



فصلنامه علمی المپیاد ریاضی

سال چهارم، شماره شانزدهم، زمستان ۱۴۰۳

فصلنامه علمی المپیاد ریاضی

پرگار ۱

فصل نامه کمیته علمی المپیاد ریاضی ایران

سال چهارم، شماره شانزدهم، زمستان ۱۴۰۳

صاحب امتیاز: کمیته علمی المپیاد ریاضی ایران

فهرست

آ مطالب این شماره

سرمقاله

۱ سردبیر

رمزنگاری و نظریه اعداد

۲ علی پرتوفرد

تابع نسبت

۷ محمدرضا عطارانزاده

اریاب چند جمله ای ها

۱۸ علی نظربلند، آروین طاهری

نگاهی موزون به نامساوی

۲۶ مهدی یار عمید سرداری

روش های احتمالاتی

۳۲ علی پرتوفرد

زیگموندی

۴۱ رادان محسنی

مسائل کولموگروف

۵۱ تحریریه پرگار

داستان سه سوال!

۵۵ تحریریه پرگار

تحریریه:

مهدی یار عمید سرداری

علی پرتوفرد

آروین طاهری

رادان محسنی

علی نظربلند

پارسیا تجلایی

محمدرضا عطارانزاده

همکاران این شماره:

علیرضا جنتی

حسام رجبزاده

امیرحسین محمدزاده

شایان طایفه

سپهر علیپور

امیرحسین زارعی

مهراد حصاری

رایان اسدی

نوید صفایی

ویراستاران:

علی پرتوفرد

آروین طاهری

متین غیائی

صفحه بندی:

حسن نوروزی

طرح روی جلد:

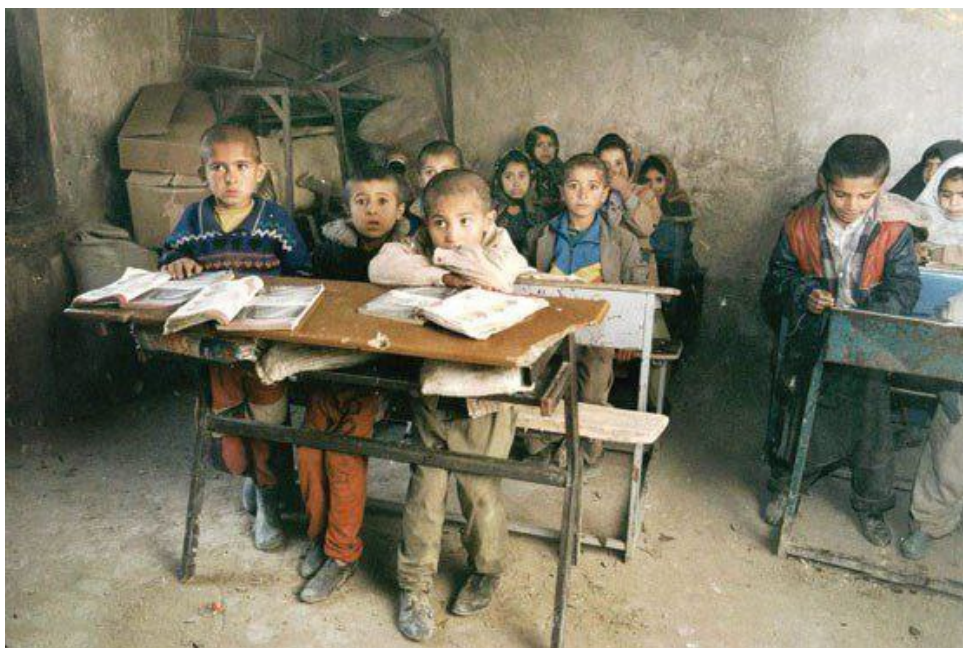
احسان عرب

وبگاه:

MathYSC.com/

رایانامه:

pargarmagazine@gmail.com



تقدیم به تمام دانش‌آموزانی

که شوق تدریس را

در معلم‌هایشان زنده نگاه می‌دارند...

سرمقاله

از تفریحات جوانی من قدم زدن در قفسه کتاب‌های ریاضی انتشارات خوارزمی و نگاه کردن به کتاب‌های ریاضی تازه چاپ‌شده بود. امروز که به این انتشارات رفتم تا دو تا از کتاب‌های مورد علاقه خود را برای هدیه دادن به شاگردانم بخرم دیدم که نه تنها کتاب ریاضی جدیدی در کتاب‌فروشی نیست بلکه کتاب‌های قبلی هم دیگر چاپ نمی‌شوند و در بازار موجود نیستند، به جای آن می‌توانید از کتاب‌فروشی ماگ و اشیای رنگارنگ و پرزرق و برق بخرید!

در روزگاری هستیم که علم جایگاه خود را به عنوان یک ارزش از دست داده است، ابتذال به افتخار تبدیل شده، بعضی از قهرمانان نسل ما که مشوق ما به ریاضیات بودند امروز پشیمان یا خموده‌اند، ریاضیات حتی در دانشکده‌های ریاضی غریبه و سربار محسوب می‌شود و هوش مصنوعی بسیاری از مشاغلی که به طور سنتی باعث توجه به ریاضی در سیاست‌گذاری و جامعه بود را تهدید می‌کند، آیا زمان مرگ ریاضیات فرا رسیده است؟

به نظر نگارنده ریاضیات زنده است تا وقتی که شعر، عشق، حق‌طلبی، زیبایی و انسانیت زنده باشند، تا زمانی که صفا و سادگی در مقابل تجمل و تفاخر خریداری داشته باشد. این‌ها مفاهیمی هستند که از عمق وجود انسان‌ها سرچشمه می‌گیرند و لزوماً نیاز به سیستم و امکانات برای بروز ندارند، تا زمانی که ریاضیات می‌تواند افرادی که هیچ وجه مشترک دیگری ندارند را به هم پیوند دهد، تا زمانی که کودکانی وجود دارند که از دیدن زیبایی ریاضی نعره شوق می‌زنند، تا زمانی که دو نفر در قطار و مترو و تاکسی برای استفاده از زمان باطلشان با هم به یک سوال جالب ریاضی فکر می‌کنند و تا زمانی که انسانی وجود داشته باشد که به یک مساله ریاضی فکر کند تنها به این دلیل که برای دانستن جواب آن کنجکاو است ریاضیات زنده است.

هرگز نمیرد آن که دلش زنده شد به عشق ثبت است بر جریده عالم دوام ما



رمزنگاری و نظریه اعداد

۱.۲ روش‌های رمزنگاری

به طور سنتی نظریه اعداد از خالص‌ترین شاخه‌های ریاضی به شمار می‌آمد، به این معنا که به ظاهر ارتباطی با دنیای مادی نداشت و تنها به خاطر زیبایی ذاتی و کنجکاوی مطالعه می‌شد. ریاضیدان انگلیسی، هاردی ادعا می‌کرد به خاطر این که به نظریه اعداد علاقه‌مند است که هیچ کاربردی ندارد.

با این حال یکی از شگفتی‌های ریاضی کارآمدی عجیب آن در دنیای واقعی است، هر مفهومی در ریاضیات هر چقدر مجرد و تصادفی به نظر برسد دیر یا زود مستقیم یا غیر مستقیم به جهان مادی مرتبط می‌شود. از حدود صد سال پیش هم سروکله بازیگران مهم نظریه اعداد در سایر علوم و فناوری‌ها پیدا شد.

یکی از این فناوری‌ها رمزنگاری است. هدف اصلی رمزنگاری تضمین کردن ایمنی ارتباط است، شخص الف قصد ارسال پیامی به شخص ب را دارد او این پیام را رمز کرده و برای شخص ب می‌فرستد تا او به وسیله کلیدی که در اختیار دارد پیام را رمزگشایی کند، هدف این است که اشخاص غیر نتوانند در این بین به پیام پی ببرند. اولین روش‌های رمزنگاری روش‌های رمزنگاری متقارن بودند. رمزنگاری متقارن بدین معناست کلید رمزنگاری و رمزگشایی یکسان هستند و دو طرف باید از قبل کلید رمزنگاری را بین خود مشخص کنند. یک روش ساده رمزنگاری متقارن توسط سزار پادشاه رم استفاده می‌شد، روش بدین صورت بود که ابتدا به حروف الفبا به چشم اعدادی به پیمانه ۲۶ نگاه کنید سپس همه اعداد را سه واحد شیف‌ت دهید و پیام را بازنویسی کنید.

مثلاً ممکن بود سزار پیامی به فرمانده‌اش بفرستد:

زش شاصپ مب هتب متهو هیطاز جب نوپ بت ذهوب میپز

اگر پیک در بین مسیر به دست دشمن اسیر می‌شد، پیام به نظر بی‌معنی جلوه می‌کرد اما فرمانده که از کلید آگاه بود پیام را این گونه معنا می‌کرد:

در روزی که ماه کامل می‌شود به دشمن حمله کنید.

اشکال این روش ساده رمزنگاری این است که حتی بدون دانستن کلید هم قابل شکستن است، خوب است فکر کنید که چگونه می‌توانستید پیام بالا را بدون داشتن کلید بشکنید. این مشکل یک موقعیت فرضی نیست، یکی از دلایل شکست آلمان در جنگ‌های جهانی این بود که در هر دو جنگ رمزنگاری مورد استفاده آلمان توسط ریاضیدانانی که برای متفکین کار می‌کردند شکسته شد.

روش‌های رمزنگاری متقارن هوشمندانه‌تری وجود دارند که این ایراد را ندارند، با این حال همه روش‌های رمزنگاری متقارن یک ایراد ذاتی دارند، کلید باید قبلاً به نحوی بین فرستنده و گیرنده پیام مخابره شده باشد.

