از تابع زتای اویلر تا Lـ توابع آرتین

علی چراغی

۱ مقدمه

یکی از مسائل بسیار قدیمی در ریاضیات، مطالعه ی اعداد اول و بررسی توزیع آن ها در اعداد طبیعی است. اقلیدس[۱] اولین کسی بود که اثبات کرد بی نهایت عدد اول وجود دارد. بعد از او اویلر[۲] در کتاب مقدمه ای بر آنالیز بی نهایت، [۱]، برای اولین بار با استفاده از آنالیز، بی نهایت بودن تعداد اعداد اول را ثابت می کند. در واقع او سری $\sum_{p \text{ اول}} \frac{۱}{p}$ را بررسی کرده و اثبات می کند که این سری به بی نهایت واگراست و گامی در جهت شناخت بیشتر اعداد اول برداشت. همچنین این اثبات او شروعی برای نظریه تحلیلی اعداد به حساب می آید. سپس او تابع زتا را تعریف می کند و بعضی از مقادیر آن را بدست می آورد. پس از اویلر، دیریکله[۳] در سال ۱۸۴۰، با استفاده از مشخصه های اعداد صحیح پیمانه ای، تابع زتای اویلر را گسترش می دهد و با استفاده از آن قضیه معروف خود را ثابت می کند: "در هر تصاعد حسابی اولیه، بی نهایت عدد اول وجود دارد." او این توابع گسترش یافته را با نماد L نمایش می دهد و به همین دلیل این نوع توابع به Lـ توابع[۴] معروف می شوند. ریمان[۵] در مقاله ی [۲]، که تنها مقاله ی او در نظریه اعداد محسوب می شود، تابع زتای اویلر را به اعداد مختلط گسترش می دهد و ادعا می کند اگر صفرهای تابع زتا در محدوده های خاصی نباشند، آنگاه قضیه اعداد اول (و حتی بهتر از آن) بدست می آید. همچنین او در این مقاله مهمترین حدس ریاضیات به نام فرض ریمان را مطرح می کند. این حدس در مورد صفرهای تابع زتا در ناحیه ی خاصی صحبت می کند که در صورت درست بودن، درک بیشتری از توزیع اعداد اول و تعداد بسیاری از مسائل دیگر می شود. بعد از او ددکیند[۶] تابع زتا را به میدان های عددی گسترش می دهد و نشان می دهد اطلاعات مهمی از میدان های عددی در آن توابع کدگذاری شده اند. آرتین[۷] در سال ۱۹۲۳ و در دومین مقاله ی منتشر شده از او، [۳]، Lـ توابع جدیدی را تعریف می کند که گسترش Lـ توابع دیریکله محسوب می شوند و مانند توابع زتا و Lـ توابع درک بالاتری از میدان های عددی به ما می دهند.

در مقاله پیش رو، روندی تاریخی برای معرفی Lـ توابع آرتین به کار گرفته شده است. همچنین در بیشتر اثبات ها، طرح اثبات داده شده یا خواننده ارجاع داده شده است. همچنین برای سادگی فقط توسیع های میدان اعداد گویا در نظر گرفته شده است.

[۱] Euclid
[۲] Euler
[۳] Dirichlet
[۴] L-functions
[۵] Riemann
[۶] Dedekind
[۷] Artin

۲ نامتناهی بودن تعداد اعداد اول

اقلیدس در ۳۰۰ سال قبل از میلاد، اثبات خود را از بی نهایت بودن اعداد اول ارائه می دهد. البته در اثبات خود اقلیدس، از آنجایی که نمادگذاری برای اعداد مرسوم نبوده، او فقط برای مثال هایی این روش را توضیح می دهد ولی مشخص است منظور او برای حالت کلی بوده است.

قضیه. (اقلیدس) بی نهایت عدد اول وجود دارد.

برهان. فرض کنید این طور نباشد و $p_1, p_2, \dots, p_n$ تنها اعداد اول باشند. در این صورت از آنجایی که هر عدد به اعداد اول تجزیه می شود، عدد$1+N = p_1p_2\cdots p_n$ نیز باید حداقل یکی از این اعداد اول مثل p_i را داشته باشد. در حالی که بوضوح $p_i|p_1p_2\cdots p_n$، پس

$$p_i|N - p_1p_2\cdots p_n = 1$$

که تناقض است. □

اویلر در [۱]، ایده ی جدیدی برای اثبات نامتناهی بودن تعداد اعداد اول عرضه می کند که دیدگاهی آنالیزی برای حل مسائل "گسسته" نظریه اعداد می دهد.

قضیه. (اویلر) بی نهایت عدد اول وجود دارند.

تبصره. این اثبات، اثبات خود اویلر است و دقت کافی را ندارد، ولی می توان آنرا دقیق کرد.

