

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

ریاضیات گسسته

دوره پیش دانشگاهی

رشته علوم ریاضی

۱۳۹۳

SHANNON.IR

وزارت آموزش و پرورش
سازمان پژوهش و برنامه‌ریزی آموزشی

برنامه ریزی محتوا و نظارت بر تألیف : دفتر تألیف کتاب های درسی ابتدایی و متوسطه نظری

نام کتاب : ریاضیات گسسته - ۲۹۶/۱

شورای برنامه ریزی : یحیی تابش، محمّدحسن بیژن‌زاده، امیرنادر، حمیده داریوش همدانی و

جواد حاجی بابائی

مؤلفان : مهدی بهزاد، علی رجالی، علی عمیدی و عبداللّه محمودیان

ویراستار : علی عمیدی

آماده‌سازی و نظارت بر چاپ و توزیع : اداره کل نظارت بر نشر و توزیع مواد آموزشی

تهران : خیابان ایرانشهر شمالی - ساختمان شماره ۴ آموزش و پرورش (شهید موسوی)

تلفن : ۹-۸۸۸۳۱۱۶۱، دورنگار : ۸۸۳۰۹۲۶۶، کدپستی : ۱۵۸۴۷۴۷۳۵۹

وبسایت : www.chap.sch.ir

صفحه‌آرا : فائزه محسن شیرازی

طراح جلد : علیرضا رضائی کُر

ناشر : شرکت چاپ و نشر کتاب‌های درسی ایران - تهران - کیلومتر ۱۷ جاده مخصوص کرج - خیابان ۶۱ (داروپخش)

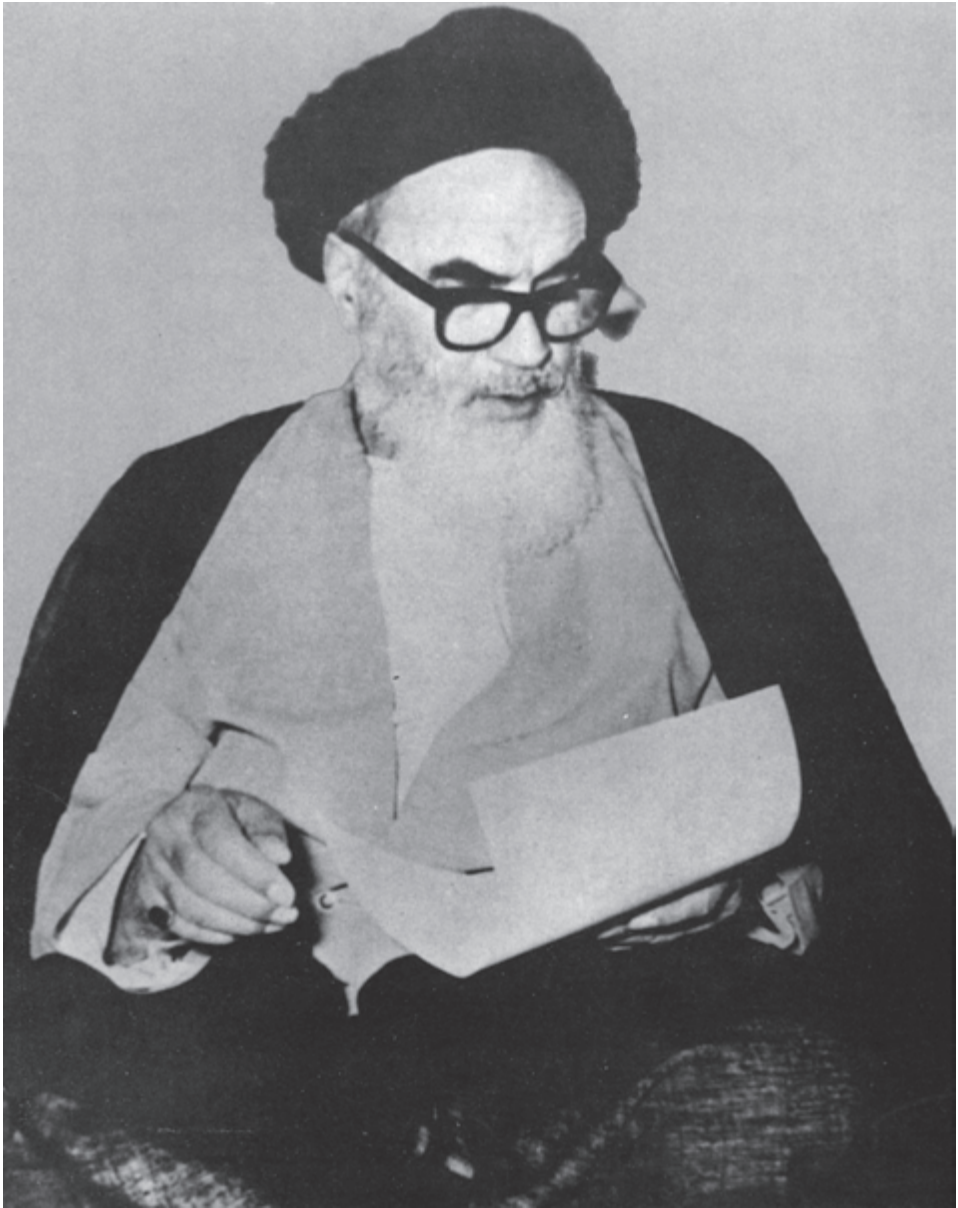
تلفن : ۵-۴۴۹۸۵۱۶۱، دورنگار : ۴۴۹۸۵۱۶۰، صندوق پستی : ۱۳۹-۳۷۵۱۵

چاپخانه : شرکت چاپ و نشر کتاب‌های درسی ایران «سهامی خاص»

سال انتشار و نوبت چاپ : چاپ بیستم ۱۳۹۳

حق چاپ محفوظ است.

شابک ۹۶۴-۰۵-۰۱۰۳-۴ ISBN 964-05-0103-4



اگر شما دیدید که غربی‌ها در صنعت پیشرفتی دارند، اشتباه نشود، خیال نکنید
که در فرهنگ هم پیشرفت دارند. جوانان ما، دانشمندان ما، اساتید دانشگاه‌های ما از
غرب ترسند، اراده کنند در مقابل غرب، قیام کنند و نترسند...

امام خمینی

فهرست مطالب

۱	قسمت اول : گراف‌ها و کاربردهای آن
۲	فصل ۱- آشنایی با گراف‌ها
۱۰	فصل ۲- چند ویژگی ساده و چند رده‌ی خاص گراف‌ها
۱۷	فصل ۳- درخت و ماتریس
۲۴	قسمت دوم : نظریه‌ی اعداد
۲۵	فصل ۴- کلیات و تقسیم‌پذیری
۳۸	فصل ۵- اعداد اول
۴۸	فصل ۶- همنهشتی
۵۷	قسمت سوم : مباحثی دیگر از ترکیبیات
۵۸	فصل ۷- مدل‌های شهودی و تجسمی در ترکیبیات
۷۵	قسمت چهارم : احتمال
۷۶	فصل ۸- احتمال
۹۴	فصل ۹- توزیع‌های گسسته‌ی احتمال

معلمان محترم، صاحب نظران، دانش آموزان عزیز و اولیای آنان می توانند نظر اصلاحی خود را در باره مطالب
این کتاب از طریق نامه به نشانی تهران - صندوق پستی ۱۵۸۵۵/۴۶۴ - گروه دسی مربوط و یا پیام نگار (Email)
talif@talif.sch.ir ارسال نمایند.

دفترتالیف کتاب های دسی ابتدایی و متوسط نظری

پیشگفتار

در سال‌های اخیر به دلیل پیشرفت علوم و تکنولوژی به‌ویژه علوم کامپیوتر، نه تنها به درس‌هایی چون حسابان (حساب دیفرانسیل و انتگرال) که در حیطه‌ی ریاضیات پیوسته قرار دارد توجه می‌شود، بلکه درس‌ها و کتاب‌های بسیاری تحت عنوانی چون «ریاضیات گسسته»، «ترکیبیات» و «ریاضیات متناهی» ارائه شده‌اند نیز مورد توجه قرار دارند. اغلب این درس‌ها و کتاب‌ها که با مجموعه‌های متناهی و گاه با مجموعه‌های شمارا سروکار دارند، گراف‌ها، روش‌های شمارشی، ساختارهای ترکیبیاتی، مباحثی از نظریه‌ی اعداد و احتمال و کاربردهایی چون کدگذاری و رمزنگاری را شامل‌اند. وجه اشتراک تقریباً همه‌ی این زمینه‌ها گسسته بودن طبیعت مباحث تحت بررسی است که در آن‌ها مفاهیمی چون حد و پیوستگی معمولی کمتر مطرح‌اند، ولی به ابزارهای کارآمد و فوق‌العاده زیبای دیگری مجهزند. پویایی و وجود مسائل فراوان حل نشده و ظاهراً ساده از مشخصات دیگر این شاخه‌اند. به‌طورکلی این شاخه امروزه سهم بزرگی در انجام برخی از پژوهش‌های علمی دارد و با توجه به گستردگی زمینه‌های کاربردی آن مورد توجه بسیاری از دانش‌پژوهان است. به این دلایل و به دلیل زیبایی و قدرتی که ریاضیات گسسته در پرورش تفکر ریاضی افراد دارد مدتی است که آموزش مبانی آن در برنامه‌های درسی دوره‌ی متوسطه بسیاری از کشورها آغاز شده است و محققاً در ایران نیز تدریس آن در دوره‌ی پیش‌دانشگاهی لازم است. در این کتاب مؤلفان مطالبی را که جنبه‌ی پایه‌ای و عمومی داشته و صرفاً طبیعتی گسسته دارند مطرح کرده و با ارائه مثال‌های فراوان به روشن شدن مفاهیم افزوده‌اند. برخی از اطلاعات اضافی نیز که جزء برنامه‌ی درسی نیستند به صورت مجله‌ی ریاضی آمده‌اند.

توجه دبیران محترم را به این نکته جلب می‌کند که چون دانش‌آموز دوره‌ی پیش‌دانشگاهی باید خود با مطالعه‌ی شخصی به حل تمرین‌ها و درک مطالب فرعی بپردازد و نیز به دلیل کمی وقت تدریس، نباید انتظار داشت که همه‌ی تمرین‌ها در کلاس مطرح شوند؛ حل یک مسأله از هر نوع کافی است.

در پایان متذکر می‌شویم که مؤلفان پیشنهادها و نظرهای مفید را با تشکر پذیرا هستند و از همه‌ی استادان، دبیران و دانشجویان به ویژه شرکت‌کنندگان در دوره‌های آموزشی این درس که در تکمیل پیش‌نویس کتاب راهنمای ما بوده‌اند صمیمانه قدردانی می‌کنند.

قسمت اول

گراف‌ها و کاربردهای آن

مقدمه

در این قسمت که شامل سه فصل است با الفبای نظریه‌ی گراف‌ها و کاربردهایش آشنا می‌شویم. عمده‌تاً از طبیعت جذاب گراف‌ها استفاده می‌کنیم، شهود را به کار می‌بندیم و با مثال‌های ملموس و معماهای گوناگون مفاهیم را روشن می‌سازیم. در عین حال در بست تسلیم شهود نمی‌شویم و در مواردی اثبات دقیق قضایا را ارائه می‌دهیم. گاه از کاربردهایی استفاده می‌کنیم که ممکن است تاحدی بدیهی به نظر برسند، اما هرگز معماها و مسائل ظاهراً کوچک را که انگیزه بخش‌اند دست کم نمی‌گیریم، زیرا در موارد بسیاری این‌گونه مسائل سرآغاز ایده‌ها و حتی نظریه‌های مهم ریاضی بوده‌اند. از دانش‌پژوهانی که دوره‌ی دبیرستان را پشت سر گذاشته‌اند انتظار داریم ذهن پویای خود را به کار اندازند و برای پاسخگویی به سؤال‌های عدیده‌ای که خود طرح می‌کنند، با پرسش‌هایی که در متن مطرح می‌شوند ابتدا مثال‌های ساده و بعد رده‌های خاص گراف‌ها را مورد توجه قرار دهند و مطمئن باشند که در این زمینه می‌توانند مسائلی را مطرح کنند که در عین سادگی بیان، بزرگ‌ترین ریاضیدانان نیز از حل آن‌ها عاجز باشند.

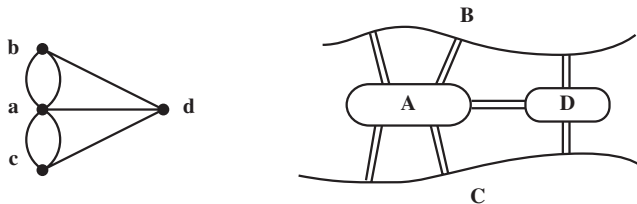
فصل ۱

آشنایی با گراف‌ها

در این فصل با بیان چند مثال زمینه را برای تعریف انواع گراف‌ها آماده می‌کنیم و آن را با ارائه‌ی چند تعریف و قرارداد پایان می‌دهیم.

۱-۱- چند مثال

در قرن هیجدهم میلادی شهر کونیگسبرگ از دو ساحل یک رودخانه و دو جزیره تشکیل شده بود. در آن زمان هفت پل این چهار منطقه را به هم وصل می‌کردند. معمّای زیر سال‌ها شهروندان را سرگرم کرده بود: آیا امکان دارد با آغاز از یکی از این مناطق در شهر گشتی زد، از هر پل یک بار و تنها یک بار گذشت، و به مکان اول بازگشت؟ اوایل در سال ۱۷۳۶ با حل مسأله‌ی پل‌های کونیگسبرگ نظریه‌ی گراف‌ها را بنیان گذاشت. وی به هر یک از این چهار منطقه نقطه‌ای از صفحه را تخصیص داد و به ازای هر پل بین دو منطقه، پاره خط یا کمانی بین دو نقطه‌ی متناظر با آن‌ها رسم کرد. بدین ترتیب مطابق شکل ۱ به مدلی ریاضی دست یافت و به سادگی پاسخ معما را که منفی است دریافت.



شکل ۱- نمای شهر کونیگسبرگ و گراف مربوط به آن

امروزه این مدل را یک گراف یا، به سبب وجود «چند» به اصطلاح خط بین دو نقطه، به‌طور دقیق‌تر یک گراف چندگانه می‌نامند. اینک ما هم می‌توانیم مسائل مختلفی را به زبان نظریه‌ی گراف‌ها

بیان کنیم.

مثال ۱: فرض می‌کنیم پنج تیم به نام‌های a, b, c, d و e باید دو به دو با یکدیگر مسابقه بدهند. پس از چندی می‌بینیم که:

a با b, c و e مسابقه داده (و بر همگی پیروز شده است).

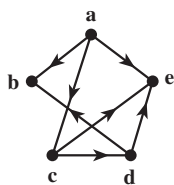
b با a و d روبه‌رو شده (و از هر دو شکست خورده است).

c با a, b, d و e مسابقه داده (بر d و e پیروز شده و از a شکست خورده است).

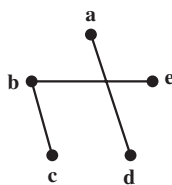
d با b, c و e بازی کرده (و b و e را شکست داده و از c شکست خورده است).

e با a, b, c و d مسابقه داده است (پیروزی‌ها و شکست‌های e قبلاً مشخص شده‌اند).

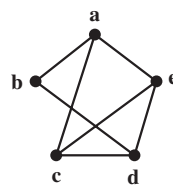
این وضعیت را می‌توانیم به صورت یک نمودار در صفحه مشخص کنیم. به ازای هر تیم یک نقطه در نظر می‌گیریم و دو نقطه را با پاره‌خط یا کماتی به هم وصل می‌کنیم هرگاه تیم‌های متناظر با هم مسابقه داده باشند. شکل ۲ مدل مربوط به این وضعیت را نشان می‌دهد.



شکل ۴



شکل ۳



شکل ۲

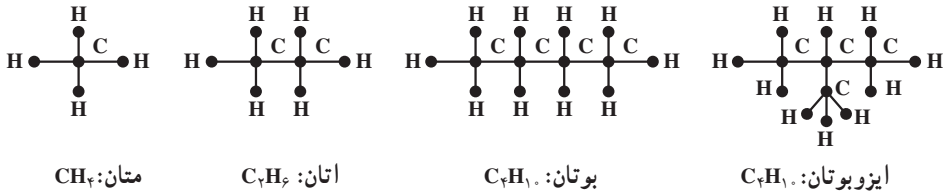
سه شکل مربوط به مثال ۱

ممکن است به این وضعیت نمودار دیگری هم نسبت داد و آن نمودار مربوط به مسابقات انجام نشده است. برای این کار باز هم به ازای هر تیم یک نقطه در نظر می‌گیریم و این بار دو نقطه را با پاره‌خطی به هم وصل می‌کنیم هرگاه دو تیم مربوط با هم بازی نکرده باشند. نمودار مربوط به این وضعیت که در شکل ۳ نمایش داده شده است نشان می‌دهد که برای تکمیل این دور از مسابقات سه مسابقه دیگر باید برگزار شوند.

فرض می‌کنیم که این مسابقات حتماً باید برنده هم داشته باشند. (برندگان را قبلاً مشخص کرده‌ایم). لذا می‌توانیم هنگام رسم شکل ۲ به جای مثلاً پاره‌خط، پاره‌خطی جهت‌دار رسم کنیم که جهت آن از برنده به سوی بازنده باشد. با این ترتیب شکل ۴ به دست می‌آید. این گراف نشان می‌دهد

که مثلاً تیم e از سه تیم a، c و d شکست خورده و هنوز برنده نشده است. چنین گرافی را گراف جهت‌دار می‌نامیم.

مثال ۲: در درس شیمی دیده‌ایم که به هیدروکربن‌های اشباع شده نمودارهایی نسبت می‌دهند تا ساختار شیمیایی آن‌ها را به نمایش بگذارند. در شکل ۵ چند نمونه از این هیدروکربن‌ها را که فرمول عمومی آن‌ها C_nH_{2n+2} است می‌بینید.



شکل ۵- چند نمونه از هیدروکربن‌ها

مثلاً نمودار مربوط به اتان که چگونگی پیوند کربن‌ها و هیدروژن‌ها را نشان می‌دهد ظرفیت کربن و هیدروژن را نیز مشخص می‌کند. در شکل ۵ می‌بینیم که با چهار کربن و ده هیدروژن دو هیدروکربن اشباع شده‌ی «مختلف» وجود دارند. بیش از دو تا چی؟ طبیعتاً پاسخ به این سؤال برای n‌های بزرگتر از ۴ آسان نیست.

مثال ۳: شرکتی مایل است برای چهار شغل تمام وقت A_1 ، A_2 ، A_3 و A_4 کارمند استخدام کند. پنج نفر به نام‌های B_1 ، B_2 ، B_3 ، B_4 و B_5 برای تصدی این شغل‌ها داوطلب می‌شوند که طبق فهرست زیر برخی صلاحیت تصدی بیش از یک کار را دارند:

B_1 می‌تواند سه شغل A_1 ، A_2 و A_3 را اداره کند.

B_2 می‌تواند دو شغل A_3 و A_4 را ببیند.

B_3 قادر است هر یک از شغل‌های A_2 ، A_3 و A_4 را انجام دهد.

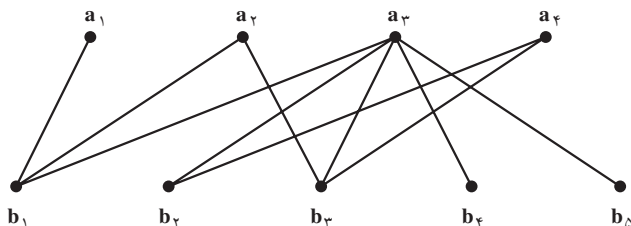
B_4 و B_5 هم می‌توانند تنها متصدی شغل A_3 باشند.

آیا با این پنج نفر، شرکت می‌تواند برای پست‌های خالی متصدی پیدا کند؟ این مسأله چند

جواب دارد؟

برای بررسی این وضعیت باز هم یک مدل می‌سازیم. به این صورت که در صفحه، چهار نقطه متناظر با چهار شغل موردنظر و پنج نقطه‌ی دیگر متناظر با پنج داوطلب مذکور در نظر می‌گیریم و

مطابق شکل ۶ هر نقطه‌ی b_i ، $1 \leq i \leq 5$ ، را با پاره‌خط یا پاره‌خط‌هایی به نقاطی چون a_j ، $1 \leq j \leq 4$ ، در صورتی وصل می‌کنیم که داوطلب B_i که با نقطه‌ی b_i در تناظر است صلاحیت انجام شغل A_j را که با نقطه‌ی a_j در تناظر است داشته باشد.



شکل ۶- گراف مربوط به مثال ۳

واضح است که برای تصدی A_1 تنها یک داوطلب وجود دارد و لذا این شغل به B_1 تخصیص داده می‌شود. حال تنها B_3 برای تصدی A_2 باقی می‌ماند. چون B_3 و B_4 تنها داوطلبان احراز پست A_4 هستند و B_3 قبلاً به کار A_2 گماشته شده است، A_4 باید الزاماً به B_4 سپرده شود. حال برای تصدی A_3 دو داوطلب باقی می‌مانند: B_5 و B_4 . پس این مسئله تنها دو جواب دارد و شرکت مجبور است B_1 را به کار A_1 ، B_3 را به کار A_2 ، B_4 را به کار A_4 و B_5 یا B_4 را به کار A_3 بگمارد.

Δ

۱-۲- چند تعریف و قرارداد

در زندگی پیچیده‌ی امروزی به مسائل فراوانی برمی‌خوریم که برای حل آن‌ها مجبوریم از مدلی ریاضی مانند گراف استفاده کنیم. لذا لازم است این وضعیت‌ها را به صورت مجرد درآوریم و با الهام گرفتن از همین مسائل به بررسی ویژگی‌های این مجردات بپردازیم. نظریه‌ی گراف‌ها به همین ترتیب به وجود آمده و به سرعت در حال رشد و شکوفایی است.

همان‌گونه که دیدیم گراف‌ها انواع گوناگون دارند. مثلاً برخی جهت‌دار و برخی چندگانه‌اند. برخی هم نامتناهی‌اند، به این معنا که بی‌نهایت نقطه یا بی‌نهایت خط دارند. اینک در بین انواع گراف‌ها تعریف رسمی ساده‌ترین نوع را ارائه می‌کنیم. در این قسمت تقریباً همه جا سروکار ما با همین گراف‌های (ساده) است.

تعریف: گراف (ساده‌ی) G زوجی مرتب چون (V, E) است که در آن V مجموعه‌ای متناهی و ناتهی است و E زیرمجموعه‌ای از مجموعه‌ی تمام زیرمجموعه‌های دو عضوی V است. اعضای V را رأس‌های G و اعضای E را یال‌های G می‌نامیم. مجموعه‌ی رأس‌های G را با $V(G)$ و مجموعه‌ی یال‌های آن را با $E(G)$ هم نمایش می‌دهیم.

به یاد داشته باشید که هر عضو یک مجموعه تنها یک بار در آن ظاهر می‌شود. مثلاً نمی‌نویسیم $\{a, a, a, b, b\}$ بلکه می‌نویسیم $\{a, b\}$.

مثال ۴: اگر $V = \{a, b, c, d, e\}$ و $E = \{\{a, d\}, \{b, c\}, \{b, e\}\}$ آن‌گاه بنا به تعریف،

$G = (V, E)$ گرافی است که پنج رأس و سه یال دارد. Δ

قرار داد: اگر در گراف G ، $u, v \in V(G)$ و $\{u, v\} \in E(G)$ ، برای سادگی، به جای $\{u, v\}$ می‌نویسیم uv و می‌گوییم در G دو رأس u و v مجاورند. در این صورت گاهی گفته می‌شود رأس u (همچنین رأس v) بر یال uv واقع است. اصطلاح رایج دیگر این است که در G یال uv از رأس u (همچنین از رأس v) می‌گذرد یا مرور می‌کند. رأس‌های u و v دو سر یال uv نام دارند.

مثال ۵: اگر $V = \{a, b, c, d, e\}$ و $E = \{ab, ac, ae, bd, cd, ce, de\}$ آن‌گاه بنا به تعریف،

$G = (V, E)$ گرافی است که پنج رأس و هفت یال دارد. در این گراف مثلاً دو رأس a و b مجاورند زیرا $ab \in E$ ولی دو رأس b و e مجاور نیستند، زیرا $be \notin E$. واضح است که در این گراف از رأس a سه یال و از رأس b دو یال می‌گذرد. Δ

توجه دارید که هر گراف را می‌توان با یک نمودار، موسوم به نمودار گراف، نیز نمایش داد. برای این کار به ازای هر رأس G نقطه یا دایره‌ی کوچک دلخواهی، مثلاً در صفحه، در نظر می‌گیریم و دو نقطه‌ی متمایز را با پاره خط یا کمائی به هم وصل می‌کنیم به شرطی که مجموعه‌ی متشکل از دو رأس متناظر با آن دو نقطه عضوی از E باشد. یک نمودار گراف مثال ۴ را در شکل ۳ و یک نمودار گراف مثال ۵ را در شکل ۲ نمایش داده‌ایم. شکل ۶ نموداری از گراف $G = (V, E)$ را نمایش می‌دهد که در آن:

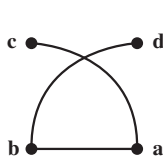
$$V = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, b_5\}$$

$$E = \{a_1b_1, a_2b_1, a_2b_3, a_3b_1, a_3b_2, a_3b_3, a_3b_4, a_3b_5, a_4b_2, a_4b_3\}$$

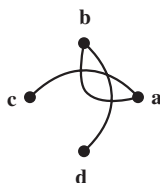
در این گراف از رأس a_3 پنج یال مرور می‌کنند؛ ولی از هر یک از دو رأس a_1 و b_5 تنها یک

یال می‌گذرد.

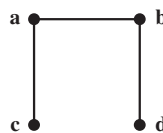
مثال ۶: اگر $V(G) = \{a, b, c, d\}$ و $E(G) = \{ab, ac, bd\}$ آن گاه G گرافی است که چهار رأس و سه یال دارد. سه نمودار از این گراف را در شکل‌های زیر رسم کرده‌ایم.



شکل ۹



شکل ۸



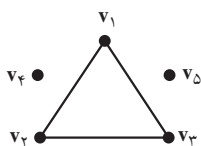
شکل ۷

سه نمودار مربوط به گراف مثال ۶

واضح است که در شکل‌های ۸ و ۹ نقطه‌ی برخورد کمان‌های ac و bd متناظر با هیچ رأس این گراف نیست.

برای راحتی گاهی نمودار گراف را با خود آن یکی می‌گیریم و به همین دلیل رأس را نقطه و یال را خط هم می‌نامیم. توجه دارید که نمودار گراف برای درک بهتر مطلب رسم می‌شود و باید حتی‌الامکان ساده باشد.

مثال ۷: فرض کنید گراف G با $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$ و $E(G) = \{v_1v_2, v_1v_3, v_2v_3\}$ داده شده است. آن گاه G پنج رأس و سه یال دارد. در این گراف مثلاً رأس v_4 با هیچ رأس دیگر مجاور نیست. نمودار G به صورت زیر است که سه «بخش جدا از هم» دارد.



شکل ۱۰- گراف مربوط به مثال ۷

مثال ۸: گراف مربوط به بوتان که در شکل ۵ رسم شده است ۱۴ رأس و ۱۳ یال دارد. این گراف تنها یک «بخش» دارد و در آن مثلاً رأسی وجود دارد که دقیقاً با چهار رأس دیگر مجاور است ولی به طور مثال رأسی وجود ندارد که دقیقاً با سه رأس دیگر مجاور باشد.

توجه کنید که اگر در تعریف گراف (ساده‌ی) G تغییر کوچکی بدهیم تعریف گراف جهت‌دار به دست می‌آید که کاربردهای فراوان دارد.

تعریف: گراف جهت‌دار G زوجی مرتب چون (V, E) است که در آن V مجموعه‌ای متناهی و ناتهی است و E زیرمجموعه‌ای از مجموعه‌ی تمام زوج‌های مرتب متشکل از اعضای V است. می‌توانیم به هر گراف جهت‌دار هم نموداری نسبت دهیم. به عنوان مثال، اگر $V = \{a, b, c, d, e\}$ و $E = \{(a, b), (a, c), (a, e), (c, d), (c, e), (d, b), (d, e)\}$ آنگاه (V, E) گراف جهت‌داری است که نمودار آن در شکل ۴ نمایش داده شده است. توجه دارید که در یک گراف جهت‌دار به ازای هر $u, v \in V$ با شرط $u \neq v$ حداکثر دو به اصطلاح یال جهت‌دار یکی از u به v و دیگری از v به u وجود دارند.^۱

۱-۳- تمرین‌ها

- ۱- در مثال ۳ اگر علاوه بر شرایط داده شده، B_5 قادر به انجام کار A_4 نیز باشد شرکت به چند طریق می‌تواند پست‌های خالی را پر کند؟
- ۲- در مثال ۳ اگر علاوه بر شرایط داده شده، B_6 قادر به انجام کار A_4 نیز باشد شرکت به چند طریق می‌تواند پست‌های خالی را پر کند؟ (پاسخ ۴ است.)
- ۳- مسلماً دبیرستان شما در مسابقه‌های زیادی شرکت می‌کند. یکی از مسابقه‌ها را در نظر بگیرید و در پایان گراف یا گراف جهت‌دار مربوط به آن را مشخص کنید.
- ۴- گراف $G = (V, E)$ با $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ و $E = \{v_1v_2, v_1v_4, v_2v_3, v_2v_4, v_3v_4, v_5v_6, v_5v_7\}$ را در نظر بگیرید. الف) نمودار این گراف را رسم کنید.
- ب) اگر این رأس‌ها هفت شهر و این یال‌ها جاده‌های موجود بین این شهرها را نمایش دهند، آیا تنها با عبور از این جاده‌ها می‌توان از هر شهری به شهر دیگر سفر کرد؟
- پ) این گراف از چند «بخش جدا از هم» تشکیل شده است؟ (پاسخ ۳ است.)
- ۵- در زبان عربی کلمه‌ی «شجر» به معنای درخت است و درخت گراف خاصی است که بعداً در فصل ۳ بررسی خواهد شد. درباره‌ی ارتباط بین «شجره نامه‌ی خانوادگی» و گراف‌ها چه می‌دانید؟ شجره‌نامه‌ی خانوادگی خود را رسم کنید.

۱- در تعریف گراف جهت‌دار بسیاری از مؤلفان E را مجموعه‌ای از زوج‌های مرتب متشکل از اعضای متمایز V می‌گیرند. بدانید که با این شرط مثلاً با ۲ رأس ۳ و با ۸ رأس ۱۰۷۹۳۰۳۵۹۰۱۹۲۰۸۴۸ گراف جهت‌دار «متفاوت» وجود دارند!

۶- شش بازه‌ی باز $(۰,۲)$, $(۱,۴)$, $(۲,۵)$, $(۳,۴)$, $(۳,۸)$, $(۶,۹)$ از اعداد حقیقی داده شده‌اند. با این بازه‌ها گرافی چون G می‌سازیم که رأس‌هایش متناظر با این بازه‌ها باشند و دو رأس G با این شرط مجاور باشند که بازه‌های مربوط متمایز باشند و اشتراک آن‌ها تهی نباشد. مثلاً چون اشتراک بازه‌های $(۰,۲)$ و $(۱,۴)$ تهی نیست رأس‌های مربوط باید مجاور باشند. اما چون اشتراک بازه‌های $(۰,۲)$ و $(۲,۵)$ تهی است رأس‌های مربوط به این دو بازه نباید مجاور باشند. (چنین گرافی را گراف بازه‌ها می‌نامیم.)

