courbes algébriques et les variétés qui s’en déduisent.* Actualités Scientifiques et Industrielles, Hermann, 1948.