برهان. عدد زیر را در نظر بگیرید:

$$P_n = (\frac{1}{1-\frac{1}{2^n}})(\frac{1}{1-\frac{1}{3^n}})(\frac{1}{1-\frac{1}{5^n}})\cdots$$

که اعداد ۲، ۳، ۵، ... روی اعداد اول تغییر می کنند. در این صورت از بسط $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ داریم:

$$P_n = (1+\frac{1}{2^n}+\frac{1}{2^{2n}}+\cdots)(1+\frac{1}{3^n}+\frac{1}{3^{2n}}+\cdots)\cdots$$

و با ضرب این جملات در هم و استفاده از این که تجزیه یکتا به اعداد اول وجود دارد، داریم:

$$P_n = 1+\frac{1}{2^n}+\frac{1}{3^n}+\frac{1}{4^n}+\cdots \qquad (1)$$

حال از فرم ضربی P_n لگاریتم می گیریم:

$$\log P_n = \log(\frac{1}{1-\frac{1}{2^n}}) + \log(\frac{1}{1-\frac{1}{3^n}}) + \log(\frac{1}{1-\frac{1}{5^n}}) + \cdots$$

و از بسط $\log(\frac{1}{1-x}) = \sum_{m=1}^{\infty} \frac{x^m}{m}$ استفاده می کنیم:

$$\begin{aligned}\log P_n = &(\frac{1}{2^n} + \frac{1}{2}(\frac{1}{2^{2n}}) + \frac{1}{3}(\frac{1}{2^{3n}}) + \cdots) + \\ &(\frac{1}{3^n} + \frac{1}{2}(\frac{1}{3^{2n}}) + \frac{1}{3}(\frac{1}{3^{3n}}) + \cdots) + \\ &\cdots\end{aligned}$$

حال با تغییر دادن آرایش آن داریم:

$$\begin{aligned}\log P_n = &(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \cdots) + \\ &\frac{1}{2}(\frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \cdots) + \\ &\frac{1}{3}(\frac{1}{2^{3n}} + \frac{1}{3^{3n}} + \frac{1}{5^{3n}} + \cdots) + \\ &\cdots\end{aligned} \qquad (2)$$

حال n را برابر ۱ قرار می دهیم و داریم از (۱):

$$P_1 = 1+\frac{1}{2}+\frac{1}{3}+\cdots = \log(\frac{1}{1-1}) = \log\infty$$

و از (۲) :

$$\begin{aligned}\log P_1 = &(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots) + \\ &\frac{1}{2}(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \cdots) + \\ &\frac{1}{3}(\frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{5^3} + \cdots) + \\ &\cdots\end{aligned}$$

حال مجموع جملات دوم به بعد سری بالا، مثلا طبق آزمون انتگرال، مقداری متناهی خواهد بود و داریم:

$$\log P_۱ = \log\log\infty \approx \frac{۱}{۲} + \frac{۱}{۳} + \frac{۱}{۵} + \cdots$$

و کار تمام است. □

واضح است که اثبات بالا دقت کافی را ندارد ولی هر گام آن را می توان با همین روند دقیق کرد و پس از دقیق کردن متوجه می شویم که:

$$\sum_{p\le x}\frac{۱}{p} \sim \log\log x$$

۳ تابع زتای اویلر

اویلر در اثبات قضیه قبل از موجودی به نام P_n استفاده می کند که

$$P_n = \frac{۱}{۱^n} + \frac{۱}{۲^n} + \frac{۱}{۳^n} + \cdots$$

پس اویلر تعریف زیر را برای تابع زتای خود ارائه می دهد:

تعریف. تابع زتای اویلر برای اعداد حقیقی $s > ۱$ به شکل زیر تعریف می شود:

$$\zeta(s) = \sum_{n=۱}^{\infty}\frac{۱}{n^s}$$

پس در واقع، در اثبات قضیه قبل داشتیم $P_n = \zeta(n)$ و همچنین برای P_n یک فرم ضربی داشتیم که اویلر برای حالت کلی تری این فرم ضربی را ارائه میدهد:

قضیه. (اویلر) برای $s > ۱$ داریم:

$$\zeta(s) = \prod_{p\ \text{اول}}\left(\frac{۱}{۱ - \frac{۱}{p^s}}\right)$$

برهان. مانند قبل، به دلیل تجزیه یکتای اعداد طبیعی بزرگتر از ۱ به اعداد اول. □

به این فرم ضربی، تجزیه اویلری [۸] تابع زتا می گویند.

اویلر چند مقدار این تابع را بدست آورد:

قضیه. (اویلر) برای $n \in \mathbb{N}$ داریم:

$$\zeta(۲n) = \frac{۲^{۲n-۱}\pi^{۲n}}{(۲n)!}|B_{۲n}|$$

که B_nها اعداد برنولی هستند.

همچنین اویلر با بررسی سری $\sum_{n=۱}^{\infty} n^k x^n$، سعی کرد مقادیر تابع ζ را برای اعداد منفی پیدا کند. اگرچه او تعریف دقیقی برای تابع زتا در اعداد منفی نداشت(!) ولی احتمالا می دانست که آنرا مانند تابع فاکتوریل می توان به کل اعداد حقیقی گسترش داد.

قضیه. (اویلر)

$$\frac{\zeta(۱-n)}{\zeta(n)} = \frac{۲^{۱-n}cos(\frac{n\pi}{۲})n!}{\pi^n}$$

همچنین اویلر حدس زیر را مطرح می کند که به دو طریق در مقاله ریمان اثبات می شود.

حدس. (اویلر) برای هر عدد حقیقی مثبت s،

$$\frac{\zeta(۱-s)}{\zeta(s)} = \frac{۲^{۱-s}\cos\left(\frac{s\pi}{۲}\right)\Gamma(s+۱)}{\pi^s}$$

که تابع $\Gamma(s)$ توسیع فاکتوریل به کل اعداد حقیقی است و با رابطه زیر تعریف می شود:

$$\Gamma(s) = \int_{۰}^{\infty} e^{-x}x^s\frac{dx}{x}$$

۴ Lـ توابع دیریکله

دیریکله در سال ۱۸۴۰، قضیه ی معروف خود را ثابت می کند:

[۸] Euler factorization

قضیه. (دیریکله) اگر r و m دو عدد طبیعی نسبت به هم اول باشند، آنگاه در تصاعد حسابی $\{mk+r|k\in\mathbb{N}\}$ بی نهایت عدد اول وجود دارد.

