لُژاندر و تجزیهٔ فاکتوریل‌ها

مهدی حسنی
دانشیار گروه ریاضی دانشگاه زنجان
mehdi.hassani@znu.ac.ir

اشاره
در این نوشتار دربارهٔ «قضیهٔ لژاندر» در خصوص تجزیهٔ عددهای فاکتوریلی صحبت می‌کنیم. با وجود بزرگ بودن فاکتوریل‌ها، روش منسوب به لُژاندر روشی کارآمد و سریع برای به‌دست آوردن نمای عوامل اول در تجزیهٔ آن‌ها ارائه می‌کند. این روش با تلفیق ملاحظاتی که اشاره خواهد شد، به مراتب بسیار سریع‌تر قابل اجراست. ضمن آنکه همین ملاحظات کمک خواهند کرد که نگاهی عمیق‌تر به توزیع نمای عددهای اول در تجزیهٔ فاکتوریل‌ها داشته باشیم.

مقدمه

یکی از مواردی که در عمل تجزیه به عوامل اول را می‌توان اجرا کرد، تجزیهٔ فاکتوریل‌هاست. طبق معمول، برای $n\in N$ می‌نویسیم:

$n!=۱\times۲\times\ldots\times n,$

و قرار می‌دهیم: $۰!=۱$. به این ترتیب، اگر p عددی اول باشد و $p\le n$، آن‌گاه: $p|n!$. همچنین، اگر: $p>n$ آن‌گاه: $p\nmid n!$. لذا وقتی $n!$ را به عوامل اول تجزیه می‌کنیم، تمام عددهای اول نابیشتر از n و فقط همین عددها در تجزیه ظاهر خواهند شد. قضیه‌ای منسوب به ریاضی‌دان فرانسوی، **آدرین- ماری لژاندر**، توان دقیق این عوامل اول را با حجم پایینی از محاسبات تعیین می‌کند. برای اثبات قضیه به لم زیر نیاز داریم:

لم ۱. تعداد مضارب: فرض کنید $a,b\in N$. تعداد مضارب مثبت b که نابیشتر از a هستند، برابر $\left[\frac{a}{b}\right]$ است.

اثبات: فرض کنید تعداد مضارب مذکور q باشد. در این صورت داریم:

$۱b,۲b,۳b,\ldots,qb\le a\ ,(q+۱)b>a.$

لذا: $qb\le a<(q+۱)b$ و در نتیجه: $q\le\frac{a}{b}<q+۱$. این نتیجه می‌دهد: $q=\left[\frac{a}{b}\right]$ و اثبات کامل است.

قضیهٔ ۲. قضیهٔ لژاندر: اگر $\upsilon_p(n!)$ نشانگر بزرگ‌ترین توان عدد اول p در تجزیهٔ $n!$ به عوامل اول باشد، آن‌گاه داریم:

$$\upsilon_p(n!)=\sum_{\alpha=۱}^{\infty}\left[\frac{n}{p^{\alpha}}\right]$$

اثبات: $\upsilon_p(n!)$ برابر حاصل‌جمع تعداد مضارب نابیشتر از n عددهای $p^۱,p^۲,p^۳,\ldots$ است که با استفاده از لم مضارب (لم بالا) برابر جمع داده شده در صورت قضیه است.

مثال ۳. برای درک محتوای اثبات بالا، بهتر است مثالی عددی را بررسی کنیم. فرض کنید می‌خواهیم $\upsilon_۲(۲۰!)$ را به‌دست آوریم. داریم:

$$\begin{aligned}۲۰!=&۱\times\underline{۲}\times۳\times\underline{\underline{۴}}\times۵\times\underline{۶}\times۷\times\underline{\underline{\underline{۸}}}\times۹\times\underline{۱۰}\times۱۱\\&\times\underline{\underline{۱۲}}\times۱۳\times\underline{۱۴}\times۱۵\times\underline{\underline{\underline{\underline{۱۶}}}}\times۱۷\times\underline{۱۸}\times۱۹\times\underline{\underline{۲۰}}\end{aligned}$$

