فرهنگ و اندیشهٔ ریاضی
شماره ۳۷ (پاییز ۱۳۸۵) صص. ۲۱ تا ۳۶

فاکتوریل تعمیم یافته

منصور معتمدی

تقدیم به استاد ارجمند دکتر جواد بهبودیان

چکیده

تابع فاکتوریل با استفاده از مفهومی بنام $P-$ ترتیب، به هر زیرمجموعهٔ حلقهٔ اعداد صحیح تعمیم‌پذیر است. هدف این نوشتار آگاهی از چگونگی این تعمیم است. در پایان به مفهوم ایدال فاکتوریل در حوزه‌های ددکیند اشاره خواهد شد.

مقدمه

تابع فاکتوریل را که بر مجموعه اعداد طبیعی تعریف می‌شود، می‌توان بر هر زیر مجموعه اعداد صحیح تعریف کرد. این کار با استفاده از مفهومی به نام $P-$ترتیب که توسط باهرگاوا[1] معرفی شده است، انجام می‌گیرد. وی به خاطر پژوهش‌هایی که در این زمینه انجام داده موفق شده است جایزهٔ دومرگن را در سال ۱۹۹۶ میلادی دریافت کند. این جایزه هر ساله از طرف انجمن ریاضی آمریکا[2]، مجمع ریاضی آمریکا[3] و مجمع ریاضیات صنعتی و کاربردی[4] به افرادی که پژوهش های ارزشمندی در سطح کارشناسی انجام می‌دهند، اهدا می‌شود. جایزهٔ مذکور در سال ۲۰۰۳ میلادی به سبب ادامه تحقیقات در همین زمینه به ام. وود[5] تعلق گرفت. هدف این نوشتار معرفی مفهوم $P-$ ترتیب و استفاده از آن در تعمیم تابع فاکتوریل است. در بخش نخست به بعضی پیش نیازها، اشاره می‌شود. در بخش دوم یکی از موارد نمود مفهوم فاکتوریل را عنوان می‌کنیم. در بخش سوم معرفی حلقهٔ چندجمله‌ای‌ها با مقدار صحیح مورد نظر است. در بخش چهارم مفهوم $P-$ ترتیب معرفی و مثال هایی بیان می‌شود. در بخش پایانی تعمیم‌های بیشتر به حوزه‌های ددکیند به اختصار خواهد آمد.

1) Bhargava 2) AMS 3) MAA 4) SIAM 5) M. Wood

۱. پیش نیازها

تعریف ۱.۱. اگر n یک عدد طبیعی باشد، تابع فاکتوریل به استقرا چنین تعریف می‌شود

$$n! = \begin{cases} ۱ & \text{اگر } n = ۱ \\ (n-۱)!n & \text{اگر } n > ۱ \end{cases}$$

برای سهولت در محاسبات قرار می‌دهیم $۰! = ۱$.
بدین ترتیب ملاحظه می‌شود که

$$n! = ۱ \times ۲ \times \cdots \times n$$

قضیهٔ ۱.۱. برای اعداد صحیح a، b و n برابری زیر همواره برقرار است:

$$\left[\frac{[\frac{n}{a}]}{b}\right] = \left[\frac{n}{ab}\right]$$

(نماد $[x]$ یعنی بزرگ‌ترین عدد صحیحی که در x می‌گنجد.)

برهان. درستی برابری را می‌توان با استفاده از الگوریتم تقسیم به اثبات رساند.

نتیجهٔ ۱.۱. اگر p عدد اوّلی باشد، آن گاه

$$\left[\frac{[\frac{n}{p^{\alpha}}]}{p^{\beta}}\right] = \left[\frac{n}{p^{\alpha+\beta}}\right].$$

برهان. بدیهی است.

نتیجهٔ ۲.۱. اگر $n = n_۱ + n_۲ + \cdots + n_k$ و n_i ها اعداد طبیعی باشند، آن گاه

$$\left[\frac{n}{a}\right] \geq \left[\frac{n_۱}{a}\right] + \left[\frac{n_۲}{a}\right] + \cdots + \left[\frac{n_k}{a}\right].$$

برهان. اگر فرض کنیم $a_i = \left[\frac{n_i}{a}\right]$، پس برای هر $۱ \lneq i \lneq k$

$$n_i = aq_i + r_i \qquad ۱ \lneq r_i \lneq a$$

و علاوه بر آن $q_i = \left[\frac{n_i}{a}\right]$. از این رو

$$n = n_۱ + n_۲ + \cdots + n_k = a(q_۱ + q_۲ + \cdots + q_k) + r_۱ + r_۲ + \cdots + r_k$$

و

$$\left[\frac{n}{a}\right] = q_1 + q_2 + \cdots + q_k + \left[\frac{r_1 + r_2 + \cdots + r_k}{a}\right]$$

بنابراین

$$\left[\frac{n}{a}\right] \geq q_1 + q_2 + \cdots + q_k = \left[\frac{n_1}{a}\right] + \left[\frac{n_2}{a}\right] + \cdots + \left[\frac{n_k}{a}\right].$$

نمادگذاری

فرض کنیم p عددی اوّل است. بزرگ‌ترین نمای p که عدد m را می‌شمارد با $e_p(m)$ نشان می‌دهیم. برهان قضیهٔ بعد در کتاب‌های مقدماتی نظریهٔ اعداد وجود دارد.

قضیه ۲.۱. (لژاندر[1]). بزرگ‌ترین نمای عدد اوّل p که $n!$ را می‌شمارد برابر است با

$$e_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^s}\right]$$

با این فرض که $\left[\frac{n}{p^{s+1}}\right] = 0$.

