

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

ریاضیات گسسته

دورهٔ پیش دانشگاهی

رشتهٔ علوم ریاضی

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 برنامه‌ریزی : یحیی تابش، محمدحسن بیژن‌زاده، امیرنادری، حمیده داریوش همدانی و جواد حاجی بابائی

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

ویراستار : علی عمیدی

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

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

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

وبسایت : www.chap.sch.ir

مدیر امور فنی و چاپ : لیدا نیک‌روش

رسام : مریم دهقان‌زاده

طراح جلد : علیرضا رضائی‌کُر

صفحه‌آرا : شهرزاد قنبری

حروفچین : زهرا ایمانی‌نصر، سیده فاطمه محسنی

مصحح : رعنا فرج‌زاده‌دروئی، فاطمه گیتی جبین

امور آماده‌سازی خبر : فریبا سیر

امور فنی رایانه‌ای : حمیدنابت کلاچاهی، راحله زادفتح‌اله

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

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

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

سال انتشار و نوبت چاپ : چاپ بیست و یکم ۱۳۹۴

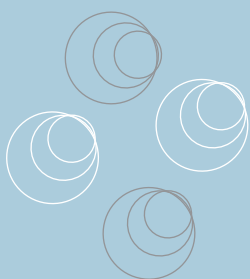
حق چاپ محفوظ است.

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 نترسند، اراده کنند در مقابل غرب، قیام کنند و نترسند...

امام خمینی



فهرست

قسمت اول: گراف‌ها و کاربردهای آن

- ۱ فصل ۱- آشنایی با گراف‌ها ۲
- ۱۰ فصل ۲- چند ویژگی ساده و چند رده خاص گراف‌ها ۱۰
- ۱۷ فصل ۳- درخت و ماتریس ۱۷

قسمت دوم: نظریه اعداد

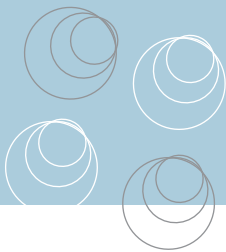
- ۲۴ فصل ۴- کلیات و تقسیم پذیری ۲۴
- ۳۸ فصل ۵- اعداد اول ۳۸
- ۴۸ فصل ۶- همنهشتی ۴۸

قسمت سوم: مباحثی دیگر از ترکیبیات

- ۵۷ فصل ۷- مدل‌های شهودی و تجسمی در ترکیبیات ۵۷

قسمت چهارم: احتمال

- ۷۴ فصل ۸- احتمال ۷۴
- ۹۱ فصل ۹- توزیع‌های گسسته احتمال ۹۱



پیشگفتار

در سال‌های اخیر به دلیل پیشرفت علوم و تکنولوژی به ویژه علوم کامپیوتر، نه تنها به درس‌هایی چون حسابان (حساب دیفرانسیل و انتگرال) که در حیطه ریاضیات پیوسته قرار دارد توجه می‌شود، بلکه درس‌ها و کتاب‌های بسیاری تحت عناوینی 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 ترکیباتی، مباحثی از نظریه اعداد و احتمال و کاربردهایی چون کدگذاری و رمزنگاری را شامل‌اند. وجه اشتراک تقریباً همه 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. بویایی و وجود مسائل فراوان حل نشده و ظاهراً ساده از مشخصات دیگر این شاخه‌اند. به طور کلی 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 دوره متوسطه بسیاری از کشورها آغاز شده است و محققاً در ایران نیز تدریس آن در دوره پیش‌دانشگاهی لازم است.

در این کتاب مؤلفان مطالبی را که جنبه 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 برنامه درسی نیستند به صورت مجله ریاضی آمده‌اند.

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

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

گراف‌ها و کاربردهای آن



مقدمه

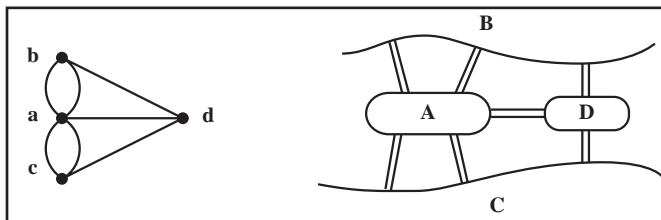
در این قسمت که شامل سه فصل است با الفبای نظریهٔ گراف‌ها و کاربردهایش آشنا می‌شویم. عمدتاً از طبیعت جذاب گراف‌ها استفاده می‌کنیم، شهود را به کار می‌بندیم و با مثال‌های ملموس و معماهای گوناگون مفاهیم را روشن می‌سازیم. در عین حال در بست تسلیم شهود نمی‌شویم و در مواردی اثبات دقیق قضایا را ارائه می‌دهیم. 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 این گونه مسائل سرآغاز ایده‌ها و حتی نظریه‌های مهم ریاضی بوده‌اند. از دانش پژوهانی که دورهٔ دبیرستان را پشت سر گذاشته‌اند انتظار داریم ذهن پویای خود را به کار اندازند و برای پاسخگویی به سؤال‌های عدیده‌ای که خود طرح می‌کنند، یاپرسش‌هایی 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.

آشنایی با گراف‌ها

در این فصل با بیان چند مثال زمینه را برای تعریف انواع گراف‌ها آماده می‌کنیم و آن را با ارائه 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. معمای 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؟ اوپلر در سال ۱۷۳۶ با حل مسأله پل‌های کونیگسبرگ نظریه 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 نقطه 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، به طور دقیق تر یک گراف چندگانه می نامند. اینک ما هم می توانیم مسائل مختلفی را به زبان نظریه گراف ها بیان کنیم.

مثال ۱: فرض می کنیم پنج تیم به نام های a, b, c, d, e باید دو به دو با یکدیگر مسابقه بدهند. پس از چندی می بینیم که:

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

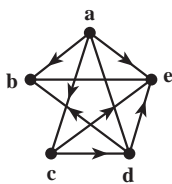
b با a و d روبه رو شده (و از هر دو شکست خورده است).

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

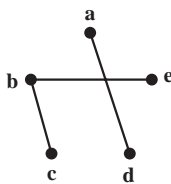
d با b, c, e بازی کرده (و b و e را شکست داده و از c شکست خورده است).

e با a, b, c, d مسابقه داده است (پیروزی ها و شکست های e قبلاً مشخص شده اند).

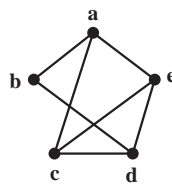
این وضعیت را می توانیم به صورت یک نمودار در صفحه مشخص کنیم. به ازای هر تیم یک نقطه در نظر می گیریم و دو نقطه را با پاره خط یا کمائی به هم وصل می کنیم هرگاه تیم های متناظر با هم مسابقه داده باشند. شکل ۲ مدل مربوط به این وضعیت را نشان می دهد.



شکل ۲



شکل ۳

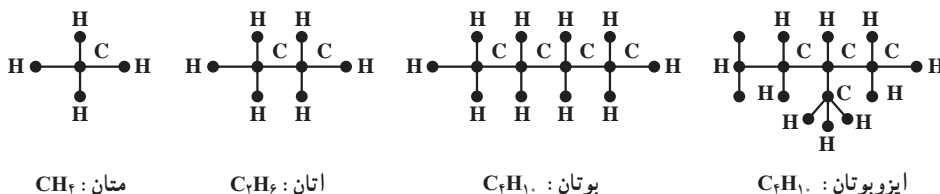


شکل ۴

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 می گیریم و این بار دو نقطه را با پاره خطی به هم وصل می کنیم هرگاه دو تیم مربوط با هم بازی نکرده باشند. نمودار مربوط به این وضعیت که در شکل ۳ نمایش داده شده است نشان می دهد که برای تکمیل این دور از مسابقات سه مسابقه دیگر باید برگزار شوند. فرض می کنیم که این مسابقات حتماً باید برنده هم داشته باشند. (برندگان را قبلاً مشخص کرده ایم). لذا می توانیم هنگام رسم شکل ۲ به جای مثلاً پاره خط، پاره خطی جهت دار رسم کنیم که جهت آن از برنده به سوی بازنده باشد. با این ترتیب شکل ۴ به دست می آید. این گراف نشان می دهد که مثلاً تیم e از سه تیم a, c, d شکست خورده و هنوز برنده نشده است. چنین گرافی را گراف جهت دار می نامیم.

مثال ۲: در درس شیمی دیده ایم که به هیدروکربن های اشباع شده نمودارهایی نسبت می دهند تا ساختار شیمیایی آنها را به نمایش بگذارند. در شکل ۵ چند نمونه از این هیدروکربن ها را که فرمول عمومی آنها C_nH_{2n+2} است می بینید.



شکل ۵ - چند نمونه از هیدروکربن ها

مثلاً نمودار مربوط به اتان که چگونگی پیوند کربن ها و هیدروژن ها را نشان می دهد ظرفیت کربن و هیدروژن را نیز مشخص می کند. در شکل ۵ می بینیم که با چهار کربن و ده هیدروژن دو هیدروکربن اشباع شده «مختلف» وجود دارند. بیش از دو تا چی؟ طبیعتاً پاسخ به این سؤال برای n های 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 نام های B_1, B_2, B_3, B_4 و B_5 برای تصدی این شغل ها داوطلب می شوند که طبق فهرست زیر برخی صلاحیت تصدی بیش از یک کار را دارند:

B_1 می تواند سه شغل A_1, A_2 و A_3 را اداره کند.

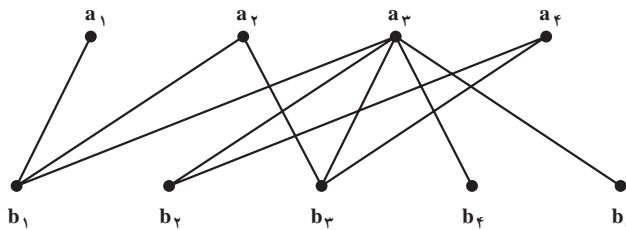
B_2 می تواند دو شغل A_3 و A_4 را بپذیرد.

B_3 قادر است هر یک از شغل های A_1, A_2 و A_3 را انجام دهد.

B_4 و B_5 هم می توانند تنها متصدی شغل A_3 باشند.

آیا با این پنج نفر، شرکت می تواند برای پست های خالی متصدی پیدا کند؟ این مسأله چند جواب دارد؟

برای بررسی این وضعیت باز هم یک مدل می سازیم. به این صورت که در صفحه، چهار نقطه متناظر با چهار شغل موردنظر و پنج نقطه دیگر متناظر با پنج داوطلب مذکور در نظر می گیریم و مطابق شکل ۶ هر نقطه b_i ، $1 \leq i \leq 5$ را با پاره خط یا پاره خط هایی به نقاطی چون a_j ، $1 \leq j \leq 4$ ، در صورتی وصل می کنیم که داوطلب B_i که با نقطه b_i در تناظر است صلاحیت انجام شغل A_j را که با نقطه 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_2 برای تصدی A_2 باقی می‌ماند. چون B_2 و B_3 تنها داوطلبان احراز پست A_2 هستند و B_2 قبلاً به کار A_2 گماشته شده است، باید الزاماً به B_3 سپرده شود. حال برای تصدی A_3 دو داوطلب باقی می‌مانند: B_4 و B_5 . پس این مسأله تنها دو جواب دارد و شرکت مجبور است B_1 را به کار A_1 ، B_2 را به کار A_2 ، B_3 را به کار A_3 و B_4 یا B_5 را به کار A_3 بگمارد. ▲

۲-۱- چند تعریف و قرارداد

در زندگی پیچیدهٔ 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. نظریهٔ 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 (ساده) G زوجی مرتب چون (V, E) است که در آن V مجموعه‌ای متناهی و E زیرمجموعه‌ای از مجموعه تمام زیرمجموعه‌های دو عضوی V است. اعضای V را رأس‌های G و اعضای E را یال‌های G می‌نامیم. مجموعه رأس‌های G را با $V(G)$ و مجموعه 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. ▲

قرار داد: اگر در گراف G ، $u, v \in V(G)$ و $\{u, v\} \in E(G)$ ، برای سادگی، به جای $\{u, v\}$ می نویسیم uv و می گوئیم در G دو رأس u و v مجاورند. در این صورت گاهی گفته می شود 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) می گذرد یا مرور می کند. رأس های u و v دو سر یال uv نام دارند.

مثال ۵: اگر $V = \{a, b, c, d, e\}$ و $E = \{ab, ac, ae, bd, cd, ce, de\}$ آن گاه 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 می گذرد. ▲

توجه دارید که هر گراف را می توان با یک نمودار، موسوم به نمودار گراف، نیز نمایش داد. برای این کار به ازای هر رأس G نقطه یا دایره کوچک دلخواهی، مثلاً در صفحه، در نظر می گیریم و دو نقطه متمایز را با پاره خط یا کمانی به هم وصل می کنیم به شرطی که مجموعه 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 داده ایم. شکل ۶ نموداری از گراف $G = (V, E)$ را نمایش می دهد که در آن:

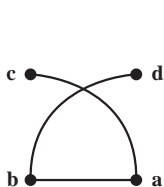
$$V = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, b_5\}$$

$$E = \{a_1b_1, a_2b_1, a_3b_3, a_4b_1, a_1b_2, a_2b_3, a_3b_4, a_4b_5, a_1b_4, a_2b_5\}$$

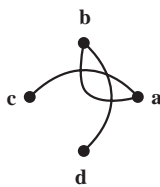
در این گراف از رأس a_3 پنج یال مرور می کنند؛ ولی از هر یک از دو رأس a_1 و b_5 تنها یک یال می گذرد.

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.

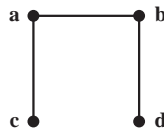
سه نمودار از این گراف را در شکل های زیر رسم کرده ایم.



شکل ۹



شکل ۸

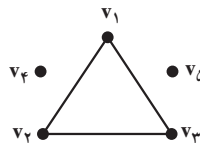


شکل ۷

واضح است که در شکل‌های ۸ و ۹ نقطه 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 ویال 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. آن‌گاه 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 (ساده) G تغییر کوچکی بدهیم تعریف گراف جهت دار به دست می‌آید که کاربردهای فراوان دارد.

تعریف: گراف جهت دار G زوجی مرتب چون (V, E) است که در آن V مجموعه‌ای متناهی و ناتهی است و E زیرمجموعه‌ای از مجموعه تمام زوج‌های مرتب متشکل از اعضای V است.
می‌توانیم به هر گراف جهت دار 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 جهت داری است که نمودار آن در شکل ۴ نمایش داده شده است. توجه دارید که در یک گراف جهت دار به ازای هر $u, v \in V$ با شرط $u \neq v$ حداکثر دو به اصطلاح یال جهت داری یکی از u به v و دیگری از v به u وجود دارند.^۱

۱- در تعریف گراف جهت دار 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 ۸۴۸، ۱۹۲، ۳۵۹، ۷۹۳، ۱ گراف جهت دار «متفاوت» وجود دارند!

۱-۳- تمرین‌ها

۱- در مثال ۳ اگر علاوه بر شرایط داده شده، B_5 قادر به انجام کار A_7 نیز باشد شرکت به چند طریق می‌تواند پست‌های خالی را پر کند؟

۲- در مثال ۳ اگر علاوه بر شرایط داده شده، B_7 قادر به انجام کار A_7 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

$$E = \{v_1v_2, v_1v_4, v_2v_3, v_2v_4, v_3v_4, v_4v_5, v_5v_6, v_6v_7\}$$

(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 کلمه «شجر» به معنای درخت است و درخت گراف خاصی است که بعداً در فصل ۳ بررسی خواهد شد. درباره ارتباط بین «شجره نامه خانوادگی» و گراف‌ها چه می‌دانید؟ شجره نامه خانوادگی خود را رسم کنید.

۶- شش بازه باز $(0, 2)$ ، $(1, 4)$ ، $(2, 5)$ ، $(3, 4)$ ، $(3, 8)$ ، $(6, 9)$ ، 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 $(0, 2)$ و $(1, 4)$ تهی نیست رأس‌های مربوط باید مجاور باشند. اما چون اشتراک بازه‌های $(0, 2)$ و $(2, 5)$ 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 بازه مناسب نشان دهید گراف شکل ۳ را می‌توان گراف بازه‌ها دانست.

(پ) نشان دهید گراف شکل ۲ نمی‌تواند گراف بازه‌ها باشد؛ یعنی، پنج بازه 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.