الف) نمودار گراف بازه‌های داده شده را رسم کنید.

ب) با معرفی پنج بازه‌ی مناسب نشان دهید گراف شکل ۳ را می‌توان گراف بازه‌ها دانست.

پ) نشان دهید گراف شکل ۲ نمی‌تواند گراف بازه‌ها باشد؛ یعنی، پنج بازه‌ی باز نمی‌توان یافت که گراف مربوط به آن‌ها، طبق تعریف، «همان» گراف شکل ۲ باشد.

توجه: گراف‌هایی که از بازه‌ها به دست می‌آیند در باستان‌شناسی، ژنتیک و در تحلیل ادبی کاربرد دارند. درک عمیق این کاربردها مستلزم آگاهی از زمینه‌های مربوط است.

مجله‌ی ریاضی

می‌گویند در روزگاران پیش نقشه‌کش‌ها از این «واقعیت» آگاه بودند که هر نقشه‌ی جغرافیایی مسطح یا کروی را می‌توان با حداکثر چهاررنگ طوری رنگ کرد که مناطق «مجاور» رنگ‌های متفاوت داشته باشند. شاید هم مسأله‌ی چهاررنگ از تراوشات ذهن ریاضیدانان باشد. به هر تقدیر، نخستین مرجع مکتوب این مسأله‌نامه‌ی مورخ ۲۳ اکتبر ۱۸۵۲ میلادی، دموورگن به ویلیام همیلتن است. مسأله‌ی چهاررنگ که به «مرض» چهاررنگ هم شهرت یافت بیش از یک قرن به‌طور جدی ذهن بسیاری را به خود مشغول داشت و در نظریه‌ی گراف‌ها معادل‌های بسیاری برای آن مطرح شد. سرانجام در سال ۱۹۷۷ میلادی ک. آپل وو. هکن با استفاده از قضیه‌های فراوان و ۱۲۰۰ ساعت از وقت یکی از سریع‌ترین کامپیوترهای زمان این مسأله‌ی سرکش رامهار و «قضیه‌ی» چهاررنگ را «ثابت» کردند. اما، هنوز هم مرض چهاررنگ شیوع دارد و بسیاری به فکر ارائه‌ی اثباتی سنتی و حتی الامکان ساده برای آن هستند.



فصل

چند ویژگی ساده و چند رده‌ی خاص گراف‌ها

در این فصل ابتدا چند ویژگی ساده از گراف‌ها را ذکر می‌کنیم و سپس برای آشنایی بیشتر با گراف‌ها به معرفی چند رده‌ی خاص از آن‌ها می‌پردازیم و باز هم می‌کوشیم به‌طور شهودی مفاهیم را روشن کنیم.

۲-۱- مرتبه، اندازه و درجه

می‌دانیم که اگر مجموعه‌ای p ، $p \in \mathbb{N}$ ، عضو داشته باشد تعداد زیرمجموعه‌های دو عضوی آن $p(p-1)/2$ است که با $\binom{p}{2}$ نمایش داده می‌شود. بنابراین اگر گرافی p رأس و q یال داشته باشد داریم:

$$0 \leq q \leq \binom{p}{2} = p(p-1)/2$$

تعریف: در هر گراف $G = (V, E)$ تعداد اعضای مجموعه‌ی V را مرتبه‌ی G و تعداد اعضای مجموعه‌ی E را اندازه‌ی G می‌نامیم و معمولاً آن‌ها را، به ترتیب، با p و q نمایش می‌دهیم. مرتبه‌ی G را با $p(G)$ و اندازه‌ی آن را با $q(G)$ هم نمایش می‌دهیم.

مثال ۱: مرتبه‌ی گراف شکل ۲ از فصل ۱ پنج و اندازه‌ی آن هفت است. مرتبه‌ی گراف مربوط به مثلاً بوتان (شکل ۵ از فصل ۱) ۱۴ و اندازه‌ی آن ۱۳ است. توجه کنید که در مورد سایر گراف‌های این شکل نیز رابطه‌ی $p = q + 1$ برقرار است.

Δ

تعریف: درجه‌ی رأس v از گراف G برابر با تعداد یال‌هایی از G است که از رأس v می‌گذرند. این عدد را با $\deg_G v$ و گاهی به‌طور ساده با $\deg v$ نمایش می‌دهیم. اگر $\deg v$ یک عدد فرد باشد v را یک رأس فرد و اگر یک عدد زوج باشد v را یک رأس زوج از گراف G می‌نامیم.

مثال ۲: در شکل ۲ از فصل ۱ داریم: $\deg a = 3$ و $\deg b = 2$. این گراف چهار رأس فرد و یک رأس زوج دارد. در شکل ۶ از فصل ۱ داریم: $\deg a_1 = 1$ و $\deg a_3 = 5$. این گراف شش رأس فرد و سه رأس زوج دارد. توجه کنید که در هر دو مثال مجموع درجه‌های تمام رأس‌ها یک عدد زوج است. در قضیه‌ی زیر نشان می‌دهیم این مطلب همواره درست است. Δ

قضیه‌ی ۱: اگر $V = \{v_1, v_2, \dots, v_p\}$ مجموعه‌ی رأس‌های گراف G با اندازه‌ی q باشد، آن‌گاه $\sum_{i=1}^p \deg v_i = 2q$.

اثبات: هر یال تنها دو سر دارد، یعنی دقیقاً از دو رأس G می‌گذرد و لذا در طرف چپ فرمول بالا هر یال دو بار به حساب می‌آید. \square

توجه کنید درجه‌ی هر رأس گرافی که اصلاً یال نداشته باشد صفر است. لذا، در این حالت هر دو طرف برابری مذکور در قضیه‌ی ۱ صفر به حساب می‌آیند.

نتیجه: تعداد رأس‌های فرد هر گراف، زوج است.

اثبات: مجموع جمع‌وندهای (یعنی مجموع عامل‌های) زوج عبارت $\sum_{i=1}^p \deg v_i$ را با A و مجموع جمع‌وندهای فرد آن را با B نمایش می‌دهیم. پس داریم $\sum_{i=1}^p \deg v_i = A + B$. عدد $2q = \sum_{i=1}^p \deg v_i$ عدد زوج است، زیرا مجموع هر تعداد عدد زوج همواره زوج است. در نتیجه $B = 2q - A$ نیز زوج است. بنابراین تعداد جمع‌وندهای B ، یعنی تعداد رأس‌های فرد گراف، باید زوج باشد. \square

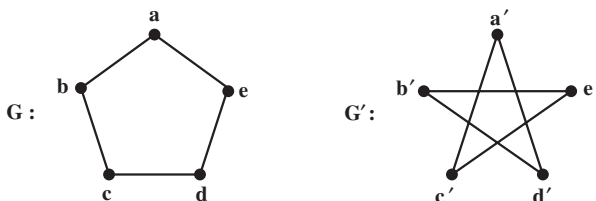
تعریف: بزرگترین عدد در بین درجه‌های رأس‌های گراف G را **ماکسیمم درجه‌ی** G می‌نامیم و آن را با $\Delta(G)$ یا به‌طور ساده با Δ نمایش می‌دهیم. کوچکترین عدد در بین درجه‌های رأس‌های گراف G را **مینیمم درجه‌ی** G می‌نامیم و آن را با $\delta(G)$ یا به‌طور ساده با δ نمایش می‌دهیم.

مثال ۳: در شکل ۶ از فصل ۱ داریم: $\Delta = 5$ و $\delta = 1$. در تمام گراف‌های مربوط به هیدروکربن‌ها $\Delta = 4$ و $\delta = 1$. Δ

۲-۲- گراف‌های منتظم، کامل و تهی

تعریف: عدد صحیح و نامنفی r داده شده است. گراف G از مرتبه‌ی p را r - منتظم می‌نامیم هرگاه درجه‌ی هر رأس G برابر با r باشد، هر گراف $(p-1)$ - منتظم از مرتبه‌ی p را گراف کامل هم می‌نامیم و آن را با K_p نمایش می‌دهیم.

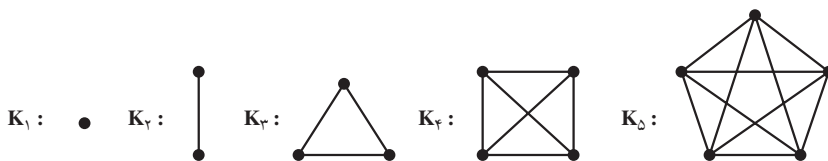
مثال ۴: هر یک از دو گراف شکل ۱، دو - منتظم است ولی چون در این دو مثال $p=5$ و $2 \neq 4 = p-1$ این دو گراف کامل نیستند. توجه کنید که در گراف کامل G از مرتبه‌ی p درجه‌ی هر رأس $p-1$ است و لذا به‌ازای هر $u, v \in V(G)$ ، $u \neq v$ داریم $uv \in E(G)$.



شکل ۱- گراف‌های ۲- منتظم

Δ

مثال ۵: در شکل زیر پنج گراف کامل K_p ، $1 \leq p \leq 5$ ، رسم شده‌اند. در مورد هر یک از این مثال‌ها دیده می‌شود که تعداد یال‌های K_p برابر با $p(p-1)/2$ است.



شکل ۲- گراف‌های کامل از مرتبه‌های ۱ تا ۵

Δ

قضیه‌ی ۲: تعداد یال‌های گراف کامل K_p ، $p \in \mathbb{N}$ برابر با $p(p-1)/2$ است.
اثبات: مجموع درجه‌های رأس‌های گراف K_p برابر با $p(p-1)$ است. پس، بنابر قضیه‌ی ۱، نصف این عدد برابر با $q(K_p)$ است.

□

قرارداد: گراف G - منتظم از مرتبه p را با K_p نمایش می‌دهیم. چون K_p هیچ یال ندارد، یعنی $E(K_p) = \emptyset$ ، این گراف را گراف تهی هم می‌نامیم. گراف‌های تهی با p رأس، $1 \leq p \leq 5$ ، را در شکل ۳ می‌بینید.



شکل ۳- گراف‌های تهی از مرتبه‌های ۱ تا ۵

۳-۲- مسیر گراف و دورگراف

تعریف: اگر u و v دو رأس متفاوت از گراف دلخواه G باشند، یک مسیر از u به v از گراف G دنباله‌ای متشکل از $m+1$ رأس $m \in \mathbb{N}$ ، دو به دو متفاوت G است که از u آغاز و به v ختم می‌شود و هر دو رأس متوالی این دنباله در G مجاورند. عدد m را طول این مسیر از گراف G می‌نامیم. می‌پذیریم که دنباله‌ی متشکل از تنها یک رأس v یک مسیر با طول صفر از v به v از گراف G باشد.

در واقع یک مسیر از رأس u به رأس v از گراف G را به این ترتیب به دست می‌آوریم که با در نظر گرفتن نموداری از G ابتدا u را یادداشت می‌کنیم؛ از یک یال مار ب u (در صورت وجود) می‌گذریم و الزاماً به رأسی تازه می‌رسیم و آن را به عنوان دومین عضو دنباله یادداشت می‌کنیم. از آن جا یالی تازه از G را برمی‌گزینیم و از آن به رأس سوم می‌رسیم که آن را نیز یادداشت می‌کنیم و این عمل را ادامه می‌دهیم تا در صورت امکان پس از گذشتن از m یال دوبه دو متفاوت، $m \geq 0$ ، به v برسیم. در پایان v را نیز یادداشت می‌کنیم. رأس‌هایی را که یادداشت کرده‌ایم دنباله‌ای است که یک مسیر از u به v از گراف G را به دست می‌دهد.

مثال ۶: در شکل ۲ از فصل ۱ از a به b پنج مسیر وجود دارند. در این گراف مثلاً

$$a,b \quad a,c,d,b \quad a,c,e,d,b$$

سه مسیر متفاوت با طول، به ترتیب از چپ به راست، ۱، ۳، و ۴ از رأس a به رأس b هستند.

(دو مسیر دیگر از a به b را بنویسید و طول آن‌ها را مشخص کنید.) Δ

واضح است که اگر در گرافی از u به v مسیری وجود داشته باشد در آن گراف از رأس v به u هم مسیری وجود دارد. لذا وجود یا عدم وجود مسیر «بین» دو رأس گراف معنی دارد.

تعریف: گراف G را همبند می‌نامیم هرگاه بین هر دو رأس آن مسیری وجود داشته باشد. در غیر این صورت G را ناهمبند می‌نامیم.

مثال ۷: گراف شکل ۲ از فصل ۱ همبند است. ولی گراف شکل ۳ از فصل ۱ و گراف تهی \bar{K}_p ، $p \geq 2$ ، همبند نیستند. البته \bar{K}_1 نیز همبند است. به مثال ۷ از فصل ۱ بازگردید. گفتیم که این گراف از سه «بخش جدا از هم» تشکیل شده است. این گراف ناهمبند است زیرا مثلاً بین دو رأس v_1 و v_4 مسیری وجود ندارد.

تعریف: یک دور از گراف G دنباله‌ای چون $v_1, v_2, \dots, v_m, v_{m+1} = v_1$ باشد شرط $m \geq 3$ متشکل از $m+1$ رأس G است که در آن v_i ها، $1 \leq i \leq m$ ، دوه‌دو متمایزند و هر دو رأس متوالی این دنباله در G مجاورند. عدد m را طول این دور از گراف G می‌نامند.

مثال ۸: هیچ یک از گراف‌های شکل ۵ از فصل ۱ دور ندارد. همچنین گراف تهی \bar{K}_p دور ندارد. ولی به‌ازای هر $p \geq 3$ گراف کامل K_p دور دارد. در واقع، به‌ازای هر عدد طبیعی n ، $3 \leq n \leq p$ ، گراف K_p دوری به طول n دارد. گراف شکل ۶ از فصل ۱ دوری ندارد که طولش فرد باشد ولی دوری به طول ۴ (دنباله‌ی b_2, a_3, b_3, a_4, b_4) و دوری به طول ۶ (دنباله‌ی $b_1, a_4, b_3, a_4, b_2, a_3, b_1$) دارد.

۲-۴- تمرین‌ها

۱- فرض کنید گراف G ، $3 -$ منتظم است و داریم $q = 2p - 3$. مرتبه‌ی G با p و اندازه‌ی آن با q نمایش داده شده است.

الف) ویژگی‌های گراف G را مشخص کنید.

ب) گرافی رسم کنید که این ویژگی‌ها را داشته باشد.

پ) گراف دیگری رسم کنید که واجد این ویژگی‌ها باشد.

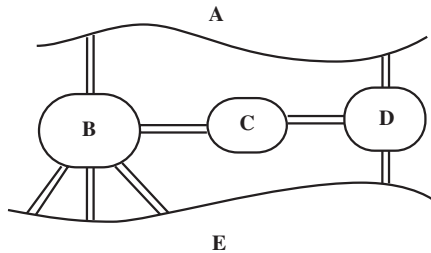
۲- الف) گراف شکل ۶ از فصل ۱ را در نظر بگیرید و پارامترهای p ، q ، Δ و δ را بیابید.

ب) درجه‌های تمام رأس‌های این گراف را به صورت دنباله‌ای چون $s: d_1, d_2, \dots, d_n$ بنویسید

که به‌ازای هر $1 \leq i \leq n$ داشته باشیم $d_{i+1} \leq d_i$. (دنباله‌ی حاصل را دنباله‌ی درجه‌های رأس‌های

گراف می‌نامیم.)

- (پ) چرا گرافی وجود ندارد که $S: 5, 3, 3, 1, 0$ دنباله‌ی درجه‌های رأس‌های آن باشد؟
- ۳- الف) گرافی ارائه کنید که دنباله‌ی درجه‌های رأس‌هایش $S: 2, 3, 3, 3, 2, 2, 2, 0, 0, 0$ باشد.
- (ب) آیا پاسخ یکتاست؟ چرا؟
- ۴- چند گراف ۳- منتظم از مرتبه‌ی ۱۵ وجود دارند؟ چرا؟
- ۵- با استقرار بر q قضیه‌ی ۱ را اثبات کنید.
- ۶- گرافی ناهمبند و ۳- منتظم مثال بزنید که ۸ رأس و ۱۲ یال داشته باشد.
- ۷- گرافی همبند و ۳- منتظم مثال بزنید که ۸ رأس و ۱۲ یال داشته باشد.
- ۸- فرض کنید طبق شکل، شهری از یک رودخانه و پنج منطقه‌ی A, B, C, D, E تشکیل شده است و این منطقه‌ها با هشت پل به هم راه دارند.



- الف) گراف چندگانه‌ی مربوط به این شهر را رسم کنید.
- (ب) آیا با آغاز از یکی از منطقه‌های پنجگانه و عبور از پل‌ها می‌توان از هر پل دقیقاً یک بار گذشت و به منطقه‌ی آغاز بازگشت؟
- (پ) آیا با آغاز از یکی از منطقه‌های پنجگانه می‌توان از هر پل دقیقاً یک بار گذشت؟ در این حالت لازم نیست منطقه‌ی آغاز گشت با منطقه‌ی پایان آن یکی باشد.
- ۹- در گراف کامل K_p ، $2 \leq p \leq 4$ ، تعداد مسیرهای «متفاوت» از یک رأس u به یک رأس v ، $u \neq v$ ، را بیابید.

- ۱۰- الف) گراف شکل ۶ از فصل ۱ «چند» دور دارد؟ (پاسخ ۳ است: دو دور از مرتبه‌ی ۴ و یک دور از مرتبه‌ی ۶. پاسخ را توجیه کنید.)
- (ب) هر یک از دورها را به صورت دنباله‌ای از رأس‌ها نمایش دهید که رأس اول و آخر دنباله مثل هم و بقیه همراه با این رأس مشترک دو به دو متفاوت باشند؛ به علاوه، هر دو رأس متوالی این

دنباله در G مجاور باشند.

راهنمایی. یکی از دورهای G را می‌توان به یکی از صورت‌های زیر نوشت :

$$\begin{array}{ll} b_1, a_2, b_3, a_3, b_1 & b_1, a_3, b_3, a_2, b_1 \\ a_2, b_3, a_3, b_1, a_2 & a_2, b_1, a_3, b_3, a_2 \\ b_3, a_3, b_1, a_2, b_3 & b_3, a_2, b_1, a_3, b_3 \\ a_3, b_1, a_2, b_3, a_3 & a_3, b_3, a_2, b_1, a_3 \end{array}$$

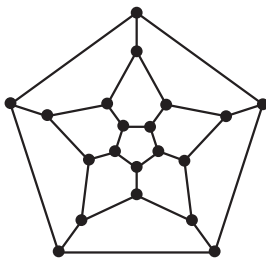
۱۱- هفده نفر به سفر می‌روند و قبل از سفر قرار می‌گذارند هر کس به پنج نفر دیگر نامه بفرستد. آیا امکان دارد هر کس به آن پنج نفری نامه بفرستد که از آن‌ها نامه دریافت می‌کند؟ چرا؟

۱۲- اگر گراف G از مرتبه‌ی p ، $p \geq 3$ ، دوری از مرتبه‌ی p داشته باشد، آن‌گاه G را گراف همیلتنی می‌نامیم. مثلاً هر K_p ، $p \geq 3$ ، گراف همیلتنی است.

(الف) نشان دهید هر گراف همیلتنی همبند است.

(ب) اگر G همیلتنی باشد آن‌گاه به ازای هر $v \in V(G)$ داریم $\deg v \geq 2$.

(پ) آیا گراف زیر گراف همیلتنی است و چرا؟



۱۳- (الف) گراف G داده شده است. فرض کنید $u, v \in V(G)$ نشان دهید «وجود یک مسیر از u به v » یک رابطه‌ی هم‌ارزی بر مجموعه‌ی $V(G)$ است.

(ب) اگر G گراف شکل ۳ از فصل ۱ باشد، افرازهای حاصل از رابطه‌ی هم‌ارزی مذکور در بند (الف) را بیابید.

(پ) پاسخ بند (ب) را با فرض این‌که G گراف شکل ۶ یا گراف شکل ۱۰ باشد بیابید.

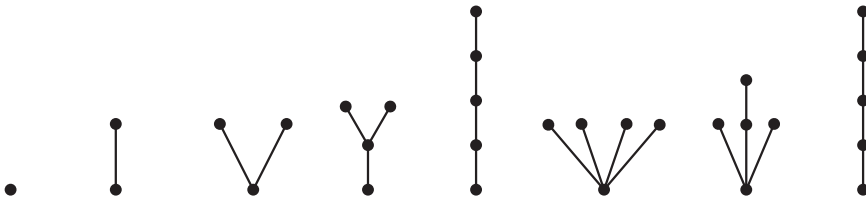
فصل ۳

درخت و ماتریس

در این فصل کوتاه ابتدا رده‌ی خاص دیگری از گراف‌ها موسوم به درخت‌ها را معرفی می‌کنیم و به بررسی ویژگی‌های آن‌ها می‌پردازیم. سرانجام به هر گراف یک ماتریس نسبت می‌دهیم و نشان می‌دهیم که هر گراف را می‌توان با یک ماتریس بسیار خاص نیز نمایش داد.

۳-۱- درخت

گراف همبندی را که هیچ دور نداشته باشد درخت می‌نامیم. گراف‌های K_1 و K_2 درخت‌اند و به ترتیب «تنها» درخت‌های با یک و دو رأس هستند. در شکل ۱ تمام درخت‌های از مرتبه‌ی p ، $1 \leq p \leq 5$ را رسم کرده‌ایم.



شکل ۱- درخت‌های از مرتبه‌ی ۱ تا ۵

گراف مربوط به هر هیدروکربن C_nH_{2n+2} نیز یک درخت است. می‌بینیم که در هر یک از این مثال‌ها بین هر دو رأس دقیقاً یک مسیر وجود دارد. این مطلب همواره درست است. قضیه‌ی ۱- بین هر دو رأس هر درخت مفروض دقیقاً یک مسیر وجود دارد. اثبات: اثبات در حالتی که دو رأس متمایز نباشند واضح است. فرض کنید u و v دو رأس

تمایز درختی چون G باشند. چون G همبند است بین u و v دست کم یک مسیر وجود دارد. اگر G دو مسیر مختلف (در واقع دو دنباله‌ی مختلف از رأس‌های متمایز G) از u به v وجود داشته باشند، آن‌گاه این دو مسیر مختلف «ایجاب» می‌کنند که دوری در G وجود داشته باشد. پس G درخت نیست و این، یک تناقض است. \square

مطلب دیگری که از درخت‌های شکل ۱ برمی‌آید این است که، به جز K_1 ، هر یک دست کم دو رأس از مرتبه‌ی یک دارد. این مطلب نیز همواره درست است.

قضیه‌ی ۲: هر درختی که بیش از یک رأس داشته باشد دست کم دو رأس از درجه‌ی یک دارد.

اثبات: از به اصطلاح استقرای تعمیم یافته روی مرتبه‌ی درخت G استفاده می‌کنیم. اگر $p = 2$ آن‌گاه $G = K_2$ و درستی حکم واضح است. فرض می‌کنیم حکم در مورد هر درخت با $k \geq 2$ رأس درست است. سپس درختی چون G از مرتبه‌ی $k+1$ را در نظر می‌گیریم. اگر G رأسی چون v از درجه‌ی یک داشته باشد آن‌گاه با حذف رأس v و تنها یال مارّ بر آن گرافی مانند G' به دست می‌آوریم که درخت است و $k \geq 2$ رأس دارد. پس بنا به فرض استقراء، G' و در نتیجه G دست کم دو رأس از درجه‌ی یک دارد. پس فرض می‌کنیم درجه‌ی هیچ رأسی از G از دو کمتر نباشد. در این صورت رأسی چون u از G را در نظر می‌گیریم. با آغاز از u و انتخاب یالی از G که از u می‌گذرد مسیری چون P را به این ترتیب می‌پیماییم که هر بار پس از رسیدن به رأسی تازه یالی از G را در پیش می‌گیریم که اولاً از آن رأس بگذرد، ثانیاً قبلاً مورد استفاده قرار نگرفته باشد، و ثالثاً انتهای دیگر آن رأسی تازه‌تر از G باشد. این کار باید در جایی متوقف شود. چون درجه‌ی هر رأس دست کم دو است توقف آن با رسیدن به یکی از رأس‌های قبل میسر است و لذا دوری در G به وجود می‌آید. این تناقض قضیه را ثابت می‌کند. \square

به مثال‌های گوناگون درخت‌ها نظر افکنید، می‌بینید که در مورد تمام آن‌ها قضیه‌ی زیر درست است.

قضیه‌ی ۳: اگر G درختی با p رأس و q یال باشد آن‌گاه

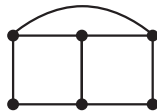
$$p = q + 1.$$

اثبات: با استقراء بر p قضیه را ثابت می‌کنیم. اگر $p = 1$ آن‌گاه $q = 0$ و داریم $p = q + 1$. فرض کنید قضیه در مورد هر درختی با k ، $k \geq 1$ ، رأس درست باشد. حال درختی چون G را در نظر می‌گیریم که $k+1$ رأس دارد. باید نشان دهیم تعداد یال‌های آن k است. بنا به قضیه‌ی قبل G رأسی

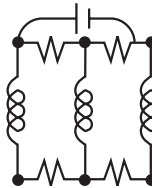
چون v دارد که $\deg v = 1$. با حذف رأس v و تنه‌های آن بر آن درختی چون G' ایجاد می‌شود که مرتبه‌اش k است. بنابه فرض استقراء، گراف G' دارای $k-1$ یال است. پس درخت G دقیقاً k یال دارد. □

مجله‌ی ریاضی

درخت در رشته‌های مختلفی مانند شیمی، مهندسی برق، و علم محاسبه کاربرد دارد. کرشلف در سال ۱۸۴۷ میلادی هنگام حل دستگاه‌های معادلات خطی مربوط به شبکه‌های الکتریکی درخت‌ها را کشف، و نظریه‌ی درخت‌ها را بارور کرد. در شکل زیر N یک شبکه‌ی الکتریکی و G گراف مربوط به آن است.



G



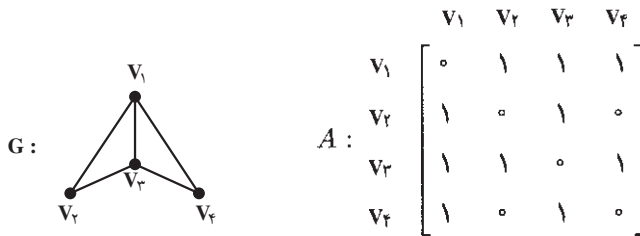
N

کیلی در سال ۱۸۵۷ میلادی درخت‌ها را در ارتباط با شمارش ایزومرهای مختلف هیدروکربن‌ها کشف کرد. وقتی مثلاً می‌گوییم دو ایزومر مختلف C_4H_{10} وجود دارند منظورمان این است که دو درخت «متفاوت» با ۱۴ رأس وجود دارند که درجه‌ی ۴ رأس از این ۱۴ رأس چهار و درجه‌ی هر یک از ۱۰ رأس باقیمانده یک است.

اگر هزینه‌ی کشیدن مثلاً راه‌آهن بین هر دو شهر از p شهر مفروض مشخص باشد ارزان‌ترین شبکه‌ای که این p شهر را به هم وصل می‌کند با مفهوم یک درخت از مرتبه‌ی p ارتباط نزدیک دارد. به‌جای مسأله‌ی مربوط به راه‌آهن می‌توان وضعیت مربوط به شبکه‌های برق‌رسانی، لوله‌کشی نفت، لوله‌کشی گاز، و ایجاد کانال‌های آبرسانی را در نظر گرفت. برای تعیین یک شبکه با نازل‌ترین هزینه از قاعده‌ای به نام الگوریتم صرفه‌جویی استفاده می‌شود که کاربردهای فراوان دارد.

۳-۲- گراف‌ها و ماتریس‌ها

گراف $G = (V, E)$ با $V = \{v_1, v_2, v_3, v_4\}$ و $E = \{v_1v_2, v_1v_3, v_1v_4, v_2v_3, v_3v_4\}$ را که در شکل ۲ رسم شده است در نظر بگیرید. به این گراف ماتریسی 4×4 چون $A = (a_{ij})$ به شرح زیر نسبت می‌دهیم. در مقابل چهار سطر و چهار ستون این ماتریس طبق شکل ۲ می‌نویسیم v_1 ، v_2 ، v_3 و v_4 . درایه‌ی a_{ij} از این ماتریس ۱ است هر گاه $v_i v_j \in E$ و ۰ است هر گاه $v_i v_j \notin E$.



$$A : \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$$

شکل ۲- گراف و ماتریس مجاورت آن

توجه کنید که :

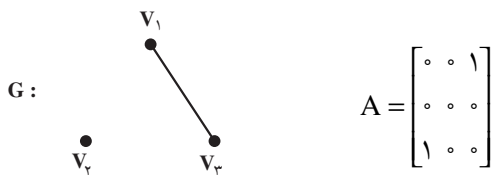
- (۱) درایه‌های روی قطر اصلی همگی صفرند زیرا گراف‌های (ساده‌ی) موضوع بحث ما «طوقه» ندارند، یعنی هیچ رأسی با خودش مجاور نیست.
- (۲) تعداد سطرهای این ماتریس برابر است با تعداد ستون‌های آن، یعنی ماتریس A مربعی است.

(۳) هر درایه‌ی ماتریس A یا صفر است یا یک، یعنی همواره $a_{ij} \in \{0, 1\}$.

(۴) ماتریس A متقارن است، یعنی همواره $a_{ij} = a_{ji}$ ، زیرا اگر $v_i v_j \in E$ آن‌گاه $v_j v_i \in E$. واضح است که به هر گراف دلخواه G همواره می‌توان ماتریسی چون A با ویژگی‌های چهارگانه بالا نسبت داد. این ماتریس را ماتریس مجاورت گراف G می‌نامیم و آن را با $A(G)$ یا به‌طور ساده با A نمایش می‌دهیم.

جالب این‌جاست که به هر ماتریس با ویژگی‌های چهارگانه بالا می‌توان یک گراف نسبت داد. مثلاً اگر ماتریس A از شکل ۳ را به ما بدهند فوراً می‌توانیم گراف G از همین شکل را به آن نسبت دهیم. برای این کار به ازای سطر (یا ستون) اول ماتریس نقطه‌ای چون v_1 ، به ازای سطر (یا ستون) دوم ماتریس نقطه‌ای چون v_2 و همین‌طور به ازای سطر (یا ستون) سوم نقطه‌ی دیگر v_3 را در نظر

می گیریم و نقطه‌ی v_i را به نقطه‌ی v_j با خطی به هم وصل می کنیم هرگاه درایه‌ی مربوط در ماتریس داده شده یک باشد و در غیر این صورت آن دو را به هم وصل نمی کنیم.



شکل ۳- ماتریس با شرایط چهارگانه‌ی بالا و گراف آن

پس می بینیم که یک گراف با p رأس در واقع چیزی جز یک ماتریس مربعی $p \times p$ با شرایط چهارگانه‌ی بالا نیست. و لذا برای مطالعه‌ی گراف‌ها می توان صرفاً ماتریس‌های مربعی متقارنی را مطالعه کرد که درایه‌های آن‌ها از مجموعه‌ی $\{0, 1\}$ انتخاب می شوند و درایه‌های روی قطر اصلی آن‌ها صفرند. بنابراین نظریه‌ی گراف‌ها را می توان شاخه‌ای از جبر هم تلقی کرد.