در سال ۱۹۷۶ دیف و هلمن مفهوم انقلابی کلید عمومی رمزنگاری را معرفی کردند. بدین معنا که کلید رمزنگاری در اختیار عموم قرار دارد تا با آن پیام‌های خود را رمز کنند اما تنها دریافت‌کنندگان مجاز کلید رمزگشایی را دارند و می‌توانند به محتوای این پیام‌ها دست یابند. تقریباً تمام دنیای اینترنت از تراکشن‌های بانکی گرفته تا سیستم ورود به سایت‌های مختلف با رمز عبور و نام کاربری بر این شیوه رمزنگاری استوار شده‌اند. اما چطور می‌توان سیستمی طراحی کرد که کلید



شکل ۱. انگیم، ماشین رمزنگاری آلمان‌ها

رمزنگاری و رمزگشایی آن متفاوت باشد؟ خوب است خودتان کمی به این سوال فکر کنید. می‌خواهیم یک روش برای این کار معرفی کنیم که روش رمزنگاری RSA نام دارد:

گام اول: امین دو عدد اول بزرگ p, q را انتخاب می‌کند و $n = pq$ را محاسبه می‌کند.

گام دوم: امین عدد e را که نسبت به $\phi(n)$ اول باشد انتخاب کرده و زوج (n, e) را به عنوان کلید عمومی منتشر می‌کند.

گام سوم: وارون ضربی e به پیمانه $\phi(n)$ را محاسبه می‌کند، آن را d می‌نامد و زوج (n, d) را به عنوان کلید اختصاصی نزد خود نگه می‌دارد.

از نظر عملی روش‌های به نسبت سریعی برای چک کردن اول بودن یک عدد موجودند که در مقاله‌ای دیگر به آن‌ها خواهیم پرداخت. به کمک این روش‌ها می‌توان اعداد اول بزرگی پیدا کرد که توسط امین مورد استفاده قرار گیرند. حال بابک می‌خواهد پیامی رمزی به امین بفرستد. او ابتدا پیامش را به صورت یک عدد x به پیمانه n کد می‌کند و سپس y یعنی باقی‌مانده x^e بر n را برای امین می‌فرستد. از آن جا که طبق قضیه اویلر $x^{ed} \equiv x \pmod{n}$ ، امین برای این که به محتوای واقعی پیام پی ببرد کافی است y^d را به پیمانه n محاسبه کند. روش‌های نسبتاً سریعی برای این کار وجود دارند. حال فرض کنید شما در میانه راه به پیام بابک به امین دست یافته‌اید و قصد دارید به محتوای پیام پی ببرید. در واقع شما باید x را پیدا کنید که در معادله $x^e \equiv y \pmod{n}$ صدق می‌کند. به این مساله مساله لگاریتم گسسته می‌گویند.

ساده‌ترین راهی که برای حل این معادله به نظر می‌رسد این است که $\phi(n)$ و سپس d را محاسبه کنیم، اما چگونه می‌توان $\phi(n)$ را محاسبه کرد؟ اگر بخواهیم از تعریف استفاده کنیم باید بزرگترین مقسوم‌علیه مشترک تمام اعداد کوچکتر از n را با n محاسبه کنیم، این کار به تعداد محاسبات بسیار زیادی نیاز دارد که اگر n به اندازه کافی بزرگ باشد از توان کامپیوترهای امروزی خارج است. ایده دیگر استفاده از فرمول $\phi(n)$ است، اگر p, q را داشتیم سریعاً می‌توانستیم $\phi(n) = (p-1)(q-1)$ را محاسبه کنیم اما امین p, q را به طور عمومی منتشر نکرده پس برای یافتن آن‌ها باید n را تجزیه کنیم اما تا کنون هیچ راه سریعی برای این کار پیدا نشده است.

مساله جالب دیگری که در رمزنگاری مطرح می‌شود مساله امضای دیجیتال است. در بسیاری از موارد، فرستنده پیام باید بتواند هویت خود را به گیرنده ثابت کند، برای این کار فرد فرستنده، پیام شبیه بالا یک کلید رمزنگاری تولید می‌کند و کلید عمومی (n, e) را منتشر می‌کند. حال هر گاه بخواهد پیام m را ارسال کند ابتدا σ یعنی باقی‌مانده m^d به پیمانه n محاسبه می‌کند و سپس دو تایی (m, σ) را ارسال می‌کند. امین برای این که مطمئن شود این پیام توسط بابک فرستاده شده چک می‌کند که $m \equiv \sigma^e \pmod{n}$ هست یا نه.

۲.۲ یک روش حمله

آیا راهی به جز چک کردن همه حالات برای شکستن این شیوه رمزنگاری به ذهن شما می‌رسد؟ خوب است کمی به این موضوع فکر کنید.

اعداد طبیعی ساختاری دارند که باعث می‌شود حل مساله لگاریتم گسسته برای آن‌ها کمی ساده‌تر از این مساله در حالت کلی باشد: یکتایی تجزیه.

این کار چه طور می‌تواند به ما برای حل مساله کمک کند؟ ابتدا توجه کنید که بنابر قضیه باقی‌مانده چینی برای حل مساله لگاریتم گسسته به پیمانه n کافی است این مساله را برای توان‌های اعداد اول حل کنیم. هم‌چنین از آن جا که به پیمانه توان اعداد اول ریشه اولیه وجود دارد کافی است مساله لگاریتم گسسته در پایه ریشه اولیه g را حل کنیم.

برای این کار ابتدا مجموعه B از اعداد اول را انتخاب می‌کنیم، ابتدا می‌خواهیم لگاریتم این اعداد را بیابیم. سعی می‌کنیم توان‌هایی از g پیدا کنیم که تمام عوامل اولشان عضو B باشد، بدین صورت یک رابطه بین لگاریتم اعضای B بدست می‌آوریم، این کار را آن قدر تکرار می‌کنیم تا با حل دستگاه معادلات خطی حاصل بتوان لگاریتم اعضای B را محاسبه کرد. حال برای محاسبه لگاریتم عنصر دلخواه h شروع به ضرب توان‌های g در h می‌کنیم تا عددی بیابیم که تمام عوامل اول آن در B باشد و به کمک لگاریتم اعضای B ، لگاریتم h را محاسبه می‌کنیم.

مثال. فرض کنید می‌خواهیم لگاریتم گسسته ۳۷ را نسبت به $(۳, ۱۲۱۷)$ محاسبه کنیم. ابتدا $B = \{۲, ۳, ۵, ۷, ۱۱, ۱۳\}$ را تشکیل می‌دهیم و مشاهده می‌کنیم:

$$۳^{۶۰۸} \equiv -۱, ۳^۱ \equiv ۳, ۳^{۲۴} \equiv -۲ \cdot ۷ \cdot ۱۳, ۳^{۲۵} \equiv ۵^۲ \pmod{۱۲۱۷}$$

$$۳^{۳۰} \equiv -۲ \cdot ۵^۲, ۳^{۵۴} \equiv -۵ \cdot ۱۱, ۳^{۸۷} \equiv ۱۳$$

از این تساوی‌ها دستگاه معادلات زیر به پیمانه ۱۲۱۶ بدست می‌آید:

$$۱ \equiv L(۳), ۲۴ \equiv ۶۰۸ + ۲L(۲) + L(۷) + L(۳), ۲۵ \equiv ۳L(۵), ۳۰ \equiv ۶۰۸ + L(۲) + ۲L(۵)$$

$$۵۴ \equiv ۶۰۸ + L(۵) + L(۱۱), ۸۷ \equiv L(۱۳)$$

با حل این معادلات به دست می‌آوریم:

$$L(۳) \equiv ۱, L(۱۳) \equiv ۸۷, L(۲) \equiv ۲۱۶, L(۱۱) \equiv ۱۰۵۹, L(۷) \equiv ۱۱۳$$

حال داریم:

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11$$

بنابراین خواهیم داشت:

$$L(37) \equiv 3L(2) + L(7) + L(11) \equiv 588 \pmod{1216}$$

ثابت می‌شود که زمان اجرای این الگوریتم تقریباً $\sqrt{2 \ln p \ln \ln p}$ می‌باشد. این زمان برای p های به اندازه کافی بزرگ طولانی است، اما بازیگرانی در نظریه اعداد وجود دارند که حل مساله مشابه در مورد آن‌ها حتی از این زمان هم بیشتر طول می‌کشد و بنابراین می‌توان با طول کلید کوتاه‌تری همان امنیت را بدست آورد.

۳.۲ خم‌های بیضوی

تعریف ۱.۳.۲

یک خم بیضوی E معادله‌ای به شکل $y^2 = f(x)$ است که f ریشه مضاعف نداشته باشد. منظور از نقاط این خم بیضوی روی

$$\mathbb{R}, \mathbb{Q}, \mathbb{Z}, F_p$$

جواب‌های این معادله در هر یک از این مجموعه‌هاست (منظور از F_p اعداد به پیمانه p هستند). اگر اعداد دو و سه در دنیایی که به آن علاقمندیم وارون‌پذیر باشند می‌توان معادله بالا را با تغییر متغیر به فرم $y^2 = x^3 + Ax + B$ درآورد که به آن صورت وایراستراس می‌گویند.

ساختار مهمی که باعث اهمیت خم‌های بیضوی می‌شود عمل جمع روی خم بیضوی است. به طور هندسی اگر x, y دو نقطه روی خم بیضوی باشند و l خط واصل این دو نقطه باشد، این خط خم بیضوی را در یک نقطه دیگر هم قطع می‌کند چرا که معادله خم بیضوی درجه سه است. این نقطه را $x \odot y$ می‌نامیم. قرینه $x \odot y$ نسبت به محور طول‌ها را جمع x, y روی این خم بیضوی تعریف می‌کنیم و آن را با $x + y$ نشان می‌دهیم. می‌توان نشان داد که این عمل جمع جابجایی و شرکت‌پذیر است. هم‌چنین نقطه ∞ عضو خنثی این عمل و قرینه کردن نسبت به محور طول‌ها قرینه کردن نسبت به این عمل را به ما می‌دهند. بنابراین عمل تعریف شده اصطلاحاً خم بیضوی را به یک گروه تبدیل می‌کند.