برای اثبات این قضیه، دیریکله مجبور به تعمیم دادن تابع زتا شد. در واقع ایده ی او این بود که اثبات کند $\sum_{p\overset{m}{\equiv}r}\frac{1}{p}$ واگرا به بی نهایت است و با استفاده از آن قضیه اش را نتیجه بگیرد. برای تعریف Lـ توابع دیریکله باید ابتدا مشخصه های دیریکله را تعریف کنیم:

تعریف. تابع $\chi:\mathbb{Z}\to\mathbb{C}$ را یک مشخصه دیریکله به پیمانه m می نامیم هرگاه خواص زیر را داشته باشد:

- اگر a نسبت به m اول نباشد: $\chi(a)=0$
- اگر a نسبت به m اول باشد: $|\chi(a)|=1$
- اگر $a,b\in\mathbb{Z}$ آنگاه $\chi(a)\chi(b)=\chi(ab)$ (کاملا ضربی بودن)
- برای همه $k\in\mathbb{Z}$ داریم: $\chi(k+m)=\chi(k)$

پس مشخصه ی دیریکله در واقع یک هومومورفیسم از $(\mathbb{Z}/m\mathbb{Z})^*$ به $\mathbb{C}^*$ است. همچنین تابع $\chi_0\equiv 1$ را مشخصه بدیهی می نامیم.

تعریف. فرض کنید χ یک مشخصه ی دیریکله باشد. Lـ تابع دیریکله ی وابسته به آن را به شکل زیر تعریف می کنیم:

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

اگر χ مشخصه بدیهی باشد، سری بالا برای $s>1$ همگراست و برابر با تابع زتای اویلر است.

اگر χ مشخصه بدیهی نباشد، سری بالا برای $s>0$ همگراست.

این تابع این خاصیت را دارد که اعداد متفاوت به پیمانه m را از هم "جدا" می کند. مثلا اگر χ_1 مشخصه ی دیریکله به پیمانه ۴ باشد که با $\chi_1(1)=1$ و $\chi_1(3)=-1$ شناسایی می شود، آنگاه Lـ تابع وابسته به آن برابر است با:

$$L(s,\chi_1)=\sum_{n=1}^{\infty}\frac{\chi_1(n)}{n^s}=\sum_{n\overset{4}{\equiv}1}\frac{1}{n^s}-\sum_{n\overset{4}{\equiv}3}\frac{1}{n^s}$$

همچنین Lـ توابع به دلیل کاملا ضربی بودن χ، تجزیه اویلری دارند:

قضیه. اگر $L(s,\chi)$ یک Lـ تابع دیریکله باشد. در این صورت برای s هایی که Lـ تابع تعریف می شود داریم:

$$L(s,\chi)=\prod_{p\text{ اول}}\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right)$$

برهان. با استفاده از کاملا ضربی بودن χ و بسط تیلور $\frac{1}{1-x}$، داریم:

$$\begin{aligned}L(s,\chi)&=\prod_{p\text{ اول}}\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right)\\&=\prod_{p\text{ اول}}\left(1+\frac{\chi(p)}{p^s}+\frac{\chi(p^2)}{p^{2s}}+\cdots\right)\\&=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\end{aligned}$$

معمولا مقدار Lـ توابع در نقطه $s=1$ اهمیت زیادی دارد. مثلا مهم ترین حکمی که دیریکله برای اثبات قضیه خود به آن احتیاج داشت قضیه زیر بود:

قضیه. (دیریکله) اگر χ یک مشخصه دیریکله نابدیهی باشد آنگاه $L(1,\chi)\neq 0$.

سپس دیریکله با استفاده از Lـ توابع، اعداد اول به پیمانه m جدا می کند و برای هر کدام از آن دسته ها از اعداد اول، ثابت می کند:

قضیه. (دیریکله) اگر m و r دو عدد طبیعی نسبت به هم اول باشند، آن گاه ثابت A (وابسته به r و m) وجود دارد که:

$$\sum_{p\overset{m}{\equiv}r,p\leq x}\frac{1}{p}=\frac{1}{\phi(m)}\log\log x+A+O\left(\frac{1}{\log x}\right)$$

برهان. رجوع شود به فصل ۷ از [۴] .

این قضیه، قضیه دیریکله را نتیجه می دهد و در واقع اثبات می کند "چگالی" اعداد اول برای r های نسبت به m اول متفاوت نیز یکسان است.

۵ تابع زتای ریمان

ریمان در مقاله معروف خود، [۲]، تابع زتای اویلر را به تمام اعداد مختلط گسترش می دهد و با استفاده از آن تلاشی برای اثبات "قضیه اعداد اول" می کند:

قضیه. (قضیه اعداد اول) فرض کنید x یک عدد حقیقی مثبت باشد و تابع $\pi(x)$ را برابر با تعداد اعداد اول از ۱ تا x تعریف کنید. در این صورت داریم:

$$\pi(x) \sim \frac{x}{\log x}$$

که این یعنی $\frac{\pi(x)}{x/\log x} \to ۱$ وقتی x به بی نهایت میل می کند.