قضیه‌ی ۴: فرض کنید A ماتریس مجاورت گراف G با $V(G) = \{v_1, \dots, v_p\}$ باشد. آن‌گاه

درایه‌ی واقع در سطر i ام و ستون i ام ماتریس A^2 برابر است با درجه‌ی رأس v_i در گراف G .
اثبات: درایه‌ی واقع در سطر i ام و ستون i ام ماتریس A^2 برابر است با مجموع حاصل ضرب‌های درایه‌های نظیر به نظیر سطر i ام A و ستون i ام A . چون A متقارن است این درایه از حاصل ضرب‌های درایه‌های نظیر به نظیر سطر i ام A و سطر i ام A حاصل می شود. تعداد یک‌های موجود در سطر i ام A برابر است با درجه‌ی رأس v_i و لذا برای محاسبه‌ی درایه‌ی موردنظر از ماتریس A^2 باید به اندازه‌ی $\deg v_i = 1 \times 1 = 1$ را با هم جمع کنیم. □

۳-۳- تمرین‌ها

- ۱- گراف همبندی معرفی کنید که مجموع مرتبه و اندازه‌ی آن ۸ باشد.
- ۲- گراف همبندی معرفی کنید که حاصل ضرب مرتبه و اندازه‌ی آن ۲۰ باشد.
- ۳- فرض کنید ماکسیمم درجه‌ی یک درخت T برابر با k باشد. ثابت کنید که T دست کم k رأس از درجه‌ی یک دارد.
- ۴- گرافی از مرتبه‌ی ۶ و اندازه‌ی ۶ معرفی کنید که ۲- منتظم باشد.

۵- تمام درخت‌های از مرتبه‌ی ۶ را رسم کنید.

۶- دو ماتریس M_1 و M_2 به صورت زیر داده شده‌اند.

$$M_2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad M_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

آن را که معرف یک گراف است مشخص کنید و نمودار آن را بکشید.

۷- اگر ماتریس مجاورت گراف K_p ، $p \in \mathbb{N}$ ، را با M نمایش دهیم نشان دهید هر درایه‌ی

واقع بر روی قطراصلی ماتریس M^2 برابر با $p-1$ است.

۸- الف) قضیه‌ی ۱ را با استفاده از استقراء روی مرتبه‌ی یک درخت و با به کار بردن قضیه‌ی

۲ ثابت کنید.

ب) اثباتی را که در متن برای قضیه‌ی ۱ ارائه شده است با اثباتی که طبق بند الف) این تمرین

به دست می‌آید مقایسه کنید و با ذکر دلیل به پرسش‌های زیر پاسخ دهید:

- کدام اثبات شهودی‌تر است؟

- کدام اثبات «دقیق‌تر» است؟

- کدام اثبات را بیشتر می‌پسندید؟

۹- الف) در شکل زیر یک گراف ناهمبند G رسم شده است. رأس‌های G را با $v_1, v_2,$

v_3, v_4, v_5, v_6 و v_7 چنان برچسب بزنید که ناهمبند بودن G از ماتریس مجاورت آن آشکار

باشد.



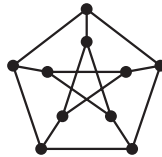
ب) اگر این فکر را در مورد یک گراف ناهمبند و دلخواه G به کار ببریم ماتریس مجاورتش چه

صورتی خواهد داشت؟

۱۰- الف) با توجه به تعریف ماتریس مجاورت گراف (ساده) ماتریس مجاورت گراف جهت‌دار

را تعریف کنید.

- (ب) ماتریس مجاورت گراف جهت‌دار شکل ۴ از فصل ۱ را بنویسید.
- ۱۱- گراف همبند G داده شده است. اگر $u, v \in V(G)$ فاصله‌ی u از v در G که با $d(u, v)$ نمایش داده می‌شود برابر است با طول کوتاه‌ترین مسیر از u به v در G . نشان دهید:
- الف) $d(u, v) = 0$ اگر و تنها اگر $u = v$.
- (ب) به ازای هر $u, v \in V(G)$ داریم $d(u, v) = d(v, u)$.
- (پ) به ازای هر $u, v, w \in V(G)$ داریم $d(u, w) \leq d(u, v) + d(v, w)$.
- ۱۲- گراف زیر موسوم به گراف پترسن را در نظر بگیرید.
- الف) در این گراف دوری مشخص کنید که طول آن هر یک از اعداد ۵، ۶، ۸، و ۹ باشد.
- (ب) آیا این گراف همبندی است؟ چرا؟



مراجع

- 1- M. Behzad, G. Chartrand, and L. Lesniak-Foster, Graphs and Digraphs, Wadsworth International Group, Belmont, Calif. 1979.
- 2- O. Ore, and R. J. Wilson, Graphs and their Uses, The Mathematical Association of America, 1990. ^۱

قسمت دوم

نظریه‌ی اعداد

مقدمه

نظریه‌ی اعداد یکی از شاخه‌های زیبا و جالب ریاضی است که ریشه در تاریخ بشر دارد و به دلیل زیبایی و کارایی همواره مورد علاقه بوده است. پیشرفت‌های علوم دیگر مانند کامپیوتر و رمزنگاری که تکیه بر نظریه‌ی مقدماتی اعداد دارند، به شادابی و زنده بودن این شاخه از دانش بشری کمک کرده‌اند.

در این قسمت مباحثی مقدماتی از نظریه‌ی اعداد را ارائه می‌دهیم و انتظار داریم دانش‌آموزان عزیز با توجه به محتوای غنی این رشته و نیز تأثیر مثبت حل مسائل آن در جهت تقویت تفکر ریاضی، مسائلی جالب از نظریه‌ی اعداد را انتخاب و حل کنند.

فصل ۴

کلیات و تقسیم‌پذیری

۴-۱- برخی از اصول نظریه‌ی اعداد

نظریه‌ی اعداد شاخه‌ای از ریاضیات است که بیشتر به خواص اعداد طبیعی

$1, 2, 3, \dots$

می‌پردازد. در مورد چگونگی به‌وجود آمدن اعداد طبیعی اطلاع درستی در دست نیست، اما شواهدی وجود دارند که نشان می‌دهند بشر اولیه اعداد طبیعی را برای شمارش مورد استفاده قرار داده است و به تدریج روش‌هایی را برای نمایش اعداد و انجام محاسبات اختراع کرده است.

شمارش گوسفندان قبل از رفتن به چرا و پس از بازگشت آن‌ها با استفاده از مفهوم تناظر یک به یک بین مجموعه‌ی گوسفندها و زیرمجموعه‌ای از اعداد طبیعی، یا به صورت یک انگشت، یا یک علامت روی سنگ و یا کنار گذاشتن یک تکه چوب به جای هر گوسفند، حتی هنوز هم گاهی به‌طور ابتدایی معمول است. این عمل که برای تهیه‌ی آمار و حتی رأی‌گیری‌های ساده هم به کار می‌رود از شواهد اولیه‌ی شناخت اعداد طبیعی است.

دنباله‌ی اعداد طبیعی از ۱ شروع می‌شود و هر عضو دیگر آن با افزودن یک واحد به عدد قبلی به دست می‌آید.

در سال‌های گذشته، با مجموعه‌ی اعداد طبیعی

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

و عمل‌های جمع و ضرب آن‌ها و با ویژگی‌های این دو عمل اصلی و نیز با عمل تفریق روی مجموعه‌ی اعداد صحیح

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

آشنا شده‌ایم.

ما در این جا ساختار اعداد صحیح را به روش اصل موضوعی مطرح نکرده بلکه فقط اصل موضوع «خوش‌ترتیبی» و یا معادل آن اصل موضوع «استقرای ریاضی» را به عنوان زیربنای قضیه‌های نظریه‌ی اعداد بیان می‌کنیم.

اصل خوش‌ترتیبی

هر زیرمجموعه‌ی ناتهی از اعداد طبیعی دارای کوچک‌ترین عضو است، یعنی اگر $S \subset \mathbb{N}$ و $S \neq \emptyset$ ، آن‌گاه عضوی از S مانند s_0 وجود دارد که به ازای هر s متعلق به S ،

$$s_0 \leq s$$

(کوچک‌ترین عضو مجموعه‌ی A را عضو ابتدای مجموعه‌ی A هم می‌نامند).^۱

اصل استقرای ریاضی

هر زیرمجموعه‌ی S از \mathbb{N} که دارای دو خاصیت زیر باشد، با مجموعه‌ی \mathbb{N} برابر است:

(الف) $1 \in S$

(ب) هرگاه $n \in S$ ، آن‌گاه $n+1 \in S$.

با پذیرفتن هریک از اصل‌های فوق می‌توان اصل دیگر را به عنوان یک قضیه اثبات کرد.

۴-۲- معادل‌های اصل استقرای ریاضی

معادل‌های دیگری برای اصل استقرای ریاضی وجود دارند که برخی را در این جا مطرح

می‌کنیم:

(الف) فرض کنیم $P(n)$ عبارتی درباره‌ی عدد طبیعی n باشد. اگر $P(1)$ درست باشد و به ازای هر عدد طبیعی n از درستی $P(n)$ ، درستی $P(n+1)$ نتیجه شود، آن‌گاه به ازای هر عدد طبیعی n درست است.

تعمیم این مطلب به صورت زیر است:

(ب) فرض کنیم $P(n)$ عبارتی درباره‌ی عدد صحیح n باشد. اگر به ازای یک $m \in \mathbb{Z}$ ، $P(m)$ درست باشد و اگر به ازای هر $n \geq m$ ، از درستی $P(n)$ درستی $P(n+1)$ نتیجه شود، آن‌گاه به ازای هر

۱- نماد $s_0 = \min S$ برای کوچک‌ترین عضو مجموعه‌ی S به کار می‌رود.

ازای هر عدد صحیح $n \geq m$ درست است.

می توان ثابت کرد که الف، ب، و اصل استقرای ریاضی دو به دو معادل اند.

در کتاب جبر و احتمال، مثال های متعددی وجود دارند که ما را با نحوه ی استفاده از اصل

استقرای ریاضی آشنا می کنند. در این جا ذکر یک نکته را ضروری می دانیم:

در اثبات به روش استقرا باید درستی هر دو شرط بررسی شوند. مثلاً، عبارت زیر را در نظر

بگیرید:

$$1 + 3 + 5 + \dots + (2n - 1) = n^2 + 3$$

اگر چه گام دوم استقرای ریاضی (یعنی اثبات درستی به ازای $n + 1$)، با فرض درست بودن به

ازای n) برقرار است ولی هیچ عدد طبیعی n در این عبارت صدق نمی کند.

همان طور که گفتیم می توان ثابت کرد که اصل خوش ترتیبی و اصل استقرای ریاضی معادل اند.

یعنی می توان به دلخواه یکی را اصل گرفت و دیگری را به عنوان قضیه ثابت کرد؛ مثلاً داریم:

قضیه ی ۱: اصل استقرای ریاضی از اصل خوش ترتیبی نتیجه می شود.

اثبات: فرض کنیم $P \subset \mathbb{N}$ ، $1 \in P$ و اگر $n \in P$ آن گاه $n + 1 \in P$. می خواهیم ثابت کنیم

$P = \mathbb{N}$. اگر چنین نباشد پس $T = \mathbb{N} - P \neq \emptyset$. لذا کوچک ترین عضوی دارد که آن را t_0

می نامیم. $t_0 \neq 1$ (چرا؟)، پس $t_0 - 1 \in \mathbb{N}$ و $t_0 - 1 < t_0$. لذا $t_0 - 1 \notin T$ ، یعنی $t_0 - 1 \in P$ پس

$t_0 \in P$ ، که با $t_0 \in T$ در تناقض است. در نتیجه $P = \mathbb{N}$. □

اصل استقرای قوی ریاضی

هر زیرمجموعه ی S از \mathbb{N} که دارای دو خاصیت زیر باشند، با مجموعه ی \mathbb{N} برابر است:

الف) $1 \in S$

ب) اگر اعداد طبیعی کوچک تر از n در S باشند، آن گاه $n \in S$.

اصل استقرای قوی ریاضی با اصل استقرای ریاضی و در نتیجه با اصل خوش ترتیبی معادل

است. برای نشان دادن نحوه ی استفاده از اصل استقرای قوی ریاضی، به مثال زیر توجه کنید:

مثال ۱: چند جمله ی اول دنباله ی موسوم به دنباله ی اعداد لوکا عبارت اند از:

$$1, 3, 4, 7, 11, 18, 29, 47, \dots$$

اگر جمله ی n ام را با L_n نمایش دهیم این دنباله از به اصطلاح «رابطه ی بازگشتی» زیر

$$L_n = L_{n-1} + L_{n-2} \quad n \geq 3$$

و شرایط اولیه‌ی

$$L_3 = 3, L_1 = 1$$

به دست می‌آید. با استفاده از اصل استقرای قوی ریاضی ثابت می‌کنیم که به ازای هر عدد طبیعی n ,

$$L_n < \left(\frac{\sqrt{5}}{2}\right)^n$$

اگر $S = \{n \in \mathbb{N} : L_n < \left(\frac{\sqrt{5}}{2}\right)^n\}$ ، آن‌گاه $1 \in S$ و $2 \in S$. (چرا؟) حال اگر $n \geq 3$ و به ازای

هر k وقتی که $k \in S$ ، $k < n$ ، آن‌گاه $L_{n-1} < \left(\frac{\sqrt{5}}{2}\right)^{n-1}$ و $L_{n-2} < \left(\frac{\sqrt{5}}{2}\right)^{n-2}$. پس

$$L_n < \left(\frac{\sqrt{5}}{2}\right)^{n-1} + \left(\frac{\sqrt{5}}{2}\right)^{n-2} = \left(\frac{\sqrt{5}}{2}\right)^{n-2} \left(\frac{\sqrt{5}}{2} + 1\right) < \left(\frac{\sqrt{5}}{2}\right)^n$$

یعنی $n \in S$. پس $S = \mathbb{N}$. لذا برای هر عدد طبیعی n داریم، $\Delta \quad L_n < \left(\frac{\sqrt{5}}{2}\right)^n$.

۴-۳- تقسیم پذیری

یکی از چهار عمل اصلی روی اعداد صحیح، تقسیم است. می‌دانیم حاصل تقسیم دو عدد صحیح الزاماً یک عدد صحیح نیست. مثلاً، حاصل تقسیم $12 - 5$ بر 5 ، عدد صحیح نیست. در مواردی حاصل تقسیم عددی بر عددی دیگر یک عدد صحیح می‌شود مثل 12 و 6 . در این حالت می‌گوییم عدد 6 عدد 12 را می‌شمارد، یا عدد 12 بر 6 تقسیم پذیر است. در واقع 12 یک مضرب 6 است: $12 = 6 \times 2$. در حالت عمومی تعریف زیر را ارائه می‌دهیم:

تعریف: عدد صحیح a را بر عدد صحیح b ، $b \neq 0$ ، تقسیم پذیر یا (بخش پذیر) می‌گوییم هرگاه عدد صحیحی مانند q یافت شود به گونه‌ای که $a = bq$. در این صورت می‌نویسیم $b|a$ و چنین می‌خوانیم: a بر b تقسیم پذیر است^۱ و یا b یک شمارنده یا مقسوم‌علیه a است. هرگاه a بر b تقسیم پذیر نباشد می‌نویسیم $b \nmid a$. در حالت $b = 0$ ، چون به ازای هر $q \in \mathbb{Z}$ ، $0 = 0 \times q$ ، می‌توان تعریف تقسیم پذیری

۱- هرگاه a بر b تقسیم پذیر باشد می‌گوییم b عدد a را می‌شمارد (عاد می‌کند)، یا a مضرب b است، یا b یک سازهی

(عامل) a است.

را گسترش داد و عبارت « \circ بر \circ تقسیم پذیر است» را نیز پذیرفت.

در مثال فوق $b=6$ ، $a=12$ ، $q=2$ و $12=6 \times 2$ و می‌نویسیم $6|12$. از تعریف بالا نتایج

زیر به دست می‌آیند:

(الف) صفر بر هر عدد b ، تقسیم پذیر است.

(ب) اعداد 1 و -1 ، هر عدد صحیح را می‌شمارند. (چرا؟)

با توجه به مفهوم رابطه که در سال‌های قبل با آن آشنا شده‌ایم، می‌توان تقسیم پذیری را به

عنوان یک رابطه با ویژگی‌های زیر بر مجموعه‌ی اعداد صحیح در نظر گرفت.

۱- این رابطه بازتابی است، زیرا برای هر عدد صحیح a داریم $a = a \times 1$ ، پس $a|a$.

۲- این رابطه ترایابی است، یعنی اگر $a|b$ و $b|c$ ، آن‌گاه $a|c$. برای اثبات می‌گوییم: یک

عدد صحیح q وجود دارد که $b = aq$ و یک عدد صحیح q' وجود دارد که $c = bq'$. در نتیجه

$$c = (aq)q' = a(qq')$$

یعنی $a|c$.

۳- این رابطه متقارن نیست، چون مثلاً $2|6$ ولی $6 \nmid 2$.

۴- این رابطه پاد متقارن نیست، چون مثلاً $2|2$ و $2|-2$ ولی $-2 \nmid 2$.

۴-۴ چند ویژگی تقسیم پذیری

با قضیه‌های زیر ویژگی‌های عمده‌ی تقسیم پذیری را ارائه می‌دهیم:

قضیه‌ی ۲: به ازای اعداد صحیح a و b ، اگر $a|b$ ، آن‌گاه

(الف) $a|b$ (ب) $a|-b$ (پ) $-a|-b$

(ت) به ازای هر عدد صحیح m ، $a|mb$. (ث) اگر $b \neq 0$ ، آن‌گاه $|a| \leq |b|$.

اثبات: اگر $a|b$ بنا به تعریف $b = aq$. در نتیجه

$$b = aq = (-a)(-q)$$

و نیز

$$-b = a(-q) = (-a)q$$

پس الف، ب و پ برقرارند. علاوه بر آن برای $m \in \mathbb{Z}$

$$mb = m(aq) = a(mq)$$

پس $a|mb$.

برای اثبات قسمت آخر چون $b = aq$ پس $|q| |a| = |b|$. ولی $b \neq 0$ در نتیجه $q \neq 0$ ، پس $|q| \geq 1$ یعنی $|a| \leq |b|$.

□

قضیه ۳: به ازای اعداد صحیح a ، b و c

الف) اگر $a|b$ ، آن گاه $a = \pm 1$ (تنها مقسوم علیه های عدد ۱، اعداد ۱ و -۱ هستند).

ب) اگر $a|b$ و $b|a$ ، آن گاه $a = \pm b$.

پ) اگر $a|b$ و $a|c$ ، آن گاه به ازای اعداد صحیح و دلخواه m و n ، داریم $a|mb + nc$.

اثبات: الف) اگر $a|b$ ، آن گاه $|a| \leq |b|$ یعنی $|a| = 0$ یا $|a| = 1$. اما اگر $|a| = 0$ ، آن گاه $a = 0$

ولی $1 \neq 0$ پس $|a| = 1$. در نتیجه $a = \pm 1$.

ب) اگر $a|b$ و $b|a$ آن گاه عدد صحیح q وجود دارد که $aq = b$ و عدد صحیح q' وجود

دارد که $a = bq'$. پس :

$$b = aq = b(qq')$$

اگر $b = 0$ الزاماً $a = 0$ و در نتیجه $a = b = 0$. اگر $b \neq 0$ آن گاه $qq' = 1$ ، یعنی $q' = 1$ و لذا

$$a = \pm b$$

پ) اگر $a|b$ و $a|c$ آن گاه عدد صحیح q وجود دارد که $b = aq$ و عدد صحیح q' وجود

دارد که $c = aq'$. به ازای اعداد صحیح دلخواه m و n داریم

$$\begin{aligned} mb + nc &= maq + naq' \\ &= (mq + nq')a \end{aligned}$$

پس :

$$a|mb + nc$$

□

۴-۵- الگوریتم تقسیم

اگر عدد صحیح a بر عدد طبیعی b تقسیم پذیر نباشد، در انجام تقسیم باقیمانده ای به جز صفر

پیدا می شود. کلیت مسئله اگرچه یک الگوریتم نیست ولی هنوز اسم سنتی خود «الگوریتم تقسیم» را

حفظ کرده و عبارت است از :

قضیه ۴: (الگوریتم تقسیم): اگر a یک عدد صحیح و b یک عدد طبیعی باشد، آن گاه اعداد یکنای $q \in \mathbb{Z}$ و r وجود دارند که

$$a = bq + r, \quad 0 \leq r < b$$

(q خارج قسمت، r باقیمانده، a مقسوم و b مقسوم علیه نامیده می شوند).

اثبات: نخست نشان می دهیم که $r, q \in \mathbb{Z}$ وجود دارند و پس از آن یکتا بودن آن ها را ثابت می کنیم. چون a, b و q اعداد صحیح اند، $S = \{a - bq > 0 : q \in \mathbb{Z}\}$ یک زیرمجموعه از اعداد طبیعی است. نشان می دهیم که S تهی نیست و اصل خوش ترتیبی را به کار می بریم. به ازای عدد صحیح $q = -|a| - 1$ ، $a - bq > 0$ ؛ زیرا

$$a - bq = a + b|a| + b \geq a + |a| + 1 > 0$$

پس به ازای این مقدار q ، $a - bq \in S$. لذا S دارای کوچک ترین عضو است. کوچک ترین عضو این مجموعه را r می نامیم. در این صورت عددی صحیح مانند q وجود دارد که $r = a - bq$. یعنی:

$$a = bq + r$$

اگر $r > b$ ، آن گاه

$$r - b = a - b(q + 1) \in S$$

ولی چون $b > 0$ پس $r - b < r$ که متناقض با کوچک ترین بودن r است، پس $r \leq b$. حال اگر $r = b$ مقدار $q_1 = q + 1$ را در نظر می گیریم. در این صورت

$$a = bq_1$$

که به جای r ، $r_1 = 0$ را در نظر می گیریم. پس همواره $0 \leq r < b$. برای اثبات یکتا بودن، فرض کنیم چنین نباشد، یعنی

$$a = bq_1 + r_1 \quad 0 \leq r_1 < b, \quad a = bq_2 + r_2 \quad 0 \leq r_2 < b$$

پس:

$$0 = b(q_1 - q_2) + r_1 - r_2$$

یا

$$r_2 - r_1 = b(q_1 - q_2)$$

یعنی $b | r_2 - r_1$. اگر $r_2 - r_1 \neq 0$ ، آن گاه $b \leq |r_2 - r_1|$. از سوی دیگر

$$-b < r_2 - r_1 < b$$

یعنی :

$$|r_2 - r_1| < b$$

که این با $b \leq |r_2 - r_1|$ تناقض دارد. پس $r_2 - r_1 = 0$. یعنی $r_2 = r_1$ و چون $b \neq 0$ ، $q_1 - q_2 = 0$

□

یعنی $q_2 = q_1$.

توجه کنید که هرگاه $r = 0$ ، آن گاه $b|a$.

مثال ۲: برای $a = 1028$ و $b = 34$ ، داریم

$$q = \left\lfloor \frac{1028}{34} \right\rfloor = 30$$

(در این جا منظور از نماد $[x]$ ، جزء صحیح عدد حقیقی x است.)

و

$$r = 1028 - 30 \times 34 = 8$$

پس :

$$1028 = 34 \times 30 + 8$$

Δ

یکی از کاربردهای قضیه ی الگوریتم تقسیم، دسته بندی اعداد بر حسب باقیمانده ی تقسیم آن ها بر عدد طبیعی و ثابت b است.

مثال ۳: باقیمانده ی هر عدد صحیح بر ۲، عدد ۰ یا ۱ است. این مطلب اعداد صحیح را به دو دسته تقسیم می کند. تمام اعدادی را که باقیمانده ی آن ها بر ۲، ۰ است، یعنی ۲ آن ها را می شمارد زوج و بقیه ی اعداد را فرد می نامند. یعنی می توان نوشت :

$$\mathbb{Z} = [0]_2 \cup [1]_2$$

که در آن

$$[0]_2 = \{n \in \mathbb{Z} : n = 2q, q \in \mathbb{Z}\} = \{n \in \mathbb{Z} : 2|n\}$$

مجموعه ی اعداد زوج، و

$$[1]_2 = \{n \in \mathbb{Z} : n = 2q + 1, q \in \mathbb{Z}\} = \{n \in \mathbb{Z} : 2 \nmid n\}$$

Δ

مجموعه ی اعداد فرد است.

به همین ترتیب هر عدد صحیح را می توان تنها به یکی از صورت های

$$4q, 4q+1, 4q+2, 4q+3$$

نوشت، که در آن $q \in \mathbb{Z}$. این مطلب اساس مبحث همنهشتی است که در سال گذشته با آن آشنا شده ایم.

۴-۶- نمایش اعداد صحیح

استفاده از دستگاه دهدهی (اعشاری) متداول ترین صورت نمایش اعداد است. اعداد طبیعی را می توان به صورت ضرایب توان های 10^0 نمایش داد. مثلاً عدد 34765 عبارت است از:

$$3 \times 10^4 + 4 \times 10^3 + 7 \times 10^2 + 6 \times 10^1 + 5 \times 10^0$$

شاید یکی از دلایل نمایش اعداد در دستگاه دهدهی یا به اصطلاح در «مبنای یا پایه ی 10^0 » وجود 10^0 انگشت دست بوده که در شمارش طبیعی به کار می رفته است. این نحوه ی نمایش را ابتدا هندی ها قبل از سال 800 میلادی اختراع کرده اند. این مطلب را محمدبن موسی خوارزمی در کتاب «جمع و تفریق، بر طبق حساب هندی» شرح داده و نمایش رقم صفر با نماد 0 هم برای اولین بار در این کتاب آمده است. اروپایی ها این دستگاه را هندی - عربی می نامند. دستگاه دیگری هم که در ریاضیات اسلامی وجود داشته، دستگاه شصت شصتی بوده که مسلمان ها فکر آن را از بابلی ها گرفتند و آن را تکمیل کردند. مبنای این نمایش عدد شصت بوده است، که در ارتباط با محاسبات نجومی و تقسیم ساعت به 60 دقیقه و دقیقه به 60 ثانیه است. با نمایش اعداد در مبنای 2 هم که در نمایش داخلی کامپیوتر به کار می رود آشنا هستیم.

به طور کلی هر عدد طبیعی بزرگ تر از 1 می تواند مبنا باشد.

قضیه ی ۵: اگر b یک عدد طبیعی بزرگ تر از 1 باشد، هر عدد طبیعی n را می توان به طریقی یکتا به صورت

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

نمایش داد، که در آن k یک عدد حسابی^۱ است و برای هر $j = 0, 1, 2, \dots, k$ ، $0 \leq a_j \leq b-1$ و $a_k \neq 0$.

اثبات: اگر الگوریتم تقسیم را متوالیاً به صورت زیر به کار گیریم، قضیه ثابت می شود. ابتدا n را بر b تقسیم می کنیم.

$$n = bq_0 + a_0 \quad 0 \leq a_0 \leq b-1$$

$$q_0 = bq_1 + a_1 \quad 0 \leq a_1 \leq b-1$$

حال q_0 را بر b تقسیم می کنیم

۱- هر عدد صحیح نامنفی را حسابی گویند.

این عمل را ادامه می دهیم

$$q_1 = bq_2 + a_2 \quad 0 \leq a_2 \leq b-1$$

$$q_j = bq_{j+1} + a_{j+1} \quad 0 \leq a_{j+1} \leq b-1$$

⋮

⋮

$$n > q_0 > q_1 > q_2 > \dots \geq 0$$

در دنباله ی q_0, q_1, q_2, \dots داریم :

(دقت کنید : $q_j > q_{j+1}$ مگر وقتی که $q_{j+1} = 0$ ، چون در غیر این حالت، $b > 1$ ، $a_{j+1} \geq 0$)

و $q_{j+1} \geq 1$ پس

$$(q_j = bq_{j+1} + a_{j+1} > q_{j+1})$$

لذا این کار را حداکثر تا n مرحله می توان ادامه داد. چون دقیقاً $n-1$ عدد صحیح مختلف

بین صفر و n وجود دارند. پس در مرحله ای $q_k = 0$ داریم :

$$q_{k-1} = b \times 0 + a_k, \quad 0 \leq a_k \leq b-1$$

اگر به ترتیب به جای هر $q_{k-1}, q_{k-2}, \dots, q_2, q_1, q_0$ حاصل تقسیم آن را بنویسیم، فرمول مورد نظر به دست می آید و بدیهی است که $a_k \neq 0$ ، زیرا اگر $a_k = 0$ آن گاه $q_{k-1} = 0$ ، و یک مرحله ی

قبل از آن توقف می کردیم. اثبات یکتایی این نمایش را در مقاطع تحصیلی بالاتر خواهید دید. □

(در این حالت n را به صورت زیر نمایش می دهند :

$$n = (a_k a_{k-1} a_{k-2} \dots a_1 a_0)_b$$

این نمایش را 1 ، نمایش عدد n در مبنای b می نامند. هریک از a_i ها را یک رقم در مبنای b

گویند و $k+1$ ، تعداد ارقام عدد n در مبنای b است و می گویند n در مبنای b ، $k+1$ رقم دارد.)

نمایش اعداد در دستگاه دودویی، یا در مبنای 2 ، به دلیل کاربرد آن در کامپیوتر و نیز تناظری

که در رابطه با پرتاب سکه در احتمال دارد بسیار جالب است. علاوه بر آن، قضیه ی 5 در رابطه با پیدا

کردن باقیمانده ی تقسیم بر برخی از اعداد به کار می رود. به مثال زیر توجه کنید.

مثال ۴: قاعده ی پیدا کردن باقیمانده ی تقسیم بر 3 یا 9

اگر $A = (a_n \dots a_1 a_0)_b$ می دانیم این عدد برابر است با

$$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_1 \times 10 + a_0$$

۱- در برخی از کتاب ها نمایش این عدد به صورت $\overline{a_k a_{k-1} \dots a_1 a_0}$ است.

$$\begin{aligned}
 &= \underbrace{(99 \cdots 9)}_n + 1) a_n + \underbrace{(99 \cdots 9)}_{n-1} + 1) a_{n-1} + \cdots + (9+1) a_1 + a \\
 &= 9 \underbrace{(11 \cdots 1)}_n a_n + \underbrace{(11 \cdots 1)}_{n-1} a_{n-1} + \cdots + a_1) + a_n + a_{n-1} + \cdots + a_1 + a.
 \end{aligned}$$

پس باقیمانده‌ی تقسیم A بر ۹ (یا ۳) برابر است با باقیمانده‌ی مجموع

$$a_n + a_{n-1} + \cdots + a_1 + a.$$

بر ۹ (یا ۳). به روش مشابه، قاعده‌ی پیدا کردن باقیمانده‌ی تقسیم یک عدد بر ۱۱ را نیز می‌توان پیدا کرد. (چگونه؟)

Δ

۴-۷- تمرین‌ها

۱- کوچک‌ترین و بزرگ‌ترین عضو مجموعه‌های زیر را در صورت وجود پیدا کنید:

$$A = \{x \in \mathbb{Z} : 0 \leq x < 5\} \quad (\text{الف})$$

$$C = \{x \in \mathbb{Z} : 0 < x \leq 1\} \quad (\text{ب})$$

$$E = \{x \in \mathbb{Z} : 0 \leq x < 1\} \quad (\text{پ})$$

(بزرگ‌ترین عضو مجموعه‌ی S عبارت است از $s_1 \in S$ ، که برای هر $s \in S$ داشته باشیم $s \leq s_1$.)

۲- زیرمجموعه‌ای از اعداد صحیح مثال بزنید که کوچک‌ترین عضو نداشته باشد.