به راحتی می‌توان معادله این عمل را هم بدست آورد. اگر $a = (x_1, y_1)$ ، $b = (x_2, y_2)$ و $a + b = (x_3, y_3)$ باشد و

$$m = \frac{y_1 - y_2}{x_1 - x_2}$$

داریم:

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_2) - y_1$$

مزیت کار کردن به پیمانه p این است که تنها متناهی نقطه خواهیم داشت. حال می‌توان مساله لگاریتم گسسته را روی این نقاط مطرح کرد، فرض کنید می‌دانیم $Q = aP$ یعنی نقطه Q از a بار جمع کردن نقطه P با خودش بدست آمده،

چطور با داشتن P, Q عدد a را پیدا کنیم. اگر خم بیضوی، پیمانه و نقطه P به درستی انتخاب شوند تمام روش‌های فعلی برای حل این مساله نمایی هستند و بنابراین بسیار کند خواهند بود. این مساله پایه یک روش مبادله کلید است که به روش دیفل-هلمن معروف است. می‌توان از این روش برای توافق امن روی یک کلید برای یک روش ایمن رمزنگای متقارن استفاده کرد.

گام اول: امین ابتدا خم بیضوی E ، عدد اول p و نقطه P از خم E در F_p را برای علی می‌فرستد.

گام دوم: علی عدد مخفی a را انتخاب می‌کند و عدد aP را برای امین می‌فرستد.

گام سوم: امین عدد مخفی b را انتخاب می‌کند و مقدار bP را برای علی می‌فرستد.

گام چهارم: اکنون هر دوی علی و امین قادر هستند مقدار abP را محاسبه کنند، از این مقدار به عنوان کلید مشترک بین خودشان استفاده خواهند کرد.

خوب است کمی فکر کنید چرا کس دیگری با شنود aP, bP نمی‌تواند به راحتی کلید مشترک را بدست آورد.

۴.۲ رمزنگاری در عصر کوانتوم

در دهه نود میلادی، پیتر شور الگوریتمی ارایه داد که در صورت ساخت یک کامپیوتر فرضی کوانتومی قابلیت شکستن روش‌های بالا را در زمان بسیار سریعی دارد. از ابتدا اختلاف نظرهای زیادی در مورد امکان‌پذیر بودن ساخت کامپیوتر کوانتومی وجود داشت، با این حال به تازگی پیشرفت‌های مهمی در ساخت نمونه‌های کوچک چنین کامپیوتری صورت گرفته است و انتظار می‌رود تا بیست سال دیگر ساخت کامپیوتر کوانتومی امکان‌پذیر باشد. بنابراین نیاز است از هم‌اکنون به دنبال روش‌های جدیدی برای رمزنگاری باشیم. به این روش‌های رمزنگاری روش‌های پساکوانتومی می‌گویند. دست بر قضا نظریه اعداد حتی نقش مهم‌تر و زیباتری در این دنیا ایفا می‌کند که از حوصله این مقاله خارج است.



تابع نسبت

۱.۳ مقدمه

فرض کنید نقاط متفاوت B, C در صفحه داده شده‌اند. تابع $f: \mathbb{R}^2 - \{B, C\} \rightarrow \mathbb{R}$ را مطابق زیر تعریف می‌کنیم.

$$f(X) = \begin{cases} -\left(\frac{XB}{XC}\right) & \text{داخل پاره خط } BC \text{ یا بالای خط } BC \text{ باشد.} \\ +\left(\frac{XB}{XC}\right) & \text{روی خط } BC \text{ اما خارج پاره خط } BC \text{ یا زیر خط } BC \text{ باشد.} \end{cases}$$

اگر کمی دقت کنید متوجه می‌شوید که قبلاً هم با این تابع سروکار داشته‌اید. مثلاً اگر نقطه A خارج خط BC و نقطه D داخل پاره خط BC را در نظر بگیرید، آنگاه D پای نیمساز زاویه BAC است اگر و تنها اگر $|f(D)| = |f(A)|$. (این گزاره معادل قضیه نیمساز است.) یا اگر نقاط X, Y را طوری در نظر بگیرید که B, C, X, Y هم دایره باشند آنگاه $XY \parallel BC$ اگر و تنها اگر $f(X)f(Y) = +1$. اما داستان زمانی جالبتر می‌شود که بدانیم لم‌های زیر در مورد تابع نسبت برقرار هستند.

۲.۳ لم‌ها

لم ۱.۲.۳ (لم نسبت)

نقاط B, C و دایره ω گذرا از B, C مفروض هستند. نقاط X, Y روی ω و نقطه Z روی خط BC قرار دارند. در این صورت X, Y, Z همخط هستند اگر و تنها اگر

$$f(Z) = f(X)f(Y).$$

لم ۲.۲.۳ (لم نسبت دایره متقاطع با BC)

نقاط B, C و دایره ω گذرا از B, C در صفحه مفروض هستند. نقاط X, Y روی ω و نقاط Z, T روی خط BC قرار دارند. در این صورت چهارضلعی $XYZT$ محاطی است اگر و تنها اگر

$$f(X)f(Y) = f(Z)f(T).$$

لم ۳.۲.۳ (لم نسبت میشل)

دوایر Ω و ω در نقاط A و M برخورد می کنند. خط ℓ_1 که از A می گذرد دوایر Ω و ω را در B و E قطع می کند. خط ℓ_2 که از A می گذرد دوایر Ω و ω را در C و F قطع می کند. در این صورت تساوی زیر برقرار است.

$$f(M) = \frac{EB}{FC}$$

برای خواندن اثبات این لم ها و حل مسائل بیشتر می توانید از منبع ۱ استفاده کنید. در این مقاله قصد داریم لم ها و مسائلی را بررسی کنیم که ایده هایی جدیدتر و کم تر شناخته شده در مورد تابع نسبت را استفاده می کنند.

لم ۴.۲.۳ (لم نسبت حالت کلی)

دو نقطه B, C در صفحه داریم. برای نقاط X, Y, Z در صفحه که $Z = XY \cap BC$ رابطه زیر برقرار است

$$f(Z) = f(X)f(Y) \cdot \frac{\sin XBY}{\sin XCY}$$

لم ۵.۲.۳ (لم نسبت دایره حالت کلی)

مثلث ABC و نقاط $X, Y \neq A, B, C$ در صفحه مفروض هستند. دایره محیطی مثلث AXY دایره محیطی مثلث ABC را برای بار دوم در Z قطع می کند. در این صورت تساوی زیر برقرار است.

$$f(Z) = \frac{f(X)f(Y)}{f(A)} \cdot \left| \frac{\sin(AXB - AYB)}{\sin(AXC - AYC)} \right|$$

لم ۶.۲.۳ (لم تغییر مبنای تابع نسبت)

فرض کنید نقاط A, B, C با همین ترتیب در جهت پادساعتگرد روی دایره ω قرار دارند. تعریف می کنیم

$$f_{B,C}(X) = \begin{cases} +(\frac{XB}{XC}) & \text{نقاط } A, X \text{ در یک طرف خط } BC \text{ باشند.} \\ -(\frac{XB}{XC}) & \text{نقاط } A, X \text{ در دو طرف خط } BC \text{ باشند.} \end{cases}$$

$$f_{A,C}(X) = \begin{cases} +(\frac{XA}{XC}) & \text{نقاط } B, X \text{ در یک طرف خط } AC \text{ باشند.} \\ -(\frac{XB}{XC}) & \text{نقاط } B, X \text{ در دو طرف خط } AC \text{ باشند.} \end{cases}$$

در این صورت برای هر نقطه دلخواه X روی ω خواهیم داشت

$$ACf_{B,C}(X) + BCf_{A,C}(X) = AB.$$

راه حل. کافیت قضیه بطلمیوس را برای چهارضلعی $ABCX$ بنویسید، سپس دو طرف تساوی را بر XC تقسیم کنید.

لم ۷.۲.۳ (لم همرسی ۳ خط حالت کلی)

نقاط B, C و دایره ω گذرا از B, C در صفحه مفروض هستند. نقاط $X_1, X_2, Y_1, Y_2, Z_1, Z_2$ نیز روی ω قرار دارند. در این صورت خطوط X_1X_2, Y_1Y_2, Z_1Z_2 هم‌رس هستند اگر و تنها اگر

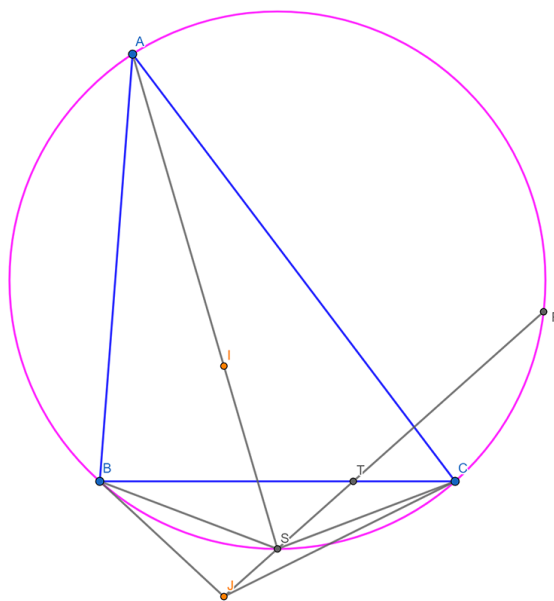
$$\begin{vmatrix} f(X_\downarrow)f(X_\uparrow) & f(X_\downarrow) + f(X_\uparrow) & 1 \\ f(Y_\downarrow)f(Y_\uparrow) & f(Y_\downarrow) + f(Y_\uparrow) & 1 \\ f(Z_\downarrow)f(Z_\uparrow) & f(Z_\downarrow) + f(Z_\uparrow) & 1 \end{vmatrix} = 0.$$

۳.۳ سوالات

مساله ۱.۳.۳ (مجله KOMAL سال ۲۰۱۷/۲۰۱۸)

در مثلث ABC ، I مرکز دایره محاطی داخلی است. خط AI دایره محیطی مثلث را در $A \neq S$ قطع می‌کند. قرینه I نسبت به خط BC را J می‌نامیم. خط SJ دایره محیطی مثلث را برای بار دوم در P قطع می‌کند. نشان دهید $AI = IP$.