قضیه ۳.۱. اگر عدد طبیعی n مجموع چند عدد طبیعی دیگر باشد، فاکتوریل مجموع بر حاصل‌ضرب فاکتوریل اجزاء بخش‌پذیر است. یعنی اگر

$$n = n_1 + n_2 + \cdots + n_k$$

آن گاه عبارت

$$\frac{n!}{n_1! n_2! \cdots n_k!}$$

عددی صحیح است.

برهان. کافی است نشان دهیم که اگر یک عدد اوّل در مخرج کسر با نمای مثبتی وجود داشته باشد، در صورت کسر با نمای کمتر ظاهر نمی‌شود. در این صورت تمام عوامل مخرج در صورت وجود خواهند داشت و حاصل عددی است صحیح. برای اثبات ادعا کافی است از نتیجه‌های قضیه ۱.۱ و نیز از قضیه لژاندر استفاده کنیم.

نتیجهٔ ۳.۱. برای تمام اعداد صحیح و نامنفی k و l، $k!l!|(k+l)!$.

برهان. این مورد حالت خاصی است از قضیه قبل. در ضمن توجه می‌کنیم که عبارت $\frac{(k+l)!}{k!l!}$ و همچنین عبارت مذکور در قضیه ۳.۱ به ترتیب ضرایب دوجمله‌ای و چندجمله‌ای و لزوماً اعداد صحیح‌اند. در این‌جا منظور آن بوده است که از استدلال ترکیبیاتی استفاده نکنیم.

نتیجهٔ ۴.۱. حاصل‌ضرب n عدد صحیح ناصفر متوالی بر $n!$ بخش‌پذیر است.

برهان. فرض کنیم $k+1, k, \cdots, k+n-1$ عدد صحیح متوالی باشند.

---

1) Legendre

عبارت

$$k(k+۱)\cdots(k+n-۱)$$

را می‌توان به صورت

$$\frac{(k+n-۱)!}{(k-۱)!}$$

نوشت. پس رابطهٔ زیر حاصل می‌شود.

$$\frac{k(k+۱)\cdots(k+n-۱)}{n!}=\frac{(k+n-۱)}{(k-۱)!n!}$$

و چون عامل $k+n-۱$ برابر مجموع عوامل n و $k-۱$ در مخرج است، بنا به قضیه ۳.۱ حاصل، عددی است صحیح، پس طرف دوم عبارت بالا عددی است صحیح، از این رو سمت چپ نیز عددی است صحیح. این دعوی، حکم قضیه را به اثبات می‌رساند.
در پایانِ این مقدمه قضیهٔ بنیادی گروه‌های آبلی متناهی ـ تولید شده را بیان می‌کنیم. از این قضیه در بخش ۴ استفاده خواهد شد.

قضیه بنیادی گروه‌های آبلی متناهی ـ تولید شده

فرض کنیم G گروه آبلی متناهی ــ تولید شده باشد. در این صورت G با مجموع مستقیم گروه‌های دوری آزاد و گروه‌های دوری که مرتبه هر یک از آن‌ها توان عددی اوّل است، یک‌ریخت است. به علاوه تعداد گروه‌های دوری آزاد، هم‌چنین اعداد اوّل و مرتبهٔ هر یک از آن‌ها ناوردا است.

۲. مقسوم‌علیه ثابت یک چندجمله‌ای با ضرایب صحیح

یکی از مواردی که تابع فاکتوریل جلوه‌گر می‌شود بزرگ‌ترین مقسوم‌علیه مشترک مجموعه مقادیری است که یک تابع چندجمله‌ای با ضرایب صحیح اختیار می‌کند.

تعریف ۱.۲. فرض کنیم f یک چندجمله‌ای با ضرایب صحیح است. مقسوم‌علیه ثابت f که آن را با $d(\mathbb{Z},f)$ نشان می‌دهیم، بزرگ‌ترین مقسوم‌علیه مشترک تمام اعداد صحیحی است که f روی $\mathbb{Z}$ اختیار می‌کند. پس

$$d(\mathbb{Z},f)=gcd\{f(a):a\in\mathbb{Z}\}$$

که در آن gcd یعنی بزرگ‌ترین مقسوم‌علیه مشترک.

مثال ۱.۲. فرض کنیم $f(x)=x^۵+x$. اگر a زوج باشد، $f(a)$ نیز زوج است و اگر a فرد باشد باز هم $f(a)$ زوج است. بنابراین لازم است که $d(\mathbb{Z},f)$ عددی زوج باشد، اما به سبب این که $f(۱)=۲$، $d(\mathbb{Z},f)=۲$. بدیهی است که اگر تمام ضرایب چندجمله‌ای در عدد طبیعی ضرب شوند، مقسوم‌علیه ثابت آن نیز در همان عدد ضرب می‌شود. بنابراین برای پاسخ به این پرسش

که $d(\mathbb{Z},f)$ چه مقادیری می‌تواند داشته باشد، کافی است که f را یک چندجمله‌ای اوّلیه در نظر بگیریم. چندجمله‌ای $p(x)$ را اوّلیه می‌نامیم اگر بزرگ‌ترین مقسوم‌علیه مشترک ضرایب آن برابر با ۱ باشد.

قضیهٔ ۱.۲. (پولیا[1]). اگر p یک چندجمله‌ای اوّلیه و از درجه k باشد، آن گاه $d(\mathbb{Z},p)$، $k!$ را می‌شمارد.