ابتدا ریمان تابع ζ را به اعداد مختلط s با $Re\ s > ۱$ گسترش می دهد. در واقع سری $\sum \frac{۱}{n^s}$ برای محدوده ی $Re\ s > ۱$ به طور مطلق همگراست و تابع زتا را در این ناحیه می توان گسترش داد.

ریمان در آنالیز مختلط بسیار قوی بوده و توانست تابع زتا را به شکلی انتگرالی به کل صفحه ی مختلط گسترش دهد و حدس اویلر (که اکنون به معادله تابعی تابع زتا معروف است) را با دو روش اثبات کند.

قضیه. (ریمان) تابع زتای اویلر را می توان به صفحه مختلط گسترش داد بطوری که بجز یک قطب ساده با مانده ی ۱ در نقطه $s = ۱$، در بقیه نقاط تحلیلی باشد.

همچنین با قضیه نسبتا ساده ای در آنالیز مختلط می توان نتیجه گرفت که این گسترش یکتا نیز هست.

حال می توان قضیه اعداد اول را به کمک تابع زتای ریمان به شکل دیگری بیان کرد:

قضیه. قضیه اعداد اول معادل است با صفر نشدن تابع زتای ریمان روی خط $\{s \in \mathbb{C} | Re\ s = ۱\}$.

برهان. رجوع شود به فصل ۱۳ از [۴].

همچنین ریمان حدسی را در مقاله اش مطرح می کند و در مورد آن می نویسد:

"... ممکن است کسی به اثبات دقیقی از این موضوع علاقه داشته باشد، ولی من تلاش برای پیدا کردن اثبات آن را کنار گذاشته ام، زیرا این موضوع برای هدف تحقیق من نیاز نیست."

این حدس "فرض ریمان" نام گرفته و ادعا می کند:

حدس. (فرض ریمان[۹]) اگر صفری از تابع زتای ریمان روی نوار $\{s \in \mathbb{C} | ۰ < Re\ s < ۱\}$ قرار داشته باشد، آن گاه آن صفر روی خط بحرانی $\{\frac{۱}{۲} + it | t \in \mathbb{R}\}$ قرار دارد.

برای این حدس تاکنون تلاش های بسیاری شده است و معادل های بسیاری برای آن یافت شده است، ولی با این وجود تاکنون حل نشده است و جزء سخت ترین مسائل حل نشده ریاضیات به حساب می آید.

فرض ریمان نتایج بسیاری دارد که از جمله آن ها می توان به تقریب بهتری از $\pi(x)$ اشاره کرد:

نتیجه. اگر فرض ریمان درست باشد و اگر انتگرال لگاریتمی[۱۰] را برابر $Li(x) = \int_۲^x \frac{dt}{\log t}$ تعریف کنیم، آن گاه:

$$|\pi(x) - Li(x)| < \frac{۱}{۸\pi}\sqrt{x}\log x$$

.

برهان. رجوع شود به [۵] .

Lـتوابع دیریکله را نیز مانند تابع زتا، می توان به طور مرومورفیک [۱۱] به کل صفحه گسترش داد و حدسی مانند فرض ریمان برای آن ها فرمول بندی کرد:

[۹] Riemann Hypothesis (RH)

[۱۰] Logarithmic integral

[۱۱] Meromorphic

حدس. (فرض تعمیم یافته ریمان[۱۲]) اگر χ یک مشخصه دیریکله باشد و صفری از تابع $L(s,\chi)$ روی نوار بحرانی

$\{s \in \mathbb{C} | ۰ < Re\ s < ۱\}$ قرار داشته باشد، آن گاه آن صفر روی خط بحرانی $\{\frac{۱}{۲} + it | t \in \mathbb{R}\}$ قرار گرفته است.

۶ نظریه جبری اعداد

نظریه جبری اعداد قسمتی از نظریه اعداد است که با استفاده از تکنیک های جبر مجرد، به مطالعه ی اعداد صحیح، اعداد گویا و توسیع های آن ها می پردازد. سوالات نظریه اعداد را می توان با استفاده از نظریه جبری اعداد فرمول بندی جدیدی کرد و با استفاده از خواص جبری ساختارهای جبری متنوع به بررسی آن ها پرداخت. نظریه جبری اعداد مخصوصا در حل بسیاری از معادلات دیوفانتی[۱۳] کمک می کند.

در این‌جا فرض می کنیم خواننده با بعضی ایده ها و ساختارهای جبری معمولی مثل حلقه، ایدآل، میدان، توسیع میدان ها، نظریه گالوا[۱۴] آشنا است.

خواننده برای درک این مفاهیم می تواند به [۶] رجوع کند. برای سادگی ما فقط با توسیع های اعداد گویا کار می کنیم و تعریف می کنیم:

تعریف. منظور از یک میدان عددی جبری، توسیعی متناهی از میدان اعداد گویا است.

مثال هایی مهم از میدان های عددی، میدان های $\mathbb{Q}(\sqrt{d})$، $\mathbb{Q}(\zeta_n)$ هستند که d یک عدد صحیح و ζ_n یک ریشه ی nـام اولیه واحد است. این میدان ها در حل بسیاری از معادلات دیوفانتی مثل قضیه آخر فرما کمک می کنند.