مجله ریاضی

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

چند ویژگی ساده و چند رده خاص گراف‌ها

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

۲-۱- مرتبه، اندازه و درجه

می‌دانیم که اگر مجموعه‌ای $p \in \mathbb{N}$ ، 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 مجموعه V را مرتبه G و تعداد اعضای مجموعه E را اندازه G می‌نامیم و معمولاً آنها را، به ترتیب، با p و q نمایش می‌دهیم. مرتبه G را با $p(G)$ و اندازه آن را با $q(G)$ هم نمایش می‌دهیم.

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

تعریف: درجه 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 $\deg a_4 = 5$. 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 قضیه زیر نشان می‌دهیم این مطلب همواره درست است. ▲

قضیه ۱: اگر $V = \{v_1, v_2, \dots, v_p\}$ مجموعه رأس‌های گراف G با اندازه 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. ■

توجه کنید درجه هر رأس گرافی که اصلاً یال نداشته باشد صفر است. لذا، در این حالت هر دو طرف برابری مذکور در قضیه 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. ■

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

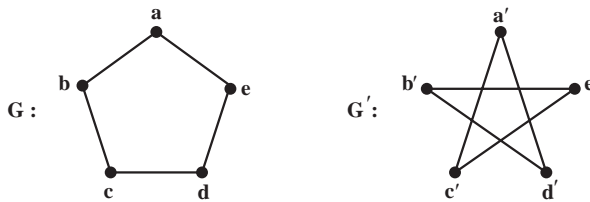
مثال ۳: در شکل ۶ از فصل ۱ داریم: $\Delta = 5$ و $\delta = 1$. در تمام گراف‌های مربوط به هیدروکربن‌ها

▲ $\Delta = 4$ و $\delta = 1$.

۲-۲- گراف‌های منتظم، کامل و تهی

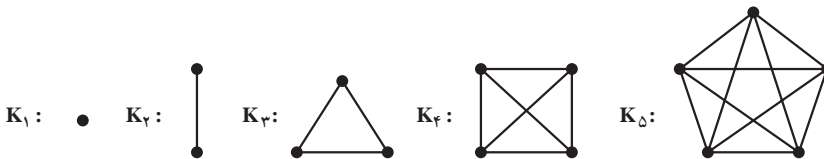
تعریف : عدد صحیح و نامنفی r داده شده است. گراف G از مرتبه p را r - منتظم می‌نامیم هرگاه درجه هر رأس G برابر با r باشد، هر گراف $(p-1)$ - منتظم از مرتبه p را گراف کامل هم می‌نامیم و آن را با K_p نمایش می‌دهیم.

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



شکل ۱- گراف‌های ۲- منتظم

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

قضیه 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 قضیه ۱، نصف این عدد برابر با $q(K_p)$ است. ■

قرارداد : گراف \circ - منتظم از مرتبه p را با \bar{K}_p نمایش می‌دهیم. چون \bar{K}_p هیچ یال ندارد، یعنی $E(\bar{K}_p) = \emptyset$ ، 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 دور گراف

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 $m \in \mathbb{N}$ ، $m+1$ رأس 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 دنباله 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 ماژر 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). ▲

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 $v_1, v_2, \dots, v_m, v_{m+1} = v_1$ با شرط $m \geq 3$ متشکل از $m+1$ رأس G است که در آن‌ها، $1 \leq i \leq m$ ، 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 به ازای هر $p \geq 3$ گراف کامل K_p دور دارد. در واقع، به ازای 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 (دنباله b_1, a_1, b_2, a_2) و دوری به طول ۶ (دنباله $b_1, a_1, b_2, a_2, b_3, a_3$) دارد. ▲

۴-۴- تمرین‌ها

۱- فرض کنید گراف G ، ۳-منتظم است و داریم $q = 2p - 3$. مرتبه G با p و اندازه 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 d_1, d_2, \dots, d_n بنویسید که به ازای هر $1 \leq i \leq n$ داشته باشیم $d_{i+1} \leq d_i$. (دنباله حاصل را دنباله درجه‌های رأس‌های گراف می‌نامیم.)

(پ) چرا گرافی وجود ندارد که $1, 3, 3, 5$: S دنباله درجه‌های رأس‌های آن باشد؟

۳- (الف) گرافی ارائه کنید که دنباله درجه‌های رأس‌هایش $0, 0, 2, 2, 3, 3, 3, 3$: S باشد. (ب) آیا پاسخ یکتاست؟ چرا؟

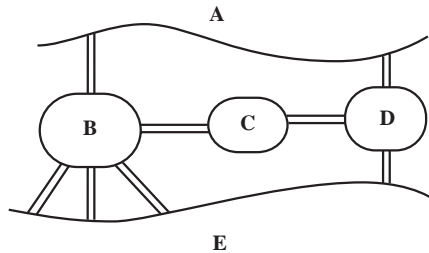
۴- چند گراف ۳-منتظم از مرتبه ۱۵ وجود دارند؟ چرا؟

۵- با استقراء بر q قضیه 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 منطقه A، B، C، D، E تشکیل شده است و این منطقه‌ها با هشت پل به هم راه دارند.



الف) گراف چندگانه 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 منطقه آغاز بازگشت؟
 پ) آیا با آغاز از یکی از منطقه‌های پنجگانه می‌توان از هر پل دقیقاً یک بار گذشت؟ در این حالت لازم نیست منطقه آغاز گشت با منطقه 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.

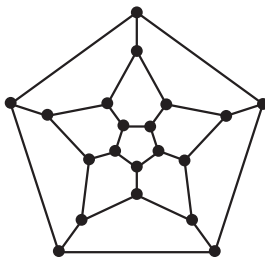
۱۰- الف) گراف شکل ۶ از فصل ۱ «چند» دور دارد؟ (پاسخ ۳ است: دو دور از مرتبه ۴ و یک دور از مرتبه ۶. پاسخ را توجیه کنید).
 ب) هر یک از دورها را به صورت دنباله‌ای از رأس‌ها نمایش دهید که رأس اول و آخر دنباله مثل هم و بقیه همراه با این رأس مشترک دو به دو متفاوت باشند؛ به علاوه، هر دو رأس متوالی این دنباله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

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

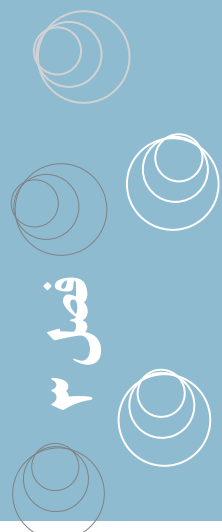
b_1, a_2, b_3, a_3, b_1	b_1, a_3, b_2, a_2, b_1
a_2, b_3, a_3, b_1, a_2	a_2, b_1, a_3, b_2, a_2
b_3, a_3, b_1, a_2, b_3	b_3, a_2, b_1, a_3, b_3
a_3, b_1, a_2, b_3, a_3	a_3, b_2, a_2, b_1, a_3

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 مرتبه p ، $p \geq 3$ ، دوری از مرتبه p داشته باشد، آن گاه G را گراف همیلتنی می نامیم. مثلاً هر K_p ، $p \geq 3$ ، گراف همیلتنی است.
- الف) نشان دهید هر گراف همیلتنی همبند است.
- ب) اگر G همیلتنی باشد آن گاه به ازای هر $v \in V(G)$ داریم $\deg_G v \geq 2$.
- 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 رابطه هم ارزی بر مجموعه $V(G)$ است.
- ب) اگر G گراف شکل ۳ از فصل ۱ باشد، افزایش حاصل از رابطه هم ارزی مذکور در بند الف) را بیابید.
- پ) پاسخ بند ب) را با فرض این که G گراف شکل ۶ یا گراف شکل ۱۰ باشد بیابید.

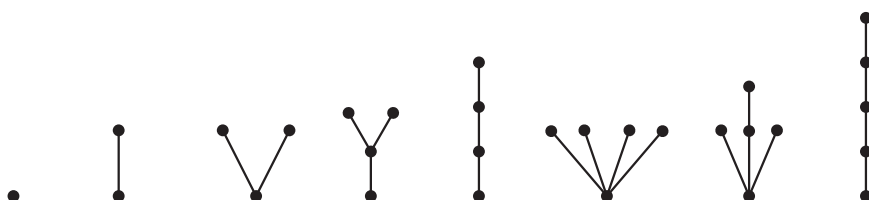


درخت و ماتریس

در این فصل کوتاه ابتدا ردهٔ 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.

۱-۳- 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 مرتبهٔ p ، $1 \leq p \leq 5$ ، را رسم کرده‌ایم.



شکل ۱- درخت‌های از مرتبهٔ 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.

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

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

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

اثبات: از به اصطلاح استقرای تعمیم یافته روی مرتبه درخت G استفاده می‌کنیم. اگر $p=2$ آن گاه $G=K_2$ و درستی حکم واضح است. فرض می‌کنیم حکم در مورد هر درخت با $k \geq 2$ رأس درست است. سپس درختی چون G از مرتبه $k+1$ را در نظر می‌گیریم. اگر G رأسی چون v از درجه یک داشته باشد آنگاه با حذف رأس v و تنها یال ماز 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 درجه یک دارد.

پس فرض می‌کنیم درجه 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 درجه 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. ■

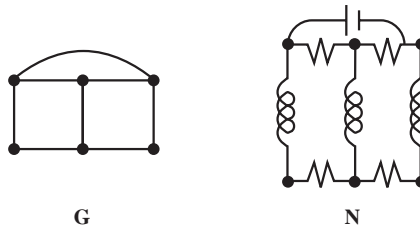
به مثال‌های گوناگون درخت‌ها نظر افکنید، می‌بینید که در مورد تمام آنها قضیه زیر درست است.

قضیه ۳: اگر G درختی با p رأس و q یال باشد آن گاه

$$p = q + 1$$

اثبات: با استقراء بر p قضیه را ثابت می‌کنیم. اگر $p=1$ آن گاه $q=0$ 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 قضیه قبل G رأسی چون v دارد که $\deg v = 1$. با حذف رأس v و تنها یال ماز بر آن درختی چون G' ایجاد می‌شود که مرتبه اش k است. بنابه فرض استقراء، گراف G' دارای $k-1$ یال است. پس درخت G دقیقاً k یال دارد. ■

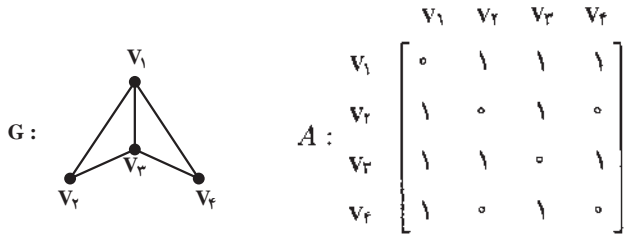
درخت در رشته‌های مختلفی مانند شیمی، مهندسی برق و علم محاسبه کاربرد دارد. کرشف در سال ۱۸۴۷ میلادی هنگام حل دستگاه‌های معادلات خطی مربوط به شبکه‌های الکتریکی درخت‌ها را کشف و نظریه درخت‌ها را بارور کرد. در شکل زیر N یک شبکه الکتریکی و G گراف مربوط به آن است.



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 ۴ رأس وجود دارند که درجه ۴ رأس از این ۴ رأس چهار و درجه هریک از ۱۰ رأس باقیمانده یک است. اگر هزینه 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 مرتبه p ارتباط نزدیک دارد. به جای مسئله 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.

۲-۳- گراف‌ها و ماتریس‌ها

گراف $G = (V, E)$ با $V = \{v_1, v_2, v_3, v_4\}$ و $E = \{v_1v_2, v_1v_3, v_1v_4, v_2v_3, v_2v_4, v_3v_4\}$ 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, v_4 و v_4 درایه a_{ij} از این ماتریس ۱ است هر گاه $v_i v_j \in E$ و ۰ است هر گاه $v_i v_j \notin E$.



شکل ۲- گراف و ماتریس مجاورت آن

توجه کنید که :

(۱) درایه‌های روی قطر اصلی همگی صفرند زیرا گراف‌های (ساده) موضوع بحث ما «طوقه» ندارند، یعنی هیچ رأسی با خودش مجاور نیست.

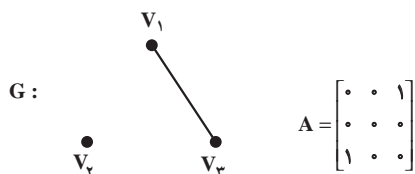
(۲) تعداد سطرهای این ماتریس برابر است با تعداد ستون‌های آن، یعنی ماتریس A مربعی است.

(۳) هر درایه 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 $v_i v_j \in E$ آن گاه $v_j v_i \in E$.

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 به طور ساده با A نمایش می‌دهیم.

جالب این جاست 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 همین طور به ازای سطر (یا ستون) سوم نقطه دیگر v_3 را در نظر می‌گیریم و نقطه v_1 را به نقطه v_j با خطی به هم وصل می‌کنیم هرگاه درایه مربوط در ماتریس داده شده یک باشد و در غیر این صورت آن دو را به هم وصل نمی‌کنیم.



شکل ۳- ماتریس با شرایط چهارگانه 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 چهارگانه بالا نیست. و لذا برای مطالعه گراف ها می توان صرفاً ماتریس های مربعی متقارنی را مطالعه کرد که درایه های آنها از مجموعه $\{0, 1\}$ انتخاب می شوند و درایه های روی قطر اصلی آن ها صفرند. بنابراین نظریه گراف ها را می توان شاخه ای از جبر هم تلقی کرد.

قضیه ۴ : فرض کنید A ماتریس مجاورت گراف G با $V(G) = \{v_1, \dots, v_p\}$ باشد. آن گاه درایه واقع در سطر i ام و ستون j ام ماتریس A^2 برابر است با درجه رأس v_i در گراف G .

اثبات : درایه واقع در سطر i ام و ستون j ام ماتریس A^2 برابر است با مجموع حاصل ضرب های درایه های نظیر به نظیر سطر i ام A و ستون j ام A . چون A متقارن است این درایه از حاصل ضرب های درایه های نظیر به نظیر سطر i ام A و سطر i ام A حاصل می شود. تعداد یک های موجود در سطر i ام A برابر است با درجه رأس v_i و لذا برای محاسبه درایه موردنظر از ماتریس A^2 باید به اندازه $\deg v_i$ عدد $1 \times 1 = 1$ را با هم جمع کنیم. ■

۳-۳- تمرین ها

- ۱- گراف همبندی معرفی کنید که مجموع مرتبه و اندازه آن ۸ باشد.
- ۲- گراف همبندی معرفی کنید که حاصل ضرب مرتبه و اندازه آن ۲۰ باشد.
- ۳- فرض کنید ماکسیم درجه یک درخت T برابر با k باشد. ثابت کنید که T دست کم k رأس از درجه یک دارد.
- ۴- گرافی از مرتبه ۶ و اندازه ۶ معرفی کنید که ۲- منتظم باشد.
- ۵- تمام درخت های از مرتبه 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 درایه واقع بر روی قطراصلی ماتریس M^2 برابر با $p-1$ است.

۸- الف) قضیه ۱ را با استفاده از استقراء روی مرتبه یک درخت و با به کار بردن قضیه ۲ ثابت کنید.

ب) اثباتی را که در متن برای قضیه 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 $u, v \in V(G)$ فاصله u از v در G که با $d(u, v)$ نمایش

داده می شود برابر است با طول کوتاه ترین مسیر از u به v در G . نشان دهید :

الف) $d(u, v) = 0$ اگر و تنها اگر $u = v$.

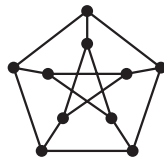
ب) به ازای هر $u, v \in V(G)$ داریم $d(u, v) = d(v, u)$.

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 همبند است؟ چرا؟



مراجع

1- M. Behzad, G. Chartrand, and L. Lesniak-Foster, Graphs and Digraphs, Wadsworth International Group, Belmont, Galif. 1979.

2- O. Ore, and R. J. Wilson, Graphs and their Uses, The Mathematical Association of America, 1990.



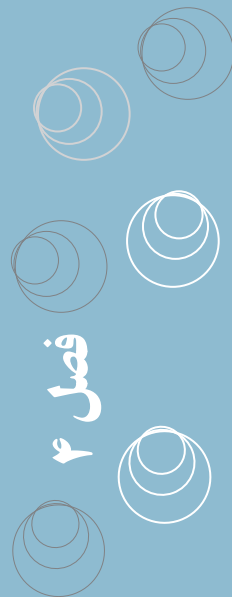
نظریه اعداد

مقدمه

نظریه 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 نظریه مقدماتی اعداد دارند، به شادابی و زنده بودن این شاخه از دانش بشری کمک کرده‌اند.