برهان. به سبب این که در بخش ۳ اثبات حالت تعمیم یافته خواهد آمد، به اثبات در این حالت خاص نخواهیم پرداخت. متذکر می‌شویم که برای هر مقسوم علیه $k!$ مانند d یک چندجمله‌ای با ضرایب صحیح و از درجه k وجود دارد که مقسوم علیه ثابت آن همان d باشد. اثبات این قسمت سهل است و به عهده خواننده گذاشته می‌شود.

۳. حلقهٔ چندجمله‌ای‌ها با مقدار صحیح

مفهوم فاکتوریل آشکارا در حلقهٔ چندجمله‌ای‌های با مقدار صحیح وجود دارد. لازم است که نخست به بیان یک تعریف بپردازیم.

تعریف ۱.۳. اگر n یک عدد صحیح نامنفی باشد قرار می‌دهیم:

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

و اگر $n=0$ قرار می‌دهیم:

$$\binom{x}{0} = 1$$

مجموعهٔ $\{\binom{x}{n}\}_{n=0}^{\infty}$ را مجموعهٔ چندجمله‌ای‌های دوجمله‌ای (برگرفته از اصطلاح ضرایب دوجمله‌ای) می‌نامیم.

قضیهٔ ۱.۳. مجموعهٔ چندجمله‌ای‌های دوجمله‌ای پایه‌ای است برای فضای برداری $\mathbb{Q}[x]$ روی Q.

برهان. ابتدا نشان می‌دهیم که $\{\binom{x}{n}\}_{n=0}^{\infty}$، $\mathbb{Q}[x]$ را تولید می‌کند. از استقرا روی درجه چندجمله‌ای استفاده می‌کنیم. فرض کنیم $f(x)=b$ که در آن b عددی گویاست، پس $f(x)=b\binom{x}{0}$ و پایه استقرا برقرار است. فرض کنیم $f(x)=a_0+a_1x+\cdots+a_nx^n$ یک چندجمله‌ای با درجه n است. اینک چندجمله‌ای $a_n n!\binom{x}{n}$ را که یک چندجمله‌ای در $\mathbb{Q}[x]$ است و ضریب x^n در آن برابر a_n می‌باشد در نظر می‌گیریم. اما درجه چندجمله‌ای $g(x)=f(x)-a_n n!\binom{x}{n}$ حداکثر $n-1$ است بنا به فرض $g(x)=\sum_i b_i\binom{x}{i}$ و از این رو $f(x)=a_n n!\binom{x}{n}+\sum_i b_i\binom{x}{i}$. اینک نشان می‌دهیم که $\{\binom{x}{n}\}_{n=0}^{\infty}$ در $\mathbb{Q}[x]$ یک مجموعهٔ مستقل خطی است. فرض کنیم $f(x)=a_0+a_1\binom{x}{1}+\cdots+a_n\binom{x}{n}$ یک ترکیب خطی دلخواه باشد. اگر $f(x)=0$، لازم است که $a_n=0$، زیرا که چندجمله‌ای با

1) Polya

نمای n فقط در $\binom{x}{n}$ موجود است. به همین دلیل و با توجه به این که $a_n = ۰$ به ترتیب به استقراء خواهیم داشت $a_{n-۱} = ۰$، $a_{n-۲} = ۰$، $\cdots$ و $a_۰ = ۰$ بنابراین تمام ضرایب صفرند.

تعریف و نمادگذاری. هر چندجمله‌ای با ضرایب گویا را که به عنوان یک تابع از $\mathbb{Z}$ به $\mathbb{Q}$ مقادیر صحیح را به مقادیر صحیح می‌نگارد یک چندجمله‌ای با مقدار صحیح می‌نامیم. مجموعه چنین چندجمله‌ای‌ها را با $Int\mathbb{Z}$ نشان می‌دهیم. پس

$$Int(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] : f(z) \in \mathbb{Z} \quad \forall z \in \mathbb{Z}\}$$

مثال ۱.۳. تمام چندجمله‌ای‌ها با ضرایب صحیح یک عضو $Int(\mathbb{Z})$ هستند.

مثال ۲.۳. اگر p عددی اوّل باشد بنا به قضیهٔ کوچک فرما چندجمله‌ای $g(x) = ۱/p(x^p - x)$، با این که ضرایب صحیح نیستند، به ازای هر عدد صحیح یک عدد صحیح است و از این رو $g(x)$ یک عضو $Int(\mathbb{Z})$ است.

لم ۱.۳. برای هر عدد صحیح $n \geq ۱$ چندجمله‌ای

$$\binom{x}{n} = \frac{x(x-۱)\cdots(x-(n+۱))}{n!}$$

یک عضو $Int(\mathbb{Z})$ است.

برهان. الف) اگر $a \geq n$، پس $\binom{a}{n}$ ضریب دوجمله‌ای است و از این رو $\binom{a}{n}$ یک عدد صحیح است.
ب) اگر $۰ \leq a \leq n-۱$، $x - a$ به موجب تعریف $\binom{x}{n}$ در صورت کسر وجود دارد پس $\binom{a}{n} = ۰$.
پ) اگر $a < ۰$ پس

$$\begin{aligned}\binom{a}{n} &= \frac{a(a-۱)\cdots(a-(n+۱))}{n!} = (-۱)^n \frac{(-a)(۱-a)\cdots(n-۱-a)}{n!} \\ &= (-۱)^n \binom{n-۱-a}{n}\end{aligned}$$

به هر حال مقدار $\binom{x}{n}$ به یکی از حالت‌های فوق منجر می‌شود و اثبات کامل است. به سادگی دیده می‌شود که $Int(Z)$ حلقه‌ای است تعویض‌پذیر و بدیهی است که

$$\mathbb{Z}[x] \subseteq Int(\mathbb{Z}) \subseteq \mathbb{Q}[x]$$

این حلقه و تعمیم‌های آن به روی یک حوزه صحیح به تفضیل مورد مطالعه قرار گرفته است. در این نوشتار به این مهم نخواهیم پرداخت. اساسی‌ترین قضیه در این‌باره قضیهٔ زیر است.