تعریف. به $z \in \mathbb{C}$ یک عدد صحیح جبری می گوییم هرگاه در یک چندجمله ای به فرم زیر صدق کند:

$$p(x) = x^n + a_{n-۱}x^{n-۱} + \cdots + a_۰ \quad (a_i \in \mathbb{Z})$$

منظور از "حلقه اعداد صحیح یک میدان عددی"، مجموعه ی اعداد صحیح موجود در آن میدان است. می توانید بررسی کنید که حلقه اعداد صحیح در یک میدان عددی، با جمع و ضرب معمولی اعداد مختلط، ساختار یک حلقه را تشکیل می دهند. "حلقه اعداد صحیح میدان اعداد گویا" همان اعداد صحیح معمولی، $\mathbb{Z}$ هستند و در این حالت $\mathbb{Z}$ خواص بسیاری مانند تجزیه به اعداد اول و ... را دارد. ولی برخلاف این حالت خاص، اعداد صحیح در یک میدان عددی لزوما به اعداد اول موجود در آن حلقه تجزیه نمی شوند، بلکه تجزیه یکتا برای ایدآل های حلقه اعداد صحیح درست است:

قضیه. فرض کنید $\mathbb{Q} \subseteq K$ یک میدان عددی و R_K حلقه ی اعداد صحیح موجود در آن میدان باشد. در این صورت هر ایدآل ناصفر $I \subseteq R_K$ را می توان به شکل زیر نوشت.

$$I = \mathfrak{P}_۱^{\alpha_۱}\mathfrak{P}_۲^{\alpha_۲}\cdots\mathfrak{P}_n^{\alpha_n}$$

که $\mathfrak{P}_i$ ها ایدآل هایی اول از R_K و α_i ها اعداد صحیح مثبت هستند. این تجزیه در حد جایگشت یکتاست.

برهان. رجوع شود به [۷].

حال فرض کنید $\mathbb{Q} \subseteq K$ یک توسیع میدان عددی و R_K حلقه اعداد صحیح موجود در آن میدان باشد و $p \in \mathbb{Z}$ یک عدد اول گویا (منظور عدد اولی در $\mathbb{Z}$ است)، در این صورت pR_K یک ایدآل ناصفر در R_K تشکیل می دهد و ما علاقه مند به تجزیه این ایدآل به ایدآل های اول موجود در R_K هستیم. این ایدآل در R_K مثلا به شکل زیر تجزیه می شود:

$$pR_K = \mathfrak{P}_۱^{e_{\mathfrak{P}_۱/p}}\mathfrak{P}_۲^{e_{\mathfrak{P}_۲/p}}\cdots\mathfrak{P}_n^{e_{\mathfrak{P}_n/p}}$$

که $\mathfrak{P}_i$ها ایدآل های اول در R_K هستند و $e_{\mathfrak{P}_i/p}$ها اعداد صحیح مثبت. ایدآل های اول $\mathfrak{P}_i$، ایدآل های اول روی p نامیده می شوند. به عدد اول $p \in \mathbb{Z}$ ، شاخه ای گوییم اگر برای i ای، $e_{\mathfrak{P}_i/p} > ۱$ و

[۱۲] Generalized Riemann Hypothesis (GRH)

[۱۳] Diophantine equations

[۱۴] Galois

در غیر این صورت به آن عدد اول، غیر شاخه ای گوییم. همچنین به اعداد $e_{\mathfrak{P}_i/p}$ اندیس انشعاب $\mathfrak{P}_i$ روی p گفته می شود. می توان ثابت کرد که تعداد اعداد اول شاخه ای در یک توسیع متناهی، متناهی است. همچنین عدد مهم دیگری در نظریه انشعاب وجود دارد به نام درجه مانده ای $\mathfrak{P}_i$ روی p، که به این شکل تعریف می شود:

تعریف. اگر $\mathfrak{P}$ روی p باشد، آن گاه $\mathbb{Z}/p\mathbb{Z} \subseteq R_K/\mathfrak{P}$ میدان هایی متناهی خواهند بود و $[R_K/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]$ درجه مانده ای $\mathfrak{P}$ روی p گفته می شود و با $f_{\mathfrak{P}/p}$ نمایش داده می شود.

از این‌جا به بعد، فرض می کنیم $K/\mathbb{Q}$ توسیعی گالوا باشد. در این حالت می توان اثبات کرد که درجه مانده ای و اندیس انشعاب، برای همه ایدآل های اول روی p عددی ثابت است. به عبارت دیگر با نمادگذاری بالا:

$$e_{\mathfrak{P}_i/p} = e_{\mathfrak{P}_j/p}, \quad f_{\mathfrak{P}_i/p} = f_{\mathfrak{P}_j/p}$$

برای همه i, j ها.

حال گروه هایی را تعریف می کنیم که در نظریه انشعاب نقش مهمی را ایفا می کنند:

تعریف. فرض کنید $Gal(K/\mathbb{Q})$ گروه گالوای توسیع $K/\mathbb{Q}$ باشد و $pR_K = \mathfrak{P}_1^{e_{\mathfrak{P}_1/p}}\mathfrak{P}_2^{e_{\mathfrak{P}_2/p}}\cdots\mathfrak{P}_n^{e_{\mathfrak{P}_n/p}}$ تجزیه عدد اول p به ایدآل های اول R_K باشد. در این صورت برای هر $\mathfrak{P}_i$ گروهی به نام گروه تجزیه[15] به شکل زیر تعریف می شود:

$$D_{\mathfrak{P}_i} = \{\sigma \in Gal(K/\mathbb{Q}) | \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$$