زیر مضارب $۲^۱$ یک خط، زیر مضارب $۲^۲$ دو خط، زیر مضارب $۲^۳$ سه خط و زیر مضارب $۲^۴$ چهار خط کشیده‌ایم. این‌ها تمام مضارب موجود و ممکن از همهٔ توان‌های ۲ هستند، و جمعشان برابر است با: $۱۸=۱+۲+۵+۱۰$. لذا داریم: $\upsilon_۲(۲۰!)=۱۸$، و با ادامهٔ روند برای سایر عوامل نتیجه می‌شود:

$$\begin{aligned}۲۰!&=(۲^{۱۸})(۳^{۸})(۵^{۴})(۷^{۲})(۱۱^{۱})(۱۳^{۱})(۱۷^{۱})(۱۹^{۱})\\&=۲۴۳۲۹۰۲۰۰۸۱۷۶۶۴۰۰۰۰\end{aligned}$$

از قضیهٔ لژاندر می‌توان نتایج خوبی در خصوص توان‌های عددهای اول در تجزیهٔ فاکتوریل‌ها گرفت. برای استنتاج این نتایج لازم است قدری دربارهٔ تابع جزء صحیح صحبت شود.

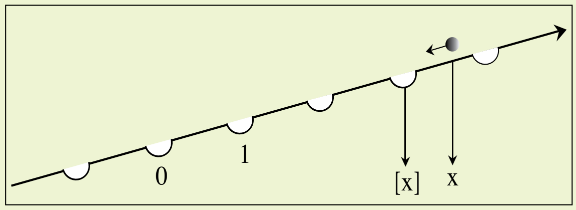
ملاحظاتی دربارهٔ تابع جزء صحیح و قضیهٔ لژاندر

یکی از مفاهیم مفیدی که عددهای حقیقی و عددهای صحیح را به هم مربوط می‌کند، تابع جزء صحیح است. از این تابع در لم مضارب و قضیهٔ لژاندر استفاده کردیم. حال تعریف و برخی خواص آن را مرور می‌کنیم.

تعریف ۴: جزء صحیح عدد $x\in R$ را با نماد $[x]$ نشان می‌دهیم و به‌صورت زیر تعریف می‌کنیم:

$$[x]=\max\{k\in Z: k\le x\}$$

شکل ۱. تعبیر شهودی جزء صحیح



فرض کنید محور عددهای حقیقی را اندکی به‌صورت صعودی مایل کرده‌ایم، به‌طوری که به شکل یک سطح شیب‌دار درآمده است (شکل ۱). همچنین در موضع مربوط به عددهای صحیح چاله‌هایی کنده‌ایم. اگر در موضع $x\in R$ گویی قرار دهیم، این گوی روی سطح حرکت می‌کند و در اولین چالهٔ واقع در سمت چپش می‌افتد. همین چاله موضع $[x]$ است. اگر گوی از همان ابتدا در چاله‌ای قرار داشته باشد ($x\in Z$)، آن‌گاه حرکتی انجام نمی‌شود و گوی در همان چاله می‌ماند؛ یعنی: $x=[x]$. به همین ترتیب از تعریف فوق و تعبیر شهودی آن در شکل ۱ خواص ابتدایی، اما کلیدی زیر حاصل می‌شوند:

$$\begin{aligned}
&\forall x\in R: x-1<[x]\le x,\\
&x=[x]\Leftrightarrow x\in Z,\\
&\forall x\in R, \forall k\in Z: [x+k]=[x]+k,\\
&\forall x\in R \exists \theta=\theta(x) \text{ s.t. } x=[x]+\theta, 0\le\theta<1.
\end{aligned}$$

در خاصیت آخر، θ را جزء کسری x می‌نامیم و آن را با $\{x\}$ نشان می‌دهیم (البته مراقبیم که این نماد مرسوم را با مجموعهٔ تک عضوی شامل x اشتباه نگیریم). لذا: $\{x\}=x-[x]$. خواص نابدیهی‌تر زیر را در استنتاج نتایج مورد نظر از قضیهٔ لژاندر احتیاج خواهیم داشت.

گزارهٔ ۵. فرض کنید: $b\in R$ و a و $n\in N$. داریم:

۱. $[a]+[b]\le[a+b]$، و $0\le[2a]-2[a]\le 1$.