قضیهٔ ۲.۳. (پولیا). چندجمله‌ای‌های

$$\binom{x}{۰}, \binom{x}{۱}, \ldots, \binom{x}{n}, \ldots$$

یک پایه برای $Int(\mathbb{Z})$ به عنوان یک $\mathbb{Z}$ مدول است.

برهان. بدیهی است که $Int(\mathbb{Z})$ یک $\mathbb{Z}$ ـ مدول است. ابتدا نشان می‌دهیم که برای هر دنباله $b_0, b_1, \cdots, b_n$ چندجمله‌ای‌های

$$g(x) = c_0\binom{x}{0} + c_1\binom{x}{1} + \cdots + c_n\binom{x}{n}$$

با ضرایب صحیح وجود دارند که

$$g(0) = b_0, g(1) = b_1, \cdots, g(n) = b_n$$

با استقرا به اثبات این ادعا می‌پردازیم. اگر $n = 0$ قرار می‌دهیم $g(x) = b_0\binom{x}{0}$ فرض کنیم حکم قضیه برای هر دنباله با طول کوچک‌تر از n صادق باشد و $b_n, \cdots, b_1, b_0$ دنباله‌ای به طول $n+1$ باشد. بنا به فرض استقرا چندجمله‌ای $f(x) = \sum_{i=0}^{n-1} c_i\binom{x}{i}$ با ضرایب صحیح وجود دارد که

$$f(0) = b_0, f(1) = b_1, \cdots, f(n-1) = b_{n-1}$$

اینک چندجمله‌ای

$$g(x) = f(x) + (b_n - f(n))\binom{x}{n}$$

را در نظر می‌گیریم. برای $0 \leq i \leq n-1$ داریم $\binom{i}{n} = 0$ زیرا که $(x-i)$ در صورت کسر $\binom{x}{n}$ موجود است. پس برای هر $1 \leq i \leq n$، $g(i) = f(i) = b_i$ اما

$$g(n) = f(n) + (b_n - f(n)) = f(n) + b_n - f(n) = b_n$$

از این رو با قراردادن

$$g(x) = f(x) + (b_n - f(x))\binom{x}{n}$$

چندجمله‌ای مطلوب به دست می‌آید. برای تکمیل اثبات فرض می‌کنیم که $h(x)$ یک چندجمله‌ای درجه n در $Int(\mathbb{Z})$ باشد. اگر

$$h(0) = b_0, h(1) = b_1, \cdots, h(n) = b_n$$

به موجب آنچه که بیان شد چندجمله‌ای $g(x) = \sum_{i=0}^{n} c_i\binom{x}{i}$ وجود دارد به طوری که

$$g(0) = h(0) = b_0, g(1) = h(1) = b_1, \cdots, g(n) = h(n) = b_n$$

از این‌جا معلوم می‌شود که برای هر x، $h(x) = g(x)$ زیرا که درجه $g(x)$ برابر n است و در $n+1$ مقدار با $f(x)$ برابر شده است.

۴. p- ترتیب

با توجه به قضیه‌ها و مثال‌هایی که تاکنون ارائه شد، معلوم می‌شود که آن‌چه رخ داده در واقع در مجموعه $\mathbb{Z}$ یا بهتر بگوییم در حلقه اعداد صحیح $\mathbb{Z}$ بوده است. اکنون این پرسش طبیعی است که

آیا می‌توان تابع فاکتوریل را به زیرمجموعه‌های $\mathbb{Z}$ تعمیم داد؟ آیا مفهوم فاکتوریل به حلقه‌های دیگر نیز قابل تعمیم است؟ در این بخش به زیرمجموعه‌های $\mathbb{Z}$ توجه می‌کنیم.

تعریف ۱.۴. فرض کنیم X یک زیرمجموعهٔ ناتهی $\mathbb{Z}$ و p یک عدد اوّل دلخواه و ثابت باشد. یک P–ترتیب X دنباله‌ای است مانند $\{a_i\}_{i=0}^{\infty}$ که از اعضای X به استقرا انتخاب می‌شود.

- عضو a_0 را به دلخواه انتخاب می‌کنیم.
- اگر اعضای $a_0, a_1, \cdots, a_{k-1}$ در S چنان انتخاب شده باشند که بزرگ‌ترین توان p که $(a_{k-1}-a_0)(a_{k-1}-a_1)\cdots(a_{k-1}-a_{k-r})$ را می‌شمارد مینیمم باشد، a_k را چنان انتخاب می‌کنیم که بزرگ‌ترین توان p که

$$(a_k-a_0)(a_k-a_1)\cdots(a_k-a_{k-1})$$

را می‌شمارد مینیمم باشد.

نکته. بی‌گمان P–ترتیب X یکتا نیست. در واقع عضو a_0 به دلخواه انتخاب می‌شود. از طرفی هر انتخاب a_k بر انتخاب های بعدی اثر می‌گذارد.

تعریف ۲.۴. بزرگ‌ترین توان عدد اوّل p که عدد a را می‌شمارد با $w_p(a)$ نشان داده می‌شود.

توجه. $w_p(a)$ نباید با $e_p(a)$ اشتباه شود. برای مثال $e_3(18)=2$ حال آن که $w_3(18)=9$.