در این قسمت مباحثی مقدماتی از نظریه 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 نظریه اعداد را انتخاب و حل کنند.

کلیات و تقسیم‌پذیری



۱-۴- برخی از اصول نظریه اعداد

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

$۱, ۲, ۳, \dots$

می‌پردازد. در مورد چگونگی به وجود 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 مجموعه 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 به طور ابتدایی معمول است. این عمل که برای تهیه آمار و حتی رأی‌گیری‌های ساده هم به کار می‌رود از شواهد اولیه شناخت اعداد طبیعی است.

دنباله 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 مجموعه 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 مجموعه اعداد صحیح

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

آشنا شده‌ایم.

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

اصل خوش‌ترتیبی

هر زیرمجموعهٔ 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 مجموعهٔ A را عضو ابتدای مجموعهٔ A هم می‌نامند).^۱

اصل استقرای ریاضی

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

$$1 \in S \quad (\text{الف})$$

$$n \in S \Rightarrow n+1 \in S \quad (\text{ب})$$

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

۲-۴- معادل‌های اصل استقرای ریاضی

معادل‌های دیگری برای اصل استقرای ریاضی وجود دارند که برخی را در اینجا مطرح می‌کنیم :
الف) فرض کنیم $P(n)$ عبارتی دربارهٔ 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 $P(n)$ به ازای هر عدد طبیعی n درست است.

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

تعمیم این مطلب به صورت زیر است :

ب) فرض کنیم $P(n)$ عبارتی دربارهٔ 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، آن گاه $P(n)$ به 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 نحوهٔ استفاده از اصل استقرای ریاضی آشنا می کنند. در اینجا 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 :

قضیهٔ 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 T 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 $t_0 - 1 + 1 = t_0 \in P$ ، که

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

اصل استقرای قوی ریاضی

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

$$1 \in S \quad (\text{الف})$$

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 نحوهٔ استفاده از اصل استقرای قوی ریاضی، به مثال زیر توجه کنید :

مثال ۱ : چند جملهٔ اول دنبالهٔ موسوم به دنبالهٔ اعداد لوکا عبارت اند از :

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

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

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

و شرایط اولیه

$$L_2 = 3, L_1 = 1$$

به دست می آید. با استفاده از اصل استقرای قوی ریاضی ثابت می کنیم که به ازای هر عدد طبیعی n ,

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

اگر $S = \left\{ n \in \mathbb{N} : L_n < \left(\frac{\sqrt{5}}{2}\right)^n \right\}$ ، آن گاه $1 \in S$ و $2 \in S$. (چرا؟) حال اگر $n \geq 3$ و به ازای هر k وقتی که $k \in S$ ، $k < n$ آن گاه $L_{n-1} < \left(\frac{\sqrt{5}}{2}\right)^{n-1}$ 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، $L_n < \left(\frac{\sqrt{5}}{2}\right)^n$. ▲

۳-۴- تقسیم پذیری

یکی از چهار عمل اصلی روی اعداد صحیح، تقسیم است. می دانیم 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 می شود مثل 12 و 6 . در این حالت می گوئیم عدد 6 عدد 12 را می شمارد، 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 می دهیم:

تعریف: عدد صحیح a را بر عدد صحیح b ، $b \neq 0$ ، تقسیم پذیر یا (بخش پذیر) گوئیم هرگاه عدد صحیحی مانند q یافت شود به گونه ای که $a = bq$. در این صورت می نویسیم $b|a$ و چنین می خوانیم: a بر b تقسیم پذیر است^۱ و یا b یک شمارنده یا مقسوم علیه a است. هرگاه a بر b تقسیم پذیر نباشد می نویسیم $b \nmid a$. در حالت $b = 0$ ، چون به ازای هر $q \in \mathbb{Z}$ ، $0 = 0 \times q$ ، می توان تعریف تقسیم پذیری را گسترش داد و عبارت « 0 بر 0 تقسیم پذیر است» را نیز پذیرفت.

۱- هرگاه a بر b تقسیم پذیر باشد می گوئیم b عدد a را می شمارد (عاد می کند)، یا a مضرب b است، یا b یک سازه (عامل) a است.

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

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

(ب) اعداد ۱ و -۱، 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 مجموعه 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 ترابیلی 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 عمده تقسیم پذیری را ارائه می‌دهیم:

قضیه 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

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

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

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

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

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

(ب) اگر $a \mid b$ و $b \mid a$ 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 $q' = \pm 1$ و لذا $q' = \pm 1$.

پس $a = \pm b$

(پ) اگر $a \mid b$ و $a \mid c$ 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

$$mb + nc = maq + naq'$$

$$= (mq + nq')a$$

پس:

$$a \mid mb + nc$$



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

یکتای $q \in \mathbb{Z}$ 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 می‌دهیم که $r, q \in \mathbb{Z}$ وجود دارند و پس از آن یکتا بودن آنها را ثابت می‌کنیم. چون a, b و q اعداد صحیح‌اند، $S = \{a - bq > 0 : q \in \mathbb{Z}\}$ یک زیرمجموعه از اعداد طبیعی است. نشان می‌دهیم که S تهی نیست و اصل خوش‌ترتیبی را به کار می‌بریم. به ازای عدد صحیح $q = -|a| - 1$ ؛ 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 کوچک‌ترین عضو است. کوچک‌ترین عضو این مجموعه را r می‌نامیم. در این صورت عددی صحیح مانند q وجود دارد که $r = a - bq$. یعنی:

$$a = bq + r$$

اگر $r > b$ ، آن‌گاه

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

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

$$a = bq_1$$

که به جای r ، $r_1 = 0$ را در نظر می‌گیریم. 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 $b \mid r_2 - r_1$. اگر $r_2 - r_1 \neq 0$ ، آن‌گاه $b \leq |r_2 - r_1|$. 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 $q_1 = q_2$.

توجه کنید که هرگاه $r = 0$ ، آن‌گاه $b \mid a$.

مثال ۲: برای $a = ۱۰۲۸$ و $b = ۳۴$ ، داریم

$$q = \left\lfloor \frac{۱۰۲۸}{۳۴} \right\rfloor = ۳۰.$$

(در اینجا منظور از نماد $\lfloor x \rfloor$ ، جزء صحیح عدد حقیقی x است.)

$$r = ۱۰۲۸ - ۳۰ \times ۳۴ = ۸$$

پس:

$$۱۰۲۸ = ۳۴ \times ۳۰ + ۸$$

یکی از کاربردهای قضیه الگوریتم تقسیم، دسته‌بندی اعداد برحسب باقیمانده تقسیم آنها بر عدد طبیعی و ثابت b است.

مثال ۳: باقیمانده هر عدد صحیح بر ۲، عدد ۰ یا ۱ است. این مطلب اعداد صحیح را به دو دسته تقسیم می‌کند. تمام اعدادی را که باقیمانده آنها بر ۲، ۰ است، یعنی ۲ آنها را می‌شمارد زوج و بقیه اعداد را فرد می‌نامند. یعنی می‌توان 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 اعداد زوج، و

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

مجموعه اعداد فرد است.

به همین ترتیب هر عدد صحیح را می‌توان تنها به یکی از صورت‌های

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

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

۴-۶. نمایش اعداد صحیح

استفاده از دستگاه دهدهی (اعشاری) متداول‌ترین صورت نمایش اعداد است. اعداد طبیعی را می‌توان به صورت ضرایب توان‌های ۱۰ نمایش داد. مثلاً عدد ۳۴۷۶۵ 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 ۱۰» وجود ۱۰ انگشت دست بوده که در شمارش طبیعی به کار می‌رفته است. این نحوه نمایش را ابتدا هندی‌ها

قبل از سال ۸۰۰ میلادی اختراع کرده‌اند. این مطلب را محمدبن موسی خوارزمی در کتاب «جمع و تفریق، بر طبق حساب هندی» شرح داده و نمایش رقم صفر با نماد ° هم برای اولین بار در این کتاب آمده است. اروپایی‌ها این دستگاه را هندی – عربی می‌نامند. دستگاه دیگری هم که در ریاضیات اسلامی وجود داشته، دستگاه شصت شصتی بوده که مسلمان‌ها فکر آن را از بابلی‌ها گرفتند و آن را تکمیل کردند. مبنای این نمایش عدد شصت بوده است، که در ارتباط با محاسبات نجومی و تقسیم ساعت به ۶۰ دقیقه و دقیقه به ۶۰ ثانیه است. با نمایش اعداد در مبنای ۲ هم که در نمایش داخلی کامپیوتر به کار می‌رود آشنا هستیم.

به‌طور کلی هر عدد طبیعی بزرگ‌تر از ۱ می‌تواند مبنا باشد.

قضیه ۵: اگر b یک عدد طبیعی بزرگ‌تر از ۱ باشد، هر عدد طبیعی n را می‌توان 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 $k = 0, 1, 2, \dots$ ، $0 \leq a_j \leq b-1$ ، $a_k \neq 0$.
اثبات: اگر الگوریتم تقسیم را متوالیاً به صورت زیر به کار گیریم، قضیه ثابت می‌شود. ابتدا n را بر b تقسیم می‌کنیم.

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

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

حال q_0 را بر b تقسیم می‌کنیم

این عمل را ادامه می‌دهیم

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

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

⋮

⋮

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

در دنباله 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

پس $q_{j+1} \geq 1$)


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

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

۱- هر عدد صحیح نامنفی را حسابی گویند.

صفر و n وجود دارند. پس در مرحله‌ای $q_k = 0$ و داریم:

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

اگر به ترتیب به جای هر $q_0, q_1, q_2, \dots, q_{k-2}, q_{k-1}$ حاصل تقسیم آن را بنویسیم، فرمول مورد نظر به دست می‌آید و بدیهی است که $a_k \neq 0$ ، زیرا اگر $a_k = 0$ آن گاه $q_{k-1} = 0$ ، و یک مرحله قبل از آن توقف می‌کردیم. اثبات یکتایی این نمایش را در مقاطع تحصیلی بالاتر خواهید دید.  (در این حالت n را به صورت زیر نمایش می‌دهند:

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

این نمایش را^۱، نمایش عدد n در مبنای b می‌نامند. هریک از a_i ها را یک رقم در مبنای b گویند و $k+1$ ، تعداد ارقام عدد n در مبنای b است و می‌گویند n در مبنای b ، $k+1$ رقم دارد. نمایش اعداد در دستگاه دودویی، یا در مبنای ۲، 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 ۵ در رابطه با پیدا کردن باقیمانده تقسیم بر برخی از اعداد به کار می‌رود. به مثال زیر توجه کنید.

مثال ۴: قاعده پیدا کردن باقیمانده تقسیم بر ۳ یا ۹

اگر $A = (a_n \dots a_1 a_0)_9$ می‌دانیم این عدد برابر است با


$$A = a_n \times 9^n + a_{n-1} \times 9^{n-1} + \dots + a_1 \times 9 + a_0.$$

$$= (\underbrace{99 \dots 9}_n + 1)a_n + (\underbrace{99 \dots 9}_{n-1} + 1)a_{n-1} + \dots + (9 + 1)a_1 + a_0.$$

$$= 9(\underbrace{11 \dots 1}_n a_n + \underbrace{11 \dots 1}_{n-1} a_{n-1} + \dots + a_1) + a_n + a_{n-1} + \dots + a_1 + a_0.$$

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

$$a_n + a_{n-1} + \dots + a_1 + a_0.$$

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

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

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 مجموعه S عبارت است از $s_1 \in S$ ، که برای هر $s \in S$ داشته باشیم $s \leq s_1$).

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

۳- ثابت کنید که هر مجموعه ناتهی از اعداد صحیح و از پایین کراندار، دارای کوچک‌ترین عضو و هر مجموعه 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 $na \geq b$.

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 اینکه برای هر عدد طبیعی $m \geq 2$ ،

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

ثابت کنید که

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

۱- نماد $s_1 = \max S$ برای بزرگ‌ترین عضو مجموعه S به کار می‌رود.

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 $a \neq 0, c \neq 0, a|b$ و $c|d$ 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 $i = 1, 2, \dots, n$ $a|b_i$ آن گاه برای اعداد صحیح دلخواه m_1, m_2, \dots

و 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 همچنین 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 همچنین 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 $5q + 6$ 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 ۱۰ است؟

پ) عدد ۱۸۶۴ را در مبنای ۲ بنویسید.

ت) عدد $(a35b06)_{16}$ را در مبنای ۱۰ بنویسید.

(دقت کنید که اگر مبنا بیشتر از ۱۰ باشد، ارقام بیشتر از ۹ را به ترتیب با a, b, c, d و ... نمایش

می دهند، یعنی مثلاً در مبنای ۱۶، $a = 10, b = 11, c = 12, d = 13, e = 14$ و $f = 15$. البته گاهی

هم عدد بالا را با $(6051130)_{16}$ هم نمایش می دهند.)

مجله ریاضی

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

الف	ب	ج	د	هـ	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 جمل (حساب ابجدی) در ضبط تاریخ حوادث به عنوان ماده تاریخ به کار می‌رود.

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 مقسوم علیهی 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.

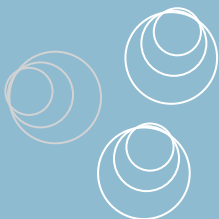
مثال ۱: اعداد ۲، ۳، ۵، ۷ و ۱۱ اول و اعداد ۴، ۶، ۸، ۹ و ۱۰ مرکب‌اند.

قضیه ۱: هر عدد صحیح به جز ۱ و -۱ حداقل یک مقسوم علیه 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 مجموعه تمام مقسوم علیه‌های 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 حتماً یک مقسوم علیه اول مانند m دارد.

قضیه ۲: بی‌نهایت عدد اول وجود دارند.^۱

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



اثبات : می‌دانیم اعداد ۲، ۳، ۵ و ... اول اند، حال اگر این دنباله متناهی باشد، فرض می‌کنیم 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 مقسوم علیه اول دارد که آن را p_j می‌نامیم. داریم :

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

پس $(p_1 p_2 \dots p_n) - m$ بر p_j تقسیم پذیر است. یعنی $p_j | 1$ که غیر ممکن است. لذا تعداد اعداد اول نامتناهی است. ■

قضیه ۳ : اگر n یک عدد مرکب باشد، آن‌گاه n حداقل یک مقسوم علیه 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 قضیه 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 $p \leq \sqrt{n}$ و $p | n$.

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

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

$$2/47, \quad 3/47, \quad 5/47$$

و چون $7 < \sqrt{47} < 6$ ، 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.

قضیه ۳ اساس فرایند غربال اراتستین است. مثلاً برای تعیین اعداد اول کوچک‌تر از ۱۰۰، تمام مضرب‌های اول اعداد کوچک‌تر از $100 = \sqrt{100}$ یعنی مضرب‌های ۲، ۳، ۵ و ۷ را از جدول اعداد از ۱ تا ۱۰۰ حذف می‌کنیم. جدول صفحه 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 شمارندهٔ مشترک دو عدد صحیح a و b گویند هرگاه $c|b$ و $c|a$.

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

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

مثال ۳: مقسوم علیه‌های 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 قضیه زیر را داریم:

قضیه ۴: بزرگ‌ترین مقسوم علیه مشترک دو عدد صحیح a و b که حداقل یکی از آنها صفر نیست، برابر است با کوچک‌ترین عضو مجموعه

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

اثبات: مجموعه 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 مقسوم علیه مشترک a و b است. اگر $c > 0$ و $c|a$ و $c|b$ ، آن‌گاه $(am_0 + bn_0)|c$ یعنی $c|d$ پس $c \leq d$. در نتیجه d بزرگ‌ترین مقسوم علیه 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 مقسوم علیه مشترک دو عدد صحیح a و b است.

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

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

پس:

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

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

همچنین

$$\begin{aligned} r_1 &= r_2 q_1 + r_2 \quad 0 \leq r_2 < r_1 \\ (a, b) &= (r_1, r_2) = (r_1, r_2) \\ &\vdots \\ r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1} \quad 0 \leq r_{n-1} < r_{n-2} \\ (a, b) &= (r_{n-3}, r_{n-2}) = (r_{n-1}, r_{n-2}) \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1} \\ (a, b) &= (r_{n-1}, r_{n-2}) = (r_{n-1}, r_n) \end{aligned}$$

چون

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

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 $r_{n-1} = r_n q_n + r_{n+1} = 0$. در نتیجه

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

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

مثال ۴ :

$$\begin{aligned} (30, 72) &= (30, 72 - 2 \times 30) = (30, 12) \\ &= (2 \times 12 + 6, 12) = (6, 12) = (6, 2 \times 6 + 0) = (6, 0) = 6 \end{aligned}$$

که معمولاً به صورت خلاصه نردبانی زیر می‌نویسند :

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

قضیه ۵ : عدد طبیعی d بزرگ‌ترین مقسوم علیه مشترک دو عدد صحیح a و b است اگر و تنها اگر

$$d|a \text{ و } d|b$$

۲) هرگاه $c|a$ و $c|b$ ، آن‌گاه $c|d$.