حال می توان هomomورفیسم $f : D_{\mathfrak{P}_i} \to Gal(\frac{R}{\mathfrak{P}_i}/\frac{\mathbb{Z}}{p\mathbb{Z}})$ را در نظر گرفت که به شکل زیر تعریف می شود:

فرض کنید $\sigma \in D_{\mathfrak{P}_i}$ در این صورت σ، $\mathfrak{P}_i$ را ثابت نگه می دارد و پس اتومورفیسمی از $R/\mathfrak{P}_i$ می دهد بطوری که $\mathbb{Z}/p\mathbb{Z}$ را ثابت نگه می دارد. پس می توان عضو $f(\sigma)$ را برابر با این اتومورفیسم از $Gal(\frac{R}{\mathfrak{P}_i}/\frac{\mathbb{Z}}{p\mathbb{Z}})$ تعریف کرد. همچنین می توان ثابت کرد که f پوشاست.

حال گروه دیگری را با استفاده از این هomomورفیسم می توان تعریف کرد (این گروه در تعریف مولفه های شاخه ای Lـتوابع آرتین به کار می آید):

تعریف. گروه اینرسی[16] $\mathfrak{P}$ را برابر با هسته ی هomomورفیسم f تعریف می کنیم و با $I_{\mathfrak{P}}$ نشان می دهیم. در واقع:

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} | \forall r \in R_K, \sigma(r) - r \in \mathfrak{P}\}$$

با استفاده از قضیه اول یکریختی داریم:

$$\frac{D_{\mathfrak{P}}}{I_{\mathfrak{P}}} \cong Gal(\frac{R}{\mathfrak{P}_i}/\frac{\mathbb{Z}}{p\mathbb{Z}})$$

همچنین به سادگی می توان دید که $D_{\mathfrak{P}_i}$ ($I_{\mathfrak{P}_i}$) مزدوج $D_{\mathfrak{P}_j}$ ($I_{\mathfrak{P}_j}$) است برای همه i, jها.

همچنین قضیه زیر را داریم:

قضیه. داریم $|I_{\mathfrak{P}}| = e_{\mathfrak{P}/p}$ و $|D_{\mathfrak{P}}| = e_{\mathfrak{P}/p}f_{\mathfrak{P}/p}$

حال در موقعیتی هستیم که اتومورفیسم فروبنیوس را تعریف کنیم:

معمول است که $\mathbb{Z}/p\mathbb{Z}$ را با $\mathbb{F}_p$ نمایش دهند. پس $\frac{R}{\mathfrak{P}_i}/\mathbb{F}_p$ یک توسیع متناهی از میدان های متناهی است و با نظریه میدان های متناهی می توان نشان داد که این توسیع ها همواره گالوا هستند و گروه گالوای آن ها دوری است و با عنصر $\sigma : x \mapsto x^p$ تولید می شود. به این عنصر، اتومورفیسم فروبنیوس این توسیع گفته می شود. پس $Gal(\frac{R}{\mathfrak{P}_i}/\frac{\mathbb{Z}}{p\mathbb{Z}})$ گروهی دوری است که با $\mathrm{Frob}_{\mathfrak{P}/p} : x \mapsto x^p$ تولید می شود. حال فرض کنید p عدد اولی غیرشاخه ای باشد و مانند قبل $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n$ ایدآل های اول روی p باشند. در این صورت از قضیه بالا $I_{\mathfrak{P}_i} = \{1\}$ برای همه iها و داریم:

$$Gal(K/\mathbb{Q}) \supseteq D_{\mathfrak{P}_i} \cong Gal(\frac{R}{\mathfrak{P}_i}/\frac{\mathbb{Z}}{p\mathbb{Z}})$$

[15] Decomposition group

[16] Inertia group

پس می توان اتومورفیسم موجود در $Gal(\frac{R}{\mathfrak{P}_i}/\frac{\mathbb{Z}}{p\mathbb{Z}})$ را به عنوان عنصری در $Gal(K/\mathbb{Q})$ نگاه کرد و از آنجایی که $D_{\mathfrak{P}_i}$ها ($i \leq n \leq ۰$) مزدوج یکدیگرند، پس مولد های آنها نیز مزدوج یکدیگرند و می توان اتومورفیسم فروبنیوس عدد اول p (به ایدآل اول روی p وابسته نیست) را برابر با آن مولفه ی ازدواج در $Gal(K/\mathbb{Q})$ تعریف کرد که ما با Frob_p نشان می دهیم.

۷ توابع زتای ددکیند

ددکیند تابع زتای ریمان را برای میدان های عددی گسترش داد و با استفاده از آن تعدادی از خواص موجود در اعداد صحیح را به حلقه اعداد صحیح میدان های عددی گسترش داد. همچنین فرض ریمان گسترش یافته[۱۷] نیز برای آن فرمول بندی شده است که نتایجی در نحوه ی تجزیه اعداد اول به ایدآل های اول در آن میدان عددی دارد. برای تعریف تابع زتای ددکیند ابتدا باید مفهومی به نام نُرم[۱۸] را تعریف کنیم:

تعریف. فرض کنید K یک میدان عددی با حلقه اعداد صحیح R_K باشد و I یک ایدآل ناصفر R_K. در این صورت منظور از نُرم I، اندیس I در R_K است و با $N_{K/\mathbb{Q}}(I)$ نمایش داده می شود.