تعریف ۳.۴. اگر $\mathrm{X}\subseteq\mathbb{Z}$ و $\{a_i\}_{i=0}^{\infty}$ یک P–دنباله X باشد دنباله افزایشی $\{v_k(\mathrm{X},p)\}$ را که جمله kام آن با

$$v_k(X,p)=\omega_p((a_k-a_0)(a_k-a_1)\cdots(a_k-a_{k-1}))$$

تعریف می‌شود، P ـ دنباله وابسته به X و متناظر با P ـ دنباله انتخابی $\{a_i\}_{i=0}^{\infty}$ می‌نامند.
نتیجه‌ای که در تعریف فاکتوریل تعمیم یافته به کار می‌رود قضیه زیر است که در ادامه آن را اثبات خواهیم کرد.

قضیه کلیدی. P–دنباله وابسته X مستقل از انتخاب P–ترتیب است.

اولین مثال را به صورت یک قضیه بیان می‌کنیم.

قضیهٔ ۱.۴. برای هر عدد اوّل p دنباله

$$0, 1, 2, \cdots$$

یک P–ترتیب برای $\mathbb{Z}$ است.

اثبات. از استقراء ریاضی استفاده می‌کنیم. گام نخست بدیهی است. اگر $0, 1, 2, \cdots, k-1$ یک P ـ ترتیب برای گام $k-1$ باشد، در گام k ام لازم است که a_k چنان انتخاب شود که بزرگ‌ترین

توان p که

$$(*) \quad (a_k - ۰)(a_k - ۱)\cdots(a_k - (k-۱))$$

را می‌شمارد مینیمم باشد. اما $(*)$ حاصل‌ضرب k عدد صحیح متوالی است و بنا به نتیجه ۴.۱ بر $k!$ بخش‌پذیر است. اما آشکارا انتخاب $a_k = k$ بزرگ‌ترین توان p که $(*)$ را می‌شمارد مینیمم می‌کند. بنابراین گام kام را برابر k انتخاب می‌کنیم. حکم قضیه بنابر استقرا ریاضی اثبات شده است.
اکنون $v_k(\mathbb{Z},p)$ را محاسبه می‌کنیم

$$\begin{aligned} v_k(\mathbb{Z},p) &= w_p((a_k - a_۰)(a_k - a_۱)\cdots(a_k - a_{k-۱})) \\ &= w_p((k-۰)(k-۱)\cdots(k-(k-۱))) \\ &= w_p(k!) \end{aligned}$$

اما اگر برای هر p، $w_p(k)$ را در هم ضرب کنیم درست $k!$ حاصل می‌شود. بنابراین $k!$ را می‌توان بر حسب این ناورداها(با توجه به قضیه کلیدی) چنین تعریف کرد

$$k! = \prod_p v_k(\mathbb{Z},p)$$

اینک با نظر به قضیهٔ کلیدی بیان تعریف زیر موجه می‌نماید.

تعریف ۴.۴. فرض کنیم X یک زیر مجموعه ناتهی $\mathbb{Z}$ است. تابع فاکتوریل X که مقدار آن در k با $k!_X$ نشان داده می‌شود به صورت

$$k!_X = \prod_p v_k(\mathbb{Z},p)$$

تعریف می‌شود، به ویژه $k!_{\mathbb{Z}} = k!$.
می‌دانیم که مجموعهٔ اعداد اوّل مجموعه‌ای نامتناهی است، در ضرب بالا، امّا، تعداد عوامل نابرابر لزوماً متناهی‌اند. به لم زیر توجه می‌کنیم.

لم ۱.۴. فرض کنیم $\mathrm{X} \subseteq \mathbb{Z}$ و $۰ \le k < |X|$ در این صورت $v_k(X,p)$ تنها برای تعدادی متناهی عدد اوّل p برابر با ۱ نیست.

اثبات. شرط $v_k(X,p) = ۱$ برقرار است اگر و تنها اگر k عضو در X وجود داشته باشد که دو به دو، به پیمانه p ناهم‌نهشت شوند. حال برای هر k عضو متمایز X به تعداد $\binom{k}{۲}$ عضو از آن‌ها می‌توان انتخاب کرد. در تجزیه این اعداد به‌حاصل‌ضرب اعداد اوّل تعدادی متناهی عدد اوّل وجود دارد. از این‌جا معلوم می‌شود که هر k عضو در X به پیمانه p باید برای همه اعداد اوّل p مگر تعدادی متناهی متمایز باشند.
در حالت $X = \mathbb{Z}$ دیدیم که برای تمام اعداد اوّل p به طور هم‌زمان P–ترتیب

$$۰, ۱, ۲, \cdots$$

وجود دارد. به طور کلی اگر برای زیر مجموعه $X\subseteq \mathbb{Z}$ این گزاره برقرار باشد، محاسبه فاکتوریل تعمیم یافته ساده‌تر خواهد بود.

لم ۲.۴. اگر $X\subseteq \mathbb{Z}$ و $\{a_i\}_{i=0}^{\infty}$ برای هر عدد اوّل p یک P–ترتیب باشد، آن گاه

$$k!_X = |(a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})|.$$

اثبات. کافی است که به تعریف‌ها توجه کنیم.