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 $a|c$ و $b|c$ آن گاه $c|d$ یعنی شرط ۲ هم برقرار است.
 برعکس اگر d در دو شرط فوق صدق کند و c یک مقسوم علیه مشترک مثبت a و b باشد، آن گاه $c|d$ یعنی $c \leq d$. پس d بزرگ ترین مقسوم علیه مشترک a و b است.
 تعریف: دو عدد صحیح a و b را نسبت به هم اول یا متباین گویند، هرگاه $(a, b) = 1$.
 مثال ۵: اعداد ۹ و ۱۰ و نیز دو عدد ۲۵ و ۴۲ نسبت به هم اول اند.
 با استفاده از قضیه ۴، می توان ثابت کرد که دو عدد صحیح a و b نسبت به هم اول اند اگر و تنها اگر اعداد صحیح m و n وجود داشته باشند که

$$1 = ma + nb$$

قضیه ۶: (لم اقلیدس). اگر $a|bc$ و $(a, b) = 1$ آن گاه $a|c$.
 اثبات: اعداد صحیح m و n را می توان پیدا کرد که برای آنها

$$1 = ma + nb$$

پس:

$$c = cma + cnb$$

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

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

یعنی $a|c$.

قضیه ۷: اگر p یک عدد اول باشد و $p|ab$ ، آن گاه $p|a$ یا $p|b$.
 اثبات: اگر p/a ، آن گاه $(p, a) = 1$ ، زیرا اگر $(p, a) = d$ و $d \neq 1$ آن گاه $d = p$. (چرا؟)
 پس $p|a$ که یک تناقض است. در نتیجه $(p, a) = 1$ ، پس طبق قضیه ۶، $p|d$.

تعریف بزرگ ترین مقسوم علیه مشترک دو عدد را به چند عدد نیز می توان تعمیم داد:
 تعریف: بزرگ ترین مقسوم علیه مشترک n عدد صحیح a_1, a_2, \dots, a_n که همگی آنها صفر نیستند عبارت است از بزرگ ترین عدد صحیحی که تمام این اعداد صحیح را بشمارد. این عدد را با (a_1, a_2, \dots, a_n) نمایش می دهند. می توان 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 :

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



۲-۵- قضیه بنیادی حساب

نقش اصلی اعداد اول به عنوان عناصر سازنده تمام اعداد صحیح بسیار اهمیت دارد. در قضیه زیر این مطلب را بدون اثبات بیان می کنیم :

قضیه ۸ : هر عدد طبیعی بزرگ تر از ۱ را می توان بدون توجه به ترتیب به طور یکتا به صورت حاصل ضرب اعداد اول نوشت. یعنی n را می توان 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 تجزیه عدد n به عامل های اول می نامند.

نکته ۱ : در تجزیه اعداد طبیعی به عامل های اول، می توان حاصل ضرب 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 اعداد اول متمایز و α_i ها اعدادی طبیعی اند. این نمایش را نمایش متعارف عدد n می نامند.

نکته ۲ : برای $n=1$ ، می توان $1 = p^0$ را در نظر گرفت، درحالی که p هر عدد اولی می تواند باشد.

نکته ۳ : به طور کلی هر عدد طبیعی را می توان 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 ، $\alpha_p(n)$ بزرگ ترین توان p است که عدد n را می شمارد و به این صورت می نویسند :

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

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 قضیه زیر را بدون اثبات بیان می کنیم :

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

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

که در آن برای هر عدد i ,

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

(دقت کنید که اگر برای عدد اول p , p/n , آن گاه توان آن را در نمایش n برابر با صفر می گیریم.)

مثال ۷:

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

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

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



۵-۳- کوچک ترین مضرب مشترک

می دانیم عدد صحیح c را مضرب مشترک دو عدد صحیح a و b نامند، هرگاه $a|c$ و $b|c$.
تعریف: عدد m را کوچک ترین 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 $a|c$ و $b|c$ آن گاه $c \leq m$. کوچک ترین مضرب مشترک دو عدد a و b را با $[a, b]$ نمایش می دهند.
وجود کوچک ترین مضرب مشترک دو عدد غیر صفر a و b را با استفاده از اصل خوش ترتیبی می توان ثابت کرد.

مثال ۸: مضرب های مشترک مثبت اعداد ۴ و ۶ عبارتند از:

$$12, 24, 36, \dots$$



که کوچک ترین آنها ۱۲ است. یعنی $[4, 6] = 12$.

قضیه های زیر را که در رابطه با کوچک ترین مضرب مشترک دو عددند بدون اثبات بیان می کنیم.

قضیه ۱۰: برای هر دو عدد صحیح غیر صفر a و b , $m = [a, b]$ اگر و تنها اگر

$$(1) \quad a|m \text{ و } b|m$$

$$(2) \quad \text{اگر } a|c \text{ و } b|c, \text{ آن گاه } m|c.$$

قضیه ۱۱: اگر $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ و $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ آن گاه

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

$$\theta_i = \max\{\alpha_i, \beta_i\}$$

که در آن برای هر i ,

۱- کوچک ترین مضرب مشترک a و b را با نماد $a \cup b$ هم نمایش می دهند.

قضیه ۱۲: برای هر دو عدد صحیح غیر صفر a و b داریم:

$$a, b = |ab|$$

مثال ۹:

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

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

$$[3^0, 72] = 2^2 \times 3^2 \times 5^1 = 36^0$$

$$[3^0, 72] \times (3^0, 72) = 36^0 \times 6 = 216^0$$

$$3^0 \times 72 = 216^0$$



تعریف: کوچک ترین مضرب مشترک اعداد صحیح غیر صفر a_1, a_2, \dots, a_n عبارت است از کوچک ترین عدد صحیح مثبت که بر همه آنها تقسیم پذیر باشد، و آن را با $[a_1, a_2, \dots, a_n]$ نمایش می دهند. می توان 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:

$$[1^0, 4, 6] = [1^0, [4, 6]] = [1^0, 12] = 6^0$$

راه اول:

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

راه دوم:

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

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

$$[1^0, 4, 6] = 2^2 \times 3^1 \times 5^1 = 6^0$$



۴-۵- تمرین ها

۱- کدام یک از اعداد زیر اول و کدام یک مرکب اند؟

۷۳۷ (ب)

۱ (الف)

۲۰۷۹۱ (ت)

۱۸۹۱ (پ)

۲- ثابت کنید بی نهایت عدد اول به صورت $4q + 3$ یافت می شوند.

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 $p_1 p_2 \dots p_n | q$ ثابت کنید به ازای یک i ، $1 \leq i \leq n$ ، $p_i = q$.

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^m و b^n هم نسبت به هم اول اند.

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

همنهستی

۱-۶- مفهوم همنهستی

مفهوم همنهستی 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 نظریه همنهستی هستند که در اوایل قرن نوزدهم به وسیله گاوس معرفی شد.

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

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

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

و یا

$$\begin{matrix} m \\ a \equiv b \end{matrix}$$

و می‌خوانند « a همنهشت با b به پیمانه m است»^۱

مثال ۱: (پیمانه ۶) $۱۶ \equiv ۳۴$ ، زیرا $۱۸ = ۱۶ - ۳۴$ بر ۶ تقسیم پذیر است. ولی (پیمانه ۶) $۵ \not\equiv ۸$ ، زیرا

$۳ = ۸ - ۵$ بر ۶ تقسیم پذیر نیست. ▲

۱- حتی در مورد اعداد حقیقی مثلاً در مورد مقادیر زاویه یا طول کمان (برحسب رادیان) در دایره مثلثاتی (پیمانه ۲π) $x \equiv y$ به کار

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

$$a \not\equiv b (m \text{ پیمانه})$$

همان‌طور که در سال قبل دیدیم، هم‌نهشتی یک رابطه هم‌ارزی روی مجموعه اعداد صحیح است و لذا رابطه هم‌نهشتی به پیمانه m ، مجموعه \mathbb{Z} را به دسته‌های هم‌ارزی افراز می‌کند. مجموعه

تمام دسته‌های هم‌نهشت به پیمانه m را با $\frac{\mathbb{Z}}{m}$ یا \mathbb{Z}_m و مجموعه تمام اعداد صحیحی را که با a هم‌نهشت به پیمانه m هستند با $[a]$ یا \bar{a} نمایش می‌دهند.

$[a]$ یک دسته هم‌ارزی و a نماینده این دسته است. اگر b عضو دیگری از دسته هم‌ارزی باشد،

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

$$[a] = [b]$$

اگر و تنها اگر

$$a \equiv b (m \text{ پیمانه})$$

مثلاً در هم‌نهشتی به پیمانه ۶ داریم :

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

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



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

نکته : بنا به تعریف، از (پیمانه 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 پیمانه m هم‌نهشت‌اند با افزودن مضربی از m بر b به دست می‌آیند. بنابراین :

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

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

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



با توجه به آنچه گفته شد گزاره‌های زیر همگی معادل‌اند.

— a به پیمانه m با b همنهشت است.

— a و b به پیمانه m همنهشت اند.

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

$$[a] = [b]$$

— a و b در یک دسته همنهشتی به پیمانه m قرار دارند.

— $a-b$ مضربی از m است.

$$m|(a-b)$$

و با استفاده از الگوریتم تقسیم می‌توان ثابت کرد که همه گزاره‌های فوق با گزاره زیر معادل اند :

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

۶-۲- برخی از ویژگی‌های همنهشتی

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

خوانده‌ایم.

۱- اگر $a \equiv b \pmod{m}$ ، آن‌گاه برای هر عدد صحیح c

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

۲- اگر $a+c \equiv b+c \pmod{m}$ ، آن‌گاه $a \equiv b \pmod{m}$

۳- اگر $a \equiv b \pmod{m}$ و $c \equiv d \pmod{m}$ ، آن‌گاه

$$ac \equiv bd \pmod{m} \text{ و } a+c \equiv b+d \pmod{m}$$

۴- هرگاه $a_1 \equiv b_1 \pmod{m}$ و \dots و $a_n \equiv b_n \pmod{m}$ ، آن‌گاه

$$a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n \pmod{m}$$

و

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_n \pmod{m}$$

۵- هرگاه $a \equiv b \pmod{m}$ آن‌گاه برای هر $n \geq 1$ ، $a^n \equiv b^n \pmod{m}$

مثال ۳: مطلوب است باقی‌مانده 2^{30} بر ۱۷

از $2^4 = 16 \equiv -1 \pmod{17}$ و $2^8 \equiv -1 \pmod{17}$ نتیجه می‌شود که $2^4 \equiv -1 \pmod{17}$ اما $2^4 \equiv (-1)^4 \pmod{17}$

یعنی $2^4 \equiv -1 \pmod{17}$ از طرف دیگر داریم $2^4 \equiv 4 \pmod{17}$ و در نتیجه

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

اما (پیمانه ۱۷) $۱۳ \equiv -۴$ ، پس (پیمانه ۱۷) $۱۳ \equiv ۲۳$ یعنی باقی مانده ۲۳ بر ۱۷ ، عدد ۱۳ است.



۳-۶- تقسیم طرفین یک رابطهٔ همنهشتی بر c

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

$$ac \equiv bc \text{ (پیمانه m)}$$

حال عکس این مطلب را بررسی می‌کنیم. یعنی آیا برای هر عدد صحیح c، اگر (پیمانه m) $ac \equiv bc$

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

می‌دانیم (پیمانه ۶) $۲۱ \equiv ۳۳$ یعنی (پیمانه ۶) $۷ \times ۳ \equiv ۱۱ \times ۳$ ولی (پیمانه ۶) $\frac{۲۱}{۳} \not\equiv \frac{۳۳}{۳}$ اما قضیه

زیر را در این مورد داریم:

قضیه ۱: در رابطهٔ همنهشتی (پیمانه m) $ac \equiv bc$ داریم

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

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 $(a - b) \frac{c}{d}$ را می‌شمارد. و چون $\left(\frac{m}{d}, \frac{c}{d} \right) = ۱$ (چرا؟) پس

$$(a - b) \frac{m}{d} \text{ یعنی:}$$

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



مثال ۴: از (پیمانه ۶) $۸ \equiv ۲$ نتیجه می‌شود (پیمانه ۳) $۴ \equiv ۱$

۴-۶- حل معادله سیاله خطی $ax+by=c$

سؤال دیگری که مطرح می شود این است که آیا می توان معادله

$$(۱) \quad ax+by=c$$

را که با معادله همنهستی

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

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

$$(۲) \quad ax_0 + by_0 = c$$

اگر عددهای صحیح x_0, y_0 وجود داشته باشند که در رابطه (۲) صدق کنند، آن گاه می گوئیم معادله سیاله خطی $ax+by=c$ جواب دارد. در این رابطه قضیه زیر را داریم:

قضیه ۲: معادله سیاله خطی $ax+by=c$ در مجموعه \mathbb{Z} جواب دارد اگر و تنها اگر بزرگ ترین مقسوم علیه مشترک a و b ، عدد c را بشمارد.

اثبات: اگر $d = (a, b)$ و $d|c$ آن گاه عدد صحیح k وجود دارد که $c = dk$ و چون d بزرگ ترین مقسوم علیه 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 معادله $ax+by=c$ صدق می کنند. 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 $d|c$. ■

می توان ثابت کرد که اگر $(a, b) = d$ و x_0 و y_0 یک جواب برای معادله خطی $ax+by=c$ باشد،

$$\text{آن گاه تمام جواب های آن به صورت } x = x_0 + k \frac{b}{d} \text{ و } y = y_0 - k \frac{a}{d} \text{ است که در آن } k \in \mathbb{Z}.$$

در مثال های زیر، روش هایی را برای حل معادله های سیاله نشان می دهیم:

مثال ۵: شخصی می خواهد با بُن، ۵۱۰۰ ریال کتاب بخرد. اگر بُن ها، ۵۰۰ ریالی و ۲۰۰ ریالی

باشند، چند بُن ۵۰۰ ریالی و چند بُن ۲۰۰ ریالی باید بپردازد؟

حل مسأله مستلزم پیدا کردن اعداد صحیح نامنفی x و y است که برای آنها
 $۲۰۰x + ۵۰۰y = ۵۱۰۰$

یا

$$۲x + ۵y = ۵۱$$

چون $(۵, ۲) = ۱$ و $۱ | ۵۱$ ، معادله فوق جواب دارد. می‌نویسیم:

$$x = \frac{۵۱ - ۵y}{۲} = \frac{۵۰ - ۴y + ۱ - y}{۲} = ۲۵ - ۲y + \frac{۱ - y}{۲}$$

پس $\frac{۱ - y}{۲}$ یک عدد صحیح است، یعنی عددی مانند m وجود دارد که $۱ - y = ۲m$ یا $y = ۱ - ۲m$.
 در نتیجه

$$x = ۲۵ - ۲ + ۴m + m = ۵m + ۲۳$$

ولی x و y منفی نیستند، پس $۱ - ۲m \geq ۰$ و $۵m + ۲۳ \geq ۰$ یا $m \leq \frac{۱}{۲}$ و $m \geq \frac{-۲۳}{۵} = -۴/۶$. پس m مقادیر $۰, -۱, -۲, -۳, -۴$ را می‌گیرد. یعنی تعداد بن‌های ۲۰۰ ریالی و ۵۰۰ ریالی به ترتیب می‌تواند جفت‌های زیر باشند:

$$۹, ۳ \quad ۷, ۸ \quad ۵, ۱۳ \quad ۳, ۱۸ \quad ۱, ۲۳$$



مثال ۶: جواب‌های عمومی معادله سیاله $۷x + ۵y = ۱۱$ را بیابید.

$$۷x + ۵y = ۱۱ \Rightarrow ۷x \equiv ۱۱ \pmod{۵}, \begin{cases} ۷ \equiv ۲ \pmod{۵} \\ ۱۱ \equiv ۱ \pmod{۵} \end{cases} \Rightarrow ۲x \equiv ۱ \pmod{۵}$$

$$\Rightarrow ۲x \equiv ۱ + ۵ \Rightarrow ۲x \equiv ۲ \times ۳ \pmod{۵} \quad (۲, ۵) = ۱ \Rightarrow x \equiv ۳ \pmod{۵}$$

$$\Rightarrow x = ۵k + ۳ \quad k=۰ \Rightarrow x_۰ = ۳ \Rightarrow y_۰ = -۲$$

$$\Rightarrow \begin{cases} x = ۳ + ۵k \\ y = -۲ - ۷k \end{cases}$$

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 اول اند. این ضابطه، تابعی روی اعداد طبیعی تعریف می‌کند که آن را تابع حسابی اویلر می‌گویند.