راه حل. دایره به مرکز I و شعاع AI را ω می‌نامیم. فرض کنید ω دایره محیطی مثلث را برای بار دوم در Q قطع کند، کافیسث نشان دهیم $f(P) = f(Q)$ در این صورت ثابت می‌شود P بر Q منطبق است و حکم ثابت می‌شود. طبق لم‌های

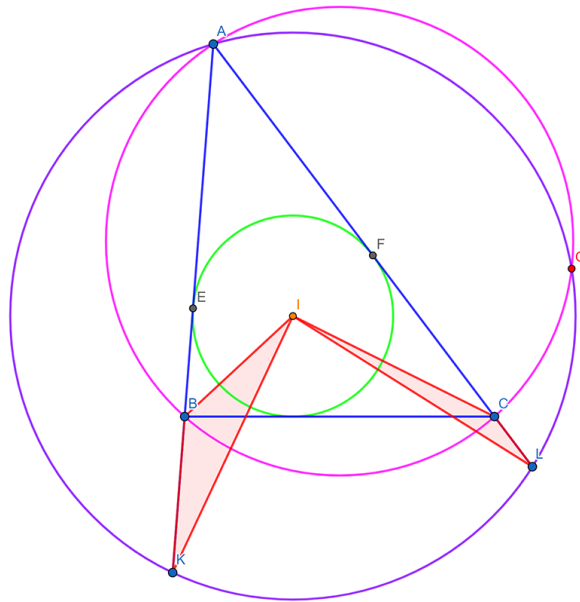


شکل ۱

تابع نسبت داریم

$$f(P) = f(J) \cdot \frac{\sin JBS}{\sin JCS} = \frac{\sin \frac{C}{\gamma}}{\sin \frac{B}{\gamma}} \cdot \frac{\sin \frac{B-A}{\gamma}}{\sin \frac{C-A}{\gamma}}$$

حال فرض کنید w خطوط AB و AC را برای بار دوم در نقاط K و L قطع کند. طبق لم نسبت میشل خواهیم داشت



شکل ۲

$$f(Q) = \frac{KB}{LC}$$

با استفاده از قضیه سینوس ها در مثلث های IBK و ICL می توانیم نسبت $\frac{KB}{LC}$ را هم محاسبه کنیم و حکم را ثابت کنیم.

مساله ۲۰۳.۳ (انتخاب تیم تایوان ۲۰۲۳)

مثلث ABC در صفحه مفروض است. I_A مرکز دایره محاطی خارجی نظیر A و D پای عمود I_A بر BC هستند. M وسط پاره خط I_AD است و نقطه T روی کمان کوچک BC از دایره محیطی مثلث طوری قرار دارد که $\angle BAT = \angle CAD$. خط I_AT دایره محیطی مثلث را برای بار دوم در S قطع می کند. تقاطع SM و BC را X می نامیم. اگر عمود منصف پاره خط AD اضلاع AB, AC را به ترتیب در E, F قطع کند نشان دهید خطوط AX, BE, CF همرس هستند.

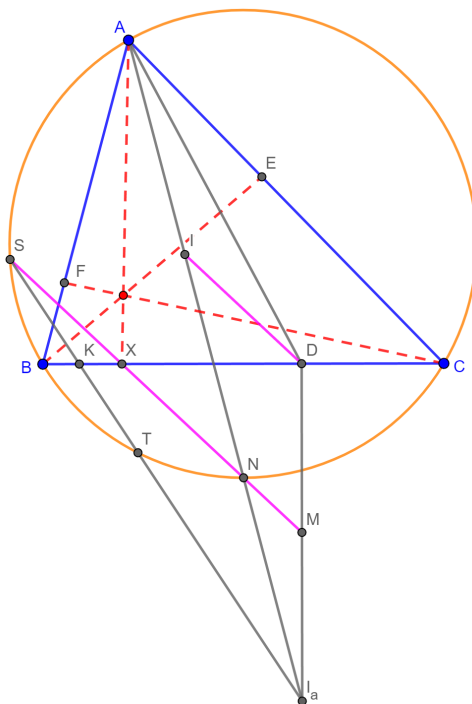
لم ۱۰۳.۳

M, N, S همخط هستند.

کافیست ثابت کنیم $\angle ANM = 180^\circ - \angle ANS$.

$$180^\circ - \angle ANS = 180^\circ - \angle ATS = \angle ATI_a$$

$$NI = NI_a \Rightarrow NM \parallel ID \Rightarrow \angle ANM = \angle AID$$



شکل ۳

پس کافیت ثابت کنیم $\angle ATI_a = \angle AID$. اما مثلث‌های ATI_a و AID متشابه هستند (چرا؟) که اثبات لم را کامل می‌کند.

حال به مسئله اصلی برمیگردیم. حکم را با استفاده از قضیه سوا ثابت می‌کنیم.

$$\frac{\sin(\angle ABE)}{\sin(\angle CBE)} = \frac{AE}{DE} \cdot \frac{\sin(A)}{\sin(\angle EDB)} = \frac{\sin(A)}{\sin(C + 2\gamma)}$$

$$\frac{\sin(\angle BCF)}{\sin(\angle ACF)} = \frac{FD}{AF} \cdot \frac{\sin(B + 2\beta)}{\sin(A)}$$

$$f(X) = f(N)f(S) = f(S) = \frac{f(K)}{f(T)} = \frac{f(T)f(I_a) \frac{\sin(\angle TBI_a)}{\sin(\angle TCI_a)}}{f(T)} = \frac{\cos(\frac{C}{\gamma})}{\cos(\frac{B}{\gamma})} \cdot \frac{\cos(\beta + \frac{B}{\gamma})}{\cos(\gamma + \frac{C}{\gamma})}$$

از رابطه آخر و لم کلید نتیجه می‌گیریم

$$\frac{\sin(\angle BAX)}{\sin(\angle CAX)} = \left(\frac{\cos(\frac{C}{\gamma})}{\cos(\frac{B}{\gamma})} \cdot \frac{\cos(\beta + \frac{B}{\gamma})}{\cos(\gamma + \frac{C}{\gamma})} \right) \frac{\sin(B)}{\sin(C)} = \frac{\sin(\frac{B}{\gamma}) \cos(\beta + \frac{B}{\gamma})}{\sin(\frac{C}{\gamma}) \cos(\gamma + \frac{C}{\gamma})}$$

در نهایت با توجه به روابط بالا نتیجه می‌شود برای اثبات حکم باید تساوی زیر را اثبات کنیم.

$$\frac{\sin(\frac{C}{\gamma})}{\sin(\frac{B}{\gamma})} = \frac{\sin(\gamma + \frac{C}{\gamma})}{\sin(\beta + \frac{B}{\gamma})}$$

فرض کنید L وسط ضلع BC باشد. می‌دانیم $IL \parallel AD$ که نتیجه می‌دهد

$$\angle LIC = \gamma + \frac{C}{2}, \angle LIB = \beta + \frac{B}{2}$$

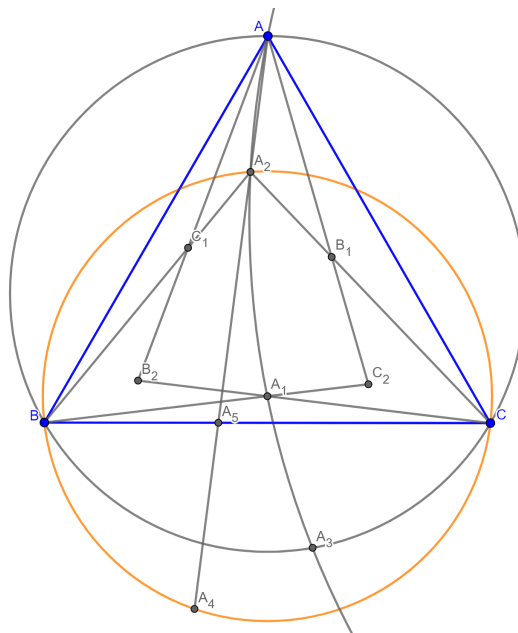
حال نوشتن لم کلید در مثلث BIC و نقطه L حکم را نتیجه می‌دهد.

مساله ۳.۳.۳ (المپیاد جهانی ریاضی ۲۰۲۳)

مثلث متساوی الاضلاع ABC مفروض است. نقاط A_1, B_1, C_1 درون مثلث طوری قرار دارند که $A_1B = A_1C, B_1C = B_1A, C_1A = C_1B$ و

$$\angle BA_1C + \angle CB_1A + \angle AC_1B = 48^\circ$$

محل تقاطع خطوط BC_1 و CB_1 را A_2 می‌نامیم. B_2 و C_2 به طور مشابه تعریف می‌شوند. ثابت کنید دواير $AA_1A_2, BB_1B_2, CC_1C_2$ از ۲ نقطه مشترک می‌گذرند.



شکل ۴

راه حل. حکم معادل با این است که ثابت کنید ۳ دایره گفته شده هم محور هستند. کافی است ۲ نقطه در صفحه پیدا کنیم که قوت هر کدام از این نقاط نسبت به هر ۳ دایره برابر باشد. زوایای A_1BC, B_1CA, C_1AB را به ترتیب α, β, γ می‌نامیم. دقت کنید که

$$\left. \begin{aligned} \angle(BA_1C) &= 180^\circ - 2\alpha \\ \angle(BA_2C) &= 60^\circ + \beta + \gamma \\ \alpha + \beta + \gamma &= 30^\circ \end{aligned} \right\} \angle(BA_1C) = 2\angle(BA_2C)$$

از آنجا که A_1 روی عمود منصف BC هم است نتیجه می‌شود A_1 مرکز دایره محیطی BA_1C است. به طور مشابه ثابت می‌شود B_1, C_1 هم مراکز دایره ACB_1, ABC_1 هستند.