مثال ۱.۴. فرض کنیم $X = 2\mathbb{Z}$ مجموعه اعداد زوج باشد، با استدلالی مشابه استدلال قضیهٔ ۱.۴ مشاهده می‌شود که

$$0, 2, 4, 6, \cdots$$

برای هر عدد اوّل یک P ـ ترتیب است. بنا به لم ۱.۴ مشاهده می‌شود که

$$k!_{2\mathbb{Z}} = (2k - 0)(2k - 2)\cdots(2k - (2k - 2))$$

مثال ۲.۴. اگر X مجموعه توان‌های عدد دو باشد، دنباله

$$1, 2, 4, 8, \cdots$$

برای هر عدد اوّل p یک عدد P ـ ترتیب است و از این رو بنا به لم ۱.۴

$$k!_x = (2^k - 1)(2^k - 2)\cdots(2^k - 2^{k-1})$$

مثال ۳.۴. اگر p یک عدد اوّل باشد و $X = \{1, p, 2p, p^2, p^2 + 1\}$ دنباله‌های

$$1, p, 2p, p^2, p^2 + 1$$

و

$$1, p, p^2, p^2 + 1, 2p$$

هر کدام P ـ ترتیب X هستند. p دنباله وابسته به آنها عبارتست از

$$1, p, p^2, p^2, 0, \cdots$$

تعریف ۵.۴. فرض کنیم $\mathrm{X}\subseteq\mathbb{Z}$ و $\{a_i\}_{i=0}^{\infty}$ یک P–ترتیب X باشند. چندجمله‌ای‌های S_i را به صورت

$$\begin{aligned} S_0(x) &= 1 \\ S_1(x) &= (x-a_0) \\ S_2(x) &= (x-a_0)(x-a_1) \\ &\vdots \\ S_i(x) &= (x-a_0)(x-a_1)\cdots(x-a_{i-1}) \\ &\vdots \end{aligned}$$

تعریف می‌کنیم. به سادگی دیده می‌شود که هر چندجمله‌ای با ضرایب صحیح را می‌توان در پایه $\{S_i\}$ نوشت. استفاده از این پایه اثبات بسیاری از قضیه‌ها را ساده‌تر می‌کند. ابتدا به اثبات یک لم می‌پردازیم.

لم ۳.۴. فرض کنیم $\mathrm{X}\subseteq\mathbb{Z}$ و $\{a_i\}_{i=0}^{\infty}$ یک P ـ ترتیب X باشد. هم‌چنین فرض کنیم

$$(*)\quad f(x)=b_0S_0(x)+b_1S_1(x)+\cdots+b_ks_k(x)$$

یک چندجمله‌ای با ضرایب صحیح باشد. در این صورت مقدار $f(x)$ برای هر عضو X بر p^e بخش‌پذیر است اگر و تنها اگر $b_iS_i(x)\ (1\le i\le k)$ برای هر عضو X بر p^e بخش‌پذیر باشد.

اثبات. فرض کنیم $f(x)$ برای هر عضو X بر p^e بخش‌پذیر باشد، اما جملاتی در سمت راست وجود داشته باشند که چنین نباشند. گیریم j کوچک‌ترین اندیس با این ویژگی باشد که $b_jS_j(x)$ به ازای مقادیر X بر p^e بخش‌پذیر نیست. در $(*)$ قرار می‌دهیم $x=a_j$. در این صورت تمام جملات با شرط $i<j$ متحداً صفرند. حال آن که مینیمم بودن j ایجاب می‌کند در تمام جملات با $i<j$، $b_iS_i(x)$ ضریب‌ها بر p^e بخش‌پذیر باشند. در نتیجه $b_jS_j(x)$ به ازای هر مقدار X بر p^e بخش‌پذیر است، زیرا باید توجه داشت که $\{a_i\}_{i=0}^{\infty}$ یک P–ترتیب X است. این تناقض حکم لم را ثابت می‌کند.

اینک می‌توان به بیان و اثبات قضیه‌ای که تعمیم قضیه پولیا در بخش ۲ است پرداخت.

قضیهٔ ۲.۴. فرض کنیم $\mathrm{X}\subseteq\mathbb{Z}$ و $f(x)$ یک چندجمله‌ای اولیه با ضرایب صحیح و از درجه k باشد. اگر

$$d(X,f)=gcd\{f(a):a\in X\}$$

آن گاه $d(X,f)$، $k!_X$ را می‌شمارد.

اثبات. برای یک P–ترتیب ثابت X مانند $\{a_i\}_{i=0}^{\infty}$، f را به شکل زیر می‌نویسیم

$$f(x)=b_0S_0(x)+b_1S_1(x)+\cdots+b_ks_k(x)$$

از آن‌جا که $f(x)$ اولیّه است. اندیس $0 \leq j \leq k$ وجود دارد که b_j بر p بخش‌پذیر نیست. اینک بنا به تعریف $d(X,f)$ مقدار $f(x)$ به ازای مقادیر X بر $w_p(d(X,f))$ بخش‌پذیر است. بنا به لم قبل $b_jS_j(x)$ بر $w_p(d(X,f))$ بخش‌پذیر است. از طرفی چون b_j و p متباین‌اند، نتیجه می‌گیریم که $S_j(x)$ به ازای هر عضو X بر $w_p(d(X,f))$ بخش‌پذیر است. به ویژه $w_p(d(X,f))$ مقدار

$$w_p(S_j(a_j)) = w_p((a_j - a_0)(a_j - a_1)\cdots(a_j - a_{j-1})) = w_p(j!_X)$$

را می‌شمارد. بنابراین $w_p(d(X,f))$، $w_p(k!_X)$ را می‌شمارد، زیرا که $j!_X$، $k!_X$ را می‌شمارد. با در نظر گرفتن تمام اعداد اوّل که با توان غیر صفر در $k!_X$ ظاهر می‌شوند و ضرب آنها نتیجه می‌گیریم که $d(X,f)$، $k!_X$ را می‌شمارد.