اگر $n = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$ در این صورت

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

بدهی است که اگر p یک عدد اول باشد آن گاه $\phi(p) = p - 1$.

قضیه اویلر: اگر m عددی طبیعی و a عددی صحیح باشد که $(a, m) = 1$ آن گاه

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

قضیه ویلسن: اگر p عددی اول باشد آن گاه

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

۵-۶- تمرین‌ها

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

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

دستهٔ همنهشتی $a + 2b$ را به پیمانهٔ ۷ مشخص کنید.

۲- هرگاه $(a \equiv b \pmod{m})$ و d یک مقسوم علیه m باشد، نشان دهید $(a \equiv b \pmod{d})$.

۳- ثابت کنید

الف) اگر r باقی ماندهٔ تقسیم a بر m باشد، آن گاه $a \equiv r \pmod{m}$.

ب) اگر $(a \equiv b \pmod{m})$ و c عدد صحیح باشد، آن گاه

$$ac \equiv bc \pmod{m}$$

پ) اگر $(a + b \equiv c \pmod{m})$ ، آن گاه $a \equiv c - b \pmod{m}$.

ت) اگر m و c نسبت به هم اول باشند و $(\text{پیمانه } m) ac \equiv bc$ ، آن گاه

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

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

$$(a \pm b)^2 = a^2 + b^2 \quad (\text{پیمانه } ab)$$

$$(a \pm b)^3 = a^3 \pm b^3 \quad (\text{پیمانه } ab)$$

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

۶- آخرین رقم سمت راست هریک از اعداد 3^{224} و 7^{101} را به دست آورید.

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

ندارد.

$$17x + 13y = 100 \quad (\text{ب})$$

$$2x + 5y = 11 \quad (\text{الف})$$

$$60x + 18y = 97 \quad (\text{ت})$$

$$21x + 14y = 147 \quad (\text{پ})$$

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

$$(\text{ب}) \quad 4000 \text{ ریال}$$

$$(\text{الف}) \quad 3500 \text{ ریال}$$

مجله ریاضی

برای اعداد طبیعی $n \geq 3$ معادله سیالیه $x^n + y^n = z^n$ هیچ جواب غیربدیهی در

بین اعداد صحیح ندارد.

بسیاری از مطالعات و پیشرفت های نظریه اعداد مدیون تلاش برای حل این

مسئله بوده که فرما در قرن هفدهم در حاشیه کتاب حساب دیوفانتوسی خود ادعا کرده

که این مسئله را حل کرده است. در سال 1993 با استفاده از نظریه های پیشرفته

ریاضی آندرو وایلز حلی برای آن ارائه کرد که پس از چندی اشکالی در آن پیدا شد.

ولی سرانجام در سپتامبر 1994 (شهریور ماه 1373) اشکال این حل به وسیله

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 جونل گولدشتین، آشنایی با نظریه اعداد، ترجمه 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 تألیف کتاب‌های درسی وزارت آموزش و پرورش ۱۳۶۰.
- ۶- غلامحسین مصاحب، تئوری مقدماتی اعداد. جلد اول - انتشارات دهخدا ۱۳۵۳.



مباحثی دیگر از ترکیبیات

مقدمه

در قسمت اول با نظریهٔ 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 انگیزهٔ 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 همهٔ ما از هندسه خوشمان می‌آید شهودی بودن آن است. گراف نیز همان امتیاز را دارد. به علاوه 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 مطالعهٔ 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.

مدل‌های شهودی و تجسمی در ترکیبیات

۷-۱- رابطه‌ها و گراف‌ها

مفاهیم مربوط به رابطه را که در کتاب جبر و احتمال سال سوم دیده‌ایم یادآوری می‌کنیم.
تعریف: هرگاه A و B دو مجموعه باشند، آن‌گاه یک رابطه از A به B عبارت است از زیرمجموعه‌ای از $A \times B$. زیرمجموعه‌های $A \times A$ را رابطه‌های روی A می‌گویند.

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

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

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

اعداد گویا، و روی \mathbb{R} ، مجموعه اعداد حقیقی، نیز تعریف می‌شود. ▲

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

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

پس داریم: $۹R۲$ و $۱۱R۳$ ، ولی $۳ \not R ۳$. ▲

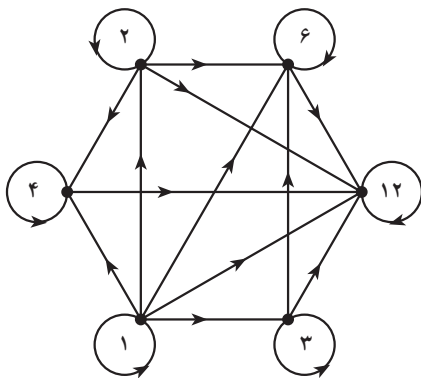
مثال ۳: مجموعه $A = \{۱, ۲, ۳, ۴, ۶, ۱۲\}$ مفروض است. به ازای هر دو عضو $a, b \in A$ تعریف

می‌کنیم: aRb هرگاه $a|b$. ▲

حال فرض کنید A یک مجموعه متناهی و R یک رابطه روی A باشد. به گراف جهت‌دار

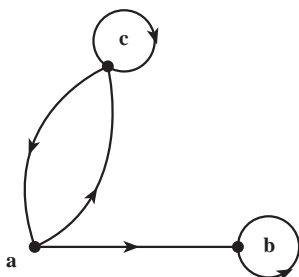
G را به صورت زیر نسبت می‌دهیم. رأس‌های G اعضای A هستند و رأس a به رأس b متصل است

هرگاه aRb .



شکل ۱- گراف جهت دار رابطه عادی کردن

به عنوان مثال، شکل ۱، گراف مربوط به رابطه‌ای را که در مثال ۳ داده شده است نشان می‌دهد. مثلاً رأس ۱ به تمام رؤوس، حتی به خود ۱، وصل است زیرا عدد ۱ تمام اعداد صحیح را می‌شمارد.



شکل ۲- گراف جهت دار یک رابطه

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

$$aRb, aRc, bRb, cRa, cRc$$

این تناظر بین گراف‌های (جهت دار) و رابطه‌ها به درک بسیاری از ویژگی‌های رابطه‌ها کمک می‌کند. مثلاً می‌توانید بازتابی، متقارن بودن یا نبودن رابطه‌ها را فوراً از روی گراف جهت دار مربوط تشخیص دهید. این ویژگی‌ها در درس‌های سال‌های قبل تعریف شده‌اند. یکی از ویژگی‌های رابطه‌ها که کاربرد فراوان دارد خاصیت پاد متقارن است. رابطه 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 رابطه «کوچک‌تر از یا مساوی با» در مثال ۱ و رابطه «عادی کردن» در مثال ۳ دو رابطه پاد متقارن اند ولی رابطه مثال ۲ پاد متقارن نیست. حال ارتباط این ویژگی‌ها را با گراف‌های جهت دار بیان می‌کنیم.

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 می‌کند.

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 آن‌گاه 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 آن گاه از رأس b به رأس a یالی موجود نباشد.

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 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. ▲

۲-۷- 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:

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

پس می توان این ماتریس را متناظر با رابطه مربوط به شکل ۲ گرفت. توجه کنید که درایه i,j ام ماتریس متناظر مساوی با ۱ است اگر و تنها اگر iRj .

اکنون می توانیم ویژگی های مربوط به رابطه ها را به زبان ماتریس ها بیان کنیم. مثلاً ویژگی بازتابی یعنی اینکه همه درایه های قطر اصلی ماتریس ۱ باشند. بقیه ویژگی ها را به زبان ماتریس بیان کنید.

در این فصل صرفاً ماتریس های صفر و یک را در نظر می گیریم. اکنون یک عمل جمع و یک عمل ضرب برای اعضای مجموعه دو عضوی $\{0,1\}$ تعریف می کنیم که از روی آن «توان دوم» را برای ماتریس ها تعریف خواهیم کرد. این توان دوم با آنچه که در جبر خطی دیده ایم فرق دارد.

تعریف: روی مجموعه $\{0, 1\}$ دو عمل $+$ و \odot موسوم به عمل‌های بولی را به ترتیب زیر تعریف می‌کنیم:

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

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

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

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

به عبارت دیگر برای به دست آوردن توان دوم یک ماتریس که در اینجا تعریف کردیم مانند توان دوم معمولی در ماتریس‌ها عمل می‌کنیم ولی در نهایت به جای هر درایه غیر صفر 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: $M^{(r)} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

تعریف: هرگاه R رابطه‌ای روی مجموعه A باشد ترکیب رابطه RoR ، رابطه‌ای روی A است که با قاعده زیر تعریف می‌شود:

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

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

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

$M(R)$ ماتریس متناظر R باشد داریم:

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

ب) $M(R) = [1]_{n \times n}$ (یعنی همه درایه‌های $M(R)$ یک‌اند) اگر و تنها اگر $R = A \times A$;

پ) $M(RoR) = [M(R)]^{(r)}$.

اثبات: بند (الف) و (ب) بلافاصله از تعریف نتیجه می‌شوند. برای اثبات بند (پ)، اول فرض

کنید $i(RoR)j$. پس عضوی مانند $k \in A$ وجود دارد به طوری که iRk و kRj . پس درایه‌های ik و

kj در ماتریس M مساوی با ۱ هستند. در نتیجه درایه ij در ماتریس $M^{(r)}$ برابر با ۱ است. حال

به عکس اگر درایه ij در ماتریس $M^{(r)}$ برابر با ۱ باشد یعنی

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

آن‌گاه حداقل یکی از جمعوندها باید مساوی با ۱ باشد. مثلاً $m_{ik} \odot m_{kj} = 1$ از آنجا $m_{ik} = m_{kj} = 1$ ،
 که نتیجه می‌شود: iRk و kRj . پس بنا به تعریف خواهیم داشت $j \in (RoR)i$.



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

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

مفروض است. مطلوب است محاسبه RoR .

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

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



و از آنجا $RoR = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 4), (3, 3), (3, 4)\}$

تعریف: فرض کنید ماتریس‌های صفر و یک $A = [a_{ij}]_{m \times n}$ و $B = [b_{ij}]_{m \times n}$ از اندازه $m \times n$ باشند. گوئیم A کوچک‌تر از یا مساوی B است و می‌نویسیم $A \leq B$ 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 ماتریس‌های متناظر با رابطه‌های R_1 و R_2 روی یک مجموعه A باشند، آن‌گاه $R_1 \subseteq R_2$ اگر و تنها اگر $M_1 \leq M_2$.

قضیه ۲: مجموعه n عضوی A ، $n \in \mathbb{N}$ ، و رابطه 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 $I_n \leq M$. (I_n ماتریس همانی $n \times n$ است).

(ب) R متقارن است اگر و تنها اگر $M = M^T$. (ماتریس M^T ترانژاده M است و آن ماتریسی است که از قراردادن سطرهای M به جای ستون‌های M ، با حفظ ترتیب، به دست می‌آید).

(پ) R تراییبی است اگر و تنها اگر $M^{(2)} \leq M$.

(ت) R پاد متقارن است اگر و تنها اگر $M \wedge M^T \leq I_n$. (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 $M \ll M^{(2)}$. باید نشان دهیم R تراییبی است. هر گاه xRy و yRz ، آن‌گاه در ماتریس M ، درایه سطر x ام و ستون y ام و همچنین درایه سطر y ام و ستون z ام برابر ۱ است. در نتیجه درایه واقع در سطر x ام و ستون z ام در ماتریس $M^{(2)}$ برابر ۱ است. چون $M \ll M^{(2)}$ پس درایه سطر x ام و ستون z ام ماتریس M نیز باید ۱ باشد یعنی xRz .

به عکس، فرض کنید R تراییبی باشد. باید نشان دهیم که $M \ll M^{(2)}$. فرض کنید m_{xz} ، درایه واقع در سطر x ام و ستون z ام در ماتریس $M^{(2)}$ ، 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 تراییبی است xRz . پس $m_{xz} = 1$ یعنی نشان داده‌ایم که $M \ll M^{(2)}$.

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 درایه ij 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 درایه ij ام در M مساوی با ۱ باشد آن‌گاه درایه ji ام در M مساوی با ۰ است. پس در این صورت نیز درایه ij ام در $M \wedge M^T$ برابر با ۰ است. یعنی $M \wedge M^T \ll I_n$.

به عکس از $M \wedge M^T \ll I_n$ نتیجه می‌شود که همه درایه‌های غیر قطری $M \wedge M^T$ 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 $m_{ij} = 1, m_{ji} = 0$ یا $m_{ij} = 0, m_{ji} = 1$. که نتیجه می‌شود : اگر iRj و jRi آن‌گاه $i = j$.

اثبات بقیه حکم‌ها را به عنوان تمرین به عهده دانش آموزان می‌گذاریم.

قضیه‌های ۱ و ۲ ارتباط بین رابطه‌ها و ماتریس‌های صفر و یک را نشان می‌دهند. این قضیه‌ها با وجود سادگی اهمیت زیادی دارند. زیرا بهترین راه معرفی یک رابطه به کامپیوتر از طریق ماتریس صفر و یک است. از طریق حکم‌های فوق می‌توان با کامپیوتر ویژگی‌های هر رابطه‌ای را بررسی کرد.

مثال ۷ : با استفاده از قضیه ۲ می‌توان یک الگوریتم نوشت و با برنامه کامپیوتری هم ارزی بودن رابطه‌ای را که روی یک مجموعه متناهی A داده شده است امتحان کرد. یعنی رابطه R یک رابطه 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) $M = M^T$

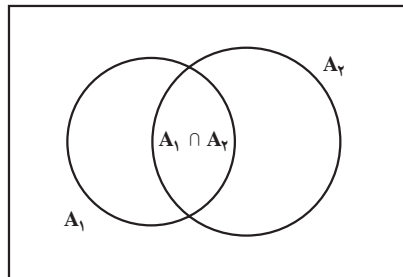
(پ) $M^{(2)} \ll M$

۳-۷- 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 دیده‌اید. اگر A یک مجموعه متناهی باشد تعداد عناصر آن را با $|A|$ نشان می‌دهیم. فرض کنید A_1 و A_2 دو مجموعه متناهی باشند. داریم:

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

با توجه به شکل ۳ رابطه (۱) درست است، زیرا در مجموع $|A_1| + |A_2|$ هر عضوی که فقط به یکی از مجموعه‌های A_1 یا A_2 متعلق باشد یک بار به حساب می‌آید ولی هر عضوی که به هر دو مجموعه A_1 و A_2 تعلق داشته باشد دو بار شمرده می‌شود. 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 می‌آید.



شکل ۳- نمودار ون برای دو مجموعه

رابطه (۱) وجه تسمیه «شمول و عدم شمول» را نیز توجیه می‌کند. زیرا در شمارش اعضای مجموعه $A_1 \cup A_2$ ، اول همه 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 مجموعه $A = \{n \in \mathbb{N} : 1 \leq n \leq 6300\}$ نه بر ۵ تقسیم پذیرند و نه بر ۳؟

فرض کنید A_1 زیرمجموعه A متشکل از مضارب ۳ و A_2 زیرمجموعه A متشکل از مضارب ۵ باشند. می‌خواهیم $|A_1 \cup A_2|$ را پیدا کنیم (\bar{B} متمم مجموعه B را نمایش می‌دهد). داریم:

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

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

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

و چون $A_1 \cap A_2$ مجموعه 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 رابطه (۱) داریم :

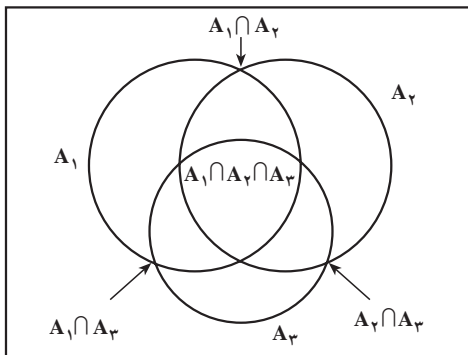
$$|A_1 \cup A_2| = 2100 + 1260 - 420 = 2940$$

$$\cdot \quad |\overline{A_1 \cup A_2}| = 6300 - 2940 = 3360$$

حال برای $n = 3$ اصل شمول و عدم شمول را مطالعه می کنیم. ▲

قضیه ۳ : فرض کنید A_1 و A_2 و A_3 سه زیر مجموعه متناهی از یک مجموعه A باشند. داریم

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \quad (2)$$



شکل ۴- نمودار ون برای سه مجموعه

اثبات : نشان می دهیم که هر عضو x از A به تعداد مساوی در دو طرف رابطه (۲) به حساب می آید. به شکل ۴ توجه کنید.