نتیجه می‌گیریم $B_1B_2 = B_1A, C_1C_2 = C_1A$ در نتیجه $\angle AB_2B_1 = \angle AC_2C_1 = \angle B_1AC_1$. پس چهارضلعی $B_1C_2B_2C_1$ محاطی است. به طور مشابه ثابت می‌شود چهارضلعی های $B_1A_1B_2A_2, C_1A_1C_2A_2$ هم محاطی هستند. نتیجه می‌شود خطوط A_1A_2, B_1B_2, C_1C_2 در مرکز اصلی ۳ دایره گفته شده هم‌رس هستند. به وضوح قوت این نقطه نسبت به دایره $AA_1A_2, BB_1B_2, CC_1C_2$ هم برابر است.

برای پیدا کردن نقطه دوم روی محور اصلی ۳ دایره‌ی مسئله نشان می‌دهیم خطوط AA_3, BB_3, CC_3 (که در ادامه تعریف شده‌اند). هم‌رس هستند. در این صورت نقطه هم‌رسی این ۳ خط در خاصیت مورد نظر صدق می‌کند. تقاطع دوم دایره AA_1A_2 و دایره ABC را A_3 می‌نامیم. B_3, C_3 به طور مشابه تعریف میشوند. مشابه با سوال قبل اگر نشان دهیم خطوط AA_3 هم‌رس هستند این نقطه هم‌رسی روی محور اصلی ۳ دایره خواهد بود. طبق قضیه سوای سینوسی برای اثبات هم‌رسی این ۳ خط کافیت نشان دهیم

$$\prod_{cyc} \frac{A_3B}{A_3C} = 1.$$

طبق لم نسبت دایره حالت کلی می‌دانیم

$$\prod_{cyc} \frac{A_3B}{A_3C} = \prod_{cyc} \frac{\frac{A_1B}{A_1C} \cdot \frac{A_2B}{A_2C}}{\frac{AB}{AC}} \cdot \left| \frac{\sin(AA_3B - AA_1C)}{\sin(AA_3C - AA_1C)} \right| = \prod_{cyc} \frac{A_2B}{A_2C} \cdot \frac{\sin(AA_2B - AA_1B)}{\sin(AA_2C - AA_1C)}$$

تقاط دوم دایره محیطی BA_1C و خط AA_2 را A_3 می‌نامیم. با توجه به اینکه A_1 مرکز دایره BA_1C است نتیجه می‌گیریم

$$\angle(AA_3B) - \angle(AA_1B) = \angle(CBA_1)$$

و

$$\angle(AA_3C) - \angle(AA_1C) = \angle(BCA_1)$$

پس کافیت نشان دهیم

$$\prod_{cyc} \frac{A_3B}{A_3C} \cdot \frac{A_2B}{A_2C} = 1$$

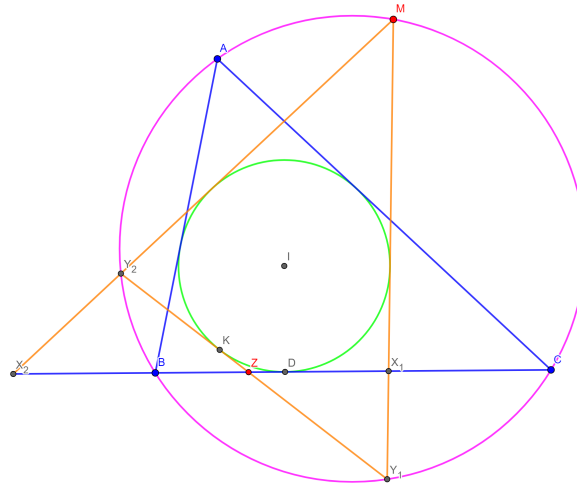
اگر تقاطع AA_2 و ضلع BC را A_4 بنامیم باید نشان دهیم

$$\prod_{cyc} \frac{A_4B}{A_4C} = 1$$

که طبق قضیه سوای معادل با هم‌رسی خطوط AA_2 است. ولی اثبات این هم‌رسی با استفاده از سوای سینوسی و کمی محاسبات ساده است و حکم اثبات می‌شود.

مساله ۴.۳.۳ (انتخابی تیم تایوان ۲۰۱۴)

مثلث ABC و نقطه دلخواه M روی دایره محیطی این مثلث مفروضاند. مماس‌های مرسوم از M بر دایره محاطی داخلی مثلث، ضلع BC را در نقاط X_1, X_2 قطع می‌کند. ثابت کنید دایره محیطی مثلث MX_1X_2 از نقطه میکستی‌لینیر داخلی A می‌گذرد.



شکل ۵

راه‌حل. دوائر محیطی و محاطی را به ترتیب Ω و ω و نقطه میکستی‌لینیر را T می‌نامیم. دقت کنید طبق لم‌های نسبت حکم معادل با این است که $f(T) = \frac{f(X_1)f(X_2)}{f(M)}$. تقاطع‌های MX_1 و MX_2 با Ω را به ترتیب Y_1 و Y_2 می‌نامیم. همچنین فرض کنید خط Y_1Y_2 ضلع BC را در Z قطع کند و در K بر ω مماس شود. می‌دانیم

$$\left. \begin{aligned} f(Y_1)f(M) &= f(X_1) \\ f(Y_2)f(M) &= f(X_2) \\ f(Y_1)f(Y_2) &= f(Z) \end{aligned} \right\} \frac{f(X_1)f(X_2)}{f(M)} = f(Z)f(M)$$

پس کافی است نشان دهیم $f(M)f(Z) = f(T)$.

نشان می‌دهیم با تغییر M روی Ω مقدار $f(Z)f(M)$ تغییر نمی‌کند. در این صورت اگر برقراری حکم را برای تنها برای یک M خاص روی دایره ثابت کنیم حکم به طور کلی ثابت می‌شود.

لم ۲.۳.۳

تبدیل $M \rightarrow K$ حافظ ناهمساز است.

اثبات لم به خواننده واگذار می‌شود.

از طرفی تبدیل $Z \rightarrow K$ هم جزو تبدیل‌های حافظ ناهمساز شناخته شده است. نتیجه می‌گیریم تبدیل $M \rightarrow Z$ هم حافظ ناهمساز است. توجه کنید که این تبدیل نقاط B و C را به یکدیگر تبدیل می‌کند. حال اگر این تبدیل نقاط دلخواه

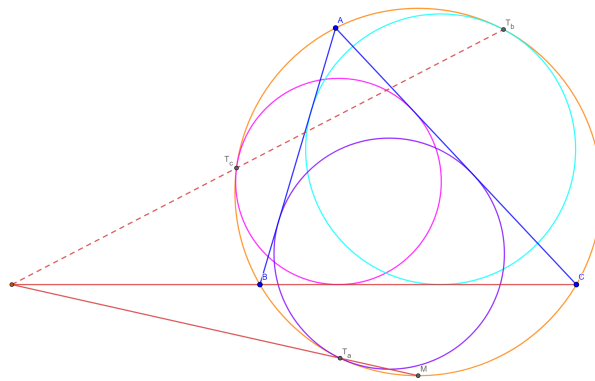
M_1 و M_2 روی Ω را به نقاط Z_1 و Z_2 روی BC تبدیل کند خواهیم داشت

$$(B, C; M_1, M_2) = (C, B; Z_1, Z_2) \Rightarrow \frac{\frac{M_1 B}{M_1 C}}{\frac{M_2 B}{M_2 C}} = \frac{\frac{Z_1 C}{Z_1 B}}{\frac{Z_2 C}{Z_2 B}} \Rightarrow f(M_1)f(Z_1) = f(M_2)f(Z_2)$$

پس ادعا ثابت می‌شود و برای کامل شدن راه حل کافیت درستی حکم را تنها برای یک نقطه M خاص روی دایره محیطی بررسی کنیم.

مساله ۵.۳.۳

مثلث ABC را در نظر بگیرید. M وسط کمان کوچک BC دایره محیطی مثلث است. نقاط T_a, T_b, T_c به ترتیب نقاط میکستیلینر متناظر A, B, C هستند. ثابت کنید $T_b T_c$ و MT_a روی BC هم‌رس هستند.



شکل ۶

راه حل. کافیت نشان دهیم $f(M)f(T_a) = f(T_b)f(T_c)$. طبق خواص نقاط میکستیلینر می‌دانیم

$$\frac{T_a B}{T_a C} = \left(\frac{\sin(\frac{C}{2})}{\sin(\frac{B}{2})} \right)^2.$$

همچنین طبق لم تغییر مبنای تابع نسبت (یا بطلمیوس در چهارضلعی $AT_c BC$) به دست می‌آید

$$\frac{T_c B}{T_c C} = \frac{AB}{\frac{T_c A}{T_c B} \cdot BC + AC} = \frac{\sin(C)}{\left(\frac{\sin(\frac{B}{2})}{\sin(\frac{A}{2})} \right)^2 \sin(A) + \sin(B)}$$

به طور مشابه به دست می‌آید

$$\frac{T_b B}{T_b C} = \frac{\frac{T_b A}{T_b C} BC + AB}{AC} = \frac{\left(\frac{\sin(\frac{C}{2})}{\sin(\frac{A}{2})} \right)^2 \sin(A) + \sin(C)}{\sin(B)}$$

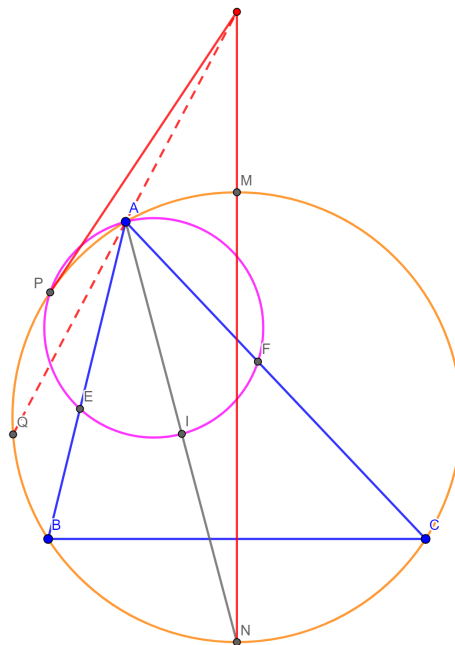
حال بررسی تساوی $f(M)f(T_a) = f(T_b)f(T_c)$ صرفاً محاسبات ساده خواهد بود.