نکته: در قضیه ۲.۴ $k!_X$ و هر مقسوم‌علیه آن می‌تواند مقسوم‌علیه $d(X,f)$ باشد. برای اثبات این ادعا کافی است چندجمله‌ای

$$F(x) = (x - a_{0,k})(x - a_{1,k})\cdots(x - a_{k-1,k})$$

که در آن $\{a_{i,k}\}_{i=0}^{\infty}$ دنباله‌ای در $\mathbb{Z}$ است که برای هر عدد اوّل p که $k!_X$ را می‌شمارد، جمله به جمله به پیمانه $v_k(X,p)$ با یک P–ترتیب X هم‌نهشت است. در این صورت آشکار است که $d(X,F) = k!_X$. به علاوه اگر r یک مقسوم‌علیه $k!_X$ باشد، آن گاه $d(X,F(x+r)) = r$. بنابراین هر عامل $k!_X$ می‌تواند به عنوان مقسوم‌علیه ثابت یک چندجمله‌ای اوّلیه قابل حصول باشد.

نتیجهٔ ۱.۴. اگر k و l اعدادصحیح نامنفی باشند، آن گاه برای $X \subseteq \mathbb{Z}$، $k!_X l!_X | (k+l)!_X$.

اثبات. چندجمله‌ای‌های اوّلیه $F_k(x)$ و $F_{n-k}(x)$ را در نظر می‌گیریم به طوری که $d(X,F_k) = k!_X$ و $d(X,F_{n-1}) = (n-k)!_X$. با ضرب این دو چندجمله‌ای چندجمله‌ای اولیه $F = F_kF_{n-k}$ با درجه n به دست می‌آید، به طوری که $d(X,F)$، $k!_X(n-k)!_X$ را می‌شمارد. اما باز هم بنا به قضیه قبل می‌دانیم که $d(X,F)$ باید $n!_X$ را بشمارد پس $k!_X(n-k)!_X | n!_X$.

لم ۴.۴. اگر $X \subseteq Y$، آن گاه $k!_X | k!_Y$.

اثبات. برای هر چندجمله‌ای f به وضوح $d(X,f)$، $d(X,F)$ را می‌شمارد. از این رو به ویژه $d(X,F) = k!_X$، $d(Y,F)$ را می‌شمارد. اما بنا به قضیه ۲.۴، $d(X,F)$ باید $k!_X$ را بشمارد. از این‌جا معلوم می‌شود که $k!_X | k!_Y$.

قضیهٔ ۳.۴. اگر $X \subseteq \mathbb{Z}$ و $\{a_0, a_1, \cdots, a_n\} \subseteq X$ آن گاه

$$a_1!_X a_2!_X \cdots a_n!_X \Big| \prod_{i<j}(a_i - a_j)$$

اثبات. فرض کنیم p یک عدد اوّل ثابت باشد. مجموعه $\{a_0, a_1, \cdots, a_n\}$ را Y می‌نامیم. پس

$Y \subseteq X$ و برای هر $0 \leq k \leq n$

$$v_k(y,p) = w_p((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1}))$$

با ضرب تمام روی kها و سپس روی تمام p ها داریم:

$$a_0!_Y a_1!_Y \cdots a_n!_Y \prod_{i<j}(a_j - a_i)$$

اینک بنا به لم قبل $k!_X$، $k!_Y$ را می‌شمارد. بنابراین

$$a_0!_Y a_1!_Y \cdots a_n!_Y \prod_{i<j}(a_i - a_j)$$

می‌دانیم هر چندجمله‌ای با ضرایب صحیح یک تابع که آن را تابع چندجمله‌ای می‌نامیم از $\mathbb{Z}$ به $\mathbb{Z}/n\mathbb{Z}$ به وجود می‌آورد. اما هر تابع لزوماً از این طریق به دست نمی‌آید. می‌توان نشان داد که تعداد توابع چندجمله‌ای از $\mathbb{Z}$ به $\mathbb{Z}/n\mathbb{Z}$ برابر است با

$$\prod_{k=0}^{n-1} \frac{n}{gcd(n,k!)}$$

در حالت خاصی که در آن n یک عدد اوّل باشد مقدار فوق برابر خواهد بود با n^n که از آن نتیجه می‌شود، هر تابع از $\mathbb{Z}/n\mathbb{Z}$ به $\mathbb{Z}/n\mathbb{Z}$ یک تابع چندجمله‌ای است. قضیه بعد تعمیم بیشتر قضیه فوق به هر زیر مجموعه $\mathbb{Z}$ است.

قضیهٔ ۴.۴. فرض کنیم $X \subseteq \mathbb{Z}$ در این صورت تعداد توابع چندجمله‌ای از X به $\mathbb{Z}/n\mathbb{Z}$ برابر است با

$$\prod_{k=0}^{n-1} \frac{n}{gcd(n,k!_X)}$$

اثبات. طریقه اثبات کم و بیش مانند اثبات قضیه‌های قبل است. در این‌جا کافی است حالتی را در نظر بگیریم که n توانی از یک عدد اوّل است و آن گاه از قضیه باقی‌مانده چینی استفاده کنیم. در اینجا از بیان جزئیات خودداری می‌کنیم.

قضیهٔ ۵.۴. (تعمیم قضیهٔ پولیا برای حلقه‌های چندجمله‌ای با مقادیر صحیح). اگر $X \subseteq \mathbb{Z}$ و قرار دهیم

$$Int(X,\mathbb{Z}) = \{f(x) \in \mathbb{Q}(x) : f(x) \in \mathbb{Z}, \forall x \in X\}$$

آن گاه $Int(X,\mathbb{Z})$ یک زیر حلقه $Q[x]$ است که به عنوان یک $\mathbb{Z}$ ـ مدول با چندجمله‌ای‌های

$$\frac{S_k(x)}{k!_X}$$

به‌وجود می‌آید. $S_k(x)$ همان چندجمله‌ای‌هایی هستند که پیشتر تعریف شده‌اند.