حال می توان تابع زتای ددکیند را تعریف کرد:

تعریف. تابع زتای ددکیند برای میدان عددی K، به شکل زیر تعریف می شود:

$$\zeta_K(s) = \sum_{I \subseteq R_K} \frac{۱}{(N_{K/\mathbb{Q}}(I))^s}$$

که I روی ایدآل های ناصفر R_K حرکت می کند.

این تابع برای s مختلط با $Re\ s > ۱$ همگراست.

اولا به سادگی می توان دید که در حالت $K = \mathbb{Q}$ تابع زتای ددکیند، همان تابع زتای ریمان است.

برای تابع زتای ددکیند، نیز به دلیل ضربی بودن تابع نُرم می توان تجزیه ای به فرم اویلر پیدا کرد:

قضیه. برای s مختلط با $Re\ s > ۱$ داریم:

$$\zeta_K(s) = \prod_{P \subseteq R_K} (\frac{۱}{۱ - N_{K/\mathbb{Q}}(P)^{-s}})$$

که P روی ایدآل های اول ناصفر R_K حرکت می کند.

هکه[۱۹] توانست این تابع را به کل صفحه مختلط به طور مرومورفیک گسترش دهد و همچنین معادله ای تابعی برای آن پیدا کند و پس حدسی مانند فرض ریمان برای آن فرمول بندی شد:

حدس. (فرض ریمان گسترش یافته) برای هر میدان عددی K، اگر صفری از $\zeta_K(s)$ در $\{s \in \mathbb{C} | ۰ < Re\ s < ۱\}$ باشد، آن گاه آن صفر روی خط $Re\ s = \frac{۱}{۲}$ قرار دارد.

۸ نمایش خطی گروه های متناهی

ما برای تعریف Lـتوابع آرتین به یک توسیع از مشخصه های دیریکله به نام نمایش های خطی گروه ها نیاز داریم که در این بخش به مقدمات آن پرداخته می شود.

در این بخش همیشه فرض می کنیم G یک گروه متناهی است.

تعریف. منظور ما از یک نمایش خطی از G، یک عمل خطی گروه G بر یک فضای برداری V متناهی بعد روی اعداد مختلط است. به عبارت دیگر، یک نمایش خطی گروه G یک هوموморفیسم $\rho : G \to GL_n(V)$ است. به V، یک Gـفضا گفته می شود.

درجه یک نمایش خطی، طبق تعریف، بُعد V است. نمایش (ρ, V) یک نمایش تحویل ناپذیر است هرگاه هیچ زیرفضای سره پایا تحت عمل G نداشته باشد. دو نمایش خطی (ρ, V) و (ρ', V') معادل نامیده می شوند هرگاه V و V' به عنوان Gـفضا یکی باشند، این مفهوم به این معناست که یک ایزومورفیسم خطی $f : V \to V'$

[۱۷] Extended Riemann Hypothesis (ERH)

[۱۸] Norm

[۱۹] Hecke

باشد بطوری که:

$$f \circ \rho(g) = \rho'(g) \circ f$$

هر نمایش خطی (ρ, V) به جمع مستقیم نمایش های تحویل ناپذیر خطی تجزیه می شود. به عبارت دیگر:

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_s$$

که V_iها Gـ فضا هستند و V_iها نمایش هایی تحویل ناپذیرند.

مشخصه ی یک نمایش (ρ, V) برابر با تابع زیر است:

$$\chi : G \to \mathbb{C}, \quad \chi(\sigma) = \mathrm{Tr}(\rho(\sigma))$$

است که از آن جایی که اثر[20] یک ماتریس فقط به مولفه ی ازدواج آن بستگی دارد، پس χ در حد ازدواج ثابت می ماند. دو نمایش معادلند اگر و تنها اگر مشخصه های آن ها مساوی باشند. مشخصه ای که همواره برابر ۱ است، مشخصه ی اصلی[21] نامیده می شود.

۹ Lـ توابع آرتین

فرض کنید $K/\mathbb{Q}$ یک توسیع گالوا با گروه گالوای G باشد و فرض کنید (ρ, V) یک نمایش خطی از G باشد. برای $\sigma \in G$ و $v \in V$، عمل $\rho(\sigma)v$ را با σv نمایش می دهیم.

فرض کنید $p \in \mathbb{Z}$ یک عدد اول و $\mathfrak{P}$ یک ایدآل اول روی p باشد. در این صورت اگر $D_{\mathfrak{P}}$ گروه تجزیه و $I_{\mathfrak{P}}$ گروه اینرسی $\mathfrak{P}/p$ باشد، آن گاه از نتایج بخش های قبل، $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ با عنصر فروبنیوس $\mathrm{Frob}_{\mathfrak{P}/p}$ تولید می شود و پس اتومورفیسم فروبنیوس یک درون ریختی فضای متناهی بعد

$$V^{I_{\mathfrak{P}}} := \{v \in V | \forall i \in I_{\mathfrak{P}}; iv = v\}$$

است و می توان "چندجمله ای مشخصه" اتومورفیسم $\mathrm{Frob}_{\mathfrak{P}/p}$ را با تابع زیر تعریف کرد:

$$Charpol(\mathrm{Frob}_{\mathfrak{P}/p})(t) = \mathrm{Det}(I - t\mathrm{Frob}_{\mathfrak{P}/p})$$

تعریف می کنیم. از بخش های قبل می دانیم که $\mathrm{Frob}_{\mathfrak{P}/p}$ در حد ازدواج با خود p مشخص می شود. پس از آنجا که چندجمله ای مشخصه ماتریس های مزدوج یکی است، پس این چندجمله ای مشخصه، فقط با p مشخص می شود و به انتخاب ایدآل اول روی آن بستگی ندارد.