دو حالت داریم :

حالت ۱ : اگر x متعلق به هیچ کدام از مجموعه های A_1 و A_2 و A_3 نباشد، آن گاه x در دو طرف رابطه (۲)، صفر بار به حساب می آید.

حالت ۲ : فرض کنید x به s مجموعه از مجموعه های A_1 و A_2 و A_3 تعلق داشته باشد $(1 \leq s \leq 3)$. آن گاه x یک بار در طرف چپ به حساب می آید، و در طرف راست نیز

اگر $s=1$ ، یک بار به حساب می آید،

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

اگر $s=3$ ، در این صورت هم $3-3+1=1$ بار به حساب می آید.

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 مجموعه ۴ عضوی B به یک مجموعه ۳ عضوی A را پیدا کنید. باید توجه کرد که منظور از تابع $f: B \longrightarrow A$ تابعی است که روی همه اعضای B تعریف شده است و تابع $f: B \longrightarrow A$ را پوشا می‌نامیم هرگاه $R_f = A$.

فرض کنید $B = \{b_1, b_2, b_3, b_4\}$ و $A = \{a_1, a_2, a_3\}$. مجموعه تمام توابع $f: B \longrightarrow A$ 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 $3 \cdot 3 \cdot 3 \cdot 3 = 81$ است. حال فرض کنید A_i مجموعه توابعی باشد که هیچ عضوی از B را به a_i نسبت نمی‌دهند.

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

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

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

$$|A_1 \cap A_2| = |A_1 \cap A_3| = |A_2 \cap A_3| = 1$$

و

$$|A_1 \cap A_2 \cap A_3| = 0$$

و

$$|A_1 \cup A_2 \cup A_3| = 2^4 + 2^4 + 2^4 - (1 + 1 + 1) + 0 = 45$$

پس:

$$|\overline{A_1 \cup A_2 \cup A_3}| = 81 - 45 = 36$$

و از آنجا

که تعداد توابع پوشای از B به A است.

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

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

اگر x_i را تعداد گل‌های انتخاب‌شده از نوع i ام بگیریم به سادگی دیده می‌شود که یک تناظر یک به یک بین انتخاب‌ها و جواب‌های معادله فوق موجود است. اثبات برابری تعداد انتخاب‌ها با مقدار داده شده را به عنوان تمرین به عهده 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. ▲

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

مجموعه‌های A_1 ، A_2 و A_3 را به ترتیب زیر تعریف می‌کنیم:

$$A_i = \{ \text{جواب‌های معادله فوق به شرطی که } x_i > 2 \}, i = 1, 2, 3$$

باید تعداد مجموعه $\overline{A_1 \cup A_2 \cup A_3}$ را پیدا کنیم. بنابر فرمول (۲) از قضیه 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 مجموعه تمام جواب‌های صحیح و نامنفی معادله 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 معادله $x_1 + x_2 + x_3 = 1$. زیرا کافی است که در جواب معادله اخیر به x_1 عدد ۳ اضافه کنیم تا یک جواب معادله $x_1 + x_2 + x_3 = 4$ با شرط $x_1 > 2$ به دست آید و برعکس. اما به سادگی دیده می‌شود که تعداد جواب‌های صحیح و نامنفی معادله $x_1 + x_2 + x_3 = 1$ مساوی است با ۳. پس $|A_1| = 3$ و به همین ترتیب $|A_2| = |A_3| = 3$.

از طرف دیگر داریم

$$A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$$

همین طور $A_1 \cap A_2 \cap A_3 = \emptyset$. پس $|A_1 \cup A_2 \cup A_3| = 15 - 3 - 3 - 3 = 6$. در حقیقت جواب فوق چنین اند:

$$(\emptyset, 2, 2), (1, 1, 2), (1, 2, 1), (2, \emptyset, 2), (2, 1, 1), (2, 2, \emptyset)$$

در قسمت نظریه اعداد با تابع حسابی اویلر ϕ به عنوان «مجله ریاضی» آشنا شده ایم. منظور از $\phi(n)$ عبارت است از تعداد اعداد صحیح و مثبت m که کوچک تر از n یا مساوی با آن بوده و m و n نسبت به هم اول باشند. قضیه زیر حالت خاصی از قضیه ای کلی درباره این تابع است.

قضیه ۴: فرض کنید عدد صحیح و مثبت n برابر با حاصل ضرب سه عدد اول و متمایز به صورت زیر باشند:

$$n = p_1 p_2 p_3$$

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \quad \text{در این صورت}$$

اثبات: مجموعه های A_i را به ترتیب زیر تعریف می کنیم:

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

حال اصل شمول و عدم شمول را برای مجموعه های A_i می نویسیم. داریم:

$$i = 1, 2, 3 \quad \phi(n) = |A_1 \cup A_2 \cup A_3|$$

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

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

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

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

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

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

مثال ۱۲ : ثابت کنید $\phi(42) = 12$.

چون $42 = 2 \cdot 3 \cdot 7$ ، حکم از قضیه ۴ به دست می آید :

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

این نتیجه را می توان مستقیماً هم بررسی کرد. زیرا تمام اعداد صحیح و مثبت نایبتر از ۴۲ که نسبت به آن اول هستند عبارت اند از :

۱، ۵، ۱۱، ۱۳، ۱۷، ۱۹، ۲۳، ۲۵، ۲۹، ۳۱، ۳۷، ۴۱



۴-۷- تمرین ها

۱- فرض کنید $A = \{1, 2, 3, 4\}$. برای هریک از حالت های زیرگرافی رسم کنید که رابطه 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 افرازهای مختلف را پیدا کنید).

۳- فرض کنید $A = \{1, 2, 3, 4\}$. دو رابطه 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 ۱ را اثبات کنید.

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

۶- فرض کنید R یک رابطه بازتابی روی مجموعه متناهی A باشد. نشان دهید که رابطه 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 $E < F$ را بیابید.

۸- با استفاده از قضیه هایی که در این فصل خوانده اید نشان دهید که آیا رابطه زیر روی مجموعه

$A = \{1, 2, 3, 4\}$ یک رابطه هم ارزی 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)

می نامیم، هرگاه حاصل جمع درایه های هر سطر، حاصل جمع درایه های هر ستون، حاصل جمع درایه های

قطر اصلی و حاصل جمع درایه های قطر فرعی با هم مساوی باشند. به عنوان 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 می گیرد همیشه عدد ۵ است.

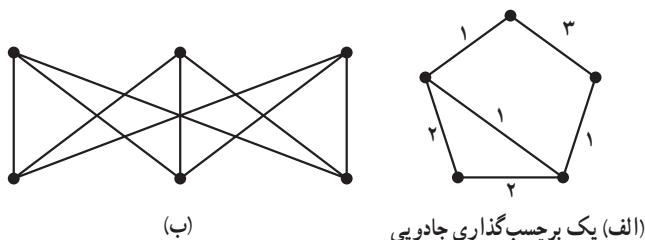
۱۰- گراف G داده شده است. یک برچسب گذاری جادویی G عبارت است از متناظر کردن

اعدادی، معمولاً صحیح و مثبت، به یال های G به طوری که حاصل جمع اعداد متناظر با یال های ماز

بر هر رأس عددی ثابت باشد. در گرافی که در شکل ۵ (الف) داده شده است اعدادی که روی یال‌ها نوشته شده‌اند یک برچسب‌گذاری جادویی را نشان می‌دهد، زیرا حاصل جمع اعداد متناظر به یال‌های مارّ بر هر رأس مساوی با ۴ است.

با استفاده از مربع 3×3 یک برچسب‌گذاری 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 است با $\binom{n+k-1}{n}$.



شکل ۵

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

(الف) $x_1 + x_2 + x_3 = 7$

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

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

۱۳- مطلوب است تعداد شماره‌شناسنامه‌های پنج‌رقمی 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 مجله A را می‌خوانند، ۵۰ نفر مجله B، ۵۰ نفر مجله 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 مجله A و B و C را می‌خوانند. مطلوب است تعداد دانش‌آموزانی که:

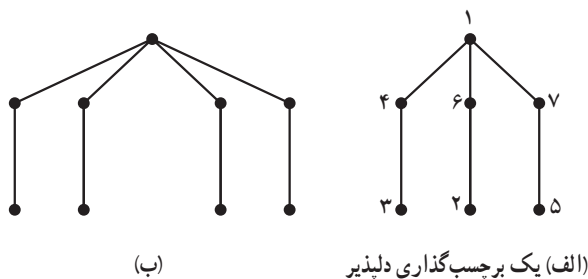
(الف) هیچ مجله‌ای نمی‌خوانند؛

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



شکل ۶

مراجع

۱- ایوان نیون، ریاضیات انتخاب یا چگونه بدون شمارش بشماریم. ترجمه 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.

مجله ریاضی

مربع وفقی یکی از ساختارهای ترکیبیاتی است که ریاضی دانان شرق درباره آن کارهای بسیاری انجام داده اند و روش های ساخت این مربع ها برای اندازه های مختلف منسوب به این دانشمندان است. اصولاً ساختارهای ترکیبیاتی یکی از مهم ترین مباحث ترکیبیات است که دارای کاربردهای فراوان نیز هستند. از مهم ترین ساختارهای ترکیبیاتی مربع های لاتین و طرح های بلوکی است. یک مربع لاتین عبارت است از یک ماتریس $n \times n$ با درایه های $1, 2, 3, \dots, n$ به طوری که در هر سطر و در هر ستون درایه های تکراری نباشند.

مربع های لاتین با مربع های وفقی نیز ارتباط دارند. یکی از کاربردهای مربع های لاتین در مبحث رمزنگاری است. به ازای هر n داده شده می توان یک مربع لاتین از مرتبه n ساخت. از مربع هایی که در زیر به ازای $n = 4$ و $n = 5$ ساخته شده اند می توان به راحتی برای حالت کلی نیز ایده گرفت.

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

دقت کنید که در هر دو مربع فوق بعضی از درایه های واقع در دو گوشه چپ بالا و راست پایین را پررنگ نوشته ایم. در مربع اول ۴ تا و در مربع دوم ۶ تا از این درایه های پررنگ قرار دارند. جالب این است که اگر در هریک از این دو مربع فقط این درایه ها را به ما بدهند می توانیم بقیه درایه ها را به طور یکتا به دست آوریم.

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

مقدمه

امروزه همهٔ سازمان‌های دولتی و خصوصی، در هر رشته‌ای که باشند، اعم از اقتصادی، صنعتی، اجتماعی و غیره برای تعیین سیاست و روند کار آیندهٔ 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 پایهٔ آن علم آمار با شاخه‌های متعدّدش، 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، نظریهٔ اطلاعات، علوم فضایی، نظریهٔ رمزنگاری و امثال آنها به سرعت گسترش یافته است. با این وجود تصور می‌رود هنوز در اوایل راهی هستیم که سه سده 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 جنبهٔ احتمال که صورتی گسسته دارد سخن می‌گوییم. شاید که راهنمای شما برای ادامهٔ راه باشد.

احتمال

۸-۱- یادآوری

خلاصه‌ای از آنچه را که سال گذشته دربارهٔ 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 پدیدهٔ تصادفی می‌نامند. مجموعهٔ همهٔ نتایج ممکن را فضای نمونه‌ای آزمایش تصادفی می‌نامیم. فضای نمونه‌ای را با S نشان می‌دهیم. هر نتیجهٔ 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 :

برابر شدن دو تیم $c =$ باختن تیم $b = A$ بردن تیم $a = A$

پس مجموعهٔ $S = \{a, b, c\}$ فضای نمونه‌ای است و هر عضو این مجموعه برآمدی است که

ممکن است رخ دهد. از سه برآمد تنها یکی رخ می‌دهد. ▲

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 می‌گویند. سال گذشته اعمال روی پیشامدها را که همان اعمال روی مجموعه‌ها هستند دیده‌اید.

تذکر: منظور از «رخداد» یک پیشامد وقوع آن پیشامد، یعنی مشاهدهٔ عضوی از آن پیشامد

به عنوان نتیجهٔ 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 مثال 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 مجموعه 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 آنقدر 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 بازه $(0,1)$.

ت) وقتی فضای نمونه‌ای S را برای آزمایشی 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 آن‌گاه

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

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

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 مجموعه 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 اصل ۳ 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 آن‌گاه

$$P(A) = \frac{m}{n}$$

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، تک‌عضوی مانند $\{a\}$ باشد برای سادگی احتمال آن را به جای $P(\{a\})$ به صورت $P(a)$ می‌نویسیم.


وقتی فضای نمونه‌ای گسسته است در تخصیص اندازه 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 $2^0 = 1048576$ است. در این حالت اگر اندازه 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 بازی‌های یکی بوده‌اند، و جمعاً 1^0 بار تیم A برنده، 6 بار بازنده شده و 4 بار برابر کرده باشد. پس $\frac{1}{2^0}$ بارها برنده، $\frac{6}{2^0}$ بارها بازنده شده و $\frac{4}{2^0}$ بارها برابر کرده است. در این صورت معقول است که بگوییم فردا تیم A با احتمال $\frac{5}{1^0}$ برنده، با احتمال $\frac{3}{1^0}$ بازنده خواهد شد و با احتمال $\frac{2}{1^0}$ 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.

$$P(a) = \frac{5}{1^0}, \quad P(b) = \frac{3}{1^0}, \quad P(c) = \frac{2}{1^0}$$

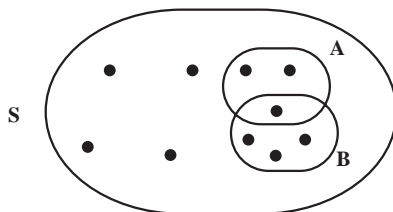
می‌توانیم از روی اطلاعات دیگر، مثلاً ملاحظه مسابقات تمرین چند روز قبل دو تیم، احتمال‌های دیگری را به برآمدها نسبت دهیم. با معلوم بودن S و P می‌توانیم احتمال هر پیشامد S را مشخص کنیم، مثلاً

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

یعنی احتمال اینکه تیم A برنده شود یا برابر کند $\frac{7}{10}$ است.  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 بازه $(0, 1)$ 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 مجموعه 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 $A \cup B$ را 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

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



فضای نمونه‌ای : S

برآمد : \bullet

پیشامد : A

پیشامد : B

شکل ۱- نمایش فضای نمونه‌ای، برآمد و پیشامد

فرمول صفحه قبل به شما اجازه می دهد 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. برایی های زیر را نیز یادآوری می کنیم.

اگر پیشامد \bar{A} متمم پیشامد A باشد آن گاه

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

که بی درنگ نتیجه می شود

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

همچنین اگر $A \subseteq B$ ، آن گاه

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

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

و

اینک پس از این یادآوری ها به بیان مطالبی جدید در زمینه احتمال می پردازیم.

۸-۲- مدل احتمال شرطی

فرض کنید می خواهیم آزمایشی تصادفی را انجام دهیم. ابتدا فضای نمونه ای را مشخص می کنیم و احتمالی به رخداد هر پیشامد نسبت می دهیم و بدین ترتیب مدل احتمال را معین می کنیم. این مدل را می شناسید. حال اگر اطلاعی اضافی درباره فضای نمونه ای داشته باشیم، مثلاً به دلیلی بدانیم که پیشامد B از این فضای نمونه ای رخ داده است آن گاه معمولاً مدل احتمال قبلی به هم می ریزد و آگاهی از رخداد حتمی پیشامد B در مقدار احتمال سایر پیشامدها اثر می گذارد، که در این صورت احتمال های پیشامدهای فضای نمونه ای با احتمال های مدل قبلی تفاوت دارند. اگر بتوانیم تحت این شرط که پیشامد B حتماً رخ می دهد احتمال پیشامدهای دیگر فضای نمونه ای را مشخص کنیم مدل احتمال جدیدی به دست می آید که آن را مدل احتمال شرطی می نامیم. قبل از توضیح بیشتر مثالی می زنیم.