مساله ۶.۳.۳ (کمپ تمرینی مالزی ۲۰۲۱)

مثلث حاده ABC با دایره محیطی Γ در صفحه مفروض است. I مرکز دایره محیطی مثلث است. نقطه P روی Γ طوری قرار دارد که $\angle API = 90^\circ$. نقطه Q روی Γ طوری قرار دارد که

$$QB \cdot \tan \angle B = QC \cdot \tan \angle C$$

و A و Q در یک طرف BC هستند. ثابت کنید عمود منصف BC مماس در P بر Γ و AQ هم‌مرس هستند.



شکل ۷

راه حل. وسط کمان بزرگ از دایره محیطی مثلث را M و وسط کمان کوچک را N می‌نامیم. طبق لم هم‌مرسی ۳ خط در حالت کلی کافیست ثابت کنیم

$$\begin{vmatrix} f(P)^2 & 2f(P) & 1 \\ f(A)f(Q) & f(A) + f(Q) & 1 \\ f(M)f(N) & f(M) + f(N) & 1 \end{vmatrix} = 0$$

پای عمودهای وارد از I بر AB و AC را E و F می‌نامیم. از محاطی بودن چهارضلعی $APEF$ نتیجه می‌گیریم

$$f(P) = \frac{BE}{CF} = \frac{\cot(\frac{B}{2})}{\cot(\frac{C}{2})}$$

طبق فرض مسئله هم واضح است

$$f(Q) = \frac{\tan(C)}{\tan(B)}$$

همچنین به وضوح $f(M) = +1, f(N) = -1, f(A) = \frac{\sin(C)}{\sin(B)}$ پس کافیت نشان دهیم

$$\begin{vmatrix} \frac{\cot(\frac{B}{r})}{\cot(\frac{C}{r})} & \frac{\cot(\frac{B}{r})}{\cot(\frac{C}{r})} & 1 \\ \frac{\tan(C)\sin(C)}{\tan(B)\sin(B)} & \frac{\sin(C)}{\sin(B)} + \frac{\tan(C)}{\tan(B)} & 1 \\ -1 & 0 & 1 \end{vmatrix} = 0$$

که یک محاسبات (نسبتا) ساده است.

(راهنمایی برای ادامه محاسبات: تمامی درایه‌های ماتریس فوق را بر حسب نسبت‌های مثلثاتی زوایای $\frac{B}{r}$ و $\frac{C}{r}$ نشان دهید.)



ارباب چندجمله‌ای‌ها

۱.۴ چکیده

در این مقاله به دنبال بررسی نحوه تبدیل مساله به چندجمله‌ای و استفاده کاربردی از آن‌ها برای حل مسائلی عجیب هستیم.

۲.۴ تبدیل مساله به چندجمله‌ای

۱.۲.۴ پوشاندن رئوس مکعب

فرض کنید یک مکعب دارید و می‌خواهید با کمترین تعداد صفحات لازم برای پوشاندن تمام رئوس آن را پیدا کنید. به راحتی می‌توان دید که این تعداد، ۲ است (صفحاتی که از دو قاعده‌ی مکعب می‌گذرند). اما اگر این قید را بدهند که آن صفحات از همه رئوس مکعب به جز دقیقاً یکی از رئوس بگذرند چطور؟ با کمی کار هندسی (یا جبری، هر جور راحتید!) می‌توان دید که دیگر با ۲ تا صفحه نمی‌توان همه رئوس مکعب به جز یکی را پوشاند. و از آن طرف با ۳ تا صفحه می‌شود! کافیت بدون کم شدن از کلیت صورت مساله، مکعب واحدی که مختصات رئوسش $(1, 1, 1), (1, 1, 0), \dots, (0, 0, 0)$ است در نظر بگیرید و صفحات $x + y + z = i$ را برای $i = 1, 2, 3$ رسم کنید. این ۳ صفحه، تمام رئوس به جز $(0, 0, 0)$ را می‌پوشانند. اما مساله وقتی جالب‌تر می‌شود که بخواهیم آن را در n بعد بررسی کنیم. یعنی مکعب واحد n بعدی را بگیرید که مختصات رئوسش $(1, 1, \dots, 1), (1, 1, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 0)$ است و می‌خواهیم کم‌ترین تعداد ابرصفحه‌های $n-1$ بعدی را پیدا کنیم که همه رئوس مکعب به جز مبدا را بپوشانند؛ یعنی هر راس به جز مبدا روی حداقل یکی از این ابرصفحه‌ها باشد. تعریف ابرصفحه هم مشابه تعریف صفحه در ۳ بعد است: مکان هندسی نقاطی که مختصاتشان در معادله‌ای به فرم $a_1x_1 + \dots + a_nx_n = b$ صدق می‌کند. با کمی دقت متوجه می‌شوید که مثالی مشابه با مثال حالت $n = 3$ ، در این حالت هم کار می‌کند. یعنی n ابرصفحه با معادلات

$$x_1 + x_2 + \dots + x_n = i, 1 \leq i \leq n$$

از تمام رئوس مکعب واحد به جز مبدا می‌گذرد. اما چرا این تعداد، کمینه است؟ برای پاسخ به این سوال، بیایید ببینیم اینکه مجموعه‌ی مشخصی از نقاط، با تعدادی ابرصفحه پوشانده شوند، چگونه تعبیر می‌شود؟ اگر بخواهیم جبری به این موضوع نگاه کنیم، و مثلاً فقط یک ابرصفحه قرار باشد این نقاط را بپوشاند، صرفاً باید معادله $a_1x_1 + \dots + a_nx_n = b$ برای مختصات تمام آن نقاط برقرار باشد. اگر دو تا ابرصفحه داشته باشیم چطور؟ مختصات آن نقاط، یا باید در $a_1x_1 + \dots + a_nx_n = b_1$ صدق کنند، یا در $a_{r1}x_1 + \dots + a_{rn}x_n = b_r$ پس برای هر کدام از نقاطی که با

دو ابرصفحه پوشانده شده‌اند:

$$(a_{11}x_1 + \dots + a_{1n}x_n - b_1)(a_{21}x_1 + \dots + a_{2n}x_n - b_2) = 0$$

و به طور کلی اگر m ابرصفحه بخوانند تعدادی نقطه را بپوشانند، باید مختصات آن نقاط، ریشه چندجمله‌ای n متغیره

$$(a_{11}x_1 + \dots + a_{1n}x_n - b_1)(a_{21}x_1 + \dots + a_{2n}x_n - b_2) \dots (a_{m1}x_1 + \dots + a_{mn}x_n - b_m)$$

باشند. پس اگر در مساله اصلی هم، m ابرصفحه با معادله‌های $a_{i1}x_1 + \dots + a_{in}x_n = 1$ که $1 \leq i \leq m$ بخوانند نقاط مکعب واحد را (به جز مبدا) بپوشانند، باید برای هر انتخابی از نقاطی که t تا از درایه‌هایشان ۱ و بقیه ۰ است (که t ناصفر است) داشته باشیم:

$$(a_{11}x_1 + \dots + a_{1n}x_n - 1)(a_{21}x_1 + \dots + a_{2n}x_n - 1) \dots (a_{m1}x_1 + \dots + a_{mn}x_n - 1) = 0 \quad (1)$$

شاید برایتان سوال شود که چرا فرض کردیم b_i ها همگی برابر با ۱ هستند؟ دلیلش این است که معادله‌های ابرصفحه‌ها، همگن هستند و می‌توانیم دو طرف معادله‌ها را در هر ضرب دلخواهی ضرب کنیم. و حالا، یا کمی تغییر، چندجمله‌ای نهایی خود را می‌سازیم!

$$f(x_1, \dots, x_n) = \prod_{i=1}^m (1 - (a_{i1}x_1 + \dots + a_{in}x_n)) - (1 - x_1)(1 - x_2) \dots (1 - x_n) = 0. \quad (2)$$

چندجمله‌ای ساخته شده، صرفاً در یک عبارت با چندجمله‌ای ۱ تفاوت دارد؛ و دقیقاً همین یک تفاوت باعث می‌شود تا معادله ۲ به ازای تمامی نقاط ورودی برقرار باشد؛ که یعنی به ازای هر انتخاب از ۰ و ۱ ها مثل $\alpha_1, \alpha_2, \dots, \alpha_n$ می‌دانیم $f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$. ضمناً توجه کنید که چون در مساله ما $\{0, 1\}$ ، می‌دانیم $x_i^2 = x_i$ پس چندجمله‌ای n متغیره f تشکیل شده از جمع تک جمله‌ای‌هایی به فرم $X_I = x_{i_1}x_{i_2} \dots x_{i_k}$ که

$$I = \{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$$

یک نکته جادویی در مورد f وجود دارد که در ادامه باعث حل مساله ما خواهد شد. می‌توانید ضرب تک جمله‌ای $x_1x_2x_3 \dots x_n$ را در f دقیق حساب کنید؟ واضح است که بخاطر فرض کوچکتر بودن m از n ضرب این عبارت دقیقاً برابر $(-1)^n$ خواهد شد (به ۲ دقت کنید!) که عبارتی ناصفر است. حالا، سوالی پیش می‌آید. آیا ممکن است ضرب خطی‌ای از عبارات به فرم X_I که $I \subseteq \{1, 2, \dots, n\}$ در همه نقاط ۰ و ۱ ای برابر ۰ شوند؟ البته به طوری که تمام ضرایب آن‌ها صفر نباشد.

$$f(x_1, x_2, \dots, x_n) = \sum_{I \subseteq \{1, \dots, n\}} c_I X_I = 0 \quad (3)$$

در بین تمام I هایی که ضرب X_I در عبارت ۳ صفر نیست، آن مجموعه‌ای را انتخاب کنید که هیچ I دیگری زیرمجموعه آن نباشد و آن را Ω بنامید. عضوهای آن مجموعه را برای مثال $\omega_1, \omega_2, \dots, \omega_k$ فرض کنید. حال، تمامی $x_{\omega_1}, x_{\omega_2}, \dots, x_{\omega_k}$ ها را برابر ۱ بگذارید و باقی x_j ها را ۰ ورودی دهید. به عبارت ۳ نگاه کنید؛ پس از ورودی داده شده این عبارت صرفاً یک

بخش ناصفر خواهد داشت.

$$\sum_{\forall I \in \{1, \dots, n\}} c_I \cdot X_I = c_{\Omega} \cdot x_{\omega_1} x_{\omega_2} \cdots x_{\omega_k} = c_{\Omega} = 0$$

که با فرض ناصفر بودن ضریب X_{Ω} در تناقض است؛ و مساله به پایان می‌رسد. $\square$ و به این صورت، فرض ابتدایی ما درباره کوچکتر بودن m از n به تناقض می‌خورد؛ که حکم سوال از این تناقض نتیجه می‌شود.