۳- ثابت کنید که هر مجموعه‌ی ناتهی از اعداد صحیح و از پایین کراندار، دارای کوچک‌ترین

عضو و هر مجموعه‌ی ناتهی از اعداد صحیح و از بالا کراندار دارای بزرگ‌ترین عضو است.

(یادآوری می‌کنیم که $A \subset \mathbb{Z}$ از بالا کراندار است اگر عددی مانند $n \in \mathbb{Z}$ یافت شود که به

ازای هر $a \in A$ ، $a \leq n$ و همچنین $A \subset \mathbb{Z}$ از پایین کراندار است اگر عددی مانند $n \in \mathbb{Z}$ یافت

شود که برای هر $a \in A$ ، $n \leq a$.)

۴- خاصیت ارشمیدسی:

ثابت کنید اگر a و b دو عدد طبیعی باشند، آن‌گاه یک عدد طبیعی n وجود دارد به طوری که

$$na \geq b.$$

۱- نماد $s_1 = \max S$ برای بزرگ‌ترین عضو مجموعه‌ی S به‌کار می‌رود.

۵- ثابت کنید $\binom{n}{k}$ برای اعداد طبیعی n و $0 \leq k \leq n$ همیشه عدد طبیعی است.

۶- الف) برای $n \geq 2$ ، ثابت کنید:

$$\binom{2}{2} + \binom{3}{2} + \dots + \binom{n}{2} = \binom{n+1}{3}$$

ب) با استفاده از قسمت الف و این که برای هر عدد طبیعی $m \geq 2$ ،

$$2 \binom{m}{2} + m = m^2$$

ثابت کنید که

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(n+2)}{6}$$

۷- کدام یک از اعداد زیر بر ۲۲ تقسیم پذیرند؟

الف) ۰ (ب) ۴۴۴

پ) ۱۷۱۶ (ت) ۳۲۵۱۶

۸- الف) اگر a, b, c, d اعداد صحیح باشند و $a \neq 0, c \neq 0, a|b, c|d$ و ثابت کنید

$ac|bd$.

ب) نشان دهید اگر a, b و $c \neq 0$ اعداد صحیح باشند، آن گاه $a|b$ اگر و تنها اگر $ac|bc$.

پ) ثابت کنید اگر برای هر $a|b_i, i=1, 2, \dots, n$ آن گاه برای اعداد صحیح دلخواه m_1, m_2, \dots, m_n داریم

$$a | m_1 b_1 + m_2 b_2 + \dots + m_n b_n$$

۹- خارج قسمت و باقیمانده را در الگوریتم تقسیم هریک از اعداد زیر، وقتی که بر ۱۷ تقسیم

شوند به دست آورید.

الف) ۱۰۰ (ب) ۴۴-

۱۰- الف) ثابت کنید حاصل جمع دو عدد صحیح زوج و هم چنین حاصل جمع دو عدد

صحیح فرد، زوج است.

ب) ثابت کنید حاصل ضرب دو عدد فرد، فرد است.

۱۱- الف) ثابت کنید حاصل ضرب هر دو عدد به صورت $4q+1$ و هم چنین حاصل ضرب هر

- دو عدد به صورت $4q + 3$ ، به صورت $4q + 1$ است. ($q \in \mathbb{Z}$)
- (ب) ثابت کنید منبع هر عدد فرد به صورت $8q + 1$ است.
- ۱۲- نشان دهید حاصل ضرب دو عدد به صورت $6q + 5$ به صورت $6q + 1$ است.
- ۱۳- ثابت کنید حاصل ضرب ۳ عدد طبیعی متوالی بر ۶ تقسیم پذیر است.
- ۱۴- الف) عدد ۲۳۶ را در مبنای ۷ بنویسید.
- (ب) عدد $(10010011)_2$ برابر چه عددی در مبنای 10 است؟
- (پ) عدد 1864 را در مبنای ۲ بنویسید.
- (ت) عدد $(a35b06)_8$ را در مبنای 10 بنویسید.
- (دقت کنید که اگر مبنا بیشتر از 10 باشد، ارقام بیشتر از ۹ را به ترتیب با a, b, c, d و ... نمایش می‌دهند، یعنی مثلاً در مبنای ۱۶، $a=10, b=11, c=12, d=13, e=14, f=15$. البته گاهی هم عدد بالا را با (605110310) هم نمایش می‌دهند.)

مجله‌ی ریاضی

دستگاه اعداد رمزی را ابتدا یونانی‌ها به کار گرفتند. در این دستگاه، اعداد را با حروف نمایش می‌دادند. در دوره‌ی بعد از ظهور اسلام نیز به وفور از حروف ابجد استفاده می‌شد و محاسباتی با آن‌ها صورت می‌گرفت. این طریقه محاسبه را حساب جُمَّل می‌گویند و جدول آن به شرح زیر است:

۱	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
	ک	ل	م	ن	س	ع	ف	ص	
	۲۰	۳۰	۴۰	۵۰	۶۰	۷۰	۸۰	۹۰	
ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
۱۰۰	۲۰۰	۳۰۰	۴۰۰	۵۰۰	۶۰۰	۷۰۰	۸۰۰	۹۰۰	۱۰۰۰

حساب جُمَّل (حساب ابجدی) در ضبط تاریخ حوادث به عنوان ماده‌ی تاریخ به کار می‌رود.

فصل ۵

اعداد اول

در فصل قبل، تقسیم پذیری هر دو عدد صحیح به عنوان یک رابطه مطرح شد. برخی از اعداد بر تعداد زیادی از اعداد طبیعی تقسیم پذیرند، مثل ۲۴ که بر اعداد طبیعی ۱، ۲، ۳، ۴، ۶، ۸، ۱۲ و ۲۴ تقسیم پذیر است. با این حال دسته‌ای دیگر از اعداد طبیعی هیچ مقسوم‌علیهی به جز ۱ و خود آن عدد ندارند. این اعداد غیر ۱ را اعداد اول می‌نامند.

تعریف: هر عدد طبیعی غیر از ۱ را که جز بر ۱ و خودش بر هیچ عدد طبیعی دیگری تقسیم پذیر نباشد عدد اول گویند. هر عدد طبیعی به جز ۱ را که اول نیست، عدد مرکب می‌نامند.

مثال ۱: اعداد ۲، ۳، ۵، ۷ و ۱۱ اول و اعداد ۴، ۶، ۸، ۹ و ۱۰ مرکب‌اند.

قضیه ۱: هر عدد صحیح به جز ۱ و -۱ حداقل یک مقسوم‌علیه اول دارد.

اثبات: هر عدد صحیح مورد نظر را a می‌نامیم. اگر $a = 0$ ، هر عدد اولی آن را می‌شمارد.

اگر $a \neq 0$ ، فرض می‌کنیم S مجموعه‌ی تمام مقسوم‌علیه‌های بزرگ‌تر از ۱ عدد صحیح a باشد. S تهی نیست، چون $|a| \in S$. کوچک‌ترین عضو S را m می‌نامیم. (چرا S کوچک‌ترین عضو دارد؟) m اول است، زیرا اگر m اول نباشد آن‌گاه عدد طبیعی $m_1 > 1$ ، $m_1 \neq m$ وجود دارد که $m_1 | m$. پس m_1 هم عضو S است (چرا؟) که با کوچک‌تر بودن m در تناقض است. پس a حتماً یک مقسوم‌علیه اول مانند m دارد.

قضیه ۲: بی‌نهایت عدد اول وجود دارند.

اثبات: می‌دانیم اعداد ۲، ۳، ۵ و ... اول‌اند، حال اگر این دنباله متناهی باشد، فرض می‌کنیم

۱- این قضیه را اقلیدس در حدود سال ۳۰۰ قبل از میلاد اثبات کرده است.

p_1, p_2, \dots, p_n تنها عدد اول باشند. $m = p_1 p_2 \dots p_n + 1$ را در نظر می‌گیریم. چون m یک عدد طبیعی و مخالف p_1, p_2, \dots, p_n است، m باید مرکب باشد. پس یک مقسوم‌علیه اول دارد که آن را P_j می‌نامیم. داریم:

$$p_j | m, p_j | p_1 p_2 \dots p_n$$

پس $m - (p_1 p_2 \dots p_n) = 1$ بر p_j تقسیم‌پذیر است. یعنی $p_j | 1$ که غیر ممکن است. لذا تعداد

□

اعداد اول نامتناهی است.

قضیه‌ی ۳: اگر n یک عدد مرکب باشد، آن‌گاه n حداقل یک مقسوم‌علیه اول کوچک‌تر از

\sqrt{n} یا مساوی با آن دارد.

اثبات: چون n مرکب است، پس $n = ab$ به طوری که $1 < a \leq b < n$. اگر $a > \sqrt{n}$ ، آن‌گاه

$b > \sqrt{n}$ و در نتیجه $n = ab > n$ که یک تناقض است. پس حتماً $a \leq \sqrt{n}$. چون $a \neq 1$ ، پس بنابر

قضیه‌ی ۱ عدد اول p وجود دارد که $p | a$ و چون $a | n$ پس $p | n$. اما $p \leq a$ ، یعنی عدد اول p

وجود دارد که $p | n$ و $p \leq \sqrt{n}$.

به کمک قضیه‌ی ۳ می‌توان اول بودن هر عددی را بررسی کرد.

مثال ۲: می‌خواهیم تحقیق کنیم عدد ۴۷ اول است یا نه. مشاهده می‌کنیم:

$$2/47, 3/47, 5/47$$

و چون $6 < \sqrt{47} < 7$ ، لذا تنها اعداد اول کوچک‌تر از $\sqrt{47}$ یا مساوی با آن اعداد ۲، ۳ و ۵

هستند که هیچ‌کدام ۴۷ را نمی‌شمارند. پس ۴۷ اول است.

قضیه‌ی ۳ اساس فرایند غربال اراتستن است. مثلاً برای تعیین اعداد اول کوچک‌تر

از ۱۰۰، تمام مضرب‌های اول اعداد کوچک‌تر از $\sqrt{100} = 10$ یعنی مضرب‌های ۲، ۳، ۵ و

۷ را از جدول اعداد از ۱ تا ۱۰۰ حذف می‌کنیم. جدول صفحه‌ی بعد نمونه‌ای از غربال

اراتستن است.

	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰
۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰
۳۱	۳۲	۳۳	۳۴	۳۵	۳۶	۳۷	۳۸	۳۹	۴۰
۴۱	۴۲	۴۳	۴۴	۴۵	۴۶	۴۷	۴۸	۴۹	۵۰
۵۱	۵۲	۵۳	۵۴	۵۵	۵۶	۵۷	۵۸	۵۹	۶۰
۶۱	۶۲	۶۳	۶۴	۶۵	۶۶	۶۷	۶۸	۶۹	۷۰
۷۱	۷۲	۷۳	۷۴	۷۵	۷۶	۷۷	۷۸	۷۹	۸۰
۸۱	۸۲	۸۳	۸۴	۸۵	۸۶	۸۷	۸۸	۸۹	۹۰
۹۱	۹۲	۹۳	۹۴	۹۵	۹۶	۹۷	۹۸	۹۹	۱۰۰

و در نتیجه تنها اعداد اول بین ۱ تا ۱۰۰ عبارت‌اند از :

۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹, ۳۱, ۳۷, ۴۱, ۴۳, ۴۷, ۵۳, ۵۹, ۶۱, ۶۷, ۷۱, ۷۳, ۷۹, ۸۳, ۸۹, ۹۷

۵-۱- بزرگ‌ترین مقسوم‌علیه مشترک

می‌دانیم که عدد صحیح c را مقسوم‌علیه یا شمارنده‌ی مشترک دو عدد صحیح a و b گویند

هرگاه $c|a$ و $c|b$.

تعریف: عدد طبیعی d را بزرگ‌ترین مقسوم‌علیه مشترک (ب.م.م) دو عدد صحیح a و

b (که حداقل یکی از آن‌ها مخالف صفر است) گویند، اگر d یک مقسوم‌علیه مشترک a و b باشد، و

مقسوم‌علیه‌های مشترک دیگر a و b ، از d کوچک‌تر باشند. بزرگ‌ترین مقسوم‌علیه مشترک دو عدد

a و b را با (a, b) نمایش می‌دهند.

۱- مقسوم‌علیه مشترک a و b را با نماد $a \square b$ هم نمایش می‌دهند.

مثال ۳: مقسوم‌علیه‌های مشترک ۲۴ و ۸۴ عبارت‌اند از:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$$

پس:

$$(24, 84) = 12$$

با استفاده از نتایج اصل خوش‌ترتیبی می‌توان ثابت کرد که ب.م.م دو عدد صحیح (که هر دو صفر نیستند) همواره وجود دارد. (چرا؟) علاوه بر آن قضیه‌ی زیر را داریم:

قضیه‌ی ۴: بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح a و b که حداقل یکی از آنها صفر نیست، برابر است با کوچک‌ترین عضو مجموعه‌ی

$$S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$$

اثبات: مجموعه‌ی S حداقل یک عضو دارد (چرا؟) پس دارای کوچک‌ترین عضو است. فرض می‌کنیم d کوچک‌ترین عضو S باشد،

$$d = m_0 a + n_0 b > 0, \quad m_0, n_0 \in \mathbb{Z}$$

از الگوریتم تقسیم داریم

$$a = dq + r, \quad 0 \leq r < d$$

اگر $r > 0$ می‌دانیم $r \notin S$ چون $r < d$ ، ولی

$$r = a - m_0 a q - n_0 b q = (1 - m_0 q)a - (n_0 q)b$$

ترکیب خطی a و b است که با کوچک‌ترین بودن d در تناقض است. پس $r = 0$. یعنی $d|a$. به همین ترتیب $d|b$. یعنی d مقسوم‌علیه مشترک a و b است. اگر $c|a$ ، $c|b$ و $c > 0$ ، آن‌گاه $c|(am_0 + bn_0)$ یعنی $c|d$ پس $c \leq d$. در نتیجه d بزرگ‌ترین مقسوم‌علیه مشترک a و b است.

□

می‌توان ثابت کرد که هرگاه $a = bq + r$ آن‌گاه $(a, b) = (b, r)$. (چرا؟)

این مطلب، زیربنای الگوریتم اقلیدس برای یافتن بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح a و b است.

الگوریتم اقلیدس بدین‌گونه عمل می‌کند که اگر $r_0 = a > 0$ و $r_1 = b > 0$ ، آن‌گاه

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1$$

۱- برای هر $ma + nb$ ، $m, n \in \mathbb{Z}$ را یک ترکیب خطی a و b می‌نامند.

پس :

$$(a, b) = (r_0, r_1) = (r_1, r_2)$$

هم چنین

$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2$$

$$(a, b) = (r_1, r_2) = (r_1, r_3)$$

⋮

$$r_{n-2} = r_{n-1} q_{n-2} + r_{n-1} \quad 0 \leq r_{n-1} < r_{n-2}$$

$$(a, b) = (r_{n-3}, r_{n-2}) = (r_{n-1}, r_{n-2})$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$

$$(a, b) = (r_{n-1}, r_{n-2}) = (r_{n-1}, r_n)$$

چون

$$a = r_0 > r_1 > r_2 \cdots \geq 0$$

پس از چند مرحله باقیمانده صفر خواهد شد، زیرا بیشتر از a عدد صحیح مختلف بین صفر و a نیست. پس برای یک عدد طبیعی n داریم $r_{n+1} = 0$ و $r_{n-1} = r_n q_n$ در نتیجه

$$(a, b) = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

که r_n آخرین باقیمانده‌ی غیر صفر در این رشته از تقسیم‌های متوالی است.

مثال ۴:

$$(30, 72) = (30, 72 - 2 \times 30) = (30, 12)$$

$$= (2 \times 12 + 6, 12) = (6, 12) = (6, 2 \times 6 + 0) = (6, 0) = 6$$

که معمولاً به صورت خلاصه‌ی نردبانی زیر می‌نویسند :

خارج قسمت	۲	۲	۲
۷۲	۳۰	۱۲	۶
باقیمانده	۱۲	۶	۰

△

قضیه‌ی ۵: عدد طبیعی d بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح a و b است اگر و

تنها اگر

$$(1) \quad d|a \text{ و } d|b \text{ و}$$

$$(2) \quad \text{هرگاه } c|a \text{ و } c|b \text{ و } c|d \text{ .}$$

اثبات: اگر $d = (a, b)$ آن‌گاه $d|a$ و $d|b$ یعنی شرط ۱ برقرار است. علاوه بر آن اعداد

صحیح m و n وجود دارند که

$$d = ma + nb$$

حال اگر $c|a$ و $c|b$ آن‌گاه $c|d$ یعنی شرط ۲ هم برقرار است.

برعکس اگر d در دو شرط فوق صدق کند و c یک مقسوم‌علیه مشترک مثبت a و b باشد،

$$\square \quad \text{آن‌گاه } c|d \text{ یعنی } c \leq d \text{ . پس } d \text{ بزرگ‌ترین مقسوم‌علیه مشترک } a \text{ و } b \text{ است.}$$

تعریف: دو عدد صحیح a و b را نسبت به هم اول یا متباین گویند، هرگاه $(a, b) = 1$.

$$\Delta \quad \text{مثال ۵: اعداد } 9 \text{ و } 10 \text{ و نیز دو عدد } 25 \text{ و } 42 \text{ نسبت به هم اول‌اند.}$$

با استفاده از قضیه‌ی ۴، می‌توان ثابت کرد که دو عدد صحیح a و b نسبت به هم اول‌اند اگر و

تنها اگر اعداد صحیح m و n وجود داشته باشند که

$$1 = ma + nb$$

قضیه‌ی ۶: (لم اقلیدس). اگر $a|bc$ و $(a, b) = 1$ آن‌گاه $a|c$.

اثبات: اعداد صحیح m و n را می‌توان پیدا کرد که برای آن‌ها

$$1 = ma + nb$$

پس:

$$c = cma + cnb$$

اما چون $a|bc$ ، پس $bc = aq$. در نتیجه

$$c = cma + naq = (cm + nq)a$$

$$\square \quad \text{یعنی } a|c \text{ .}$$

قضیه‌ی ۷: اگر p یک عدد اول باشد و $p|ab$ ، آن‌گاه $p|a$ یا $p|b$.

اثبات: اگر $p \nmid a$ ، آن‌گاه $(p, a) = 1$ ، زیرا اگر $(p, a) = d$ و $d \neq 1$ آن‌گاه $d = p$. (چرا؟)

پس $p|a$ که یک تناقض است. در نتیجه $(p, a) = 1$ ، پس طبق قضیه‌ی ۶، $p|b$.

\square

تعریف بزرگ‌ترین مقسوم‌علیه مشترک دو عدد را به چند عدد نیز می‌توان تعمیم داد:
تعریف: بزرگ‌ترین مقسوم‌علیه مشترک n عدد صحیح a_1, a_2, \dots, a_n که همگی آن‌ها صفر نیستند عبارت است از بزرگ‌ترین عدد صحیحی که تمام این اعداد صحیح را بشمارد. این عدد را با (a_1, a_2, \dots, a_n) نمایش می‌دهند. می‌توان ثابت کرد که

$$(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{n-2}, (a_{n-1}, a_n))$$

مثال ۶:

$$\begin{aligned} (24, 30, 72) &= (24, (30, 72)) \\ &= (24, 6) = 6 \end{aligned}$$

Δ

۵-۲- قضیه‌ی بنیادی حساب

نقش اصلی اعداد اول به عنوان عناصر سازنده‌ی تمام اعداد صحیح بسیار اهمیت دارد. در قضیه‌ی زیر این مطلب را بدون اثبات بیان می‌کنیم:

قضیه‌ی ۸: هر عدد طبیعی بزرگ‌تر از ۱ را می‌توان بدون توجه به ترتیب به‌طور یکتا به صورت حاصل‌ضرب اعداد اول نوشت. یعنی n را می‌توان به صورت $n = p_1 p_2 \dots p_k$ نمایش داد که در آن برای هر i ، p_i عددی اول است. این نمایش را تجزیه‌ی عدد n به عامل‌های اول می‌نامند. نکته‌ی ۱: در تجزیه اعداد طبیعی به عامل‌های اول، می‌توان حاصل‌ضرب چند عدد اول مساوی را به صورت توانی از آن نوشت، یعنی

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}$$

که در آن p_i ها اعداد اول متمایز و α_i ها اعدادی طبیعی‌اند. این نمایش را نمایش متعارف عدد n می‌نامند.

نکته‌ی ۲: برای $n=1$ ، می‌توان $1 = p^0$ را در نظر گرفت، درحالی‌که p هر عدد اولی می‌تواند باشد.

نکته‌ی ۳: به‌طور کلی هر عدد طبیعی را می‌توان به صورت زیر نمایش داد:

$$n = \prod_p p^{\alpha_p(n)} = 2^{\alpha_2(n)} 3^{\alpha_3(n)} 5^{\alpha_5(n)} \dots$$

که در آن \prod_p به مفهوم ضرب روی تمام اعداد اول است و برای هر عدد اول p ، $\alpha_p(n)$ بزرگ‌ترین توان p است که عدد n را می‌شمارد و به این صورت می‌نویسند:

$$p^{\alpha_p(n)} \parallel n$$

یعنی $p^{\alpha_p(n)} \mid n$ ولی $p^{\alpha_p(n)+1} \nmid n$ (واضح است که اگر $p > n$ ، حتماً $\alpha_p(n) = 0$)

حال قضیه‌ی زیر را بدون اثبات بیان می‌کنیم:

قضیه‌ی ۹: اگر $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ و $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ ، آن‌گاه

$$d = (a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}$$

که در آن برای هر عدد i ,

$$\gamma_i = \min\{\alpha_i, \beta_i\}$$

(دقت کنید که اگر برای عدد اول p ، $p \nmid n$ ، آن‌گاه توان آن را در نمایش n برابر با صفر

می‌گیریم.)

مثال ۷:

$$30 = 2^1 \times 3^1 \times 5^1$$

$$72 = 2^3 \times 3^2 = 2^3 \times 3^2 \times 5^0$$

$$\text{پس } (30, 72) = 2^1 \times 3^1 \times 5^0 = 6$$

Δ

۵-۳- کوچک‌ترین مضرب مشترک

می‌دانیم عدد صحیح c را مضرب مشترک دو عدد صحیح a و b نامند، هرگاه $a \mid c$ و $b \mid c$.

تعریف: عدد m را کوچک‌ترین مضرب مشترک (ک.م.م) دو عدد صحیح a و b نامند،

هرگاه m مضرب مشترک مثبت دو عدد a و b باشد و اگر $a \mid c$ و $b \mid c$ آن‌گاه $m \leq c$. کوچک‌ترین

مضرب مشترک دو عدد a و b را با $[a, b]$ نمایش می‌دهند.

وجود کوچک‌ترین مضرب مشترک دو عدد غیرصفر a و b را با استفاده از اصل خوش‌ترتیبی

می‌توان ثابت کرد.

۱- کوچک‌ترین مضرب مشترک a و b را با نماد $a \sqcup b$ هم نمایش می‌دهند.

مثال ۸: مضرب‌های مشترک مثبت اعداد ۴ و ۶ عبارت‌اند از:

$$۱۲, ۲۴, ۳۶, \dots$$

Δ

که کوچک‌ترین آن‌ها ۱۲ است. یعنی $[۴, ۶] = ۱۲$.

قضیه‌های زیر را که در رابطه با کوچک‌ترین مضرب مشترک دو عددند بدون اثبات بیان

می‌کنیم.

قضیه‌ی ۱۰: برای هر دو عدد صحیح غیرصفر a و b ، $m = [a, b]$ اگر و تنها اگر

$$a \mid m \text{ و } b \mid m$$

(۲) اگر $a \mid c$ و $b \mid c$ ، آنگاه $m \mid c$.

قضیه‌ی ۱۱: اگر $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ و $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ ، آنگاه

$$m = [a, b] = p_1^{\theta_1} p_2^{\theta_2} \dots p_n^{\theta_n}$$

که در آن برای هر i ، $\theta_i = \max\{\alpha_i, \beta_i\}$

قضیه‌ی ۱۲: برای هر دو عدد صحیح غیرصفر a و b داریم:

$$a, b = |ab|$$

مثال ۹:

$$۳۰ = ۲^1 \times ۳^1 \times ۵^1$$

$$۷۲ = ۲^3 \times ۳^2 = ۲^3 \times ۳^2 \times ۵^0$$

$$[۳۰, ۷۲] = ۲^3 \times ۳^2 \times ۵^1 = ۳۶۰$$

$$[۳۰, ۷۲] \times (۳۰, ۷۲) = ۳۶۰ \times ۶ = ۲۱۶۰$$

$$۳۰ \times ۷۲ = ۲۱۶۰$$

Δ

تعریف: کوچک‌ترین مضرب مشترک اعداد صحیح غیرصفر a_1, a_2, \dots, a_n عبارت است از

کوچک‌ترین عدد صحیح مثبت که بر همه‌ی آن‌ها تقسیم‌پذیر باشد، و آن را با $[a_1, a_2, \dots, a_n]$ نمایش

می‌دهند.

می‌توان ثابت کرد که

$$[a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_{n-2}, [a_{n-1}, a_n]]$$

مثال ۱۰:

$$[1^\circ, 4, 6] = [1^\circ, [4, 6]] = [1^\circ, 12] = 6^\circ$$

راه اول:

$$10 = 2^1 \times 5^1 = 2^1 \times 3^0 \times 5^1$$

راه دوم:

$$4 = 2^2 = 2^2 \times 3^0 \times 5^0$$

$$6 = 2 \times 3 = 2^1 \times 3^1 \times 5^0$$

$$[1^\circ, 4, 6] = 2^2 \times 3^1 \times 5^1 = 6^\circ$$

Δ

۴-۵- تمرین‌ها

۱- کدام یک از اعداد زیر اول و کدام یک مرکب‌اند؟

الف) ۱ ب) ۷۳۷ پ) ۱۸۹۱ ت) ۲۰۷۹۱

۲- ثابت کنید بی‌نهایت عدد اول به صورت $4q + 3$ یافت می‌شوند.

۳- اعداد زیر را به عوامل اول تجزیه کنید:

الف) ۹۵۵۵ ب) -۹۹۷۳ پ) ۳۷۴۲۳ ت) ۲۸۰۰۰

۴- نشان دهید که هر عدد طبیعی بزرگ‌تر از ۱ را می‌توان به صورت حاصل ضرب یک مربع

کامل و یک عدد صحیح بدون عامل مربع به جز ۱ (یعنی عددی که بر هیچ عدد مربعی جز ۱ قابل قسمت نباشد) نوشت.

۵- اگر p_1, p_2, \dots, p_n و q اعداد اول باشند و $q | p_1 p_2 \dots p_n$ ثابت کنید به ازای یک i ,

$$p_i = q, \quad 1 \leq i \leq n$$

۶- الف) نشان دهید اگر a نسبت به b و c اول باشد، نسبت به bc هم اول خواهد بود.

ب) نشان دهید اگر a نسبت به b_1, b_2, \dots, b_n اول باشد، نسبت به $b_1 b_2 \dots b_n$ هم اول

خواهد بود.

۷- نشان دهید اگر a و b نسبت به هم اول باشند و $c | a + b$ ، آن‌گاه c نیز نسبت به a و b اول

خواهد بود.

۸- الف) اگر a و b نسبت به هم اول باشند، نشان دهید که برای اعداد طبیعی m و n ، a^n و

b^m هم نسبت به هم اول‌اند.

ب) اگر برای عدد طبیعی n ، $a^n | b^n$ ثابت کنید $a | b$.

فصل ۶

همنهشتی

۶-۱- مفهوم همنهشتی

مفهوم همنهشتی را در سال‌های قبل دیده‌ایم. در زیر خلاصه‌ای از آنچه را که خوانده‌ایم بیان داشته و قضیه‌های مربوط به آن را مطرح می‌کنیم.

مسائلی از قبیل روزهای هفته، ساعت و ماه که حالت گردشی داشته و با افزودن عدد ثابتی (۷ روز، ۲۴ ساعت و یا ۱۲ ماه) به وضعیت و شرایط قبلی برمی‌گردند به عنوان مثال‌هایی عملی از نظریه‌ی همنهشتی هستند که در اوایل قرن نوزدهم به وسیله‌ی گاوس معرفی شد.

تعریف: فرض می‌کنیم m یک عدد طبیعی باشد، دو عدد صحیح a و b را به پیمانه‌ی m همنهشت گویند هرگاه $a - b$ مضرب m باشد، یعنی $a - b$ بر m تقسیم‌پذیر باشد.

همنهشت بودن دو عدد a و b به پیمانه‌ی m را به صورت‌های زیر نمایش می‌دهند:

$$a \equiv b \pmod{m} \text{ (پیمانه‌ی } m \text{)}$$

و یا

$$a \equiv b \pmod{m}$$

و می‌خوانند « a همنهشت با b به پیمانه‌ی m است»

مثال ۱: (پیمانه‌ی ۶) $۱۶ \equiv ۳۴$ ، زیرا $۱۸ = ۳۴ - ۱۶$ بر ۶ تقسیم‌پذیر است. ولی

(پیمانه‌ی ۶) $۵ \not\equiv ۸$ ، زیرا $۳ = ۸ - ۵$ بر ۶ تقسیم‌پذیر نیست.

△

۱- حتی در مورد اعداد حقیقی مثلاً در مورد مقادیر زاویه یا طول کمان (برحسب رادیان) در دایره‌ی مثلثاتی

(پیمانه‌ی 2π) $x \equiv y$ به کار می‌رود.

توجه کنید که نقیض (پیمانه‌ی m) $a \equiv b$ را چنین می‌نویسند :

$$a \not\equiv b \text{ (پیمانه‌ی } m)$$

همان‌طور که در سال قبل دیدیم، هم‌نهشتی یک رابطه‌ی هم‌ارزی روی مجموعه‌ی اعداد صحیح است و لذا رابطه‌ی هم‌نهشتی به پیمانه‌ی m ، مجموعه‌ی \mathbb{Z} را به دسته‌های هم‌ارزی افزایش می‌کند. مجموعه‌ی تمام دسته‌های هم‌نهشت به پیمانه‌ی m را با $\frac{\mathbb{Z}}{m}$ یا \mathbb{Z}_m و مجموعه‌ی تمام اعداد صحیحی را که با a هم‌نهشت به پیمانه‌ی m هستند با $[a]$ یا \bar{a} نمایش می‌دهند.

$[a]$ یک دسته‌ی هم‌ارزی و a نماینده‌ی این دسته است. اگر b عضو دیگری از دسته‌ی

هم‌ارزی $[a]$ باشد، داریم $[a] = [b]$ و به طور کلی می‌توان ثابت کرد که

$$[a] = [b]$$

اگر و تنها اگر

$$a \equiv b \text{ (پیمانه‌ی } m)$$

مثلاً در هم‌نهشتی به پیمانه‌ی ۶ داریم :

$$[15] = [3] = [-3] = \dots$$

$$[-5] = [1] = [7] = \dots$$

Δ

اگر چه در دسته‌های هم‌نهشتی، هر عدد از یک دسته‌ی هم‌نهشتی می‌تواند نماینده‌ی آن دسته انتخاب شود اما معمولاً کوچک‌ترین عدد صحیح غیرمنفی متعلق به هر دسته‌ی هم‌نهشتی را به عنوان نماینده انتخاب می‌کنند.