مثال ۳: می خواهید یک تاس قرمز و یک تاس سفید را با هم بریزید. تاس ها همگن اند. می دانید که فضای نمونه ای ۳۶ برآمد دارد:

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

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 شماره های دو

تاس حتماً کوچک تر از ۷ است. پیشامد «مجموع دو شماره کوچک تر از ۷» را B می‌نامیم. پیشامد B از برآمدهای زیر تشکیل می‌شود:

$(1,1), (1,2), (1,3), (1,4), (1,5)$

$(2,1), (2,2), (2,3), (2,4)$

$(3,1), (3,2), (3,3)$

$(4,1), (4,2)$

$(5,1)$

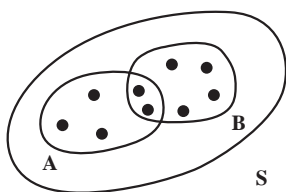
یعنی پیشامد B ، متشکل از ۱۵ برآمد از ۳۶ برآمد فضای نمونه‌ای است. وقتی شرط می‌کنیم که B حتماً رخ می‌دهد، یعنی یکی از این ۱۵ برآمد نتیجه ریختن دو تاس است.

برآمدهایی مثل $(1,6)$ یا $(2,5)$ یا $(4,5)$ و غیره که مجموع دو شماره 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 کوچک تر 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 $(1,1)$ ، $(2,2)$ و $(3,3)$ هستند. چون احتمال رخداد هر برآمد مساوی $\frac{1}{15}$ است، لذا

$$P(A|B) = P\{(1,1), (2,2), (3,3)\} = \frac{3}{15}$$

در مثال بالا، احتمال شرطی، یعنی $P(A|B)$ را به سادگی حساب کردیم زیرا فضای نمونه‌ای آزمایش یکنواخت، یا برآمدها متساوی‌الاحتمال یعنی هم شانس بودند، ولی اگر احتمال برآمدها یکی نباشند کار

کمی مشکل است. قبل از اینکه 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 آنکه 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 رابطه مستقیم با $P(A \cap B)$ باشد. این رابطه را به صورت،

$$(۱) \quad P(A|B) = K P(A \cap B)$$

فرض می‌کنیم. در این برابری اگر به جای پیشامد A پیشامد B قرار بگیرد نتیجه می‌شود

$$P(B|B) = K P(B \cap B)$$

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 رابطه 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 اینکه 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.

تذکر: اگر فضای نمونه‌ای گسسته و هم‌شانس باشد می‌توانیم رابطه احتمال شرطی را ساده کرده و به صورت $P(A|B) = \frac{n(A \cap B)}{n(B)}$ از آن استفاده کنیم.

مثال ۴: سازنده قطعات یدکی یک کارخانه از روی تجربه‌های گذشته می‌داند احتمال اینکه سفارشی به موقع برای ارسال آماده شود ۹/۰ است و احتمال اینکه سفارشی به موقع برای ارسال آماده و به موقع تحویل مشتری شود برابر ۸/۰ است. احتمال اینکه سفارشی به موقع تحویل شود به شرط آنکه به موقع ارسال شده باشد چقدر است؟

ابتدا قرار می‌دهیم:

A = پیشامد آماده بودن به موقع، برای ارسال

B = پیشامد تحویل به موقع سفارش، به مشتری

بنابر داده‌های مسأله، $P(A) = \frac{5}{9}$ و $P(A \cap B) = \frac{2}{9}$

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. آنچه می‌خواهیم، $P(B|A)$ است، یعنی احتمال تحویل به موقع سفارش به مشتری به شرط آنکه به موقع ارسال شده باشد. بنابر تعریف احتمال شرطی

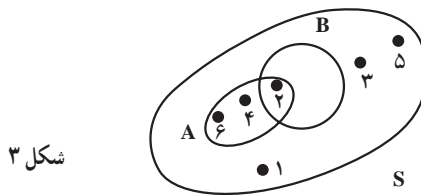
$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{2}{9}}{\frac{5}{9}} = \frac{2}{5}$$

مثال ۵: تاسی همگن را با چشم بسته انداخته‌ایم. برآمد حاصل را نگفته‌اند، ولی اعلام کرده‌اند که برآمد حاصل عددی زوج است. احتمال اینکه شماره ۲ ظاهر شده باشد چقدر است؟
قرار می‌دهیم:

A = پیشامد ظاهر شدن شماره زوج

B = پیشامد ظاهر شدن شماره ۲

به شکل ۳ توجه کنید.



$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3} \quad \text{یا} \quad P(B|A) = \frac{n(B \cap A)}{n(A)} = \frac{1}{3} \quad \text{لذا}$$

زیرا $P(A) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$. به عبارت دیگر می‌توانید تصور کنید که فضای نمونه‌ای $\{2, 4, 6\}$ 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.

۸-۳- قاعده ضرب احتمال

از تعریف

$$P(A|B) = \frac{P(A \cap B)}{P(B)}, \quad P(B) \neq 0$$

$$P(A \cap B) = P(B) \cdot P(A|B), \quad P(B) \neq 0$$

نتیجه می شود که این رابطه به قاعده ضرب احتمال موسوم است. به کمک این قاعده می توان احتمال رخداد هم زمان دو پیشامد را تعیین کرد.

مثال ۶: جعبه ای محتوی ۱۲ لامپ است که می دانیم ۳ تای آنها معیوب اند. از این جعبه به تصادف ۱ لامپ برمی داریم. سپس مجدداً بدون جای گذاری لامپ اول، لامپ دیگری به تصادف برمی داریم. احتمال اینکه هر دو لامپ معیوب باشند چقدر است؟ ابتدا قرار می دهیم:

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 برمی داریم پس:

$$P(B|A) = \frac{2}{11}$$

لذا از قاعده ضرب احتمال داریم:

$$P(A \cap B) = P(A) \cdot P(B|A) = \frac{1}{4} \cdot \frac{2}{11} = \frac{1}{22}$$



۸-۴- استقلال دو پیشامد

پیشامدهای A و B دو پیشامد از یک فضای نمونه ای هستند که احتمال آنها مثبت است. اگر آگاهی از رخداد پیشامد B در احتمال رخداد پیشامد A مؤثر نباشد A را مستقل از B می گویند. 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 مقایسه 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 رابطه (۳) برقرار باشد. از طرفی با داشتن رابطه (۳) می‌توان به رابطه‌های $P(A|B) = P(A)$ و $P(B|A) = P(B)$ رسید. (چرا؟) یعنی رابطه (۳) شرط لازم و کافی برای استقلال A از B و B از A است. بر این اساس می‌گوییم A و B مستقل اند. پس :

تعریف : دو پیشامد A و B از یک فضای نمونه‌ای مستقل اند 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 همه 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،

$$P(۱) = P(۲) = P(۳) = P(۴) = \frac{1}{4}$$

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 :

$$P(A \cap B) = P(۱) = \frac{1}{4}$$

از طرفی :

$$P(A) = P(B) = \frac{1}{2}$$

در نتیجه :

$$P(A \cap B) = P(A) \cdot P(B) = \frac{1}{4}$$

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 $A \cap B = \phi$ ، آن گاه

$$P(A \cap B) = P(\phi) = 0$$

و اگر A و B مستقل باشند باید

$$P(A \cap B) = P(A) \cdot P(B)$$

از مقایسه دو برابری اخیر نتیجه می شود 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 آن گاه 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 همان طور که در سال پیش دیده ایم

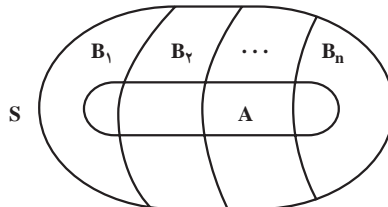
$$B_1 \cup B_2 \cup \dots \cup B_n = S$$

و هر دو پیشامد B_i و B_j وقتی $i \neq j$ ، ناسازگارند، یعنی $B_i \cap B_j = \phi, i \neq j$ ، 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 می دانیم 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 می شود 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 مهره سفید و ۱۱ مهره سیاه است. دومین ظرف شامل ۳ مهره سفید و ۹ مهره سیاه است، و سومین ظرف تنها شامل مهره های سفید است. با چشم بسته یکی از سه ظرف را انتخاب و از آن مهره ای در می آوریم. احتمال اینکه مهره سفید باشد چقدر است؟ پیشامد استخراج مهره سفید را با A نشان می دهیم. می خواهیم $P(A)$ را حساب کنیم پیشامدهای زیر را تعریف می کنیم

$B_1 = \{\text{ظرف اول انتخاب شود}\}$

$B_2 = \{\text{ظرف دوم انتخاب شود}\}$

$B_3 = \{\text{ظرف سوم انتخاب شود}\}$

بدیهی است $P(B_1) = P(B_2) = P(B_3) = \frac{1}{3}$. از طرفی

$$P(A|B_1) = \frac{5}{16}, P(A|B_2) = \frac{1}{4}, P(A|B_3) = 1$$

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- قاعده بیز

(حالت ساده). در آزمایش های معمولی مواردی وجود دارند که برآمد نهایی آزمایش به آنچه در

مراحل قبلی رخ می دهند بستگی دارد. برای توضیح این مطلب ابتدا به معرفی قاعده بیز می پردازیم.

دیدیم که اگر A و B دو پیشامد با احتمال مثبت از فضای نمونه ای یک آزمایش تصادفی باشند،

آن گاه 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 $P(A) \cdot P(B|A)$ را در برابری اول قرار دهیم، نتیجه می‌شود که

$$(5) \quad P(A|B) = \frac{P(A)}{P(B)} \cdot P(B|A)$$

این رابطه را قاعدهٔ بیز می‌نامند. قاعدهٔ بیز در حالت کلی مفصل‌تر است. تامس بیز (۱۷۶۱-۱۷۰۲) کشیشی انگلیسی بود که حالت کلی تر این قاعده را ارائه داد. در مثال زیر یک مورد استفاده از قاعدهٔ بیز را می‌بینید.

مثال ۹: وقتی یک مرکز مخابرهٔ تلگراف، پیامی را به مرکز دیگر می‌فرستد گاهی خط‌هایی در انتقال صورت می‌گیرد. 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 $\frac{1}{4}$ 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 چقدر احتمال دارد که این کد واقعاً به صورت نقطه فرستاده شده باشد؟

اگر در فرمول بیز قرار دهیم

A = پیشامد فرستادن نقطه

B = پیشامد دریافت نقطه

آن‌گاه فرمول

$$P(A|B) = \frac{P(A)}{P(B)} \cdot P(B|A)$$

به صورت زیر درمی‌آید

$$P(\text{الف} | \text{فرستادن نقطه} | \text{دریافت نقطه}) = \frac{P(\text{فرستادن نقطه})}{P(\text{دریافت نقطه})} \cdot P(\text{دریافت نقطه} | \text{فرستادن نقطه})$$

آنچه می‌خواهیم به دست آوریم طرف اول رابطه است. زیرا در مرکز N نقطه‌ای دریافت شده است و می‌خواهیم احتمال اینکه این کد به صورت نقطه فرستاده شده باشد را بدانیم. پس سه احتمال طرف دوم را حساب می‌کنیم.

۱- این روزها، در ارتباط‌های الکترونیکی از کدهای ۰ و ۱ استفاده می‌کنند.

$$P(A) = P(\text{فرستادن نقطه}) = \frac{3}{V} \quad (\text{ب})$$

$$P(B|A) = P(\text{فرستادن نقطه} | \text{دریافت نقطه}) = \frac{V}{\Delta} \quad (\text{پ})$$

محاسبه سومین احتمال یعنی $P(\text{دریافت نقطه})$ کمی مفصل تر است. وقتی نقطه ای دریافت می شود باید فکر کنیم که نقطه ای فرستاده اند و یا خطی فرستاده اند که به خطا نقطه دریافت شده است. پس

$$P(B) = P(\text{فرستادن نقطه} \cap \text{دریافت نقطه}) + P(\text{فرستادن خط} \cap \text{دریافت نقطه}) \quad (\text{ت})$$

اما از فرمول حاصل ضرب احتمال می توانیم دو جمله طرف دوم را حساب کنیم.

$$P(\text{فرستادن نقطه}) \cdot P(\text{فرستادن نقطه} | \text{دریافت نقطه}) = P(\text{فرستادن نقطه} \cap \text{دریافت نقطه})$$

$$= \frac{V}{\Delta} \cdot \frac{3}{V} = \frac{3}{\Delta}$$

$$P(\text{فرستادن خط}) \cdot P(\text{فرستادن خط} | \text{دریافت نقطه}) = P(\text{فرستادن خط} \cap \text{دریافت نقطه})$$

می دانیم که طبق داده های مثال، $P(\text{فرستادن خط}) = \frac{4}{V}$ و $P(\text{فرستادن خط} | \text{دریافت نقطه}) = \frac{1}{\Delta}$. پس:

$$P(\text{فرستادن خط} \cap \text{دریافت نقطه}) = \frac{1}{\Delta} \cdot \frac{4}{V} = \frac{1}{14}$$

اگر مقادیر این دو جمله را در (ت) قرار دهیم

$$P(B) = P(\text{دریافت نقطه}) = \frac{3}{\Delta} + \frac{1}{14} = \frac{25}{56} \quad (\text{ث})$$

حال اگر (ب)، (پ) و (ث) را در (الف) قرار دهیم جواب مسأله به دست می آید:

$$P(\text{فرستادن نقطه} | \text{دریافت نقطه}) = \frac{\frac{3}{V}}{\frac{25}{56}} \cdot \frac{V}{\Delta} = \frac{21}{25}$$

پس اگر در مرکز N نقطه ای دریافت شود احتمال $\frac{21}{25}$ وجود دارد که این کد واقعاً به صورت نقطه فرستاده شده باشد.

مثال ۱۰: در جعبه A_1 سه مهره قرمز و ۴ مهره آبی و در جعبه A_2 پنج مهره قرمز و ۳ مهره آبی وجود دارد. یکی از این دو جعبه را به تصادف انتخاب و ۱ مهره از آن خارج می کنیم و مشاهده می کنیم

که آبی است. چقدر احتمال دارد این مهره از جعبه A_1 باشد؟

پیشامد اینکه مهره از A_1 باشد $A =$

پیشامد اینکه مهره آبی باشد $B =$

$$P(A|B) = \frac{P(A)}{P(B)} \times P(B|A) = \frac{\frac{1}{2}}{\frac{1}{2} \times (\frac{4}{7} + \frac{3}{8})} \times \frac{4}{7} = \frac{32}{53}$$

۸-۷- تمرین‌ها

۱- جعبه‌ای محتوی ۳ مهره سفید و ۲ مهره سیاه است. متوالیاً دو مهره به تصادف از جعبه بدون جای گذاری برمی داریم.