اثبات. طریقه اثبات مانند همان قضیه اصلی پولیاست.
همان گونه که ممکن است خواننده تاکنون متوجه شده باشد اثبات قضیه‌های بیان شده به P–ترتیب انتخابی بستگی نداشته است. با این حال در این‌جا به اثبات قضیه کلیدی در مورد تابع فاکتوریل تعمیم یافته می‌پردازیم.

قضیه کلیدی P ـ دنباله وابسته X مستقل از انتخاب P ـ ترتیب است.

اثبات. فرض کنیم $\{a_i\}_{i=0}^{\infty}$ و $\{a'_i\}_{i=0}^{\infty}$ دو P ـ ترتیب متمایز X باشند، P–دنباله‌های وابسته و متناظر با آنها را به ترتیب با $v_k(X,p)$ و $v'_k(X,p)$ نشان می‌دهیم. ثابت خواهیم کرد که برای هر $d \geq 0$،

$$v_d(X,p) = v'_d(X,p)$$

. اگر X متناهی باشد و $d \geq |X|$، اثبات بدیهی است، پس حالت $d < |X|$ را در نظر می‌گیریم.
عدد صحیح و مثبت e را چنان انتخاب می‌کنیم که $p^e > v_d(X,p)$ و هم‌چنین $p^e > v'_d(X,p)$.
مجموعه چند جمله ای ها در $(Z/p^e\mathbb{Z})[X]$ را که به ازای مقادیر X، مقدارشان بر p^e بخش‌پذیر است با G_d نشان می‌دهیم. اینک از لم ۲.۴ می‌توان نتیجه گرفت که گروه آبلی G_d با

$$\bigoplus_{k=0}^{d} \frac{\mathbb{Z}}{v_k(X,p)\mathbb{Z}}$$

و هم‌چنین

$$\bigoplus_{k=0}^{d} \frac{\mathbb{Z}}{v'_k(X,p)\mathbb{Z}}$$

یک‌ریخت است. بنابراین اعداد $v_k(X,p)$ و $v'_k(X,p)$ (برای $0 \leq k \leq d$) که ضرایب ساختاری گرو آبلی G_d هستند بنا به قضیه بنیادی گروه های آبلی متناهی تولید شده باید برابر باشند، به ویژه $v_d(X,p) = v'_d(X,p)$ و اثبات تمام است.

۵. تعمیم‌های بیشتر به حوزه‌های ددکیند

یادآوری می‌کنیم که در حوزه‌های ددکیند R هر ایدال به صورت یکتایی به حاصل‌ضرب اعداد اوّل تجزیه می‌شود. با توجه به این ویژگی می‌توان مفهوم فاکتوریل را به حوزه های ددکیند و حتی هر زیر مجموعه آن تعمیم داد. تفاوت عمده در آنست که به هنگام ساختن P–ترتیب که P یک ایدال اوّل است فاکتوریل‌های به دست آمده را باید ایدال‌های R در نظر گرفت. در حالتی که R یک حوزهٔ ایدال‌های اصلی باشد، می‌توان مانند حلقه $\mathbb{Z}$ عمل کرد. وجود یک P–ترتیبِ همزمان برای

تمام ایدال‌های اوّل شرطی لازم برای یافتن ایدال‌های فاکتوریل است. به طور کلی، الگوریتم ساختن P–دنباله‌ها شناخته شده نیست.

طرح بعضی مسائل

۱– اگر $X \subseteq \mathbb{Z}$، تعبیر ترکیباتی $k!_X$ چیست؟

۲– اگر قرار دهیم

$$\binom{n}{k}_X = \frac{n!}{k!_X (n-k)!_X}$$

تعبیر ترکیباتی $\binom{n}{k}_X$ چیست؟

۳– چگونه می‌توان تعمیمی از $k!_X$، نظیر تابع گامای معمولی به دست آورد؟

۴– با توجه به این که $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ تعبیر فاکتوریل تعمیم‌یافته در این مورد چیست؟

به طور کلی هر گونه قضیه یا رابطه‌ای را که در مورد تابع فاکتوریل روی $\mathbb{Z}$ وجود دارد می‌توان مورد پرسش قرار داد.

مراجع

[1] M. Bhargava, P-ording and polynomial functions on arbitrary subset of Dedekind rings, J. reine angew. Math. 490(1997) 101-127.

[2] M. Bhargava, Generlized factorial and fixed divisior over subset of Dedekind domain, J. Number theory 72(1998)67-75.

[3] M. Bhargava, The factorial function and generalizations. Amer. Math. Monthly, 107(2000)783-798.

[4] J.L. Chabert, S. T. Chapman and W.W. Smith, A basis for the ring of polynomials integer-valued on prime numbers,in factorization in integral domains, Marcel Deker lecture Notes in pure and App. Math,189, New York, 1997.pp 271-284.

[5] G. Polya, Uber ganzwertige gang Functionen, Rend. Circ. Mathem. Polermo 40(1915)1-16.

[6] G. Polya, Uber ganzwertige polynome in algebraische Zahlkorpern, J, reine angew. Math. 149(1919) 117-124.

[7] B. Sury, An integral polynomial, Math. Mag, 68(1995)134-135.

[8] M. Wood, P-ordering: a metric viewpoint and the non-existence of similtaneous orderings. J. Number theory 99(2003) 36-56.

منصور معتمدی
دانشگاه شهید چمران اهواز، دانشکدهٔ ریاضی و کامپیوتر
آدرس الکترونیکی motamedi_m@scu.ac.ir