۲.۲.۴ قضیه شواله و تعمیم‌های آن

گزاره ۱.۲.۴ (قضیه شواله)

فرض کنید p عددی اول باشد و $f(x_1, x_2, \dots, x_n)$ چندجمله‌ای باشد که ضرایبش اعدادی صحیح‌اند و درجه‌اش r است و $r < n$. در این صورت اگر معادله هم‌نهشتی

$$f(x_1, x_2, \dots, x_n) \equiv 0 \pmod{p} \quad (\text{به پیمانه } p)$$

جواب داشته باشد، دست‌کم دو جواب متمایز به پیمانه p دارد.

برهان خلف می‌زنیم. فرض می‌کنیم که این معادله صرفاً یک جواب دارد؛ آن هم $x_1 = a_1, x_2 = a_2, \dots, x_n = a_n$ است. حال به دنبال ساخت یک چندجمله‌ای هستیم، که به شکل خوبی بتواند فرض‌های مساله را در خود جا بدهد. برای مثال فرض کنید می‌خواهیم مشاهده کنیم که چندجمله‌ای $g(x)$ در چند مقدار به پیمانه p صفر می‌شود. یک روش خوب بیان کردن این مساله، با چندجمله‌ای

$$Q(x) = 1 - (g(x))^{p-1}$$

است. زیرا:

$$Q(x_*) = \begin{cases} 1 & g(x_*) = 0 \\ 0 & \text{در غیر این صورت} \end{cases} \quad (۴)$$

حال، صرفاً کافیست چندجمله‌ای n متغیره خود را در این رابطه جایگذاری کنیم.

$$1 - (f(x_1, x_2, \dots, x_n))^{p-1} = \begin{cases} 1 & f(x_1, x_2, \dots, x_n) = 0 \\ 0 & \text{در غیر این صورت} \end{cases} \quad (۵)$$

می‌دانیم که تنها زمانی که چندجمله‌ای ساخته شده در عبارت ۵ برابر ۱ می‌شود، زمانی‌ست که

$$x_1 = a_1, x_2 = a_2, \dots, x_n = a_n$$

و اکنون با ساخت یک چندجمله‌ای خلاقانه دیگر، کار اثبات را به پایان می‌رسانیم!

$$Q(\mathbf{X}) = 1 - (f(x_1, x_2, \dots, x_n))^{p-1} - (1 - (x_1 - a_1)^{p-1})(1 - (x_2 - a_2)^{p-1}) \cdots (1 - (x_n - a_n)^{p-1}). \quad (۶)$$

چندجمله‌ای ساخته شده در عبارت ۶ همیشه و در همه نقاط برابر ۰ است (سر اینکه $f(x_1, x_2, \dots, x_n) = 0$ باشد حالت‌بندی کنید). حال به دو چندجمله‌ای سازنده $Q(x_1, x_2, \dots, x_n)$ نگاه کنید؛ اولی درجه حداکثر $r(p-1)$ دارد. اما دومی یک تک‌جمله‌ای دارد که درجه‌اش بسیار زیاد و برابر $n(p-1)$ است!

$$x_1^{p-1} x_2^{p-1} x_3^{p-1} \dots x_n^{p-1}$$

وقتی یک چندجمله‌ای به پیمانه p در همه نقاط برابر ۰ می‌شود، می‌دانیم که تک تک ضرایب آن پس از «ساده‌سازی» چندجمله‌ای، باید بر p بخش پذیر باشند (می‌توانید درباره ساده‌سازی چندجمله‌ای‌ها به پیمانه p به مرجع [۱] مراجعه کنید). پس این چندجمله‌ای ما ضربی از تک‌جمله‌ای $x_1^{p-1} x_2^{p-1} x_3^{p-1} \dots x_n^{p-1}$ دارد که با هیچ عبارت دیگری خط نخواهد خورد. زیرا $n(p-1) < r(p-1)$ و چون چندجمله‌ای مورد نظر باید در تمامی نقاط ۰ باشد، تناقض موردنظر حاصل می‌شود. $\square$

البته، اثبات بالا را می‌توان با تغییر اندکی، تعمیمی داد که حائز اهمیت است؛ تعمیم شواله را در گزاره زیر بیان می‌کنیم.

گزاره ۲.۲.۴ (قضیه شوالیه)

فرض کنید p عددی اول باشد و $f(x_1, x_2, \dots, x_n)$ چندجمله‌ایی باشد که ضرایبش اعدادی صحیح‌اند و درجه‌اش r است و $r < n$. در این صورت **تعداد** جواب‌های معادله هم‌نهشتی

$$f(x_1, x_2, \dots, x_n) \equiv 0 \pmod{p}$$

بر p بخش‌پذیر است!

استراتژی اثبات قضیه شوالیه (!) بسیار شبیه قبلی‌ست. فرض کنید این معادله هم‌نهشتی k جواب به پیمانه p دارد و این جواب‌ها را به این صورت نمایش می‌دهیم.

$$f(a_1^1, a_2^1, \dots, a_n^1) = f(a_1^2, a_2^2, \dots, a_n^2) = f(a_1^3, a_2^3, \dots, a_n^3) = \dots = f(a_1^k, a_2^k, \dots, a_n^k) = 0$$

حال، این بار با کمی تفاوت، چندجمله‌ای جادویی خود را می‌سازیم!

$$Q(\mathbf{X}) = 1 - (f(x_1, x_2, \dots, x_n))^{p-1} - \prod_{i=1}^n (1 - (x_i - a_i^1)^{p-1}) - \prod_{i=1}^n (1 - (x_i - a_i^2)^{p-1}) - \dots - \prod_{i=1}^n (1 - (x_i - a_i^k)^{p-1}). \quad (7)$$

چندجمله‌ای جادویی ظاهر شده در عبارت ۷ در تمامی نقاط برابر ۰ می‌شود! این بار نیز مثل قبل، بخشی از آن (عبارت اولیه) درجه کمی دارد (زیرا $n(p-1) < r(p-1)$) و در تائین درجه چندجمله‌ای بی‌تاثیر است. اما k عبارت داریم که تک‌جمله‌ای $x_1^{p-1} x_2^{p-1} x_3^{p-1} \dots x_n^{p-1}$ را در خود دارند. ضرب این تک‌جمله‌ای در همه آن‌ها برابر با یک است؛ پس ضرب این عبارت در کل برابر با k می‌شود. و می‌دانیم که تمامی ضرایب $Q(x_1, x_2, \dots, x_n)$ باید برابر صفر باشند (از آنجایی که در همگی نقاط برابر ۰ است). پس... حل است دیگر. k باید بر p بخش‌پذیر باشد! $\square$

در صورتی که با چندجمله‌ای‌های استفاده شده در اثبات قضایا بالا حساسی حال کرده‌اید، روی تعمیم تعمیم شوالیه کمی

وقت بگذارید!

گزاره ۳.۲.۴ (قضیه شوالیه تاریکی!)

فرض کنید p عددی اول باشد و $f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_m(x_1, x_2, \dots, x_n)$ چندجمله‌ای‌هایی باشند که ضرایبشان اعدادی صحیح‌اند و درجه $f_i(x_1, x_2, \dots, x_n)$ برابر با r_i باشد. می‌دانیم $r_1 + r_2 + \dots + r_m < n$. در این صورت تعداد جواب‌های معادله‌های هم‌نهشتی

$$f_1(x_1, x_2, \dots, x_n) \equiv 0 \pmod{p} \quad (\text{به پیمانه } p)$$

$$f_2(x_1, x_2, \dots, x_n) \equiv 0 \pmod{p} \quad (\text{به پیمانه } p)$$

:

$$f_m(x_1, x_2, \dots, x_n) \equiv 0 \pmod{p} \quad (\text{به پیمانه } p)$$

بر p بخش پذیر است!

۳.۲.۴ خط‌های شیطانی!

مساله ۱.۲.۴ (KOMAL A.814)

۶۶ نقطه در صفحه داریم که هیچ ۱۰ خطی نیست که از تمام این نقاط بگذرد. ثابت کنید می‌توان ۶۶ تا از آنها رو انتخاب کرد، که هیچ ۱۰ خطی نباشد که از این ۶۶ نقطه بگذرد.

قبل از اینکه مستقیم به سراغ حل سوال برویم، بیایید به این شکل به صورت سوال نگاه کنیم. فرم مساله به این شکل است که اگر تعدادی نقطه در صفحه یک ویژگی را داشته باشند، آیا نتیجه می‌شود که یک زیرمجموعه با تعداد کمتر از آن نقاط هم آن ویژگی را دارد یا نه. این ویژگی می‌تواند هر چیزی باشد اما اگر بخواهیم با دیدگاه چندجمله‌ای به چنین مساله‌ای نگاه کنیم، اول باید ببینیم اصلاً شرط مساله را چگونه باید به فرم چندجمله‌ای تفسیر کرد.