نکته: بنا به تعریف، از (پیمانه‌ی m) $a \equiv b$ نتیجه می‌شود که $a - b$ مضرب m است. یعنی

عدد صحیح k موجود است به طوری که $a - b = mk$ یا $a = b + mk$. یعنی تمام اعداد صحیحی

که با b به پیمانه‌ی m هم‌نهشت‌اند با افزودن مضربی از m بر b به دست می‌آیند. بنابراین :

$$[b] = \{b + mk : k \in \mathbb{Z}\}$$

مثال ۲: مجموعه‌ی تمام اعداد صحیح که به پیمانه‌ی ۷ با عدد ۴ هم‌نهشت‌اند عبارت است از :

$$[4] = \{4 + 7k : k \in \mathbb{Z}\} = \{\dots, -10, -3, 4, 11, 18, \dots\}$$

Δ

با توجه به آنچه گفته شد گزاره‌های زیر همگی معادل‌اند.

– a به پیمانه‌ی m با b همنهشت است.

– a و b به پیمانه‌ی m همنهشت‌اند.

– (پیمانه‌ی m) $a \equiv b$

– $[a] = [b]$

– a و b در یک دسته‌ی همنهشتی به پیمانه‌ی m قرار دارند.

– $a-b$ مضربی از m است.

– $m \mid (a-b)$

و با استفاده از الگوریتم تقسیم می‌توان ثابت کرد که همه‌ی گزاره‌های فوق با گزاره‌ی زیر معادل‌اند:

– باقیمانده‌های تقسیم a و b بر m با هم برابرند. (چرا؟)

۶-۲- برخی از ویژگی‌های همنهشتی

رابطه‌ی همنهشتی دارای ویژگی‌های مشابهی نظیر جمع و ضرب در \mathbb{Z} است. موارد زیر را

قبلاً خوانده‌ایم.

۱- اگر (پیمانه‌ی m) $a \equiv b$ ، آن‌گاه برای هر عدد صحیح c

(پیمانه‌ی m) $a+c \equiv b+c$

۲- اگر (پیمانه‌ی m) $a+c \equiv b+c$ ، آن‌گاه (پیمانه‌ی m) $a \equiv b$

۳- اگر (پیمانه‌ی m) $a \equiv b$ و (پیمانه‌ی m) $c \equiv d$ ، آن‌گاه

(پیمانه‌ی m) $a+c \equiv b+d$ و (پیمانه‌ی m) $ac \equiv bd$

۴- هرگاه (پیمانه‌ی m) $a_1 \equiv b_1$ و ... و (پیمانه‌ی m) $a_n \equiv b_n$ ، آن‌گاه

(پیمانه‌ی m) $a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n$

و

(پیمانه‌ی m) $a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_n$

۵- هرگاه (پیمانه‌ی m) $a \equiv b$ آن‌گاه برای هر $n \geq 1$ (پیمانه‌ی m) $a^n \equiv b^n$.

مثال ۳: مطلوب است باقی‌مانده‌ی 2^3 بر ۱۷

از $2^4 = 16$ و (پیمانه‌ی ۱۷) $16 \equiv -1$ نتیجه می‌شود که (پیمانه‌ی ۱۷) $2^4 \equiv -1$ اما
 (پیمانه‌ی ۱۷) $(2^4)^7 \equiv (-1)^7 \equiv -1$ یعنی (پیمانه‌ی ۱۷) $2^{28} \equiv -1$ از طرف دیگر داریم
 (پیمانه‌ی ۱۷) $2^2 \equiv 4$ و در نتیجه

$$2^{30} = 2^{28} \times 2^2 \equiv (-1) \times 4 \equiv -4 \quad (\text{پیمانه‌ی } 17)$$

اما (پیمانه‌ی ۱۷) $-4 \equiv 13$ ، پس (پیمانه‌ی ۱۷) $2^{30} \equiv 13$ یعنی باقی مانده‌ی 2^{30} بر ۱۷، عدد

Δ

۱۳ است.

۳-۶- تقسیم طرفین یک رابطه‌ی همنهشتی بر c

می‌دانیم که هرگاه (پیمانه‌ی m) $a \equiv b$ ، آنگاه برای هر عدد صحیح c،

$$ac \equiv bc \quad (\text{پیمانه‌ی } m)$$

حال عکس این مطلب را بررسی می‌کنیم. یعنی آیا برای هر عدد صحیح c، اگر (پیمانه‌ی m)

$ac \equiv bc$ آنگاه (پیمانه‌ی m) $a \equiv b$ ؟ ابتدا به مثال زیر توجه کنید:

می‌دانیم (پیمانه‌ی ۶) $21 \equiv 33$ یعنی (پیمانه‌ی ۶) $7 \times 3 \equiv 11 \times 3$ ، ولی (پیمانه‌ی ۶)

$$\frac{33}{3} \not\equiv \frac{21}{3}$$

اما قضیه‌ی زیر را در این مورد داریم:

قضیه ۱: در رابطه‌ی همنهشتی (پیمانه‌ی m) $ac \equiv bc$ داریم

$$a \equiv b \left(\frac{m}{d} \right) \quad (\text{پیمانه‌ی } \frac{m}{d})$$

که در آن $d = (m, c)$.

اثبات: از فرض نتیجه می‌شود که عدد صحیح k وجود دارد که

$$ac - bc = mk$$

یعنی:

$$(a - b)c = mk$$

اگر طرفین این تساوی را بر $d = (m, c)$ تقسیم کنیم، خواهیم داشت:

$$(a - b) \frac{c}{d} = \frac{m}{d} k$$

یعنی عدد صحیح $\frac{m}{d}$ ، عدد $\frac{c}{d}(a-b)$ را می‌شمارد. و چون $1 = (\frac{m}{d}, \frac{c}{d})$ (چرا؟) پس

$$\frac{m}{d}(a-b) \text{ یعنی:}$$

$$a \equiv b \pmod{\frac{m}{d}} \text{ (پیمانه‌ی } \frac{m}{d}\text{)}$$

□

مثال ۴: از (پیمانه‌ی ۶) $2 \equiv 8$ نتیجه می‌شود (پیمانه‌ی ۳) $1 \equiv 4$ Δ

۴-۶ حل معادله‌ی سیاله‌ی خطی $ax + by = c$

سؤال دیگری که مطرح می‌شود این است که آیا می‌توان معادله‌ی

$$(1) \quad ax + by = c$$

را که با معادله‌ی همبستگی

$$ax \equiv c \pmod{b} \text{ (پیمانه‌ی } b\text{)}$$

هم‌ارز است، در \mathbb{Z} حل کرد؟ در این معادله $a, b, c \in \mathbb{Z}$. به عبارت دیگر، آیا می‌توان عددهای صحیحی چون x_0, y_0 را یافت که

$$(2) \quad ax_0 + by_0 = c$$

اگر عددهای صحیح x_0, y_0 وجود داشته باشند که در رابطه‌ی (۲) صدق کنند، آن‌گاه می‌گوییم

معادله‌ی سیاله‌ی خطی $ax + by = c$ جواب دارد. در این رابطه قضیه‌ی زیر را داریم:

قضیه‌ی ۲: معادله‌ی سیاله‌ی خطی $ax + by = c$ در مجموعه‌ی \mathbb{Z} جواب دارد اگر و تنها

اگر بزرگ‌ترین مقسوم‌علیه مشترک a و b ، عدد c را بشمارد.

اثبات: اگر $d = (a, b)$ و $d|c$ آن‌گاه عدد صحیح k وجود دارد که $c = dk$ و چون d بزرگ‌ترین

مقسوم‌علیه مشترک a و b است، $d = am + bn$ که در آن $m, n \in \mathbb{Z}$. بنابراین

$$c = dk = a(mk) + b(nk)$$

یعنی اعداد صحیح $x_0 = mk$ و $y_0 = nk$ در معادله‌ی $ax + by = c$ صدق می‌کنند. پس

$ax + by = c$ دارای جواب است. برعکس اگر $ax + by = c$ دارای جواب باشد، اعداد صحیح

x_0 و y_0 وجود دارند که $ax_0 + by_0 = c$. اما چون $d|a$ و $d|b$ در نتیجه $d|ax_0 + by_0$

□

یعنی $d|c$.

می‌توان ثابت کرد که اگر $(a, b) = d$ و x_0 و y_0 یک جواب برای معادله‌ی خطی $ax + by = c$ باشد، آن گاه تمام جواب‌های آن به صورت $x = x_0 + k \frac{b}{d}$ و $y = y_0 - k \frac{a}{d}$ است که در آن $k \in \mathbb{Z}$.

در مثال زیر، روشی را برای حل معادله‌های سیاله نشان می‌دهیم:

مثال ۵: شخصی می‌خواهد با ۵۱۰۰ ریال کتاب بخرد. اگر ۵۰۰ ریالی و ۲۰۰ ریالی باشند، چند ۵۰۰ ریالی و چند ۲۰۰ ریالی باید بپردازد؟

حل مسأله مستلزم پیدا کردن اعداد صحیح نامنفی x و y است که برای آن‌ها

$$200x + 500y = 5100$$

یا

$$2x + 5y = 51$$

چون $(5, 2) = 1$ و $1 | 51$ ، معادله‌ی فوق جواب دارد. می‌نویسیم:

$$x = \frac{51 - 5y}{2} = \frac{50 - 4y + 1 - y}{2} = 25 - 2y + \frac{1 - y}{2}$$

پس $\frac{1 - y}{2}$ یک عدد صحیح است، یعنی عددی مانند m وجود دارد که $1 - y = 2m$. یا

$$y = 1 - 2m \text{ در نتیجه}$$

$$x = 25 - 2 + 4m + m = 5m + 23$$

ولی x و y منفی نیستند، پس $1 - 2m \geq 0$ و $5m + 23 \geq 0$ یا $m \geq \frac{-23}{5} = -4/6$ و $m \leq \frac{1}{2}$.

پس m مقادیر $0, -1, -2, -3, -4$ را می‌گیرد. یعنی تعداد بن‌های ۲۰۰ ریالی و ۵۰۰ ریالی به ترتیب می‌تواند جفت‌های زیر باشند:

$$9, 3 \quad 7, 8 \quad 5, 13 \quad 3, 18 \quad 1, 23$$

Δ

مجله‌ی ریاضی

تابع حسابی اویلر

تعریف: برای هر عدد طبیعی n ، $\phi(n)$ عبارت است از تعداد اعداد طبیعی کوچک‌تر از n یا مساوی با n که نسبت به n اول‌اند. این ضابطه، تابعی روی اعداد طبیعی تعریف می‌کند که آن را تابع حسابی اویلر می‌گویند.

بدیهی است که اگر p یک عدد اول باشد آن‌گاه $\phi(p) = p - 1$.

قضیه‌ی اویلر: اگر m عددی طبیعی و a عددی صحیح باشد که $\gcd(a, m) = 1$ آن‌گاه

$$a^{\phi(m)} \equiv 1 \pmod{m} \quad (\text{پیمانه‌ی } m)$$

قضیه‌ی ویلسن: اگر p عددی اول باشد آن‌گاه

$$(p-1)! \equiv -1 \pmod{p} \quad (\text{پیمانه‌ی } p)$$

۶-۵- تمرین‌ها

۱- دو عدد a و b به صورت‌های زیر نوشته شده‌اند:

$$a = 7k + 5, \quad b = 7k' - 2$$

دسته‌ی همنهشتی $a + 2b$ را به پیمانه‌ی ۷ مشخص کنید.

۲- هرگاه (پیمانه‌ی m) $a \equiv b$ و d یک مقسوم‌علیه m باشد، نشان دهید (پیمانه‌ی d) $a \equiv b$.

۳- ثابت کنید

الف) اگر r باقی‌مانده‌ی تقسیم a بر m باشد، آنگاه (پیمانه‌ی m) $a \equiv r$.

ب) اگر (پیمانه‌ی m) $a \equiv b$ و c عدد صحیح باشد، آنگاه

$$ac \equiv bc \pmod{m} \quad (\text{پیمانه‌ی } m)$$

پ) اگر (پیمانه‌ی m) $a + b \equiv c$ ، آنگاه (پیمانه‌ی m) $a \equiv c - b$

ت) اگر m و c نسبت به هم اول باشند و (پیمانه‌ی m) $ac \equiv bc$ ، آنگاه

$$a \equiv b \pmod{m} \quad (\text{پیمانه‌ی } m)$$

۴- ثابت کنید که برای هر دو عدد صحیح a و b

$$(a \pm b)^2 \equiv a^2 + b^2 \pmod{ab} \text{ (پیمانه‌ی } ab \text{)}$$

$$(a \pm b)^3 \equiv a^3 \pm b^3 \pmod{ab} \text{ (پیمانه‌ی } ab \text{)}$$

۵- ثابت کنید $1 - 2^{11}$ بر 23 تقسیم پذیر است.

۶- آخرین رقم سمت راست هریک از اعداد 3424 و 7101 را به دست آورید.

۷- برای هریک از معادلات سیاله‌ی زیر یا تمام جواب‌ها را به دست آورید و یا ثابت کنید جواب

ندارد.

$$17x + 13y = 100 \text{ (ب)}$$

$$2x + 5y = 11 \text{ (الف)}$$

$$60x + 18y = 97 \text{ (ت)}$$

$$21x + 14y = 147 \text{ (پ)}$$

۸- پستخانه‌ای فقط تمبرهای 140 و 210 ریالی برای فروش دارد. برای چسباندن تمبر به بسته‌هایی که مقدار تمبر لازم برای آن‌ها هریک از مقادیر زیر است، در صورت امکان ترکیبی از این دو نوع تمبر تعیین کنید.

$$4000 \text{ ریال (ب)}$$

$$3500 \text{ ریال (الف)}$$

مجله‌ی ریاضی

برای اعداد طبیعی $n \geq 3$ معادله‌ی سیاله‌ی $x^n + y^n = z^n$ هیچ جواب غیربدیهی در بین اعداد صحیح ندارد.

بسیاری از مطالعات و پیشرفت‌های نظریه‌ی اعداد مدیون تلاش برای حل این مسأله بوده که فرما در قرن هفدهم در حاشیه‌ی کتاب حساب دیوفانتوسی خود ادعا کرده که این مسأله را حل کرده است. در سال ۱۹۹۳ با استفاده از نظریه‌های پیشرفته‌ی ریاضی آندرو وایلز حلی برای آن ارائه کرد که پس از چندی اشکالی در آن پیدا شد. ولی سرانجام در سپتامبر ۱۹۹۴ (شهریور ماه ۱۳۷۳) اشکال این حل به وسیله‌ی خود وایلز و با همکاری یکی از همکارانش به نام تیلر برطرف شد.

مراجع

1 – D.M. Burton, Elementary Number Theory, Allyn and Bacon, Inc. 1976.

2 – K.H. Rosen, Elementary Number Theory and its Applications, 3rd ed., Addison Wesley 1992.

۳- ویلیام و. آدامز و لری جوئل گولدشتین، آشنایی با نظریه‌ی اعداد، ترجمه‌ی آدینه محمدنارنجانی، مرکز نشر دانشگاهی، تهران، چاپ اول ۱۳۶۲.

۴- ابوالقاسم قربانی و حسن صفاری، حساب استدلالی، چاپ ششم مؤسسه مطبوعاتی علی اکبر علمی ۱۳۴۷.

۵- غلامرضا دانش ناروئی و میرزا جلیلی، ریاضیات جدید سال چهارم متوسطه عمومی ریاضی- فیزیک. دفتر برنامه‌ریزی و تألیف کتب درسی وزارت آموزش و پرورش ۱۳۶۰.

۶- غلامحسین مصاحب، تئوری مقدماتی اعداد. جلد اول - انتشارات دهخدا ۱۳۵۳.

قسمت سوم

مباحثی دیگر از ترکیبیات

مقدمه

در قسمت اول با نظریه‌ی گراف‌ها که یکی از مباحث ترکیبیات است آشنا شدیم. در این قسمت با مباحثی دیگر از ترکیبیات آشنا می‌شویم. ترکیبیات معمولاً با مجموعه‌های متناهی سروکار دارد و لذا یکی از مباحث ترکیبیات، شمارش است. در اینجا با بعضی از ابزارهای شمارش آشنا می‌شویم. کلاً به مقدمات بسنده می‌کنیم، با این امید که دانش‌آموزان با این آشنایی اولیه انگیزه‌ی کافی پیدا کنند که خود در این مباحث به مطالعه بپردازند.

در فصل ۷ نشان می‌دهیم گراف‌ها چگونه می‌توانند به فهم مطالب دیگر ریاضی کمک کنند. گراف‌ها و ماتریس‌های متناظر با آن‌ها با شکل و شمایل شهودی که دارند به تجسم مفاهیم انتزاعی کمک می‌کنند. یکی از دلایلی که همه‌ی ما از هندسه خوشمان می‌آید شهودی بودن آن است. گراف نیز همان امتیاز را دارد. به‌علاوه چون در رسم نمودار گراف طول یال‌ها و یا مکان رأس‌ها مطرح نیست درک شهودی ساده‌تر می‌شود. در بخش ۷-۱ بعضی از این استفاده‌های شهودی را مطرح می‌کنیم. در مطالعه‌ی مجموعه‌ها نیز می‌توان نمودارهایی به آن‌ها نسبت داد. این نمودارها به درک مفاهیم کمک زیادی می‌کنند. با استفاده از این نمودارها حتی می‌توانیم مفاهیمی را که یاد گرفته‌ایم تعمیم دهیم. بخش ۷-۳ به این موضوع اختصاص دارد. با تعمیم این مفاهیم یک ابزار شمارشی به نام اصل شمول و عدم شمول را خواهیم دید. در فصل ۸ یکی دیگر از مباحث ریاضی به نام دنباله‌های بازگشتی را به عنوان یک ابزار شمارشی به کار خواهیم گرفت.



مدل های شهودی و تجسمی در ترکیبیات

۷-۱- رابطه ها و گراف ها

مفاهیم مربوط به رابطه را که در کتاب جبر و احتمال سال سوم دیده ایم یادآوری می کنیم.
 تعریف: هرگاه A و B دو مجموعه باشند، آن گاه یک رابطه از A به B عبارت است از زیرمجموعه ای از $A \times B$. زیرمجموعه های $A \times A$ را رابطه های روی A می گویند.

مثال ۱: روی مجموعه ی اعداد صحیح \mathbb{Z} یک رابطه ی R را می توان چنین تعریف کرد:

$$aRb \text{ یا } (a, b) \in R \text{ هر گاه } a \leq b.$$

این رابطه همان رابطه ی معمولی «کوچکتر از یا مساوی با» روی \mathbb{Z} است که روی Q ، مجموعه ی

اعداد گویا، و روی \mathbb{R} ، مجموعه ی اعداد حقیقی، نیز تعریف می شود. Δ

مثال ۲: برای هر دو عضو $x, y \in \mathbb{Z}$ تعریف می کنیم:

$$(x, y) \in R \text{ یا } xRy \text{ هر گاه } x - y \text{ مضربی از } ۷ \text{ باشد.}$$

پس داریم: $9R2$ و $11R-3$ ، ولی $7R3$. Δ

مثال ۳: مجموعه ی $A = \{1, 2, 3, 4, 6, 12\}$ مفروض است. به ازای هر دو عضو $a, b \in A$

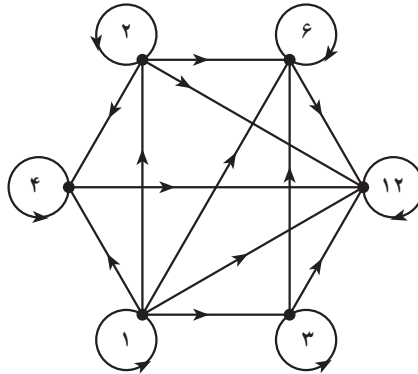
تعریف می کنیم: aRb هرگاه $a|b$. Δ

حال فرض کنید A یک مجموعه ی متناهی و R یک رابطه روی A باشد. به R گراف جهت دار

G را به صورت زیر نسبت می دهیم. رأس های G اعضای A هستند و رأس a به رأس b متصل است هرگاه aRb .

به عنوان مثال، شکل ۱، گراف مربوط به رابطه ای را که در مثال ۳ داده شده است نشان می دهد.

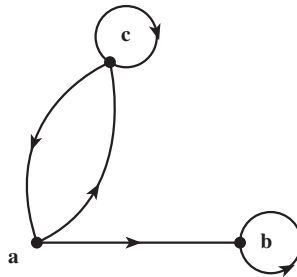
مثلاً رأس ۱ به تمام رئوس، حتی به خود ۱، وصل است زیرا عدد ۱ تمام اعداد صحیح را می شمارد.



شکل ۱- گراف جهت‌دار رابطه‌ی عا‌دکردن

متقابلاً هرگراف جهت‌دار نشانگر یک رابطه است. مثلاً از گراف شکل ۲ نتیجه می‌شود که رابطه‌ای مانند R روی مجموعه‌ی $A = \{a, b, c\}$ تعریف شده است و داریم:

aRb, aRc, bRb, cRa, cRc .



شکل ۲- گراف جهت‌دار یک رابطه

این تناظر بین گراف‌های جهت‌دار و رابطه‌ها به درک بسیاری از ویژگی‌های رابطه‌ها کمک می‌کند. مثلاً می‌توانید بازتابی، متقارن بودن یا نبودن رابطه‌ها را فوراً از روی گراف جهت‌دار مربوط تشخیص دهید. این ویژگی‌ها در درس‌های سال‌های قبل تعریف شده‌اند. یکی از ویژگی‌های رابطه‌ها که کاربرد فراوان دارد خاصیت پاد متقارن است. رابطه‌ی R را وقتی پاد متقارن گوئیم که به ازای هر زوج مرتب (a, b) ، اگر $(a, b) \in R$ و $(b, a) \in R$ آن‌گاه $a = b$. مثلاً رابطه‌ی «کوچکتر از یا مساوی با» در مثال ۱ و رابطه‌ی «عا‌دکردن» در مثال ۳ دو رابطه‌ی پاد متقارن‌اند ولی رابطه‌ی مثال ۲

پاد متقارن نیست.

حال ارتباط این ویژگی ها را با گراف های جهت دار بیان می کنیم.

یک رابطه بازتابی است اگر و تنها اگر گراف جهت دار متناظر با آن در هر رأس دارای یک طوقه باشد. طوقه یالی است که یک رأس را به خودش وصل می کند.

یک رابطه متقارن است اگر و تنها اگر گراف جهت دار متناظر با آن دارای این ویژگی باشد که هرگاه از رأسی مانند a به رأسی مانند b یک یال موجود باشد آن گاه از رأس b به رأس a نیز یالی موجود باشد.

یک رابطه پاد متقارن است اگر و تنها اگر گراف جهت دار متناظر با آن دارای این ویژگی باشد که هرگاه از رأسی مانند a به رأسی دیگر مانند b یک یال موجود باشد و از رأس b به رأسی مانند c یالی موجود باشد آنگاه از رأس a به رأسی دیگر مانند b یک یال وجود داشته باشد.

یک رابطه ترایی است اگر و تنها اگر در گراف جهت دار متناظر با آن اگر از رأسی مانند a به رأسی دیگر مانند b یک یال موجود باشد و از رأس b به رأسی مانند c یالی موجود باشد آنگاه از رأس a به رأس c نیز یک یال وجود داشته باشد.

مثال ۴: با توجه به شکل ۲ معلوم می شود که رابطه ی متناظر با این گراف جهت دار هیچ یک از ویژگی های فوق را ندارد (چرا؟). در صورتی که گراف جهت دار شکل ۱ متناظر با رابطه ای است که دارای ویژگی های بازتابی، پادمتقارن بودن، و ترایی است.

Δ

۷-۲- رابطه ها و ماتریس ها

در قسمت گراف ها به هر گراف یک ماتریس صفر و یک به نام ماتریس مجاورت نسبت داده شد. ماتریس مجاورت گراف های جهت دار هم به طور مشابه تعریف می شود. مثلاً ماتریس مجاورت گراف جهت دار شکل ۲ به صورت زیر است:

$$\begin{matrix} & a & b & c \\ \begin{matrix} a \\ b \\ c \end{matrix} & \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \end{matrix}$$

پس می توان این ماتریس را متناظر با رابطه ی مربوط به شکل ۲ گرفت. توجه کنید که درایه ی ij از ماتریس متناظر مساوی با ۱ است اگر و تنها اگر iRj.

اکنون می‌توانیم ویژگی‌های مربوط به رابطه‌ها را به زبان ماتریس‌ها بیان کنیم. مثلاً ویژگی بازتابی یعنی اینکه همه‌ی درایه‌های قطر اصلی ماتریس ۱ باشند. بقیه‌ی ویژگی‌ها را به زبان ماتریس بیان کنید.

در این فصل صرفاً ماتریس‌های صفر و یک را در نظر می‌گیریم. اکنون یک عمل جمع و یک عمل ضرب برای اعضای مجموعه‌ی دو عضوی $\{0,1\}$ تعریف می‌کنیم که از روی آن «توان دوم» را برای ماتریس‌ها تعریف خواهیم کرد. این توان دوم با آنچه که در جبر خطی دیده‌ایم فرق دارد. تعریف: روی مجموعه‌ی $\{0,1\}$ دو عمل $+$ و \odot موسوم به عمل‌های بولی را به ترتیب زیر تعریف می‌کنیم:

$$1+0=0+1=1, \quad 0+0=0, \quad 1+1=1$$

$$1\odot 1=1, \quad 1\odot 0=0\odot 1=0, \quad 0\odot 0=0$$

با توجه به تعریف بالا، توان دوم ماتریس $M = [m_{ij}]_{n \times n}$ را به صورت زیر تعریف می‌کنیم:

$$M^{(2)} = [m_{i1} \odot m_{1j} + m_{i2} \odot m_{2j} + \dots + m_{in} \odot m_{nj}]_{n \times n}$$

به عبارت دیگر برای به دست آوردن توان دوم یک ماتریس که در این جا تعریف کردیم مانند توان دوم معمولی در ماتریس‌ها عمل می‌کنیم ولی در نهایت به جای هر درایه‌ی غیرصفر که به دست آمده باشد عدد ۱ قرار می‌دهیم.

مثال ۵: اگر $M = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ ، آن‌گاه داریم: $M^{(2)} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

Δ

تعریف: هرگاه R رابطه‌ای روی مجموعه‌ی A باشد ترکیب رابطه‌ی RoR ، رابطه‌ای روی A است که با قاعده‌ی زیر تعریف می‌شود:

$$a(RoR)c \text{ هرگاه } a \in A \text{ و } b \in A \text{ وجود داشته باشد که } aRb \text{ و } bRc.$$

با توجه به تعریف‌های فوق قضیه‌ی زیر را می‌توان به سادگی اثبات کرد.

قضیه‌ی ۱: فرض کنید A یک مجموعه‌ی n عضوی، $n \in \mathbb{N}$ و R یک رابطه روی A باشد.

هرگاه $M(R)$ ماتریس متناظر R باشد داریم:

$$\text{الف) } M(R) = [O]_{n \times n} \text{ (یعنی همه‌ی درایه‌های } M(R) \text{ صفرند) اگر و تنها اگر } R = \emptyset$$

(ب) $M(R) = [1]_{n \times n}$ (یعنی همه ی درایه های $M(R)$ یک اند) اگر و تنها اگر $R = A \times A$ ؛
 (پ) $M(RoR) = [M(R)]^{(2)}$.

اثبات: بند (الف) و (ب) بلافاصله از تعریف نتیجه می شوند. برای اثبات بند (پ)، اول فرض کنید $i(RoR)$. پس عضوی مانند $k \in A$ وجود دارد به طوری که iRk و kRj . پس درایه های ik و kj در ماتریس M مساوی با ۱ هستند. در نتیجه درایه ی ij زام در ماتریس $M^{(2)}$ برابر با ۱ است. حال به عکس اگر درایه ی ij زام در ماتریس $M^{(2)}$ برابر با ۱ باشد یعنی

$$m_{i1} \odot m_{1j} + m_{i2} \odot m_{2j} + \dots + m_{in} \odot m_{nj} = 1$$

آن گاه حداقل یکی از جمعوندها باید مساوی با ۱ باشد. مثلاً $m_{ik} \odot m_{kj} = 1$. از آن جا

$m_{ik} = m_{kj} = 1$ ، که نتیجه می شود : kRj و iRk . پس بنا به تعریف خواهیم داشت $i(RoR)j$.

□

مثال ۶: مجموعه ی $A = \{1, 2, 3, 4\}$ و رابطه ی R روی A به صورت

$$R = \{(1, 1), (1, 2), (2, 3), (3, 3), (3, 4)\}$$

مفروض است. مطلوب است محاسبه ی RoR .

$$M(R) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{داریم}$$

$$[M(R)]^{(2)} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = M(RoR) \quad \text{پس:}$$

Δ از آن جا $RoR = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 4), (3, 3), (3, 4)\}$

تعریف: فرض کنید ماتریس های صفر و یک $A = [a_{ij}]_{m \times n}$ و $B = [b_{ij}]_{m \times n}$ از اندازه ی

$m \times n$ باشند. گوئیم A کوچکتر از یا مساوی با B است و می نویسیم $A \ll B$ هرگاه به ازای هر $1 \leq i \leq m$ و هر $1 \leq j \leq n$ داشته باشیم $a_{ij} \leq b_{ij}$.

روشن است که اگر M_1 و M_2 ماتریس های متناظر با رابطه های R_1 و R_2 روی یک مجموعه ی

A باشند، آنگاه $R_1 \subseteq R_2$ اگر و تنها اگر $M_1 \ll M_2$.

قضیه ۲: مجموعه‌ی n عضوی A ، $n \in \mathbb{N}$ ، و رابطه‌ی R روی آن را در نظر می‌گیریم.

فرض کنید M ماتریس متناظر با این رابطه باشد. آنگاه

(الف) R بازتابی است اگر و تنها اگر $I_n \ll M$. (I_n ماتریس همانی $n \times n$ است).

(ب) R متقارن است اگر و تنها اگر $M = M^T$. (ماتریس M^T ترانزپوزیته‌ی M است و آن ماتریسی

است که از قراردادن سطرهای M به جای ستون‌های M ، با حفظ ترتیب، به دست می‌آید.)

(پ) R ترایابی است اگر و تنها اگر $M^{(T)} \ll M$.

(ت) R پاد متقارن است اگر و تنها اگر $I_n \ll M \wedge M^T$. (ماتریس $M \wedge M^T$ با عمل روی

درایه‌های M و M^T نظیر به نظیر با ضرب مؤلفه به مؤلفه تشکیل می‌شود)

اثبات: هر کدام از حکم‌های فوق با توجه به تعریف‌های مربوط به سادگی اثبات می‌شوند. ما دو

حکم آخر را ثابت می‌کنیم.

برای اثبات (پ)، فرض کنید $M^{(T)} \ll M$. باید نشان دهیم R ترایابی است. هر گاه xRy و

yRz ، آنگاه در ماتریس M ، درایه‌ی سطر x ام و ستون y ام و همچنین درایه‌ی سطر y ام و ستون z ام برابر

۱ است. در نتیجه درایه‌ی واقع در سطر x ام و ستون z ام در ماتریس $M^{(T)}$ برابر ۱ است.

چون $M^{(T)} \ll M$ پس درایه‌ی سطر x ام و ستون z ام ماتریس M نیز باید ۱ باشد یعنی xRz .

به عکس، فرض کنید R ترایابی باشد. باید نشان دهیم که $M^{(T)} \ll M$. فرض کنید m_{xz} ،

درایه‌ی واقع در سطر x ام و ستون z ام در ماتریس $M^{(T)}$ ، مساوی ۱ باشد، آنگاه باید $y \in A$ وجود

داشته باشد که در ماتریس M : $m_{yz} = 1$ و $m_{xy} = 1$. در نتیجه باید xRy و yRz و چون R ترایابی

است xRz . پس $m_{xz} = 1$. یعنی نشان داده‌ایم که $M^{(T)} \ll M$.