الف) اگر اولین مهره سیاه باشد احتمال اینکه دومین مهره هم سیاه باشد چقدر است؟

ب) احتمال اینکه مهره دوم هم رنگ مهره اول باشد چقدر است؟

۲- برحسب تجربه گذشته می دانیم احتمال اینکه رتبه اول سال آخر رشته ریاضی دبیرستانی در مسابقه ورودی دانشگاه قبول شود ۹۵٪ است. با توجه به سوابق تحصیلی علی در این دبیرستان، احتمال اینکه او در سال آخر رشته ریاضی دبیرستان رتبه اول شود ۹٪ است. احتمال اینکه علی هم رتبه اول شود و هم در مسابقه ورودی دانشگاه قبول شود چقدر است؟

۳- سکه‌ای همگن را ۳ بار می اندازیم. 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 ۵٪ است. اگر بیماری پس از عمل زنده باشد احتمال اینکه بدن او در طول یک ماه پیوند را قبول نکند و بمیرد ۲٪ است. احتمال زنده ماندن یک بیمار پیوندی پس از این دو مرحله چقدر 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 اینکه هر ۳ لامپ معیوب باشند چقدر است؟

۶- یک فضای نمونه‌ای متشکل از ۵ برآمد a, b, c, d و e است. به شرط آنکه $P(\{a, b, c\}) = \frac{1}{4}$ ، $P(a) = \frac{1}{4}$ مطلوب است:

الف) محاسبه $P(\{b, c, d\} | \{a, b, c\})$

ب) محاسبه $P(\{a\} | \{a, b, c\})$

۷-۴ مهره به شماره‌های ۱، ۲، ۳ و ۴ را در ظرفی ریخته‌ایم. اگر بخواهیم دو مهره به تصادف از ظرف بیرون بیاوریم شش امکان (۱، ۲)، (۱، ۳)، (۱، ۴)، (۲، ۳)، (۲، ۴) و (۳، ۴) 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 مستقل‌اند؟

پ) اگر در قسمت الف، R برابر یک باشد و در قسمت ب، S همچنان ۵ باشد پیشامدها مستقل‌اند؟

۸- در دو جعبه به ترتیب ۳ و ۲۰ عدد لامپ همانند وجود دارد. در جعبه اول ۵ عدد لامپ

معیوب و در جعبه دوم ۳ عدد لامپ معیوب موجود است. از اولی ۱۰ 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 اینکه این لامپ معیوب باشد چقدر 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 اینکه این مهره سفید باشد چقدر است؟

۱۰- تکمیل بنای راهی ممکن است به دلیل اعتصاب کارگران به تأخیر افتد. فرض کنید احتمال

اینکه اعتصابی رخ دهد ۶۵٪ باشد و احتمال اینکه اگر اعتصابی نباشد کار به موقع انجام شود ۸٪ و

احتمال اینکه اگر اعتصابی باشد کار به موقع انجام شود ۳٪ باشد. احتمال اینکه کار بنای راه به موقع

انجام شود چقدر 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

$$P(B_1 \cap B_2 \cap B_3) = P(B_1)P(B_2|B_1)P(B_3|B_1 \cap B_2)$$

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.

$$P(B_i | A) = \frac{P(A | B_i)P(B_i)}{\sum_{i=1}^3 P(A | B_i)P(B_i)}, \quad i = 1, 2, 3$$

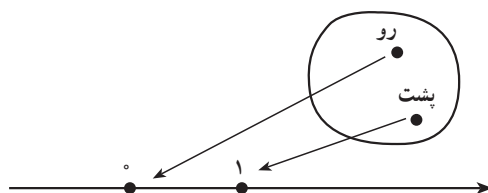
توزیع های گسسته احتمال

۹-۱- متغیر تصادفی گسسته

به طوری که قبلاً گفتیم در هر آزمایش تصادفی، فضای نمونه‌ای را مشخص می‌کنیم و به رخداد هر پیشامد آن عددی بین ۰ و ۱ به عنوان احتمال نسبت می‌دهیم. حال می‌خواهیم مجموعه دیگری را به جای فضای نمونه‌ای قرار دهیم. ابتدا به مثال‌های زیر توجه کنید.

مثال ۱: وقتی سکه‌ای را می‌اندازیم، S دارای دو برآمد رو و پشت است. تابع X را بدین صورت تعریف می‌کنیم که حوزه تعریف (دامنه) آن مجموعه S با دو عضو رو و پشت و حوزه 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 می‌گوییم که دو مقدار ۰ و ۱ را اختیار می‌کند. چون احتمال رخداد برآمد رو $\frac{1}{2}$ است پس $X=0$ که نمایش ساده $X(\text{رو}) = 0$ است و در واقع نمادی برای رخداد برآمد رو است، دارای همان احتمال $\frac{1}{2}$ و همین‌طور احتمال $X=1$ برابر $\frac{1}{2}$ است. در واقع به جای جدول را

	پشت	رو	برآمد
احتمال	$\frac{1}{2}$	$\frac{1}{2}$	

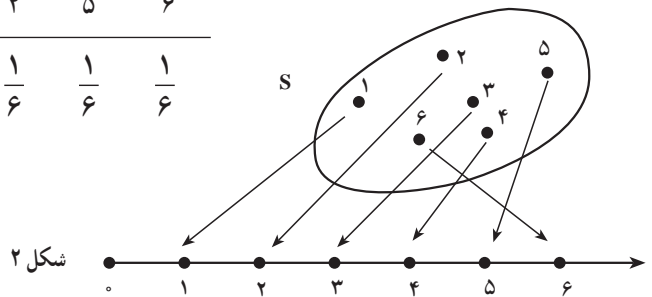
x_i	۰	۱
p_i	$\frac{1}{2}$	$\frac{1}{2}$

جدول

قرار می‌دهیم. x_i ها مقادیر X و p_i ها احتمال‌های متناظر با آنها هستند. توجه کردید که فضای نمونه‌ای، {پشت، رو}، S ، جای خود را به مجموعه $\{0, 1\}$ داده است.

مثال ۲: در انداختن یک تاس همگن مجموعه 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	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$



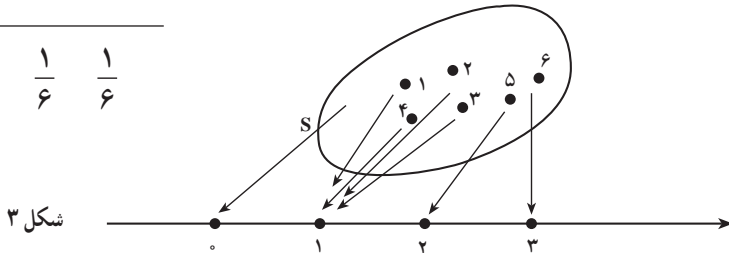
شکل ۲

مثال ۳: بر فضای نمونه‌ای S ، در مثال قبل، می‌توان متغیر تصادفی دیگری را تعریف کرد. تابع X را تابعی بگیرید که شماره‌های ۱، ۲، ۳، و ۴ را با نقطه به طول ۱ و شماره‌های ۵ را با نقطه به طول ۲، و شماره ۶ را با نقطه به طول ۳ از محور اعداد حقیقی متناظر کند (مطابق شکل ۳). در این صورت

$$\begin{cases} X(\text{شماره } 1) = X(\text{شماره } 2) = X(\text{شماره } 3) = X(\text{شماره } 4) = 1 \\ X(\text{شماره } 5) = 2 \\ X(\text{شماره } 6) = 3 \end{cases}$$

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 ۱، شماره ۲، شماره ۳، شماره ۴}، و می دانیم این پیشامد دارای احتمال $\frac{4}{6}$ است. ▲

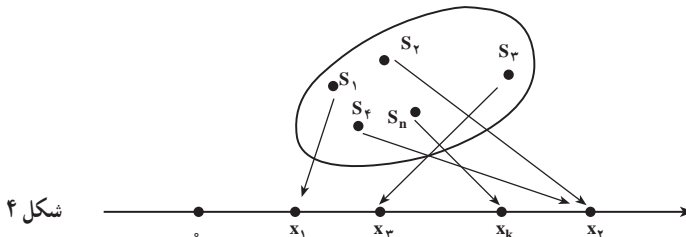
در متغیرهای تصادفی این سه مثال، تعداد مقادیری که هر متغیر اختیار می کرد متناهی بود. متغیر تصادفی را در احتمال مقدماتی به صورت زیر تعریف می کنند:

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 اعداد حقیقی یک فضای نمونه ای جدید است. اگر حوزه مقادیر X متناهی یا شمارا نامتناهی باشد متغیر تصادفی X را گسسته می گوئیم. برای درک مطلب فرض کنید فضای نمونه ای $S = \{s_1, \dots, s_n\}$ را داریم و احتمال هایی که به ترتیب به برآمدها S تخصیص داده ایم p_1, p_2, \dots, p_n باشند. تابعی مانند X را در نظر می گیریم که حوزه تعریف آن S و حوزه 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،

$$X(s_1) = x_1, X(s_2) = x_2, X(s_3) = x_3, X(s_4) = x_4, \dots, X(s_n) = x_k$$

تابع X ، متغیر تصادفی است و x_1, x_2, \dots, x_k مقادیر آن هستند.



شکل ۴

۱- در واقع متغیر تصادفی، نه متغیر است و نه تصادفی است، بلکه یک تابع روی مدل احتمال است.

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 رابطه

$$P(X = x_i) = p_i \text{ و } i = 1, 2, \dots, n$$

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: جامعه کودکان زیر ده سال را در نظر بگیرید. هر کودک را برای اینکه 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 می‌کند. ممکن است اولین نفری که در جامعه مزبور آزمایش می‌شود 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. می‌توانید مجسم کنید که ممکن است یک میلیون کودک آزمایش شوند و کودکی مبتلا پیدا نشود یعنی X می‌تواند بیش از یک میلیون هم باشد. به همین ترتیب مقادیری که X می‌تواند اختیار کند شمارا بوده ولی نامتناهی است. در این حالت داریم

$$P(X = x_i) = p_i \text{ و } i = 1, 2, \dots$$

بدیهی است، $\sum_{i=1}^{\infty} p_i = 1$. یعنی باید احتمال ۱ را بین بی‌نهایت مقدار x_i توزیع کرد. ▲

تذکر: هر تابع احتمال مربوط به متغیر تصادفی گسسته X دارای ویژگی‌های زیر است:

$$0 \leq P(X = x_i) \leq 1, \quad i = 1, 2, \dots \quad -1$$

$$\sum_i P(X = x_i) = 1 \quad \text{—۲}$$

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: سکه‌ای را متوالیاً می‌اندازیم. سکه منصف نیست. تعداد دفعاتی که سکه را می‌اندازیم تا برای اولین بار رو ظاهر شود متغیر تصادفی X می‌نامیم.

الف) X چه مقادیری اختیار می‌کند؟ 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 ۳، ۴، ۵، ...، ۱۰۰۰، ... برای بار اول رو ظاهر نشود، پس X همه مقادیر صحیح طبیعی را اختیار می‌کند.

ب) فرض می‌کنیم در پرتاب i ام برای اولین بار رو بیاید می‌خواهیم 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

$$\underbrace{TT \dots TH}_{\text{بار } (i-1)}$$

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 می‌کنیم 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 محاسبه 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.

$$P(A_1 \cap A_2 \cap \dots) = P(A_1).P(A_2) \dots$$

پس، اگر برای هر انداختن سکه یک فضای نمونه‌ای در نظر بگیریم، آن‌گاه مثلاً

$$P(TT) = q \cdot q = q^2$$

به همین ترتیب :

$$P(\underbrace{TT \dots T}_{\text{بار } (i-1)}) = \underbrace{q \cdot q \dots q}_{\text{بار } (i-1)} = q^{i-1}$$

و بالاخره :

$$P(\underbrace{TT \dots TH}_{\text{بار}(i-1)}) = q^{i-1} \cdot p$$

پس :

$$P(X = i) = q^{i-1} \cdot p$$

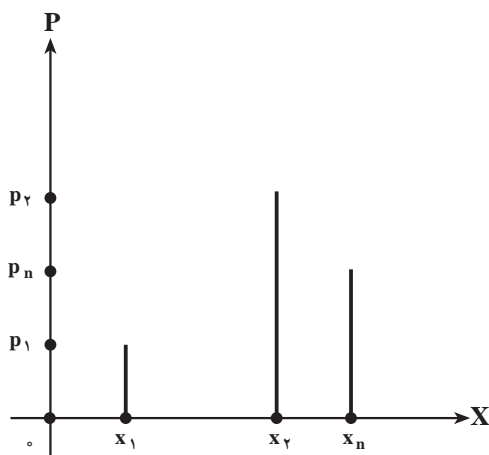
اگر i را برابر $1, 2, \dots$ بگیریم احتمال های متناظر با مقادیر X به دست می آیند. جدول زیر را می توانیم بنویسیم

x_i	۱	۲	۳	...	i	...
p_i	p	qp	q^2p	...	$q^{i-1}p$...

رابطه $P(X = i) = q^{i-1}p$ ، $i = 1, 2, \dots$ تابع احتمال متغیر تصادفی X است. ▲

شما می توانید 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 احتمال هایی دلخواه باشند، فقط لازم است که

مجموع احتمال ها ۱ باشد. اگر هر مقداری را که متغیر تصادفی X اختیار می کند طول یک نقطه، و احتمال متناظر با آن را عرض آن نقطه نسبت به دو محور متعامد بگیریم نموداری برای احتمال X به دست می آوریم. لازم نیست که واحد طول را روی دو محور یکی بگیریم. عرض های نقاط، مقادیر p_1, p_2, \dots 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 آنها 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 می‌کنیم ممکن است سالم باشد یا معیوب. به‌طور کلی وقتی کالایی را در موقع خرید امتحان می‌کنیم یا سالم است و یا ناقص. وقتی از فردی در مورد اعتیادش به سیگار سؤال می‌کنیم یا سیگاری است یا نیست. از این پدیده‌های 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 می‌کند. این آزمایش‌های دو حالت را امتحان می‌نامیم و فضای نمونه‌ای 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

x_i	۰	۱
p_i	q	p

$p + q = 1$

مرسوم است که دو برآمد امتحان را پیروزی و شکست می‌نامند. برآمدی که مورد توجه است پیروزی نامیده می‌شود. 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 می‌توان به صورت رابطه زیر هم خلاصه کرد.

$$P(X=i) = \begin{cases} p^i q^{1-i} & i=0,1 \\ 0 & \text{به ازای سایر مقادیر } i \end{cases}$$

به‌طور کلی اگر پیشامد A از یک فضای نمونه‌ای را در نظر بگیریم و رخداد A را پیروزی گرفته، احتمال پیروزی را p فرض کنیم، آن‌گاه 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 می‌شود دارای تابع احتمال بالاست.

متغیر تصادفی X را که تنها دو مقدار ۰ و ۱ را می‌پذیرد متغیر برنولی و توزیع احتمال آن را توزیع برنولی می‌گویند.

۹-۴- تمرین‌ها

۱- پنج سکهٔ منصف را باهم پرتاب می‌کنیم.

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 می‌کنیم. متغیر تصادفی X را مجموع دو عدد ظاهر شده در روی دو

تاس تعریف می‌کنیم.

الف) فضای نمونه‌ای این آزمایش را بنویسید.

ب) تابع احتمال X را به دست آورید.

پ) احتمال اینکه $X \leq 7$ باشد چقدر است؟

۳- یک تاس پرتاب می‌کنیم. متغیر تصادفی X را به صورت زیر تعریف می‌کنیم.

$$X = \begin{cases} 1 & \text{اگر عدد فرد بیاید} \\ 2 & \text{اگر عدد زوج بیاید} \end{cases}$$

الف) تابع احتمال X را بیایید.

ب) آیا X یک متغیر تصادفی برنولی است؟

۴- سکه‌ای منصف را آن قدر پرتاب می‌کنیم تا «شیر» بیاید.

الف) فضای نمونه‌ای این آزمایش را بنویسید.

ب) یک متغیر تصادفی تعریف کنید که براساس آن بتوان احتمال شیر آمدن را محاسبه کرد.

پ) احتمال اینکه اولین بار در آزمایش صدم، شیر ظاهر شود چقدر است؟

۵- توزیع احتمال متغیر تصادفی X به صورت زیر مشخص می‌شود.

$$P(X=i) = \frac{i}{i^2 + 3} \quad i = 1, 2, 3$$

$$P(X=j) = \frac{1}{14} \quad j = 4, 5, 6$$

الف) جدول توزیع X را بسازید.

ب) نمودار توزیع را رسم کنید.

پ) مقدار $P(X \geq 3)$ را حساب کنید.

۶- احتمال اینکه فردی مسن مبتلا به دیابت باشد $\frac{1}{8}$ است. در روستایی مردان مسن را تحت آزمایش قرار می‌دهند. اگر متغیر تصادفی X را برابر با تعداد افرادی تعریف کنیم که به ترتیب آزمایش می‌شوند تا اولین فرد دیابتی مشخص شود، تابع احتمال متغیر X را به دست آورید. احتمال اینکه دومین نفر دیابتی باشد چقدر است؟

۷- فضای نمونه‌ای یک آزمایش تصادفی ۳ برآمد دارد. اگر احتمال‌های متناظر با ۳ برآمد به ترتیب $\frac{1}{6}$ ، $\frac{1}{2}$ و $\frac{1}{3}$ باشد، متغیری تصادفی روی این فضا تعریف کنید.

۸- نشان دهید که تابع زیر یک تابع احتمال است.

$$P(X = x) = \frac{1}{n} [2(n - x) + 1] \quad , \quad x = 1, 2, \dots, n$$

مراجع

1 - S. Ross, A First Course in Probability, Macmilan 1976.

- ۲- جان فروند و رانلد والپول، آمار ریاضی ترجمه 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.



معلمان محترم، صاحب نظران، دانش آموزان عزیز و اولیای آنان می توانند نظر اصلاحی خود را درباره مطالب

این کتاب از طریق نامه به نشانی تهران - صندوق پستی ۴۶۳، ۱۵۸۵۵ - گروه درسی مربوط و یا پیام نگار (Email)

ارسال نمایند. talif@talif.sch.ir

دفتر تألیف کتاب های درسی ابتدایی و متوسطه نظری