۲. $\left[\frac{[a]}{n}\right]=\left[\frac{a}{n}\right]$

اثبات:

۱. می‌نویسیم:

$$\begin{aligned}
[a+b]&=\big[[a]+\{a\}+[b]+\{b\}\big]\\
&=[a]+[b]+\big[\{a\}+\{b\}\big].
\end{aligned}$$

اما چون: $0\le\{a\}+\{b\}<2$، لذا: $\big[\{a\}+\{b\}\big]\ge 0$، و حکم به‌دست می‌آید. درواقع، این اثبات نتیجه می‌دهد: $0\le[a+b]-[a]-[b]\le 1$، به‌خصوص: $0\le[2a]-2[a]\le 1$.

۲. روش اول: فرض کنید k عددی صحیح، دلخواه و ثابت باشد. با اختیار کردن: $kn\le a<(k+1)n$ نتیجه می‌شود: $kn\le[a]<(k+1)n$، و لذا: $\left[\frac{a}{n}\right]=k$ و $\left[\frac{[a]}{n}\right]=k$. چون k دلخواه است، حکم برای تمام مقادیر a نیز برقرار است.

روش دوم: می‌نویسیم:

$$\begin{aligned}
\frac{a}{n}=\left[\frac{a}{n}\right]+\theta &\Rightarrow a=n\left[\frac{a}{n}\right]+n\theta\\
&\Rightarrow [a]=\left[n\left[\frac{a}{n}\right]+n\theta\right]=n\left[\frac{a}{n}\right]+[n\theta]\\
&\Rightarrow \frac{[a]}{n}=\left[\frac{a}{n}\right]+\frac{1}{n}[n\theta]\\
&\Rightarrow \left[\frac{[a]}{n}\right]=\left[\left[\frac{a}{n}\right]+\frac{1}{n}[n\theta]\right]\\
&\qquad=\left[\frac{a}{n}\right]+\left[\frac{1}{n}[n\theta]\right]
\end{aligned}$$

حال توجه می‌کنیم که:

$$\begin{aligned}
0\le\theta<1&\Rightarrow 0\le n\theta<n\Rightarrow 0\le[n\theta]<n\\
&\Rightarrow 0\le\frac{1}{n}[n\theta]<1\Rightarrow\left[\frac{1}{n}[n\theta]\right]=0,
\end{aligned}$$

و حکم به دست می‌آید.

با استفاده از خواص فوق برای تابع جزء صحیح می‌توانیم به مشاهداتی دربارهٔ محتوای قضیهٔ لُژاندر دست یابیم که استفادهٔ عملی از این قضیه را به‌مراتب سریع‌تر می‌کند. این مشاهدات را در نتیجه زیر گردآوری می‌کنیم:

همچنین قرار دهید P نشانگر مجموعه اعداد اول باشد.

نتیجهٔ ۶. فرض کنید: $n\ge 2$.

۱. در تجزیهٔ استاندارد $n!$ به عوامل اول، توان‌ها سیر نزولی دارند.

۲. برای $p\in P$ و $\sqrt{n}<p\le n$ داریم: $\upsilon_p(n!)=\left[\frac{n}{p}\right]$.

۳. برای $p\in P$ و $\frac{n}{2}<p\le n$ داریم: $\upsilon_p(n!)=1$.

۴. تعداد صفرهای انتهایی !n برابر است با: $\upsilon_5(n!)$.

اثبات:

۱. فرض کنید: $p,q\in P$ و $p<q\le n$. در این صورت برای $\alpha\in N$ داریم:

$$p^\alpha<q^\alpha \Rightarrow \frac{n}{p^\alpha}>\frac{n}{q^\alpha}\Rightarrow \left[\frac{n}{p^\alpha}\right]\ge\left[\frac{n}{q^\alpha}\right] \Rightarrow \upsilon_p(n!)\ge\upsilon_q(n!).$$

۲. چـون $p>\sqrt{n}$، داریـم: $p^2>n$ و لـذا $0<\frac{n}{p^2}<1$. در نتیجه: $\left[\frac{n}{p^2}\right]=0$. همچنین با اسـتفاده از بند ۲ از گزارهٔ ۵، برای $\alpha\ge 3$ داریم:

$$\left[\frac{n}{p^\alpha}\right]=\left[\frac{\frac{n}{p^2}}{p^{\alpha-2}}\right]=\left[\frac{\left[\frac{n}{p^2}\right]}{p^{\alpha-2}}\right]=\left[\frac{0}{p^{\alpha-2}}\right]=0$$

در نتیجه: $\upsilon_p(n!)=\left[\frac{n}{p}\right]$.