برای اثبات حکم (ت)، فرض کنید R پاد متقارن باشد. اگر به ازای دو عضو متمایز i و j داشته

باشیم $(i, j) \notin R$ آنگاه درایه‌ی i ام در M و در نتیجه در $M \wedge M^T$ برابر با ۰ است. اگر $(i, j) \in R$

آنگاه $(j, i) \notin R$. یعنی اگر درایه‌ی i ام در M مساوی با ۱ باشد آنگاه درایه‌ی i ام در M

مساوی با ۰ است. پس در این صورت نیز درایه‌ی i ام در $M \wedge M^T$ برابر با ۰ است. یعنی

$$M \wedge M^T \ll I_n$$

به عکس از $I_n \ll M \wedge M^T$ نتیجه می‌شود که همه‌ی درایه‌های غیرقطری $M \wedge M^T$ صفرند.

یعنی به ازای $i \neq j$ داریم $m_{ij} \cdot m_{ji} = 0$. در این صورت فقط سه حالت زیر امکان پذیرند:

$m_{ij} = m_{ji} = 0$ یا $m_{ij} = 1$, $m_{ji} = 0$ و یا $m_{ij} = 1, m_{ji} = 0$. که نتیجه می شود : اگر iRj و jRi آنگاه $i = j$.

□ اثبات بقیه ی حکم ها را به عنوان تمرین به عهده دانش آموزان می گذاریم .

قضیه های ۱ و ۲ ارتباط بین رابطه ها و ماتریس های صفر و یک را نشان می دهند . این قضیه ها با وجود سادگی اهمیت زیادی دارند . زیرا بهترین راه معرفی یک رابطه به کامپیوتر از طریق ماتریس صفر و یک است . از طریق حکم های فوق می توان با کامپیوتر ویژگی های هر رابطه ای را بررسی کرد .

مثال ۷: با استفاده از قضیه ی ۲ می توان یک الگوریتم نوشت و با برنامه ی کامپیوتری هم ارزی بودن رابطه ای را که روی یک مجموعه ی متناهی A داده شده است امتحان کرد . یعنی رابطه ی R یک رابطه ی هم ارزی است اگر و تنها اگر M ، ماتریس صفر و یک متناظر با آن، دارای شرایط زیر باشد :

$$(الف) I_n \ll M$$

$$(ب) M = M^T$$

$$(پ) M^{(n)} \ll M$$

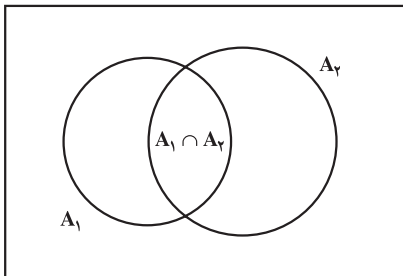
Δ

۷-۳- اصل شمول و عدم شمول

یکی از ابزارهای شمارش به اصل شمول و عدم شمول معروف است . حالت خاص آن را قبلاً در کتاب جبر و احتمال دیده اید . اگر A یک مجموعه ی متناهی باشد تعداد عناصر آن را با $|A|$ نشان می دهیم . فرض کنید A_1 و A_2 دو مجموعه ی متناهی باشند . داریم :

$$(۱) |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

با توجه به شکل ۳ رابطه ی (۱) درست است، زیرا در مجموع $|A_1| + |A_2|$ هر عضوی که فقط به



شکل ۳- نمودار ون برای دو مجموعه

یکی از مجموعه های A_1 یا A_2 متعلق باشد یک بار به حساب می آید ولی هر عضوی که به هر دو مجموعه ی A_1 و A_2 تعلق داشته باشد دو بار شمرده می شود . پس با کم کردن $|A_1 \cap A_2|$ از حاصل جمع $|A_1| + |A_2|$ هر عضو از $A_1 \cup A_2$ دقیقاً یک بار به حساب می آید .

رابطه‌ی (۱) وجه تسمیه‌ی «شمول و عدم شمول» را نیز توجیه می‌کند. زیرا در شمارش اعضای مجموعه‌ی $A_1 \cup A_2$ ، اول همه‌ی اعضای A_1 و A_2 را به حساب می‌آوریم (شمول) ولی چون در این صورت اعضای $A_1 \cap A_2$ دوبار به حساب می‌آیند آن‌ها را از شمارش خود خارج می‌کنیم (عدم شمول).

مثال ۸: چند عضو از مجموعه‌ی $A = \{n \in \mathbb{N} : 1 \leq n \leq 6300\}$ نه بر ۵ تقسیم پذیرند و نه بر ۳؟ فرض کنید A_1 زیرمجموعه‌ی A متشکل از مضارب ۳ و A_2 زیرمجموعه‌ی A متشکل از مضارب ۵ باشند. می‌خواهیم $|A_1 \cup A_2|$ را پیدا کنیم (\bar{B} متمم مجموعه‌ی B را نمایش می‌دهد). داریم:

$$|A_1| = \frac{6300}{3} = 2100$$

$$|A_2| = \frac{6300}{5} = 1260$$

و چون $A_1 \cap A_2$ مجموعه‌ی اعدادی هستند که هم بر ۳ و هم بر ۵ تقسیم پذیرند پس:

$$|A_1 \cap A_2| = \frac{6300}{(3)(5)} = 420$$

در نتیجه با توجه به رابطه‌ی (۱) داریم:

$$\begin{aligned} |A_1 \cup A_2| &= 2100 + 1260 - 420 \\ &= 2940 \end{aligned}$$

$$\Delta \quad |A_1 \cup A_2| = 6300 - 2940 = 3360$$

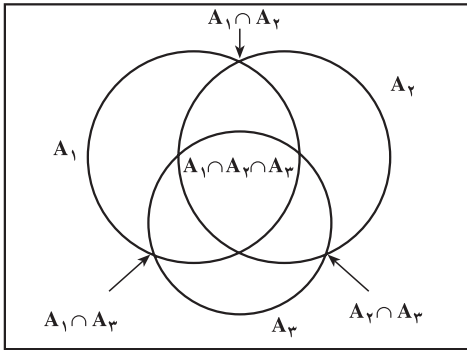
حال برای $n = 3$ اصل شمول و عدم شمول را مطالعه می‌کنیم.

قضیه‌ی ۳: فرض کنید A_1 و A_2 و A_3 سه زیرمجموعه‌ی متناهی از یک مجموعه‌ی A

باشند. داریم

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\ &\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \end{aligned} \quad (2)$$

۱- متمم مجموعه‌ی B را گاهی با B^c یا B' هم نمایش می‌دهند. به جای متمم گاهی اصطلاح مکمل را به کار می‌برند.



شکل ۴ - نمودار ون برای سه مجموعه

اثبات: نشان می‌دهیم که هر عضو x از A به تعداد مساوی در دو طرف رابطه‌ی (۲) به حساب می‌آید. به شکل ۴ توجه کنید.

دو حالت داریم:

حالت ۱: اگر x متعلق به هیچ کدام از مجموعه‌های A_1 و A_2 و A_3 نباشد، آن‌گاه x در دو طرف رابطه‌ی (۲)، صفر بار به حساب می‌آید.

حالت ۲: فرض کنید x به s مجموعه‌های A_1 و A_2 و A_3 تعلق داشته باشد ($1 \leq s \leq 3$). آن‌گاه x یک بار در طرف چپ به حساب می‌آید، و در طرف راست نیز

اگر $s=1$ ، یک بار به حساب می‌آید،

اگر $s=2$ ، باز هم $2-1=1$ بار به حساب می‌آید و

اگر $s=3$ ، در این صورت هم $3-3+1=1$ بار به حساب می‌آید. \square

اثبات بالا را می‌توان به n مجموعه تعمیم داد و قضیه‌ای بیان کرد که به اصل شمول و عدم شمول معروف است. در مثال‌های زیر خواهیم دید که چگونه بعضی از مسائل کلاسیک شمارش را می‌توان با اصل شمول و عدم شمول حل کرد.

مثال ۹: تعداد توابع پوشا از یک مجموعه‌ی ۴ عضوی B به یک مجموعه‌ی ۳ عضوی A را پیدا کنید. باید توجه کرد که منظور از تابع $f: B \rightarrow A$ تابعی است که روی همه‌ی اعضای B تعریف شده است.

فرض کنید $B = \{b_1, b_2, b_3, b_4\}$ و $A = \{a_1, a_2, a_3\}$. مجموعه‌ی تمام توابع $f: B \rightarrow A$ را با S نمایش می‌دهیم و ابتدا $|S|$ را محاسبه می‌کنیم. به ازای هر $b_j \in B$ برای $f(b_j)$ سه امکان وجود دارد، زیرا $f(b_j)$ امکان دارد a_1 ، a_2 یا a_3 باشد. این امکان‌ها به ازای هر دو عضو متمایز B به هم وابسته نیستند یعنی مثلاً به ازای هر انتخاب برای هر سه عضو B ، عضو چهارم می‌تواند دارای

سه انتخاب باشد. پس تعداد کل این توابع $3 \cdot 3 \cdot 3 = 27$ است. حال فرض کنید A_i مجموعه‌ی توابعی باشد که هیچ عضوی از B را به a_i نسبت نمی‌دهند.

$$A_i = \{f \in S : a_i \notin f(B)\} \quad i = 1, 2, 3$$

یعنی :

منظور شمارش تعداد اعضای مجموعه‌ی $\overline{A_1 \cup A_2 \cup A_3}$ است. از فرمول (۲) در قضیه‌ی ۳ استفاده می‌کنیم. مشابه استدلال فوق داریم

$$|A_1| = |A_2| = |A_3| = 2^4 = 16$$

$$|A_1 \cap A_2| = |A_1 \cap A_3| = |A_2 \cap A_3| = 1 \quad \text{و}$$

$$|A_1 \cap A_2 \cap A_3| = 0 \quad \text{و}$$

$$|A_1 \cup A_2 \cup A_3| = 2^4 + 2^4 + 2^4 - (1+1+1) + 0 = 45 \quad \text{پس:}$$

$$|\overline{A_1 \cup A_2 \cup A_3}| = 27 - 45 = 36 \quad \text{و از آنجا}$$

که تعداد توابع پوشای از B به A است. Δ

برای حل معادلات با جواب‌های صحیح و با محدودیت‌های مختلف، می‌توان از اصل شمول و عدم شمول استفاده کرد. برای توضیح این روش، اول به مثال زیر توجه کنید.

مثال ۱۰: فرض کنید k نوع مختلف گل و به تعداد فراوان از هر نوع موجود است. می‌توان ثابت کرد که تعداد انتخاب n گل از این k نوع گل که در آن تکرار نیز مجاز است برابر است با تعداد

$$\binom{n+k-1}{n}$$

جواب‌های صحیح نامنفی معادله‌ی $x_1 + x_2 + \dots + x_k = n$ و مساوی است با $\binom{n+k-1}{n}$.

اگر x_i را تعداد گل‌های انتخاب‌شده از نوع i ام بگیریم به‌سادگی دیده می‌شود که یک تناظر یک به یک بین انتخاب‌ها و جواب‌های معادله‌ی فوق موجود است. اثبات برابری تعداد انتخاب‌ها با مقدار داده شده را به عنوان تمرین به عهده‌ی دانش‌آموزان گذاشته‌ایم. باید دقت کرد که در این مثال حالت‌هایی را هم در نظر گرفته‌ایم که یک یا چند نوع گل را اصلاً انتخاب نکرده باشیم. Δ

مثال ۱۱: تعداد جواب‌های صحیح معادله‌ی $x_1 + x_2 + x_3 = 4$ را به‌طوری که به‌ازای $0 \leq x_i \leq 2, i = 1, 2, 3$ باشد پیدا کنید.

مجموعه‌های A_1, A_2, A_3 را به‌ترتیب زیر تعریف می‌کنیم:

$$A_i = \{ \text{جواب‌های معادله‌ی فوق به‌شرطی که } x_i > 2 \text{ باشد} \}, i = 1, 2, 3$$

باید تعداد مجموعه‌ی $\overline{A_1 \cup A_2 \cup A_3}$ را پیدا کنیم. بنابر فرمول (۲) از قضیه‌ی ۳ داریم:

$$\begin{aligned} |\overline{A_1 \cup A_2 \cup A_3}| &= |S| - |A_1 \cup A_2 \cup A_3| \\ &= |S| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + \\ &\quad |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3| \end{aligned}$$

که در آن S مجموعه‌ی تمام جواب‌های صحیح و نامنفی معادله‌ی فوق است. پس بنا به مثال ۱۰ داریم.

$$|S| = \binom{3+4-1}{4} = 15$$

از طرف دیگر مثلاً تعداد A_1 مساوی است با تعداد جواب‌های صحیح و نامنفی معادله‌ی $x_1 + x_2 + x_3 = 1$ زیرا کافی است که در جواب معادله‌ی اخیر به x_1 عدد ۳ اضافه کنیم تا یک جواب معادله‌ی $x_1 + x_2 + x_3 = 4$ با شرط $x_1 > 2$ به دست آید و برعکس. اما به سادگی دیده می‌شود که تعداد جواب‌های صحیح و نامنفی معادله‌ی $x_1 + x_2 + x_3 = 1$ مساوی است با ۳. پس $|A_1| = 3$ و به همین ترتیب $|A_2| = |A_3| = 3$.

$$A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset \quad \text{از طرف دیگر داریم}$$

همین‌طور $A_1 \cap A_2 \cap A_3 = \emptyset$. پس $|\overline{A_1 \cup A_2 \cup A_3}| = 15 - 3 - 3 - 3 = 6$. در حقیقت

۶ جواب فوق چنین‌اند:

$$(0, 2, 2), (1, 1, 2), (1, 2, 1), (2, 0, 2), (2, 1, 1), (2, 2, 0)$$

Δ

در قسمت نظریه‌ی اعداد با تابع حسابی اویلر ϕ به‌عنوان «مجله‌ی ریاضی» آشنا شده‌ایم. منظور از $\phi(n)$ عبارت است از تعداد اعداد صحیح و مثبت m که کوچکتر از n یا مساوی با آن بوده و m و n نسبت به هم اول باشند. قضیه‌ی زیر حالت خاصی از قضیه‌ی کلی درباره‌ی این تابع است. **قضیه‌ی ۴:** فرض کنید عدد صحیح و مثبت n برابر با حاصل ضرب سه عدد اول و متمایز به صورت زیر باشند:

$$n = p_1 p_2 p_3$$

در این صورت

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right)$$

اثبات: مجموعه‌های A_i را به ترتیب زیر تعریف می‌کنیم:

$$A_i = \{m: 1 \leq m \leq n, p_i | m\}, \quad i = 1, 2, 3$$

حال اصل شمول و عدم شمول را برای مجموعه‌های A_i می‌نویسیم. داریم:

$$\phi(n) = |A_1 \cup A_2 \cup A_3| \quad \text{و برای } i = 1, 2, 3$$

$$A_i = \left\{ p_i, 2p_i, 3p_i, \dots, \left(\frac{n}{p_i}\right)p_i \right\}$$

پس $|A_i| = \frac{n}{p_i}$. به همین ترتیب به‌ازای $i \neq j$ ، $|A_i \cap A_j| = \frac{n}{p_i p_j}$ ، و

$$|A_1 \cap A_2 \cap A_3| = \frac{n}{p_1 p_2 p_3} \quad \text{اکنون از رابطه ی (۲) در قضیه ی ۳ نتیجه می‌گیریم که:}$$

$$n - \phi(n) = |A_1 \cup A_2 \cup A_3| = \frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} - \frac{n}{p_1 p_2} - \frac{n}{p_1 p_3} - \frac{n}{p_2 p_3} + \frac{n}{p_1 p_2 p_3}$$

$$\phi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \frac{n}{p_2 p_3} - \frac{n}{p_1 p_2 p_3}$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right)$$

□

مثال ۱۲: ثابت کنید $\phi(42) = 12$.

چون $42 = 2 \cdot 3 \cdot 7$ ، حکم از قضیه ی ۴ به‌دست می‌آید:

$$\phi(42) = 42 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) = 12$$

این نتیجه را می‌توان مستقیماً هم بررسی کرد. زیرا تمام اعداد صحیح و مثبت نایبتر از ۴۲ که

نسبت به آن اول هستند عبارت‌اند از:

$$1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$$

Δ

۴-۷- تمرین‌ها

۱- فرض کنید $A = \{1, 2, 3, 4\}$. برای هریک از حالت‌های زیرگرافی رسم کنید که رابطه‌ی

متناظر با آن

(الف) بازتابی و متقارن باشد ولی ترایایی نباشد،

(ب) بازتابی و ترایایی باشد ولی متقارن نباشد،

(پ) متقارن و ترایایی باشد ولی بازتابی نباشد.

جواب های خود را با ماتریس های متناظر امتحان کنید.

۲- فرض کنید $A = \{w, x, y, z\}$. تعداد رابطه های روی A با ویژگی های داده شده در هریک

از حالت های زیر را بیابید :

(الف) بازتابی ؛

(ب) متقارن ؛

(پ) بازتابی و متقارن ؛

(ت) بازتابی و شامل (x, y) ؛

(ث) پاد متقارن ؛

(ج) پاد متقارن و شامل (x, y) ؛

(چ) متقارن و پاد متقارن ؛

(ح) پاد متقارن، متقارن و بازتابی ؛

(خ) هم ارزی (راهنمایی : تعداد افرازه های مختلف را پیدا کنید).

۳- فرض کنید $A = \{1, 2, 3, 4\}$. دو رابطه ی R و S روی A به صورت زیر داده شده اند.

$$R = \{(1, 2), (1, 3), (2, 4), (4, 4)\},$$

$$S = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 4)\}$$

رابطه های ROR و SOS را پیدا کنید.

۴- بندهای (الف) و (ب) از قضیه ی ۱ را اثبات کنید.

۵- بندهای (الف) و (ب) از قضیه ی ۲ را اثبات کنید.

۶- فرض کنید R یک رابطه ی بازتابی روی مجموعه ی متناهی A باشد. نشان دهید که رابطه ی

RoR نیز بازتابی است.

۷- ماتریس صفر و یک $E = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ را در نظر می گیریم. تعداد ماتریس های صفر

و یک F با شرط $E \ll F$ را بیابید.

۸- با استفاده از قضیه‌هایی که در این فصل خوانده‌اید نشان دهید که آیا رابطه‌ی زیر روی مجموعه‌ی $A = \{1, 2, 3, 4\}$ یک رابطه‌ی هم‌ارزی است یا خیر.

$$R = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (2,4), (4,2), (2,1), (3,1)\}$$

۹- یک ماتریس $n \times n$ از اعداد متمایز مثلاً $1, 2, 3, \dots, n^2$ را یک مربع وقتی (یا مربع جادویی) می‌نامیم، هرگاه حاصل جمع درایه‌های هر سطر، حاصل جمع درایه‌های هر ستون، حاصل جمع درایه‌های قطر اصلی، و حاصل جمع درایه‌های قطر فرعی با هم مساوی باشند. به‌عنوان مثال یک مربع وقتی 3×3 در زیر نشان داده شده است.

۲	۷	۶
۹	۵	۱
۴	۳	۸

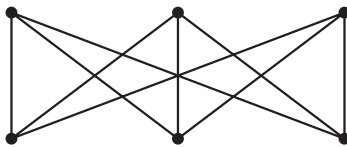
ثابت کنید که در هر مربع وقتی 3×3 که از اعضای $1, 2, 3, \dots, 9$ تشکیل شده است عضوی که در مرکز مربع قرار می‌گیرد همیشه عدد ۵ است.

۱۰- گراف G داده شده است. یک برجسب‌گذاری جادویی G عبارت است از متناظر کردن اعدادی، معمولاً صحیح و مثبت، به یال‌های G به‌طوری که حاصل جمع اعداد متناظر با یال‌های مارّ بر هر رأس عددی ثابت باشد. در گرافی که در شکل ۵ (الف) داده شده است اعدادی که روی یال‌ها نوشته شده‌اند یک برجسب‌گذاری جادویی را نشان می‌دهد، زیرا حاصل جمع اعداد متناظر به یال‌های مارّ بر هر رأس مساوی با ۴ است.

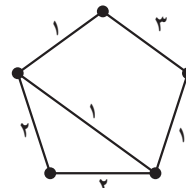
با استفاده از مربع وقتی 3×3 یک برجسب‌گذاری جادویی برای گراف شکل ۵ (ب) به دست آورید.

۱۱- ثابت کنید که تعداد انتخاب n گل از k نوع مختلف گل، که تکرار نیز مجاز باشد مساوی

$$\binom{n+k-1}{n}$$



(ب)



(الف) یک برجسب‌گذاری جادویی

شکل ۵

۱۲- تعداد جواب های صحیح و مثبت هریک از معادلات زیر را پیدا کنید.

$$x_1 + x_2 + x_3 = 7 \quad (\text{الف})$$

$$x_1 + x_2 + x_3 = 8, \quad 2 \leq x_1 \leq 3, \quad 4 \leq x_2 \leq 8, \quad x_3 \geq 1 \quad (\text{ب})$$

$$x_1 + x_2 + x_3 = 14, \quad 1 \leq x_i \leq 7, \quad i = 1, 2, 3 \quad (\text{پ})$$

۱۳- مطلوب است تعداد شماره‌ی شناسنامه‌های پنج رقمی که در آن‌ها هریک از رقم‌های ۱، ۳ و ۷ حداقل یک بار ظاهر می‌شوند.

۱۴- در یک نظرخواهی از ۱۰۰ نفر دانش‌آموز نتایج زیر به دست آمده است: ۶۰ نفر آن‌ها مجله‌ی A را می‌خوانند، ۵۰ نفر مجله‌ی B، ۵۰ نفر مجله‌ی C، ۳۰ نفر مجله‌های A و B، ۲۰ نفر مجله‌های B و C، ۴۰ نفر مجله‌های A و C و بالاخره ۱۰ نفر هر سه مجله‌ی A و B و C را می‌خوانند. مطلوب است تعداد دانش‌آموزانی که:

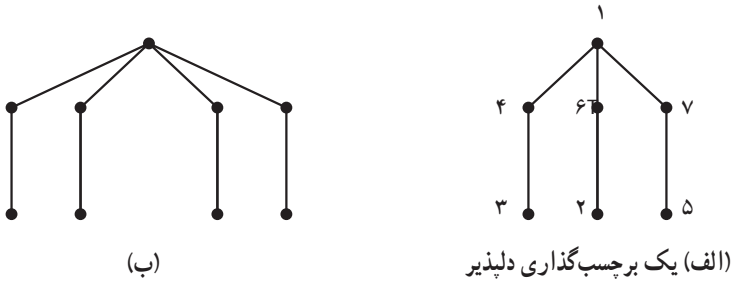
(الف) هیچ مجله‌ای نمی‌خوانند؛

(ب) دقیقاً ۲ مجله می‌خوانند؛

(پ) حداقل ۲ مجله می‌خوانند؛

۱۵- (الف) اصل شمول و عدم شمول را در حالت چهار مجموعه بنویسید و آن را اثبات کنید. (ب) در منطقه‌ای چهار روستا وجود دارد. قرار است راه‌هایی دوطرفه بین بعضی از روستاها ساخته شود به طوری که نهایتاً هیچ روستایی منفرد (یعنی بدون ارتباط با هیچ روستای دیگر) نماند. این کار به چند طریق امکان دارد؟

۱۶- برای درخت‌ها برچسب گذاری‌های مختلف تعریف می‌شود. یک برچسب گذاری دلبذیر برای یک درخت n رأسی عبارت است از نسبت دادن اعداد $1, 2, 3, \dots, n$ به رئوس آن، به طوری که برچسب یال‌ها $n-1$ عدد متمایز باشند و برچسب هر یال از قدرمطلق تفاضل برچسب رأس‌های دو انتهای آن به دست آید. مثلاً در شکل ۶ (الف) یک برچسب گذاری دلبذیر را می‌بینیم. یک برچسب گذاری دلبذیر برای درخت شکل ۶ (ب) پیدا کنید: حدس این است که «هر درخت یک برچسب گذاری دلبذیر دارد». ولی این حدس هنوز ثابت یا رد نشده است.



شکل ۶

مراجع

- ۱- ایوان نیون، ریاضیات انتخاب یا چگونه بدون شمارش بشماریم. ترجمه‌ی علی عمیدی و بتول جذبی، مرکز نشر دانشگاهی، تهران، چاپ اول ۱۳۶۸.
- 2 - R.P. Grimaldi, Discrete and Combinatorial Mathematics: An Applied Introduction, 2nd. ed., Addison- Wesley 1989.^۱

۱- مرکز نشر دانشگاهی ترجمه‌ی فارسی این مرجع را منتشر خواهد کرد.

مجله‌ی ریاضی

مربع وفقی یکی از ساختارهای ترکیبیاتی است که ریاضی دانان شرق درباره‌ی آن کارهای بسیاری انجام داده‌اند و روش‌های ساخت این مربع‌ها برای اندازه‌های مختلف منسوب به این دانشمندان است. اصولاً ساختارهای ترکیبیاتی یکی از مهم‌ترین مباحث ترکیبیات است که دارای کاربردهای فراوان نیز هستند. از مهم‌ترین ساختارهای ترکیبیاتی مربع‌های لاتین و طرح‌های بلوکی است. یک مربع لاتین عبارت است از یک ماتریس $n \times n$ با درایه‌های $1, 2, 3, \dots, n$ به طوری که در هر سطر و در هر ستون درایه‌های تکراری نباشند.

مربع‌های لاتین با مربع‌های وفقی نیز ارتباط دارند. یکی از کاربردهای مربع‌های لاتین در مبحث رمزنگاری است. به ازای هر n داده شده می‌توان یک مربع لاتین از مرتبه n ساخت. از مربع‌هایی که در زیر به ازای $n=4$ و $n=5$ ساخته شده‌اند

۱	۲	۳	۴
۲	۳	۴	۱
۳	۴	۱	۲
۴	۱	۲	۳

۱	۲	۳	۴	۵
۲	۳	۴	۵	۱
۳	۴	۵	۱	۲
۴	۵	۱	۲	۳
۵	۱	۲	۳	۴

می‌توان به راحتی برای حالت کلی نیز ایده گرفت.

دقت کنید که در هر دو مربع فوق بعضی از درایه‌های واقع در دو گوشه‌ی چپ بالا و راست پایین را پررنگ نوشته‌ایم. در مربع اول ۴ تا و در مربع دوم ۶ تا از این درایه‌های پررنگ قرار دارند. جالب این است که اگر در هر یک از این دو مربع فقط این درایه‌ها را به ما بدهند می‌توانیم بقیه درایه‌ها را به طور یکتا به دست آوریم.

تعداد درایه‌های پررنگ داده شده در حالت کلی $\left\lfloor \frac{n^2}{4} \right\rfloor$ است. حال فرض کنید درایه‌های یک مربع لاتین اطلاعاتی است که می‌خواهید به یک شخص مورد اعتماد خود بدهید. یک مربع $n \times n$ از n^2 اطلاعات تشکیل می‌شود. الگوی فوق پیشنهاد می‌کند که فقط کافی است که حدود $\frac{1}{4}$ از اطلاعات را منتقل کنید. شخص مورد اعتماد می‌تواند بقیه را به طور یکتا پیدا کند.

قسمت چهارم

احتمال

مقدمه

امروزه همه‌ی سازمان‌های دولتی و خصوصی، در هر رسته‌ای که باشند، اعم از اقتصادی، صنعتی، اجتماعی و غیره برای تعیین سیاست و روند کار آینده‌ی خود ناگزیر به برنامه‌ریزی هستند. تصمیم‌گیری‌ها و آینده‌نگری‌ها علی‌رغم وجود اطلاعاتی از گذشته و داده‌هایی از حال، همواره دستخوش عدم قطعیت‌هایی هستند که نمی‌توان در رویارویی با آن‌ها با یقین کامل برنامه‌ریزی کرد. علم احتمال و بر پایه‌ی آن علم آمار با شاخه‌های متعددش، در مقابل لجام گسیختگی این عدم قطعیت‌ها و یا به اصطلاح عرف در مقابل شانس قد علم کرده‌اند و براساس قوانین محکم ریاضی، اثر شانس را کنترل می‌کنند. استنباط آماری که پایه‌ای برای تصمیم‌گیری است بر قوانین احتمال تکیه کرده است و در حال حاضر کوچک‌ترین گام پژوهشی در هر زمینه، مستلزم استفاده از این نوع استنباط‌هاست. کاربرد احتمال در کارهای نظامی، فیزیک، ارتباطات، نظریه‌ی اطلاعات، علوم فضایی، نظریه‌ی رمزنگاری و امثال آن‌ها به سرعت گسترش یافته است. با این وجود تصور می‌رود هنوز در اوایل راهی هستیم که سه سده‌ی پیش به صورتی مقدماتی آغاز شده است. ما با شما از ابتدای این راه همراه می‌شویم و با هم چند گامی مقدماتی از این راه را طی می‌کنیم و از آن جنبه‌ی احتمال که صورتی گسسته دارد سخن می‌گوییم. شاید که راهنمای شما برای ادامه راه باشد.

فصل

احتمال

۸-۱- یادآوری

خلاصه‌ای از آنچه را سال گذشته درباره‌ی احتمال خوانده‌ایم در زیر می‌آوریم:

الف) می‌دانیم که اگر آزمایشی یا پدیده‌ای قبل از رخداد، نتیجه‌اش معلوم نباشد ولی نتیجه‌های ممکن آن مشخص باشند آن را آزمایش تصادفی یا پدیده‌ی تصادفی می‌نامند. مجموعه‌ی همه‌ی نتایج ممکن را فضای نمونه‌ای آزمایش تصادفی می‌نامیم. فضای نمونه‌ای را با S نشان می‌دهیم. هر نتیجه‌ی ممکن، یعنی هر عضو S را یک برآمد می‌گوییم. در هر آزمایش تصادفی تنها یکی از عضوهای این مجموعه رخ خواهد داد.

مثال ۱: قرار است فردا تیم A در مقابل تیم B بازی کند. تیم A چه نتیجه‌ای به دست

می‌آورد؟

به طور مطمئن نمی‌دانیم. اما نتیجه‌هایی که یکی از آن‌ها رخ می‌دهد عبارت‌اند از:

$$a = A \quad b = A \quad c = \text{باختن تیم } A$$

برابر شدن دو تیم $c =$ باختن تیم A $b = A$ بردن تیم $a = A$ پس مجموعه‌ی $S = \{a, b, c\}$ فضای نمونه‌ای است و هر عضو این مجموعه برآمدی است

که ممکن است رخ دهد. از سه برآمد تنها یکی رخ می‌دهد. Δ

ب) هر پیشامد، زیر مجموعه‌ای از فضای نمونه‌ای است. مثلاً $E_1 = \{a, b\}$ یک پیشامد است

و به معنای آن است که در بازی فردا «تیم A یا می‌برد و یا می‌بازد». در هر حال وقتی می‌گوییم

پیشامد E_1 رخ خواهد داد به معنای آن است که تنها یکی از برآمدهای آن رخ خواهد داد.

اگر $E_2 = \{a, c\}$ رخ بدهد بدان معناست که تیم A فردا یا می‌برد و یا برابر می‌کند. دو پیشامد را که

برآمد مشترکی ندارند ناسازگار می گویند. سال گذشته اعمال روی پیشامدها را که همان اعمال روی مجموعه‌ها هستند دیده‌اید.

تذکر: منظور از «رخداد» یک پیشامد وقوع آن پیشامد، یعنی مشاهده‌ی عضوی از آن پیشامد به عنوان نتیجه‌ی آزمایش است.