حال می توان Lـ توابع آرتین را تعریف کرد:

تعریف. فرض کنید $K/\mathbb{Q}$ یک توسیع گالوای متناهی با گروه گالوای G باشد. فرض کنید (ρ, V) یک نمایش خطی G با تابع مشخصه ی χ باشد. آن گاه Lـ تابع آرتین وابسته به ρ یا χ با فرم ضربی زیر تعریف می شود:

$$L(s, \chi, K/\mathbb{Q}) = \prod_{p\text{اول}} \frac{1}{Charpol(\mathrm{Frob}_p)(N(p)^{-s})}$$

برای هر $\delta > 0$، Lـ تابع آرتین به طور یکنواخت و مطلق روی ناحیه ی $Re\ s \geq 1 + \delta$ همگراست.

قضیه. ۱) برای مشخصه ی اصلی $\chi_0 \equiv 1$، تابع زتای ریمان را دریافت می کنیم:

$$L(s, \chi_0, K) = \zeta(s)$$

۲) اگر $L \supseteq K \supseteq \mathbb{Q}$ توسیع های گالوای $\mathbb{Q}$ باشند، آن گاه

$$L(s, \chi, K/\mathbb{Q}) = L(s, \chi, L/\mathbb{Q})$$

که مشخصه ی χ از $Gal(K/\mathbb{Q})$ را به عنوان یک مشخصه از $Gal(L/\mathbb{Q})$ ببینیم.

[20] Trace

[21] Principal character

۳) اگر χ_1 و χ_2 دو مشخصه از $Gal(K/\mathbb{Q})$ باشند، آن گاه

$$L(s,\chi_1+\chi_2,K/\mathbb{Q})=L(s,\chi_1,K/\mathbb{Q})L(s,\chi_2,K/\mathbb{Q})$$

۴) اگر χ_αها مشخصه های تحویل ناپذیر نمایش های $Gal(K/Q)$ باشند، آنگاه $r_\alpha\in\mathbb{C}$ وجود دارند بطوری که:

$$\zeta_K(s)=\zeta(s)\prod L(s,\chi_\alpha,K/\mathbb{Q})^{r_\alpha}$$

برهان. رجوع شود به قضیه ۴,۲ از فصل ۵ در [۸].

Lـ تابع آرتین در حالتی که توسیع آبلی باشد (توسیع گالوای متناهی با گروه گالوای آبلی)، با Lـ تابع دیریکله یکسان می شود اما از آنجایی که اثبات آن به کمی نظریه میدان های رده ای نیاز دارد خواننده علاقمند می تواند به کتاب [۸] رجوع کند.

همچنین Lـ توابع آرتین به طور مرومورفیک به صفحه مختلط گسترش می یابد و یک معادله ی تابعی مانند معادله ی تابعی تابع زتا دارند. همچنین حدس آرتین ادعا می کند که اگر مشخصه غیر اصلی باشد، آنگاه Lـ تابع آرتین وابسته به آن به طور تحلیل گسترش می یابد:

حدس. (آرتین) برای هر مشخصه تحویل ناپذیر غیراصلی، Lـ تابع آرتین $L(s,\chi,K/\mathbb{Q})$ یک گسترش تحلیلی به کل صفحه مختلط دارد.

حدس آرتین در صورت درست بودن، نتایج بسیار زیادی دارد، مثلا تحلیلی بودن $\frac{\zeta_L(s)}{\zeta_K(s)}$ برای توسیع L/K از میدان های عددی.

همچنین Lـ توابع آرتین کاربردهای بسیار زیادی دارد. مثلا همان گونه که Lـ توابع دیریکله در اثبات قضیه دیریکله به ما کمک می کنند، Lـ توابع آرتین در حل قضیه دیریکله گسترش یافته (قضیه چگالی چبوتارف[۲۲]) کاربرد دارند. همچنین آن ها در مشخص کردن توسیع های جبری میدان های عددی، با استفاده از ایدآل های موجود در خود آن میدان عددی کمک می کنند. این برنامه توسط کرونکر[۲۳] پیشنهاد شده بود و کاربردهای زیادی در نظریه جبری اعداد و نظریه تحلیلی اعداد دارند و نتایجی دارند که به فرمول بندی یک برنامه بسیار فعال در نظریه اعداد به نام "برنامه لنگلندز[۲۴] " منجر می شوند.

قدردانی

با تشکر از محمدامین حیدرشاهی برای کمک به حروفچینی مطالب.

References

[1] Euler L. *Introduction to Analysis of the Infinite - Book I*, Springer, 1988.

[2] Riemann B. *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, 1859.

[3] Artin E. *Über eine neue art von L-Reihen*, 1923.

[4] Apostol T. M. *Introduction to Analytic Number Theory*, Springer, 1976.

[5] Shoenfeld, L. *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II* , Mathematics of Computation, **30** (134): 337 - 360.

[6] Hungerford, W. H. *Algebra*, Springer, 1974.

[7] Samuel P. *Algebraic Theory of Numbers*, Translated by Allan J. Silberger. Mineola, NY: Dover, 2008.

[8] Neukirch J. *Class Field Theory*, Springer, 1986.

[۲۲] Chebotaryov

[۲۳] Kronecker

[۲۴] Langlands program