۳. داریم:

$$\frac{n}{2}<p\le n\Leftrightarrow 1\le\frac{n}{p}<2\Leftrightarrow\left[\frac{n}{p}\right]=1$$

با اسـتفادهٔ مجدد از بند ۲ گـزارهٔ ۵، برای $\alpha\ge 2$ نتیجه می‌شود:

$$\left[\frac{n}{p^\alpha}\right]=\left[\frac{\frac{n}{p}}{p^{\alpha-1}}\right]=\left[\frac{\left[\frac{n}{p}\right]}{p^{\alpha-1}}\right]=\left[\frac{1}{p^{\alpha-1}}\right]=0$$

لذا: $\upsilon_p(n!)=1$.

۴. هر صفر انتهایی به معنای یک عامل ۵×۲=۱۰ است. اما چون: $\upsilon_2(n!)\ge\upsilon_5(n!)$، لذا برای تولید عامل ۱۰ به مقدار کافی ۲ داریم. پس تعداد عوامل ۱۰ برابر $\upsilon_5(n!)$ است و همین مقدار صفرهای انتهایی نیز وجود دارد. اثبات کامل است.

در عمل با در نظر گرفتن بندهای ۲ و ۳ نتیجهٔ ۶ می‌توان فرایند تجزیهٔ !n را سرعت بخشید. برای توضیح بیشتر، !۱۰۰ را بـه حاصل‌ضرب عوامـل اول تجزیه می‌کنیـم. در تجزیهٔ !۱۰۰ تمـام عددهای اول نابیشـتر از ۱۰۰ حضور دارند. این عددها را توسـط «غربال اراتستن» به دسـت می‌آوریم و در سه دستهٔ عددهای اول کوچک $(1<p\le\sqrt{n})$، عددهای اول متوسط $(\sqrt{n}<p\le\frac{n}{2})$ و عددهای اول بزرگ $(\frac{n}{2}<p\le n)$ تقسیم‌بندی می‌کنیم:

$2,3,5,7 \qquad (1<p\le\sqrt{100})$

$11,13,17,19,23,29,31,37,41,43,47\ (\sqrt{100}<p\le\frac{100}{2})$

$53,59,61,67,71,73,79,83,89,97\ (\frac{100}{2}<p\le 100)$

بنابر بند ۳ از نتیجهٔ ۶ توان‌های عددهای اول بزرگ مندرج در سـطر سـوم در بالا در تجزیه به عوامل اول همگی برابر ۱ هستند. برای عوامل متوسط p که: $\sqrt{100}<p\le\frac{100}{2}$، بنا به بند ۲ از نتیجهٔ ۶ داریم:

$$\upsilon_p(100!)=\left[\frac{100}{p}\right]$$

پس:

$$\begin{aligned}&\upsilon_{11}(100!)=9,\ \upsilon_{13}(100!)=7,\\&\upsilon_{17}(100!)=5,\ \upsilon_{19}(100!)=5,\\&\upsilon_{23}(100!)=4,\ \upsilon_{29}(100!)=3,\\&\upsilon_{31}(100!)=3,\ \upsilon_{37}(100!)=2,\\&\upsilon_{41}(100!)=2,\ \upsilon_{43}(100!)=2,\ \upsilon_{47}(100!)=2\end{aligned}$$

درواقع وزن اصلی محاسبات روی عددهای اول به اصطلاح کوچک اسـت؛ یعنی pهایی که دارای این شـرط هسـتند: $1<p\le\sqrt{100}=10$. این عددها عبارت‌انـد از: ۷، ۵، ۳ و ۲. هرچند تعدادشان کم است، ولی از مجموع تمام توان‌ها سهم زیادی دارند. با این‌حال با در نظر گرفتن اینکه:

$$\left[\frac{n}{p^{\alpha+1}}\right]=\left[\frac{\frac{n}{p^\alpha}}{p}\right]=\left[\frac{\left[\frac{n}{p^\alpha}\right]}{p}\right],$$