(پ) اگر فضای نمونه‌ای به جای ۳ برآمد ممکن، n برآمد ممکن داشته باشد تعداد پیشامدها، یعنی تعداد زیر مجموعه‌های آن 2^n است. در مثالا بالا $2^3 = 8$ پیشامد در فضای نمونه‌ای حاصل می‌شوند که عبارت‌اند از:

$$\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \phi$$

ϕ پیشامد ناممکن است. پیشامد $S = \{a, b, c\}$ حتماً رخ می‌دهد زیرا به معنای آن است که یکی از سه برآمد a, b, c رخ می‌دهد و این مسلم است که فردا، در صورت انجام بازی، تیم A یا می‌برد، یا می‌بازد و یا برابر می‌کند. پس S رخ می‌دهد. لذا S را پیشامد مطمئن می‌گوییم. تعداد اعضای مجموعه‌ی S ، یعنی تعداد برآمدهای فضای نمونه‌ای ممکن است متناهی یا شمارا نامتناهی یا ناشمارا نامتناهی باشد. اگر لامبی را از فرایند تولید لامپ انتخاب کنیم و بخواهیم سالم بودن آن را امتحان کنیم فضای نمونه‌ای این آزمایش تصادفی دو برآمد دارد، لذا S مجموعه‌ای متناهی است. اگر هدف این باشد که سکه‌ای را آن قدر بیندازیم تا برای اولین بار رو ظاهر شود فضای نمونه‌ای این آزمایش تصادفی، بی‌نهایت برآمد دارد که می‌توان این برآمدها را با اعداد طبیعی متناظر کرد. وقتی تعداد برآمدهای فضایی نمونه‌ای متناهی یا شمارا نامتناهی باشد آن را فضای نمونه‌ای گسسته می‌گوییم. تعداد برآمدهای فضای نمونه‌ای ممکن است ناشمارا نامتناهی باشد که در این صورت فضای نمونه‌ای گسسته نیست، مثل انتخاب تصادفی نقطه در بازه‌ی $(0, 1)$.

(ت) وقتی فضای نمونه‌ای S را برای آزمایش تصادفی داریم، احتمال پیشامدهای فضای S را به صورت مقادیر حقیقی یک تابع مجموعه‌ای P تعریف می‌کنیم، که این تابع براساس ۳ اصل موضوع زیر، اعداد حقیقی را به پیشامدها یعنی به زیر مجموعه‌های S نسبت می‌دهد،

اصل موضوع ۱: احتمال هر پیشامد، عددی نامنفی است، یعنی برای هر پیشامد A از S ،

$$P(A) \geq 0$$

اصل موضوع ۲:

$$P(S) = 1$$

اصل موضوع ۳: اگر A_1, A_2, \dots, A_n دنباله‌ای متناهی^۱ از پیشامدهای دو به دو ناسازگار S باشند آن گاه

$$P(A_1 \cup A_2 \cup \dots \cup A_n) = P(A_1) + P(A_2) + P(A_3) + \dots + P(A_n)$$

این اصول موضوع منسوب به کولموگوروف هستند. هر تابع حقیقی مقدار که در این اصول صادق باشد به تابع احتمال موسوم است. فضای S و تابع P و مجموعه‌ی پیشامدها را مدل احتمال آزمایش تصادفی می‌نامند. تعریف دقیق‌تری از مدل احتمال را در مقاطع بالاتر تحصیلی می‌بینید. دیده‌اید که اگر A پیشامدی از فضای نمونه‌ای گسسته S باشد، $P(A)$ برابر با مجموع احتمال‌های برآمدهایی است که در A هستند. به خصوص اگر S دارای n برآمد باشد و تابع احتمال به هر برآمد عدد $\frac{1}{n}$ را نسبت دهد می‌توانید برقراری ۳ اصل بالا را به سهولت تحقیق کنید. همان‌طور که می‌دانید چنین فضای نمونه‌ای را یکنواخت یا متساوی‌الاحتمال می‌نامند. اگر در این فضا پیشامد A متشکل از m برآمد باشد آن گاه $P(A) = \frac{m}{n}$ است که با مفهوم فراوانی نسبی در آمار مطابقت دارد. وقتی مثلاً پیشامد $A = \{a, b, c\}$ را داریم که a, b و c برآمدها هستند احتمال این پیشامد را چنین می‌نویسیم

$$P(A) = P(\{a, b, c\})$$

در مواردی که پیشامد، تک عضوی مانند $\{a\}$ باشد برای سادگی احتمال آن را به جای $P(\{a\})$ به صورت $P(a)$ می‌نویسیم.

وقتی فضای نمونه‌ای گسسته است در تخصیص اندازه‌ی احتمال، لازم نیست که احتمال هر زیر مجموعه ممکن را مشخص کنیم، و این امتیاز بزرگی است، زیرا مثلاً اگر فضای نمونه‌ای 2^0 برآمد داشته باشد تعداد پیشامدهای S یعنی تعداد زیر مجموعه‌های آن $1048576 = 2^{20}$ است. در این حالت اگر اندازه‌ی احتمال منسوب به رخداد هر برآمد معلوم باشد مدل احتمال مشخص می‌شود. دیده‌اید که روی یک فضای نمونه‌ای می‌توان تابع‌های P ی مختلف تعریف کرد.

مثال ۲: به مثال ۱ رجوع کنید. فرض کنید در گذشته تیم A مثلاً 2^0 بار با تیم B مسابقه داده است و شرایط زمانی و مکانی و تیمی همه بازی‌ها یکی بوده‌اند، و جمعاً 1^0 بار تیم A برنده، 6 بار بازنده شده و 4 بار برابر کرده باشد. پس $\frac{1^0}{3^0}$ بارها برنده، $\frac{6}{3^0}$ بارها بازنده شده و $\frac{4}{3^0}$ بارها برابر کرده

۱- در واقع اگر دنباله‌ی پیشامدها نامتناهی نیز باشد، اصل موضوع ۳ استوار است.

است. در این صورت معقول است که بگوییم فردا تیم A با احتمال $\frac{5}{10}$ برنده، با احتمال $\frac{3}{10}$ بازنده خواهد شد و با احتمال $\frac{2}{10}$ برابر خواهد کرد. پس با توجه به فراوانی نتیجه‌های بازی‌های گذشته تابع P را به صورتی تعریف می‌کنیم که به برآمدهای فضای نمونه‌ای $S = \{a, b, c\}$ احتمال‌های زیر را تخصیص دهد

$$P(a) = \frac{5}{10} \quad P(b) = \frac{3}{10} \quad P(c) = \frac{2}{10}$$

می‌توانیم از روی اطلاعات دیگر، مثلاً ملاحظه مسابقات تمرین چند روز قبل دو تیم، احتمال‌های دیگری را به برآمدها نسبت دهیم. با معلوم بودن S و P می‌توانیم احتمال هر پیشامد S را مشخص کنیم، مثلاً

$$P(\{a, c\}) = P(a) + P(c) = \frac{7}{10}$$

یعنی احتمال این که تیم A برنده شود یا برابر کند $\frac{7}{10}$ است. Δ

وقتی فضای نمونه‌ای نامتناهی باشد تخصیص احتمال به همه برآمدها عملی نیست. در بیشتر این حالت‌ها احتمالی که به هر یک از برآمدها نسبت می‌دهند باید برابر صفر باشد و تعیین احتمال پیشامدهایی که احتمال آن‌ها صفر نیست از روی برآمدها مشکل خواهد شد. برای ساختن مدل احتمال در این حالت‌ها احتمال‌ها را به پیشامدها نسبت می‌دهیم. همان‌طور که سال قبل دیده‌ایم این فضای نمونه‌ای می‌تواند به صورت مجموعه‌ای از اعداد حقیقی مثل بازه‌ی $(0, 1)$ یا تمام خط حقیقی یا مجموعه‌ای از نقاط واقع در فضای سه بعدی مانند نقاط داخل یک مکعب و نظایر این‌ها باشد. در این صورت تابع P، همان‌طور که می‌دانیم، به هر پیشامد که متناظر با مثلاً فاصله‌ای روی خط حقیقی یا ناحیه‌ای روی دایره یا ناحیه‌ای درون مکعب و امثال آن است عددی را به عنوان احتمال نسبت می‌دهد. ما در این کتاب تنها از فضاهای نمونه‌ای گسسته صحبت می‌کنیم.

ث) همان‌طور که در (ب) گفتیم اگر A و B دو پیشامد از فضای نمونه‌ای باشند وقتی که برآمدی مشترک نداشته باشند آن‌ها را ناسازگار می‌گویند. اگر A و B برآمدهایی مشترک داشته باشند، یعنی $A \cap B$ تهی نباشد آن‌گاه $A \cap B$ که خود زیر مجموعه‌ی S است، یک پیشامد است و وقتی رخ می‌دهد که برآمدی از آن، که ناچار هم عضو A و هم عضو B است، رخ دهد. اگر پیشامد $A \cup B$

در نظر بگیریم وقتی این پیشامد رخ می‌دهد که حداقل یکی از دو پیشامد A یا B رخ دهد. واضح است این برآمد که متعلق به A و یا متعلق به B است می‌تواند متعلق به اشتراک A و B هم باشد. در سال قبل دیده‌ایم که

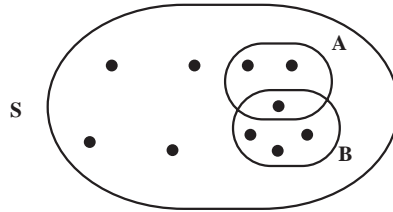
$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

S : فضای نمونه‌ای

• : برآمد

A : پیشامد

B : پیشامد



شکل ۱- نمایش فضای نمونه‌ای، برآمد و پیشامد

فرمول بالا به شما اجازه می‌دهد که وقتی از روی مدل احتمال، احتمال رخداد پیشامد A، احتمال رخداد پیشامد B و احتمال رخداد پیشامد $A \cap B$ را دارید احتمال رخداد پیشامد $A \cup B$ را به دست آورید. برابری‌های زیر را نیز یادآوری می‌کنیم. اگر پیشامد \bar{A} متمم پیشامد A باشد آن‌گاه

$$P(\bar{A}) = 1 - P(A)$$

که بی‌درنگ نتیجه می‌شود

$$P(\phi) = 1 - P(S) = 0$$

هم‌چنین اگر $A \subseteq B$ ، آن‌گاه

$$P(B - A) = P(B) - P(A)$$

$$P(A) \leq P(B)$$

و

اینک پس از این یادآوری‌ها به بیان مطالبی جدید در زمینه‌ی احتمال می‌پردازیم.

۸-۲- مدل احتمال شرطی

فرض کنید می‌خواهیم آزمایشی تصادفی را انجام دهیم. ابتدا فضای نمونه‌ای را مشخص

می‌کنیم و احتمالی به رخداد هر پیشامد نسبت می‌دهیم و بدین ترتیب مدل احتمال را معین می‌کنیم. این مدل را می‌شناسید. حال اگر اطلاعی اضافی درباره‌ی فضای نمونه‌ای داشته باشیم، مثلاً به دلیل بدانیم که پیشامد B از این فضای نمونه‌ای رخ داده است آن‌گاه معمولاً مدل احتمال قبلی به هم می‌ریزد و آگاهی از رخداد حتمی پیشامد B در مقدار احتمال سایر پیشامدها اثر می‌گذارد، که در این صورت احتمال‌های پیشامدهای فضای نمونه‌ای با احتمال‌های مدل قبلی تفاوت دارند. اگر بتوانیم تحت این شرط که پیشامد B حتماً رخ می‌دهد احتمال پیشامدهای دیگر فضای نمونه‌ای را مشخص کنیم مدل احتمال جدیدی به دست می‌آید که آن را مدل احتمال شرطی می‌نامیم. قبل از توضیح بیشتر مثالی می‌زنیم.

مثال ۳: می‌خواهید یک تاس قرمز و یک تاس سفید را با هم بریزید. تاس‌ها همگن‌اند. می‌دانید که فضای نمونه‌ای ۳۶ برآمد دارد:

$$S = \{(۶\text{قرمز}, ۶\text{سفید}), \dots, (۱\text{قرمز}, ۶\text{سفید}), \dots, (۶\text{قرمز}, ۱\text{سفید}), \dots, (۱\text{قرمز}, ۱\text{سفید})\}$$

پس از انجام آزمایش، یکی از این ۳۶ برآمد رخ خواهد داد. احتمال رخداد هر برآمد $\frac{1}{36}$ است. حال فرض کنید این اطلاع اضافی را داریم که پس از انجام آزمایش مجموع شماره‌های دو تاس حتماً کوچک‌تر از ۷ است. پیشامد «مجموع دو شماره کوچک‌تر از ۷» را B می‌نامیم. پیشامد B از برآمدهای زیر تشکیل می‌شود:

$$(1,1), (1,2), (1,3), (1,4), (1,5)$$

$$(2,1), (2,2), (2,3), (2,4)$$

$$(3,1), (3,2), (3,3)$$

$$(4,1), (4,2)$$

$$(5,1)$$

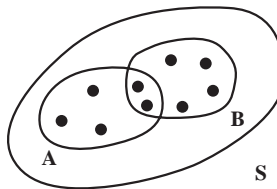
یعنی پیشامد B، متشکل از ۱۵ برآمد از ۳۶ برآمد فضای نمونه‌ای است. وقتی شرط می‌کنیم که B حتماً رخ می‌دهد، یعنی یکی از این ۱۵ برآمد نتیجه‌ی ریختن دو تاس است. برآمدهایی مثل (۱,۶) یا (۲,۵) یا (۴,۵) و غیره که مجموع دو شماره‌ی آن‌ها ۷ یا بیش از ۷ است رخ نخواهند داد. حال که می‌دانیم پیشامد B به طور مطمئن رخ می‌دهد آن را فضای نمونه‌ای جدید فرض می‌کنیم و بدین ترتیب مدل احتمال جدیدی داریم که آن را مدل احتمال شرطی با شرط

«مجموع دو شماره کوچک‌تر از ۷ است» می‌نامیم. حال اگر بخواهیم به شرط رخداد پیشامد B، احتمال رخداد یک جفت را بدانیم و پیشامد داشتن جفت را با A نشان دهیم در این صورت احتمال پیشامد داشتن جفت به شرط رخداد پیشامد B را با $P(A|B)$ نشان می‌دهیم و می‌خوانیم احتمال پیشامد A به شرط رخداد پیشامد B و یا به صورتی ساده احتمال پیشامد A به شرط B. وقتی می‌دانیم B رخ داده، تنها ممکن است یکی از ۱۵ برآمد بالا رخ دهد. بین این برآمدها جفت‌های ممکن (۱,۱)، (۲,۲) و (۳,۳) هستند. چون احتمال رخداد هر برآمد مساوی $\frac{1}{15}$ است، لذا

$$P(A|B) = P\{(1,1), (2,2), (3,3)\} = \frac{3}{5}$$

Δ

در مثال بالا، احتمال شرطی، یعنی $P(A|B)$ را به سادگی حساب کردیم زیرا فضای نمونه‌ای آزمایش یکنواخت، یا برآمدها متساوی‌الاحتمال یعنی هم‌شانس بودند، ولی اگر احتمال برآمدها یکی نباشند کار کمی مشکل است. قبل از این که تعریف کلی احتمال شرطی را مطرح کنیم، به این مطلب به صورتی شهودی می‌اندیشیم. به شکل ۲ توجه کنید.



شکل ۲

S فضای نمونه‌ای آزمایش است. B پیشامدی است که می‌دانیم رخ خواهد داد. A پیشامدی است که می‌خواهیم به شرط آن که B رخ دهد، احتمال رخدادش را بیابیم. وقتی B رخ می‌دهد که یکی از برآمدهایش رخ دهد. اگر برآمدی که رخ می‌دهد در $A \cap B$ باشد طبیعتاً A هم رخ می‌دهد. پس هر چه احتمال رخداد پیشامد $A \cap B$ بیشتر باشد احتمال رخداد پیشامد A به شرط B بیشتر است. لذا به طور شهودی $P(A|B)$ باید در رابطه‌ی مستقیم با $P(A \cap B)$ باشد. این رابطه را به صورت،

$$(۱) \quad P(A|B) = KP(A \cap B)$$

فرض می‌کنیم. در این برابری اگر به جای پیشامد A پیشامد B قرار بگیرد نتیجه می‌شود

$$P(B|B) = KP(B \cap B)$$

اما احتمال رخداد پیشامد B به شرط B برابر ۱ است زیرا B حتماً رخ می‌دهد و $B \cap B = B$ ، پس برابری بالا به صورت

$$1 = K \cdot P(B)$$

در می‌آید و داریم $K = \frac{1}{P(B)}$. اگر این مقدار را در (۱) قرار دهیم نتیجه می‌شود

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

این رابطه را به طور شهودی به دست آوردیم. براساس همین رابطه‌ی شهودی تعریف زیر را برای احتمال شرطی ارائه می‌دهیم.

تعریف احتمال شرطی: اگر A و B دو پیشامد از فضای نمونه‌ای S باشند وقتی $P(B) \neq 0$ ، احتمال پیشامد A به شرط این که پیشامد B رخ دهد به صورت

$$(۲) \quad P(A|B) = \frac{P(A \cap B)}{P(B)}$$

تعریف می‌شود. وقتی $P(B) = 0$ ، احتمال شرطی قابل تعریف نیست.

در مقاطع بالاتر خواهید دید که احتمال شرطی روی یک فضای نمونه‌ای تابع احتمالی است که در سه اصل موضوع کولموگوروف صدق می‌کند.

مثال ۴: سازنده‌ی قطعات یدکی یک کارخانه از روی تجربه‌های گذشته می‌داند احتمال این که سفارشی به موقع برای ارسال آماده شود $9/10$ است و احتمال این که سفارشی به موقع برای ارسال آماده و به موقع تحویل مشتری شود برابر $8/10$ است. احتمال این که سفارشی به موقع تحویل شود به شرط آن که به موقع ارسال شده باشد چه قدر است؟ ابتدا قرار می‌دهیم:

A = پیشامد آماده بودن به موقع، برای ارسال

B = پیشامد تحویل به موقع سفارش، به مشتری

$$\text{بنابر داده‌های مسئله، } P(A) = 9/10 \text{ و } P(A \cap B) = 8/10$$

زیرا پیشامد $A \cap B$ به معنای این است که سفارش هم به موقع آماده برای ارسال بوده و هم به موقع تحویل مشتری می‌شود. آن چه می‌خواهیم، $P(B|A)$ است، یعنی احتمال تحویل به موقع سفارش به مشتری به شرط آن که به موقع ارسال شده باشد. بنابر تعریف احتمال شرطی

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{0/8}{0/9} = \frac{8}{9}$$

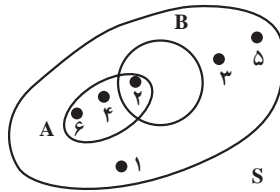
Δ

مثال ۵: تاسی همگن را با چشم بسته انداخته ایم. برآمد حاصل را نگفته اند، ولی اعلام کرده اند که برآمد حاصل عددی زوج است. احتمال این که شماره ی ۲ ظاهر شده باشد چه قدر است؟
قرار می دهیم:

A = پیشامد ظاهر شدن شماره ی زوج

B = پیشامد ظاهر شدن شماره ی ۲

به شکل ۳ توجه کنید.



شکل ۳

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3} \quad \text{لذا}$$

زیرا $P(A) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$. به عبارت دیگر می توانید تصور کنید که فضای نمونه ای {۲, ۴, ۶} است که حتماً رخ داده است و لذا روی این فضا، رخ دادن ۲ دارای یک شانس از ۳ شانس است یعنی احتمال رخداد برآمد ۲ برابر $\frac{1}{3}$ است.

Δ

۸-۳- قاعده ی ضرب احتمال

از تعریف

$$P(A|B) = \frac{P(A \cap B)}{P(B)}, \quad P(B) \neq 0$$

$$P(A \cap B) = P(B) \cdot P(A|B), \quad P(B) \neq 0 \quad \text{نتیجه می شود که}$$

این رابطه به قاعده‌ی ضرب احتمال موسوم است. به کمک این قاعده می‌توان احتمال رخداد هم‌زمان دو پیشامد را تعیین کرد.

مثال ۶: جعبه‌ای محتوی ۱۲ لامپ است که می‌دانیم ۳ تای آن‌ها معیوب‌اند. از این جعبه به تصادف ۱ لامپ برمی‌داریم. سپس مجدداً بدون جای‌گذاری لامپ اول، لامپ دیگری به تصادف برمی‌داریم. احتمال این که هر دو لامپ معیوب باشند چه قدر است؟ ابتدا قرار می‌دهیم:

A = پیشامد معیوب بودن لامپ اول

B = پیشامد معیوب بودن لامپ دوم

بنابراین $A \cap B$ پیشامد معیوب بودن هر دو لامپ است. واضح است که:

$$P(A) = \frac{3}{12} = \frac{1}{4}$$

اگر لامپ اول معیوب باشد، لامپ دوم را از بین ۱۱ لامپ باقی مانده که ۲ تای آن‌ها معیوب است برمی‌داریم پس:

$$P(B|A) = \frac{2}{11}$$

لذا از قاعده‌ی ضرب احتمال داریم:

$$P(A \cap B) = P(A) \cdot P(B|A) = \frac{1}{4} \cdot \frac{2}{11} = \frac{1}{22}$$

Δ

۸-۴ - استقلال دو پیشامد

پیشامدهای A و B دو پیشامد از یک فضای نمونه‌ای هستند که احتمال آن‌ها مثبت است. اگر آگاهی از رخداد پیشامد B در احتمال رخداد پیشامد A مؤثر نباشد A را مستقل از B می‌گویند. پس برای مستقل بودن A از B باید

$$P(A|B) = P(A)$$

ولی می‌دانیم که

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

از مقایسه‌ی دو برابری داریم:

$$\frac{P(A \cap B)}{P(B)} = P(A)$$

یا

$$(۳) \quad P(A \cap B) = P(A) \cdot P(B)$$

به سادگی می‌توان دید که اگر B از A مستقل باشد باز همین رابطه برقرار است. پس اگر A از B مستقل باشد یا B از A مستقل باشد باید رابطه‌ی (۳) برقرار باشد. از طرفی با داشتن رابطه‌ی (۳) می‌توان به رابطه‌های $P(B|A) = P(B)$ و $P(A|B) = P(A)$ رسید. (چرا؟) یعنی رابطه‌ی (۳) شرط لازم و کافی برای استقلال A از B و B از A است. بر این اساس می‌گوییم A و B مستقل‌اند. پس: **تعریف:** دو پیشامد A و B از یک فضای نمونه‌ای مستقل‌اند اگر و تنها اگر

$$P(A \cap B) = P(A) \cdot P(B)$$

اگر $P(A \cap B) \neq P(A) \cdot P(B)$ می‌گویند دو پیشامد وابسته‌اند.

مثال ۷: فرض کنید برای ریاست شرکتی ۴ داوطلب وجود دارند. احتمال انتخاب شدن همه‌ی داوطلب‌ها یکی است. برآمدهای انتخاب افراد را به ترتیب با ۱، ۲، ۳، و ۴ نمایش می‌دهیم. نشان دهید که پیشامدهای $A = \{۱, ۴\}$ و $B = \{۱, ۳\}$ از هم مستقل‌اند. فضای نمونه‌ای به صورت $S = \{۱, ۲, ۳, ۴\}$ است. بنابر داده‌های مثال،

$$P(۱) = P(۲) = P(۳) = P(۴) = \frac{۱}{۴}$$

می‌خواهیم نشان دهیم که پیشامد A یعنی انتخاب فرد اول یا چهارم، از پیشامد B یعنی از انتخاب فرد اول یا سوم مستقل است. واضح است که

$$A \cap B = \{۱, ۴\} \cap \{۱, ۳\} = \{۱\}$$

پس:

$$P(A \cap B) = P(۱) = \frac{۱}{۴}$$

از طرفی:

$$P(A) = P(B) = \frac{۱}{۲}$$

در نتیجه:

$$P(A \cap B) = P(A) \cdot P(B) = \frac{۱}{۴}$$

یعنی پیشامدهای A و B از هم مستقل اند.

توجه: اگر دو پیشامد یک فضای نمونه‌ای ناسازگار باشند یعنی برآمدی مشترک نداشته باشند و احتمال هر دو مثبت باشد آن دو پیشامد از هم مستقل نیستند. به عبارت دیگر ناسازگاری دو پیشامد به استقلال دو پیشامد ربطی ندارد. زیرا اگر $A \cap B = \phi$ ، آن‌گاه

$$P(A \cap B) = P(\phi) = 0$$

و اگر A و B مستقل باشند باید

$$P(A \cap B) = P(A) \cdot P(B)$$

از مقایسه‌ی دو برابری اخیر نتیجه می‌شود که

$$P(A) \cdot P(B) = 0$$

یعنی دو پیشامد ناسازگار وقتی مستقل اند که $P(A) = 0$ یا $P(B) = 0$ ، و اگر این دو احتمال صفر نباشند A و B مستقل نیستند.

۸-۵- فرمول احتمال کل

اگر فضای نمونه‌ای S به n پیشامد B_1, B_2, \dots, B_n افراز شده باشد و اگر A پیشامدی از S باشد آن‌گاه به شرط $P(B_i) \neq 0, i = 1, \dots, n$

$$(۴) \quad P(A) = \sum_{i=1}^n P(A \cap B_i) = \sum_{i=1}^n P(B_i)P(A|B_i)$$

زیرا همان‌طور که در سال پیش دیده‌ایم

$$B_1 \cup B_2 \cup \dots \cup B_n = S$$

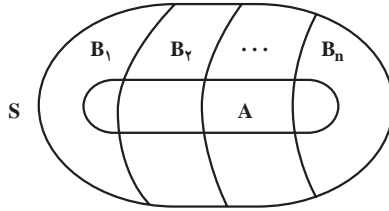
و هر دو پیشامد B_i و B_j وقتی $i \neq j$ ، ناسازگارند، یعنی $B_i \cap B_j = \phi$ ، بدیهی است که

$$A = A \cap S = A \cap (B_1 \cup B_2 \cup \dots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \dots \cup (A \cap B_n)$$

اما همه پیشامدهای طرف دوم رابطه بالا دو به دو ناسازگارند، پس، طبق اصل موضوع ۳،

داریم:

$$P(A) = P(A \cap B_1) + P(A \cap B_2) + \dots + P(A \cap B_n)$$



شکل ۴- افراز فضای نمونه‌ای

یا به صورت خلاصه، $P(A) = \sum_{i=1}^n P(A \cap B_i)$. اما می‌دانیم که با توجه به تعریف احتمال

شرطی و با فرض $P(B_i) \neq 0$ ، $P(A \cap B_i) = P(B_i)P(A|B_i)$ ، پس نتیجه می‌شود که

$$P(A) = \sum_{i=1}^n P(B_i)P(A|B_i)$$

این فرمول به فرمول احتمال کل موسوم است.

مثال ۸: سه ظرف همانند داریم. اولین ظرف شامل ۵ مهره‌ی سفید و ۱۱ مهره‌ی سیاه است.

دومین ظرف شامل ۳ مهره‌ی سفید و ۹ مهره‌ی سیاه است، و سومین ظرف تنها شامل مهره‌های سفید است. با چشم بسته یکی از سه ظرف را انتخاب و از آن مهره‌ای در می‌آوریم. احتمال این که مهره سفید باشد چه قدر است؟

پیشامد استخراج مهره‌ی سفید را با A نشان می‌دهیم. می‌خواهیم $P(A)$ را حساب کنیم

پیشامدهای زیر را تعریف می‌کنیم

$$B_1 = \{\text{ظرف اول انتخاب شود}\}$$

$$B_2 = \{\text{ظرف دوم انتخاب شود}\}$$

$$B_3 = \{\text{ظرف سوم انتخاب شود}\}$$

بدیهی است $P(B_1) = P(B_2) = P(B_3) = \frac{1}{3}$. از طرفی

$$P(A|B_1) = \frac{5}{16}, \quad P(A|B_2) = \frac{1}{4}, \quad P(A|B_3) = 1$$

حال با توجه به فرمول احتمال کل

$$P(A) = P(B_1) \cdot P(A|B_1) + P(B_2) \cdot P(A|B_2) + P(B_3) \cdot P(A|B_3)$$

$$= \frac{1}{3} \cdot \frac{5}{16} + \frac{1}{3} \cdot \frac{1}{4} + \frac{1}{3} \cdot 1 = \frac{25}{48}$$

△

۸-۶- قاعده‌ی بیز

(حالت ساده). در آزمایش‌های معمولی مواردی وجود دارند که برآمد نهایی آزمایش به آن چه در مراحل قبلی رخ می‌دهند بستگی دارد. برای توضیح این مطلب ابتدا به معرفی قاعده‌ی بیز می‌پردازیم.

دیدیم که اگر A و B دو پیشامد با احتمال مثبت از فضای نمونه‌ای یک آزمایش تصادفی باشند، آنگاه داریم

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

و

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

اگر از برابری دوم $P(A \cap B)$ یعنی $P(B|A) \cdot P(A)$ را در برابری اول قرار دهیم، نتیجه می‌شود که

$$(۵) \quad P(A|B) = \frac{P(A)}{P(B)} \cdot P(B|A)$$

این رابطه را قاعده‌ی بیز می‌نامند. قاعده‌ی بیز در حالت کلی مفصل‌تر است. تامس بیز (۱۷۶۱-۱۷۰۲) کشیشی انگلیسی بود که حالت کلی‌تر این قاعده را ارائه داد. در مثال زیر یک مورد استفاده از قاعده بیز را می‌بینید.

مثال ۹: وقتی یک مرکز مخابراتی تلگراف، پیامی را به مرکز دیگر می‌فرستد گاهی خط‌هایی در انتقال صورت می‌گیرند. به ویژه وقتی از الفبای مورس برای مخابره استفاده می‌شود و کدهای «نقطه» و «خط» را به کار می‌برند^۱ این خط‌ها بدین صورت است که کدی که مرکز M به صورت نقطه می‌فرستد در مرکز N خط دریافت می‌شود و یا برعکس. به تجربه دریافته‌اند که به طور متوسط در هر متنی که مرکزی می‌فرستد نسبت فراوانی نقطه به فراوانی خط برابر ۳ به ۴ است. هم‌چنین به طور تقریب می‌دانند که با احتمال $\frac{1}{8}$ نقطه‌ای که مرکز M می‌فرستد در مرکز N در اثر تداخل خطوط مخابره، اشتباهاً خط دریافت می‌شود و با همین احتمال خطی را که مرکز M می‌فرستد در مرکز N نقطه دریافت می‌شود. حال اگر در مرکز N کدی به صورت نقطه دریافت شده باشد چه قدر احتمال

۱- این روزها، در ارتباط‌های الکترونیکی از کدهای ۰ و ۱ استفاده می‌کنند.