می‌توان جمعوندهای $\upsilon_p(n!)$ را برای این عددهای اول با یک فرایند کاهشی و با تقسیمات متوالی بر p، آسان‌تر محاسبه کرد. برای مثال، در محاسبهٔ $\upsilon_2(100!)$ داریم:

$$\begin{aligned}\upsilon_2(100!)&=\sum_{\alpha=1}^{\infty}\left[\frac{100}{2^\alpha}\right]\\&=\left[\frac{100}{2}\right]+\left[\frac{100}{4}\right]+\left[\frac{100}{8}\right]+\left[\frac{100}{16}\right]\\&+\left[\frac{100}{32}\right]+\left[\frac{100}{64}\right]+\left[\frac{100}{128}\right]+\dots\\&=50+25+12+6+3+1+0+\dots=97.\end{aligned}$$

توضیح اینکه در محاسبهٔ جمعوندها در محاسبهٔ $\upsilon_2(100!)$

این‌گونه عمل کردیم:

$$\left[\frac{۱۰۰}{۲}\right]=۵۰\to\left[\frac{۵۰}{۲}\right]=۲۵\to\left[\frac{۲۵}{۲}\right]=۱۲$$
$$\to\left[\frac{۱۲}{۲}\right]=۶\to\left[\frac{۶}{۲}\right]=۳\to\left[\frac{۳}{۲}\right]=۱\to\left[\frac{۱}{۲}\right]=۰.$$

این زنجیره حتماً به صفر منتهی می‌شود و در عمل تعداد جمع‌وندها متناهی است (تبصرهٔ بعد را ببینید). همچنین، با بزرگ‌تر شـــدن پایه، طول زنجیره کوتاه‌تر می‌شود و سریع‌تر خاتمـــه می‌پذیـــرد. مثـــلاً در محاسـبهٔ $\upsilon_۳(۱۰۰!)$ زنجیرهٔ جمع‌وندها عبارت‌است از:

$$\left[\frac{۱۰۰}{۳}\right]=۳۳\to\left[\frac{۳۳}{۳}\right]=۱۱\to\left[\frac{۱۱}{۳}\right]=۳$$
$$\to\left[\frac{۳}{۳}\right]=۱\to\left[\frac{۱}{۳}\right]=۰.$$

لذا: $۴۸=۱+۳+۱۱+۳۳=\upsilon_۳(۱۰۰!)$. همچنین، زنجیرهٔ جمع‌وندها در محاسبهٔ $\upsilon_۵(۱۰۰!)$ عبارت‌است از:

$$\left[\frac{۱۰۰}{۵}\right]=۲۰\to\left[\frac{۲۰}{۵}\right]=۴\to\left[\frac{۴}{۵}\right]=۰.$$

بنابراین: $۲۴=۴+۲۰=\upsilon_۵(۱۰۰!)$ که برابر تعداد صفرهای انتهایی !۱۰۰ نیز هســـت. در نهایت زنجیـــرهٔ جمع‌وندها در محاسبهٔ $\upsilon_۷(۱۰۰!)$ عبارت‌است از:

$$\left[\frac{۱۰۰}{۷}\right]=۱۴\to\left[\frac{۱۴}{۷}\right]=۲\to\left[\frac{۲}{۷}\right]=۰.$$

بنابراین: $۱۶=۲+۱۴=\upsilon_۷(۱۰۰!)$. با جمع‌بندی اطلاعات به‌دست آمده نتیجه می‌گیریم:

$$\begin{aligned}۱۰۰!=&(۲^{۹۷})(۳^{۴۸})(۵^{۲۴})(۷^{۱۶})(۱۱^{۹})(۱۳^{۷})(۱۷^{۵})\\&(۱۹^{۵})(۲۳^{۴})(۲۹^{۳})(۳۱^{۳})(۳۷^{۲})(۴۱^{۲})\\&(۴۳^{۲})(۴۷^{۲})(۵۳^{۱})(۵۹^{۱})(۶۱^{۱})(۶۷^{۱})\\&(۷۱^{۱})(۷۳^{۱})(۷۹^{۱})(۸۳^{۱})(۸۹^{۱})(۹۷^{۱}).\end{aligned}$$

به کمک رایانه مشاهده می‌شود:

$$\begin{aligned}۱۰۰!=&۹۳۳۲۶۲۱۵۴۴۳۹۴۴۱۵۲۶۸۱۶۹۹۲۳۸۸۵۶۲۶۶۷۰\\&۰۴۹۰۷۱۵۹۶۸۲۶۴۳۸۱۶۲۱۴۶۸۵۹۲۹۶۳۸۹۵۲۱\\&۷۵۹۹۹۹۳۲۲۹۹۱۵۶۰۸۹۴۱۴۶۳۹۷۶۱۵۶۵۱۸۲۸\\&۶۲۵۳۶۹۷۹۲۰۸۲۷۲۲۳۷۵۸۲۵۱۱۸۵۲۱۰۹۱۶۸۶\\&۴۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰,\end{aligned}$$

که عددی است با ۱۵۸ رقم. اما با روش لُژاندر و ملاحظات بیان شده، به‌راحتی و با محاسبات ساده‌ای به عوامل اول تجزیه شد.

رفتار حدی توان‌های اعداد اول در تجزیهٔ فاکتوریل‌ها

با استفاده از قضیهٔ لُژاندر می‌توان اطلاعات مفیدی دربارهٔ $\upsilon_p(n!)$ که نشـــانگر توان عدد اول p در تجزیهٔ !n به عوامل اول اســـت، به‌دســـت آورد. یکی از این اطلاعات نامساوی زیر برای $\upsilon_p(n!)$ است.

قضیهٔ ۷. برای هر $n\in N$ و هر عدد اول p که: $p\le n$، داریم:

$$\frac{n-p}{p-۱}-\frac{\ln n}{\ln p}<\upsilon_p(n!)\le\frac{n-۱}{p-۱}\qquad(۱)$$

اثبات: قضیهٔ ۲ بیان می‌کند که:

$$\upsilon_p(n!)=\sum_{\alpha=۱}^{m}\left[\frac{n}{p^{\alpha}}\right],\ \ m=\left[\frac{\ln n}{\ln p}\right]$$

بر همین اساس و با استفاده از نامساوی $x-۱<[x]\le x$ نتیجه می‌شود:

$$n\sum_{k=۱}^{m}\frac{۱}{p^k}-m<\upsilon_p(n!)\le n\sum_{k=۱}^{m}\frac{۱}{p^k}.$$

با توجه به اینکه:

$$\sum_{k=۱}^{m}\frac{۱}{p^k}=\frac{۱}{p-۱}(۱-\frac{۱}{p^m})$$

نتیجه می‌گیریم:

$$\frac{n}{p-۱}(۱-\frac{۱}{p^m})-m<\upsilon_p(n!)\le\frac{n}{p-۱}(۱-\frac{۱}{p^m}).$$

با تلفیـــق این نامســـاوی با $\frac{\ln n}{\ln p}-۱<m\le\frac{\ln n}{\ln p}$ حکم به‌دست می‌آید.

نتیجهٔ ۸. برای هر $n\in N$ و هر عدد اول p که: $p\le n$، داریم:

$$۰<\frac{n}{p-۱}-\upsilon_p(n!)<\frac{\ln n}{\ln p}$$

تبصره ۹. نتیجهٔ بالا نشان می‌دهد که:

$$\lim_{n\to\infty}\frac{\upsilon_p(n!)}{n}=\frac{۱}{p-۱}$$

از این رابطه حدی نتیجه می‌شود:

$$\upsilon_۲(n!)\approxeq n,\qquad\upsilon_۳(n!)\approxeq\frac{n}{۲},\qquad\upsilon_۵(n!)\approxeq\frac{n}{۴}.$$

درستی این روابط را در نمونه‌های عددی محاسبه شده در بالا می‌توان مشاهده کرد.

پی‌نوشت

1. Adrien-Marie Legendre

برای مشاهدهٔ منابع کیو-آر ـ کد
را اسکن کنید