دارد که این کد واقعاً به صورت نقطه فرستاده شده باشد؟
اگر در فرمول بیز قرار دهیم

پیشامد فرستادن نقطه = A

پیشامد دریافت نقطه = B

آن‌گاه فرمول

$$P(A|B) = \frac{P(A)}{P(B)} \cdot P(B|A)$$

به صورت زیر درمی‌آید

(الف) (فرستادن نقطه | دریافت نقطه) $\cdot P$ (دریافت نقطه) = $\frac{P(\text{فرستادن نقطه})}{P(\text{دریافت نقطه})}$ (دریافت نقطه | فرستادن نقطه) P
آنچه می‌خواهیم به دست آوریم طرف اول رابطه است. زیرا در مرکز N نقطه‌ای دریافت شده است و می‌خواهیم احتمال این که این کد به صورت نقطه فرستاده شده باشد را بدانیم. پس سه احتمال طرف دوم را حساب می‌کنیم.

$$P(A) = P(\text{فرستادن نقطه}) = \frac{3}{V} \quad (\text{ب})$$

$$P(B|A) = P(\text{فرستادن نقطه} | \text{دریافت نقطه}) = \frac{V}{8} \quad (\text{پ})$$

محاسبه‌ی سومین احتمال یعنی (دریافت نقطه) P کمی مفصل‌تر است. وقتی نقطه‌ای دریافت می‌شود باید فکر کنیم که نقطه‌ای فرستاده‌اند و یا خطی فرستاده‌اند که به خطا نقطه دریافت شده است. پس

$$P(B) = P(\text{فرستادن نقطه} \cap \text{دریافت نقطه}) + P(\text{خطی فرستادن} \cap \text{دریافت نقطه}) \quad (\text{ت})$$

$$P(\text{فرستادن خط} \cap \text{دریافت نقطه})$$

اما از فرمول حاصل ضرب احتمال می‌توانیم دو جمله‌ی طرف دوم را حساب کنیم.

$$P(\text{فرستادن نقطه} \cap \text{دریافت نقطه}) = P(\text{فرستادن نقطه} | \text{دریافت نقطه}) \cdot P(\text{فرستادن نقطه})$$

$$= \frac{V}{8} \cdot \frac{3}{V} = \frac{3}{8}$$

$$P(\text{فرستادن خط} \cap \text{دریافت نقطه}) = P(\text{فرستادن خط} | \text{دریافت نقطه}) \cdot P(\text{فرستادن خط})$$

می‌دانیم که طبق داده‌های مثال، $P(\text{فرستادن خط}) = \frac{4}{V}$ و $P(\text{فرستادن خط} | \text{دریافت نقطه}) = \frac{1}{8}$.

پس :

$$P(\text{فرستادن خط} \cap \text{دریافت نقطه}) = \frac{1}{8} \cdot \frac{4}{7} = \frac{1}{14}$$

اگر مقادیر این دو جمله را در (ت) قرار دهیم

$$P(B) = P(\text{دریافت نقطه}) = \frac{3}{8} + \frac{1}{14} = \frac{25}{56} \quad (\text{ث})$$

حال اگر (ب)، (پ) و (ث) را در (الف) قرار دهیم جواب مسأله به دست می‌آید :

$$P(\text{دریافت نقطه} \mid \text{فرستادن نقطه}) = \frac{\frac{3}{7}}{\frac{25}{56}} \cdot \frac{7}{8} = \frac{21}{25}$$

پس اگر در مرکز N نقطه‌ای دریافت شود احتمال $\frac{21}{25}$ وجود دارد که این کد واقعاً به صورت

Δ

نقطه فرستاده شده باشد.

همان‌طور که در مثال فوق توجه کردید در قاعده‌ی بیز ابتدا از روی تجربه‌های گذشته و یا فراوانی‌ها احتمالی ذهنی به رخداد پیشامد B به شرط A نسبت می‌دهیم. سپس با قاعده‌ی بیز احتمال رخداد پیشامد A به شرط B را محاسبه می‌کنیم. در مثال بالا

$P(\text{فرستادن نقطه} \mid \text{دریافت نقطه})$

را از روی تجربه‌ی گذشته برابر $\frac{7}{8}$ تعیین کردیم، سپس به کمک این داده و سایر داده‌ها $P(\text{دریافت نقطه} \mid \text{فرستادن نقطه})$ را که مورد نظر بود به دست آوردیم.

۸-۷- تمرین‌ها

۱- جعبه‌ای محتوی ۳ مهره‌ی سفید و ۲ مهره‌ی سیاه است. متوالیاً دو مهره به تصادف از جعبه بدون جای‌گذاری برمی‌داریم.

(الف) اگر اولین مهره سیاه باشد احتمال این که دومین مهره هم سیاه باشد چه قدر است؟

(ب) احتمال این که مهره‌ی دوم هم‌رنگ مهره‌ی اول باشد چه قدر است؟

۲- برحسب تجربه‌ی گذشته می‌دانیم احتمال این که رتبه‌ی اول سال آخر رشته‌ی ریاضی دبیرستانی در مسابقه‌ی ورودی دانشگاه قبول شود $\frac{95}{100}$ است. با توجه به سوابق تحصیلی علی در

این دبیرستان، احتمال این که او در سال آخر رشته‌ی ریاضی دبیرستان رتبه‌ی اول شود $9/0$ است. احتمال این که علی هم رتبه‌ی اول شود و هم در مسابقه‌ی ورودی دانشگاه قبول شود چه قدر است؟
۳- سکه‌ای همگن را ۳ بار می‌اندازیم. اگر A پیشامد رخ دادن رو در دو پرتاب اول، B پیشامد رخ دادن پشت در پرتاب سوم و C پیشامد رخ دادن دقیقاً دو پشت در سه پرتاب باشد، نشان دهید که A و B مستقل اند ولی B و C مستقل نیستند.

۴- احتمال زنده ماندن در یک عمل پیوند عضو برابر $5/0$ است. اگر بیماری پس از عمل زنده باشد احتمال این که بدن او در طول یک ماه پیوند را قبول نکند و بمیرد $2/0$ است. احتمال زنده ماندن یک بیمار پیوندی پس از این دو مرحله چه قدر است؟

۵- جعبه‌ای شامل ۱۲ لامپ است که ۳ تای آن‌ها معیوب اند. اگر به تصادف ۳ لامپ متوالیاً بدون جای گذاری از جعبه برداریم احتمال این که هر ۳ لامپ معیوب باشند چقدر است؟

۶- یک فضای نمونه‌ای متشکل از ۵ برآمد a, b, c, d, e است. به شرط آن که

$$P(a) = \frac{1}{4}, P(\{a, b, c\}) = \frac{1}{4}$$

الف) محاسبه‌ی $P(\{b, c, d\}|\{a, b, c\})$

ب) محاسبه‌ی $P(\{a\}|\{a, b, c\})$

۷- ۴ مهره به شماره‌های ۱، ۲، ۳، ۴ را در ظرفی ریخته‌ایم. اگر بخواهیم دو مهره به تصادف از ظرف بیرون بیاوریم شش امکان $(1, 2)$ ، $(1, 3)$ ، $(1, 4)$ ، $(2, 3)$ ، $(2, 4)$ و $(3, 4)$ وجود دارند. تفاضل هر دو شماره را R و مجموع آن‌ها را S فرض می‌کنیم.

الف) احتمال پیشامدی را که برای آن $R = 2$ ، به دست آورید.

ب) احتمال پیشامدی را که برای آن $S = 5$ ، به دست آورید.

آیا این پیشامدها مستقل اند؟

پ) اگر در قسمت الف R برابر یک باشد و در قسمت ب S هم چنان ۵ باشد پیشامدها

مستقل اند؟

۸- در دو جعبه به ترتیب 3^0 و 2^0 عدد لامپ همانند وجود دارد. در جعبه‌ی اول ۵ عدد لامپ معیوب و در جعبه‌ی دوم ۳ عدد لامپ معیوب موجود است. از اولی 1^0 لامپ و از دومی ۸ لامپ به تصادف انتخاب می‌کنیم و آن‌ها را به صورت درهم در جعبه‌ای جدید قرار می‌دهیم. از این جعبه به تصادف لامپی برمی‌داریم. احتمال این که این لامپ معیوب باشد چه قدر است؟

۹- دو ظرف داریم. اولی شامل ۱۰ مهره سفید و ۸ مهره سیاه است و دومی شامل ۱۲ مهره سفید و ۹ مهره سیاه است. از ظرف اول به تصادف مهره‌ای در می‌آوریم و در ظرف دوم قرار می‌دهیم. آن‌گاه از ظرف دوم به تصادف مهره‌ای در می‌آوریم. احتمال این که این مهره سفید باشد چه قدر است؟

۱۰- تکمیل بنای راهی ممکن است به دلیل اعتصاب کارگران به تأخیر افتد. فرض کنید احتمال این که اعتصابی رخ دهد ۰/۶۵ باشد و احتمال این که اگر اعتصابی نباشد کار به موقع انجام شود ۰/۸ باشد و احتمال این که اگر اعتصابی باشد کار به موقع انجام شود ۰/۳ باشد. احتمال این که کار بنای راه به موقع انجام شود چه قدر است؟

۱۱- اگر A_1 ، A_2 و A_3 سه پیشامد از فضای نمونه‌ای S باشند ثابت کنید

$$P(A_1 \cup A_2 \cup A_3) \leq P(A_1) + P(A_2) + P(A_3)$$

۱۲- اگر B_1 ، B_2 و B_3 سه پیشامد از فضای نمونه‌ای S و با احتمال مثبت باشند، به معنای احتمال رخداد پیشامد B_3 به شرط رخداد هر دو پیشامد B_1 و B_2 است. با این تعریف ثابت کنید

$$P(B_1 \cap B_2 \cap B_3) = P(B_1)P(B_2|B_1)P(B_3|B_2 \cap B_1)$$

۱۳- اگر B_1 ، B_2 و B_3 سه پیشامد دو به دو ناسازگار و با احتمال مثبت باشند که اجتماع آن‌ها برابر با S است و اگر A پیشامدی از S باشد ثابت کنید.

$$P(B_i|A) = \frac{P(A|B_i)P(B_i)}{\sum_{i=1}^3 P(A|B_i)P(B_i)}, \quad i = 1, 2, 3$$

فصل ۹

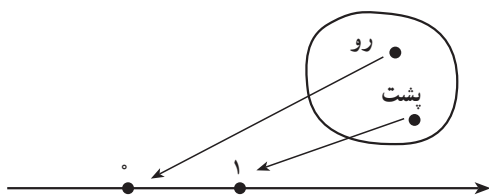
توزیع های گسسته ای احتمال

۹-۱- متغیر تصادفی گسسته

به طوری که قبلاً گفتیم در هر آزمایش تصادفی، فضای نمونه ای را مشخص می کنیم و به رخداد هر پیشامد آن عددی بین ۰ و ۱ به عنوان احتمال نسبت می دهیم. حال می خواهیم مجموعه ای دیگری را به جای فضای نمونه ای قرار دهیم. ابتدا به مثال های زیر توجه کنید.

مثال ۱: وقتی سکه ای را می اندازیم، S دارای دو برآمد رو و پشت است. تابع X را بدین صورت تعریف می کنیم که حوزه ی تعریف (دامنه) آن مجموعه ی S با دو عضو رو و پشت و حوزه ی مقادیر (برد) آن دو عدد ۰ و ۱ از محور اعداد حقیقی باشد. به عبارت دیگر

$$\begin{cases} X(\text{رو}) = 0 \\ X(\text{پشت}) = 1 \end{cases}$$



شکل ۱

چنین تابع X را متغیر تصادفی می گوئیم که دو مقدار ۰ و ۱ را اختیار می کند. چون احتمال رخداد برآمد رو $\frac{1}{2}$ است پس $X=0$ که نمایش ساده ی $X(\text{رو})=0$ است و در واقع نمادی برای رخداد برآمد رو است، دارای همان احتمال $\frac{1}{2}$ و همین طور احتمال $X=1$ برابر $\frac{1}{2}$ است. در واقع به جای جدول

	رو	پشت
برآمد	$\frac{1}{2}$	$\frac{1}{2}$
احتمال	$\frac{1}{2}$	$\frac{1}{2}$

جدول

x_i	۰	۱
p_i	$\frac{1}{2}$	$\frac{1}{2}$

را قرار می‌دهیم. x_i ها مقادیر X و p_i ها احتمال‌های متناظر با آن‌ها هستند. توجه کردید که فضای نمونه‌ای، $S = \{\text{رو، پشت}\}$ ، جای خود را به مجموعه‌ی $\{0, 1\}$ داده است. Δ

مثال ۲: در انداختن یک تاس همگن مجموعه‌ی S دارای ۶ برآمد است. به هر برآمد S ،

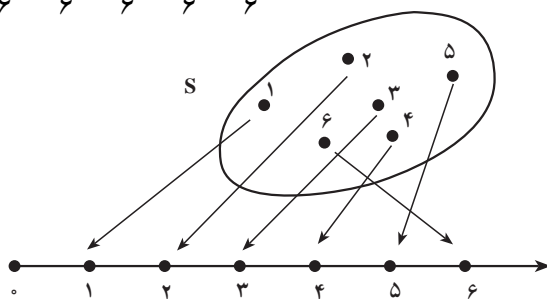
احتمال $\frac{1}{6}$ را نسبت می‌دهیم. اگر X تابعی باشد که بر هر برآمد S عددی صحیح از ۱ تا ۶ را که همان

اعداد حک شده بر وجوه تاس اند نسبت دهد، یعنی بر هر برآمد S نقطه‌ای از محور اعداد حقیقی را

نسبت دهیم، متغیر تصادفی X با مقادیر صحیح ۱ تا ۶ به وجود می‌آید که احتمال هر مقدار آن، همان

احتمال برآمد S متناظر با آن است (شکل ۲). پس جدول زیر برای ریزش تاس نتیجه می‌شود.

x_i	۱	۲	۳	۴	۵	۶
p_i	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$



شکل ۲

Δ

مثال ۳: بر فضای نمونه‌ای S ، در مثال قبل، می‌توان متغیر تصادفی دیگری را تعریف کرد.

تابع X را تابعی بگیری که شماره‌های ۱، ۲، ۳ و ۴ را با نقطه‌ی به طول ۱ و شماره‌ی ۵ را با نقطه‌ی

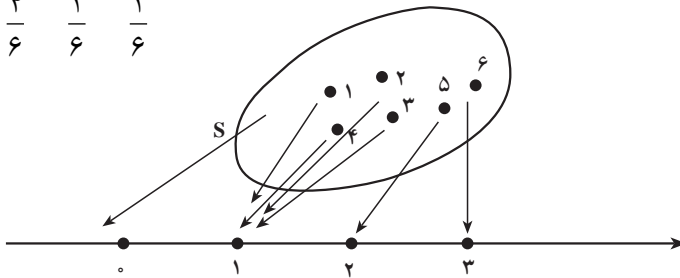
به طول ۲، و شماره‌ی ۶ را با نقطه‌ی به طول ۳ از محور اعداد حقیقی متناظر کند (مطابق شکل ۳)

در این صورت

$$\begin{cases} X (\text{شماره ی ۱}) = X (\text{شماره ی ۲}) = X (\text{شماره ی ۳}) = X (\text{شماره ی ۴}) = ۱ \\ X (\text{شماره ی ۵}) = ۲ \\ X (\text{شماره ی ۶}) = ۳ \end{cases}$$

بنابراین جدول احتمال زیر به دست می آید.

x_i	۱	۲	۳
p_i	$\frac{4}{6}$	$\frac{1}{6}$	$\frac{1}{6}$



شکل ۳

توجه کنید که رخداد $(X=1)$ یعنی رخداد پیشامد {شماره ی ۱, شماره ی ۲, شماره ی ۳, شماره ی ۴}، و می دانیم این پیشامد دارای احتمال $\frac{4}{6}$ است. در متغیرهای تصادفی این سه مثال، تعداد مقادیری که هر متغیر اختیار می کرد متناهی بود. متغیر تصادفی را در احتمال مقدماتی به صورت زیر تعریف می کنند:

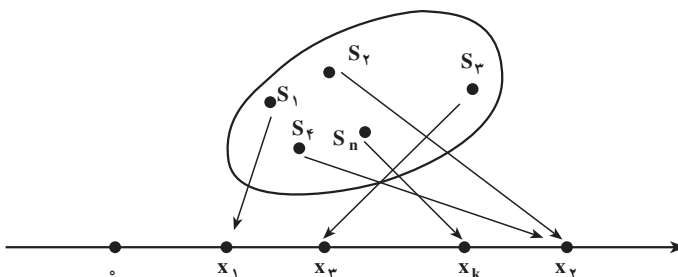
تعریف متغیر تصادفی^۱ تابعی از فضای نمونه ای S بر اعداد حقیقی است. این تابع را با X نشان می دهیم.

همان طور که در مثال های قبل دیدیم مجموعه ای اعداد حقیقی یک فضای نمونه ای جدید است. اگر حوزه ی مقادیر X متناهی یا شمارا نامتناهی باشد متغیر تصادفی X را گسسته می گویم. برای درک مطلب فرض کنید فضای نمونه ای $S = \{s_1, \dots, s_n\}$ را داریم و احتمال هایی که به ترتیب به برآمدهای S تخصیص داده ایم p_1, \dots, p_n باشند. تابعی مانند X را در نظر می گیریم که حوزه ی تعریف آن S و حوزه ی مقادیر آن نقاطی از محور اعداد حقیقی است، به قسمی که هر برآمد یا هر پیشامد S ، با نقطه ای از محور مزبور متناظر باشد. در این صورت مطابق شکل ۴،

۱- در واقع متغیر تصادفی، نه متغیر است و نه تصادفی است، بلکه یک تابع روی مدل احتمال است.

$$X(s_1) = x_1, X(s_2) = x_2, X(s_3) = x_3, X(s_4) = x_2, \dots, X(s_n) = x_k$$

تابع X ، متغیر تصادفی است و x_1, x_2, \dots, x_k مقادیر آن هستند.



شکل ۴

۹-۲- تابع جرم احتمال

تابع جرم احتمال یک متغیر تصادفی گسسته X ، تابعی است که به هر یک از مقادیر X ، یعنی به هر یک از x_i ها $i = 1, 2, \dots, k$ احتمال $P(X = x_i) = p_i$ را نسبت می‌دهد. به صورت جدول، داریم:

x_i	x_1	x_2	\dots	x_k
p_i	p_1	p_2	\dots	p_k

بدیهی است که $p_1 + p_2 + \dots + p_k = 1$. اگر نقاط به طول x_1, x_2, \dots, x_k را نقاطی مادی تلقی کنیم می‌توانیم p_1, p_2, \dots, p_k را به ترتیب جرم این نقاط بگیریم. به همین دلیل رابطه‌ی

$$P(X = x_i) = p_i \text{ و } i = 1, 2, \dots, n$$

را تابع جرم احتمال یا صرفاً تابع احتمال متغیر تصادفی X می‌نامند. جدول بالا نشان می‌دهد که مقدار کل احتمال ۱ به چه ترتیب بین مقادیر متغیر X توزیع شده است و آن را جدول توزیع احتمال می‌گویند. تعداد مقادیری که X پذیرفته است متناهی هست. گاهی تعداد مقادیری که X اختیار می‌کند نامتناهی ولی شماراست. به مثال زیر توجه کنید.

مثال ۴: جامعه‌ی کودکان زیر ده سال را در نظر بگیرید. هر کودک را برای این که ببینید به بیماری هموفیلی مبتلاست یا نه آزمایش می‌کنند. فرض کنید متغیر تصادفی را به صورت زیر تعریف کنیم:

تعداد کودکانی که باید آزمایش شوند تا اولین مورد هموفیلی ظاهر شود $X =$

ببینیم که X چه مقادیری را انتخاب می کند. ممکن است اولین نفری که در جامعه ی مزبور آزمایش می شود به هموفیلی مبتلا باشد پس در این صورت $X = 1$. ممکن است اولین نفر مبتلا نبوده، دومین نفر مبتلا باشد پس $X = 2$ و نظایر آن. می توانید مجسم کنید که ممکن است یک میلیون کودک آزمایش شوند و کودکی مبتلا پیدا نشود یعنی X می تواند بیش از یک میلیون هم باشد. به همین ترتیب مقادیری که X می تواند اختیار کند شمارا بوده ولی نامتناهی است. در این حالت داریم

$$P(X = x_i) = p_i, \quad i = 1, 2, \dots$$

بدیهی است، $\sum_{i=1}^{\infty} p_i = 1$. یعنی باید احتمال ۱ را بین بی نهایت مقدار x_i توزیع کرد.

تذکر: هر تابع احتمال مربوط به متغیر تصادفی گسسته X دارای ویژگی های زیر است:

$$i = 1, 2, \dots, \quad 0 \leq P(X = x_i) \leq 1 \quad -1$$

$$\sum_i P(X = x_i) = 1 \quad -2$$

برعکس اگر تابعی به صورت $P(X = x_i) = p_i, i = 1, 2, \dots$ دارای دو ویژگی بالا باشد یک تابع احتمال است.

مثال ۵: سکه ای را متوالیاً می اندازیم. سکه منصف نیست. تعداد دفعاتی که سکه را می اندازیم تا برای اولین بار رو ظاهر شود متغیر تصادفی X می نامیم.

الف) X چه مقادیری اختیار می کند؟ (ب) احتمال رخداد هر مقدار X چیست؟
الف) ممکن است در بار اول رو ظاهر شود پس $X = 1$. اگر بار اول رو ظاهر نشود ولی بار دوم رو بیاید $X = 2$. به همین ترتیب ممکن است تا پرتاب شماره ی ۳، ۴، ۵، ...، ۱۰۰۰، ... برای بار اول رو ظاهر نشود، پس X همه ی مقادیر صحیح طبیعی را اختیار می کند.

ب) فرض می کنیم در پرتاب i ام برای اولین بار رو بیاید می خواهیم احتمال این پیشامد یعنی $P(X = i)$ را به دست آوریم. اگر در یک بار انداختن سکه، H معرف برآمد رو و T معرف برآمد پشت باشد، پیشامد

$$\underbrace{TT \dots TH}_{(i-1) \text{ بار}}$$

بدین معناست که $i-1$ بار متوالیاً پشت بیاید و در i امین بار رو ظاهر شود. باید احتمال این پیشامد را که مستلزم رخداد i برآمد است به دست آوریم. سکه منصف نیست یعنی احتمال رو آمدن و احتمال پشت آمدن $\frac{1}{2}$ نیست. فرض می کنیم احتمال ظاهر شدن رو p و احتمال ظاهر شدن پشت q

باشد. واضح است که $p + q = 1$. هر انداختن سکه از انداختن‌های دیگر مستقل است. حال قبل از محاسبه‌ی احتمال موردنظر متذکر می‌شویم که اگر برای چند آزمایش تصادفی جدا از هم فضاهای نمونه‌ای و مدل‌های احتمال را بسازیم و اگر A_1 پیشامدی از فضای اول، A_2 پیشامدی از فضای دوم، ... باشد آن‌گاه شرط استقلال A_1, A_2, \dots از هم را به صورت زیر بیان می‌کنند.

$$P(A_1 \cap A_2 \cap \dots) = P(A_1) \cdot P(A_2) \cdot \dots$$

پس، اگر برای هر انداختن سکه یک فضای نمونه‌ای در نظر بگیریم، آن‌گاه مثلاً

$$P(TT) = q \cdot q = q^2$$

به همین ترتیب:

$$P(\underbrace{TT \dots T}_{(i-1) \text{ بار}}) = \underbrace{q \cdot q \dots q}_{(i-1) \text{ بار}} = q^{i-1}$$

و بالاخره:

$$P(\underbrace{TT \dots T}_{(i-1) \text{ بار}}H) = q^{i-1} \cdot p$$

پس:

$$P(X = i) = q^{i-1} \cdot p$$

اگر i را برابر ۱، ۲، ... بگیریم احتمال‌های متناظر با مقادیر X به دست می‌آیند. جدول زیر را

می‌توانیم بنویسیم

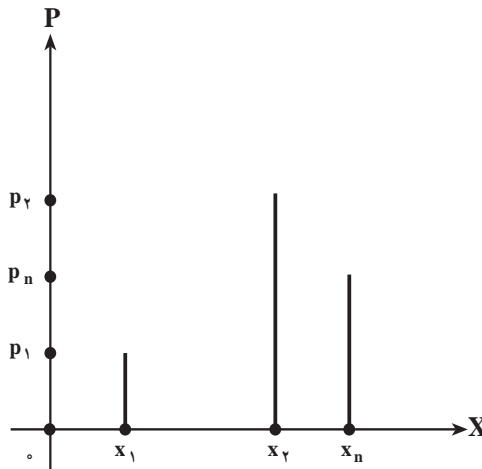
x_i	۱	۲	۳	...	i	...
p_i	p	qp	$q^2 p$...	$q^{i-1} p$...

رابطه‌ی $P(X = i) = q^{i-1} p$ ، $i = 1, 2, \dots$ تابع احتمال متغیر تصادفی X است. Δ

شما می‌توانید به میل خود جدولی تشکیل دهید که سطر اول مقادیر متغیر تصادفی X باشد (هر مقداری که مایل هستید به آن نسبت دهید) و سطر دوم آن احتمال‌هایی دلخواه باشند، فقط لازم است که مجموع احتمال‌ها ۱ باشد. اگر هر مقداری را که متغیر تصادفی X اختیار می‌کند طول یک نقطه، و احتمال متناظر با آن را عرض آن نقطه نسبت به دو محور متعامد بگیریم نموداری برای احتمال X به دست می‌آوریم.

لازم نیست که واحد طول را روی دو محور یکی بگیریم. عرض‌های نقاط، مقادیر p_i ،

p_1, \dots, p_n و p_n هستند که همه بین صفر و یک اند. طول های نقاط، مقادیر x_1, x_2, \dots, x_n هستند (مطابق شکل ۵).



شکل ۵ - نمودار میله ای

در واقع می توان طول میله های بالای x_1, x_2, \dots, x_n را احتمال های متناظر با آن ها گرفت. این نمودار را نمودار میله ای می نامند. برای هر تابع احتمال گسسته می توانید چنین نموداری رسم کنید.

همان طور که گفتیم می توانیم جدول های توزیع احتمال دلخواه فراوانی بنویسیم اما آن جدول ها و مدل هایی مورد توجه اند که ارزش کاربردی داشته باشند. ذیلاً چند توزیع احتمال مهم را ذکر می کنیم.

۹-۳- توزیع برنولی

وقتی لامپی را امتحان می کنیم ممکن است سالم باشد یا معیوب. به طور کلی وقتی کالایی را در موقع خرید امتحان می کنیم یا سالم است و یا ناقص. وقتی از فردی در مورد اعتیادش به سیگار سؤال می کنیم یا سیگاری است یا نیست. از این پدیده های دو حالتی زیادند. اگر سالم بودن کالا یا سیگاری بودن فرد را با $X=1$ و ناقص بودن کالا و سیگاری نبودن فرد را با $X=0$ نشان دهیم متغیری تصادفی داریم که دو مقدار ۰ و ۱ را اختیار می کند. این آزمایش های دو حالتی را امتحان می نامیم و فضای نمونه ای هر امتحان دو برآمد دارد. ریختن سکه هم یک امتحان است.

اگر احتمال سالم بودن کالا یا سیگاری بودن فرد را p بگیریم احتمال ناقص بودن کالا و یا سیگاری نبودن فرد برابر q است. پس جدول توزیع احتمال زیر را برای هر امتحان داریم

$$\begin{array}{c|cc} x_i & 0 & 1 \\ \hline p_i & q & p \end{array} \quad p+q=1$$

مرسوم است که دو برآمد امتحان را پیروزی و شکست می نامند. برآمدی که مورد توجه است پیروزی نامیده می شود. مثلاً ممکن است لامپها را یک به یک برای یافتن لامپی معیوب امتحان کنیم، در این صورت یافتن لامپ معیوب یک پیروزی است. این جدول را می توان به صورت رابطه‌ی زیر هم خلاصه کرد.

$$P(X=i) = \begin{cases} p^i q^{1-i} & i=0,1 \\ 0 & \text{به ازای سایر مقادیر } i \end{cases}$$

به طور کلی اگر پیشامد A از یک فضای نمونه‌ای را در نظر بگیریم و رخداد A را پیروزی گرفته، احتمال پیروزی را p فرض کنیم، آن گاه متغیر تصادفی X که به صورت

$$\begin{cases} X=1 & \text{اگر } A \text{ رخ دهد} \\ X=0 & \text{اگر } A \text{ رخ ندهد} \end{cases}$$

تعریف می شود دارای تابع احتمال بالاست.

متغیر تصادفی X را که تنها دو مقدار 0 و 1 را می پذیرد متغیر برنولی و توزیع احتمال آن را توزیع برنولی می گویند.

۹-۴- تمرینها

- ۱- پنج سکه‌ی منصف را باهم پرتاب می کنیم.
الف) فضای نمونه‌ای را بنویسید.
ب) یک متغیر تصادفی تعریف کنید که تعداد «شیرها» را نشان دهد.
پ) تابع احتمال متغیر تصادفی بند ب را بنویسید.
- ۲- دو تاس را باهم پرتاب می کنیم. متغیر تصادفی X را مجموع دو عدد ظاهر شده در روی دو تاس تعریف می کنیم.
الف) فضای نمونه‌ای این آزمایش را بنویسید.

(ب) تابع احتمال X را به دست آورید.

(پ) احتمال این که $X \leq 7$ باشد چه قدر است؟

۳- یک تاس پرتاب می کنیم. متغیر تصادفی X را به صورت زیر تعریف می کنیم.

$$X = \begin{cases} 1 & \text{اگر عدد فرد بیاید،} \\ 2 & \text{اگر عدد زوج بیاید،} \end{cases}$$

(الف) تابع احتمال X را بیابید.

(ب) آیا X یک متغیر تصادفی برنولی است؟

۴- سکه ای منصف را آن قدر پرتاب می کنیم تا «شیر» بیاید.

(الف) فضای نمونه ای این آزمایش را بنویسید.

(ب) یک متغیر تصادفی تعریف کنید که براساس آن بتوان احتمال شیر آمدن را محاسبه کرد.

(پ) احتمال این که اولین بار در آزمایش صدم شیر ظاهر شود چه قدر است؟

۵- توزیع احتمال متغیر تصادفی X به صورت زیر مشخص می شود.

$$P(X = i) = \frac{i}{i + 3} \quad i = 1, 2, 3$$

$$P(X = j) = \frac{1}{14} \quad j = 4, 5, 6$$

(الف) جدول توزیع X را بسازید.

(ب) نمودار توزیع را رسم کنید.

(پ) مقدار $P(X \geq 3)$ را حساب کنید.

۶- احتمال این که فردی مسن مبتلا به دیابت باشد $\frac{1}{4}$ است. در روستایی مردان مسن را

تحت آزمایش قرار می دهند. اگر متغیر تصادفی X را برابر با تعداد افرادی تعریف کنیم که به ترتیب

آزمایش می شوند تا اولین فرد دیابتی مشخص شود، تابع احتمال متغیر X را به دست آورید. احتمال

این که دومین نفر دیابتی باشد چه قدر است؟

۷- فضای نمونه ای یک آزمایش تصادفی ۳ برآمد دارد اگر احتمال های متناظر با ۳ برآمد به

ترتیب $\frac{1}{6}$ ، $\frac{1}{2}$ و $\frac{1}{6}$ باشد متغیری تصادفی روی این فضا تعریف کنید.

۸- نشان دهید که تابع زیر یک تابع احتمال است.

$$P(X = x) = \frac{1}{n^2} [2(n - x) + 1], \quad x = 1, 2, \dots, n$$

مراجع

1 - S. Ross, A First Course in Probability, Macmilan 1976.

- ۲- جان فروند و رانلد والپول، آمار ریاضی ترجمه‌ی علی عمیدی و محمدقاسم وحیدی اصل، مرکز نشر دانشگاهی، تهران، چاپ سوم ۱۳۷۳.
- ۳- جواد بهبودیان، آمار و احتمال مقدماتی، انتشارات آستان قدس ۱۳۶۸.
- ۴- علی عمیدی، احتمال و کاربرد آن، انتشارات دانشگاه پیام نور ۱۳۷۴.