اینجا با کمی دقت و توجه به حالت خاصی که فقط ۱ خط تعدادی نقطه را نپوشاند، می‌فهمیم که برای اینکه تعدادی نقطه توسط ۱۰ خط پوشیده نشوند، کفایت مختصات حداقل یکی از نقاط، در تساوی $P(x, y) = 0$ که P ضرب معادله خط های ۱۰ خط مذکور است، صدق نکند. حال بهتر می‌توانیم روی حل سوال مانور دهیم:

فرض کنید حکم درست نباشد. ۶۶ نقطه دلخواه را در نظر می‌گیریم. طبق فرض خلف، ۱۰ خط در صفحه از این ۶۶ نقطه می‌گذرد و ضمناً نقطه‌ای مانند A_1 از بین ۶۶ نقطه اولیه وجود دارد که روی این ۱۰ خط نباشد. فرض کنید معادله خط i امی که از آن ۱۰ نقطه می‌گذرد، $a_i x + b_i y + c_i = 0$ باشد. ضرب همه‌ی ۱۰ عبارت به فرم $a_i x + b_i y + c_i$ را در نظر می‌گیریم و اسم این حاصل ضرب را $P_1(x, y)$ می‌نامیم.

حال A_1 را به همراه ۶۵ نقطه دلخواه دیگر در نظر می‌گیریم و $P_2(x, y)$ را مشابه قبل تعریف می‌کنیم. ضمناً مشابه قبل، نقطه‌ای مانند A_2 که روی خطوط گذرا از A_1 و ۶۵ نقطه دیگر نیست را هم در نظر می‌گیریم. حال دو نقطه‌ی A_1, A_2 را به همراه ۶۴ نقطه دلخواه دیگر در نظر می‌گیریم و $P_3(x, y)$ و نقطه‌ای مانند A_3 که روی ۱۰ خط پوشاننده‌ی A_1, A_2 و ۶۴ نقطه‌ی دیگر بود را مشابه قبل تعریف می‌کنیم. این روند را تا وقتی A_{66} هم بگیریم ادامه می‌دهیم و در نهایت $P_{67}(x, y)$ را ضرب معادله ۱۰ خط گذرا از $A_1, \dots, A_{66}$ تعریف می‌کنیم.

اکنون ثابت می‌کنیم $P_1, \dots, P_{66}$ مستقل خطی‌اند. فرض کنید $\sum c_i P_i(x, y) = 0$ به ازای هر x, y برقرار باشد. با جایگذاری معادله نقطه‌ای A_1 در تساوی اخیر، نتیجه می‌شود $c_1 = 0$. سپس با جایگذاری معادله نقطه A_2 خواهیم داشت $c_2 = 0$ و همین‌گونه الی آخر. نتیجه می‌شود $c_1 = c_2 = \dots = c_{66} = 0$ و در نتیجه ضریب آخر هم برابر با ۰ می‌شود. اما از طرف دیگر، عبارت $\sum c_i P_i(x, y)$ تشکیل شده از جمع تعدادی $x^i y^j$ (ضریب یک ضریب) است که $i + j \leq 10$ که تعدادشان می‌شود $\binom{12}{2} = 66$ اما ۶۷ ضریب در معادله داریم. پس c_i های ناصفری وجود دارند که به ازای هر x, y ، $\sum c_i P_i(x, y) = 0$ با نتیجه‌ی بند قبل در تناقض است. $\square$

۴.۲.۴ یک فاصله، دو فاصله

مساله ۲.۲.۴

$a, b \in \mathbb{R}$. تعدادی نقطه در فضای d بعدی $\mathbb{R}^d$ مفروض هستند به طوری که فواصل بین هر دو نقطه متفاوت از آن‌ها یا برابر a است، یا برابر b . ثابت کنید تعداد این نقاط از $\frac{1}{2}(d^2 + 5d + 4)$ کمتر است.

قبل از بررسی مساله بالا، می‌توانیم کمی حالت ساده‌تر آن را بررسی کنیم. البته منظور از حالت ساده‌تر، حالتی است که فاصله هر دو نقطه فقط و فقط برابر a باشد (یک فاصله). به دنبال یک چندجمله‌ای هستیم که بتواند فرض‌های ما را به خوبی نشان دهد؛ پس به طبع این چندجمله‌ای باید ربطی به فاصله بین نقاط داشته باشد. عبارت زیر را در نظر بگیرید:

$$f_i(\mathbf{X}) = (\|\mathbf{X} - P_i\|^2 - a^2) \quad (8)$$

که در آن $\mathbf{X}$ نشان دهنده نقطه ورودی ما به تابع و P_i ها نیز نشان دهنده نقاط ابتدایی ما هستند. البته، نگذارید نماد گزاری بالا شما را گیج کند؛ این چندجمله‌ای صرفاً این معنا را دارد که اگر هر یک از نقاط ابتدایی‌مان را به آن ورودی دهیم برابر با ۰ می‌شود (چون با P_i فاصله دقیقاً a دارند). ولی، اگر خود P_i را به آن ورودی بدهیم چطور؟

فعلاً مساله را در حالت ساده‌تر رها می‌کنیم و به بررسی حالت دو فاصله مشغول می‌شویم. برای هر نقطه یک چندجمله‌ای می‌سازیم تا بتواند فرض‌های مساله را در خود نمایان کند.

$$f_1(\mathbf{X}) = (\|\mathbf{X} - P_1\|^2 - a^2)((\|\mathbf{X} - P_1\|^2 - b^2))$$

$$f_2(\mathbf{X}) = (\|\mathbf{X} - P_2\|^2 - a^2)((\|\mathbf{X} - P_2\|^2 - b^2))$$

⋮

$$f_n(\mathbf{X}) = (\|\mathbf{X} - P_n\|^2 - a^2)((\|\mathbf{X} - P_n\|^2 - b^2))$$

هر کدام از این چندجمله‌ای‌ها متناظراً برای هر کدام از نقاط ابتدایی‌مان ساخته شده؛ به طوری که اگر هر نقطه دیگری جز خودش را به آن ورودی دهیم برابر با ۰ می‌شود. و در صورتی که خود آن نقطه را ورودی بگیرد برابر با $a^2 b^2$ خواهد شد! لازم به ذکر است که این چندجمله‌ای‌ها در واقع d متغیره هستند و در فضای $\mathbb{R}^d$ قرار دارند. پس اگر آن‌ها را به صورت

دقیق بنویسیم اینگونه خواهند بود:

$$f_i(x_1, x_2, \dots, x_d) = \left(\sum_{j=1}^d (x_j - p_j^i)^2 - a^2 \right) \left(\sum_{j=1}^d (x_j - p_j^i)^2 - b^2 \right) \quad (9)$$

که در آن $P_i = (p_1^i, p_2^i, \dots, p_d^i)$ مختصات نقاط ابتدایی مان است.

از این جا به بعد اثبات، به خواص ابتدایی جبرخطی نیاز داریم. تمام چندجمله‌ای‌های حداکثر d متغیره را در نظر بگیرید. این‌ها یک فضای برداری می‌سازند که بررسی بعد این فضا بسیار برای ما پرکاربرد خواهد بود. ابتدا ثابت می‌کنیم که n چندجمله‌ای ساخته شده در عبارت ۹ در این فضا با هم مستقل خطی هستند؛ یعنی جمع هیچ ضرایبی از آن‌ها برابر ۰ نمی‌شود مگر اینکه تمام ضرایب برابر ۰ باشند. ضرب خطی از آن‌ها را در نظر بگیرید که برابر ۰ شده است:

$$\sum_{i=1}^n c_i \cdot f_i(\mathbf{X}) = 0 \quad (10)$$

فرض کنید $1 \leq i \leq n$ وجود دارد که $c_i \neq 0$. حال نقطه متناظر با چندجمله‌ای i ام را به معادله ۱۰ ورودی می‌دهیم.

$$\sum_{j=1}^n c_j \cdot f_j(P_i) = c_i \cdot f_i(P_i) = c_i \cdot a^2 b^2 = 0 \Rightarrow c_i = 0. \quad (11)$$

که با فرض ناصفر بودن c_i در تناقض است. خوب، پس نتیجه گرفتیم که این چندجمله‌ای‌ها مستقل خطی هستند. حالا، یک پایه برای آن‌ها معرفی می‌کنیم، به طوری که با جمع ضرایبی از آن عبارات بتوان چندجمله‌ای‌های موردنظرمان را ساخت.

ابتدا $Q := \sum_{j=1}^d dx_j^2$ را در نظر می‌گیریم که عضوی از فضای چندجمله‌ای‌های d متغیره است. حالا سعی می‌کنیم کمی f_i ها را بر حسب X خلاصه‌تر بنویسیم.

$$\begin{aligned} f_i(\mathbf{X}) &= (\|\mathbf{X} - P_i\|^2 - a^2)(\|\mathbf{X} - P_i\|^2 - b^2) \\ &= \left(Q - \sum_{j=1}^d 2x_j p_j^i + \circ \right) \left(Q - \sum_{j=1}^d 2x_j p_j^i + \square \right) \end{aligned}$$

و به راحتی با ضرب و باز کردن عبارت بالا می‌توان دریافت که همه f_i ها ترکیب خطی از چندجمله‌ای‌های d متغیره زیر هستند:

$$\begin{aligned}
 &Q^{\mathfrak{r}}, \\
 &x_j Q, \quad j = 1, 2, \dots, d \\
 &x_j^{\mathfrak{r}}, \quad j = 1, 2, \dots, d \\
 &x_i x_j, \quad 1 \leq i < j \leq d \\
 &x_j, \quad j = 1, 2, \dots, d \\
 &1.
 \end{aligned}$$

تعداد اعضای خانواده بالا برابر با $\frac{1}{\mathfrak{r}}(d^{\mathfrak{r}} + 5d + 4) + d + 1 = \frac{1}{\mathfrak{r}}(d^{\mathfrak{r}} + 5d + 4) + d + 1$ است. حال چون f_i ها خود مستقل بودند، نتیجه می‌گیریم که قطعاً پایه‌ای که برای آن‌ها معرفی کرده‌ایم تعداد بیشتری از خودشان عبارت دارد. که یعنی $n < \frac{1}{\mathfrak{r}}(d^{\mathfrak{r}} + 5d + 4) + d + 1$ و کران دلخواه ما به دست خواهد آمد. $\square$

نکته. جالب اینجاست که کران بالا تا حد خوبی دقیق است و برای هر d ، مثالی $\binom{d+1}{\mathfrak{r}}$ نقطه‌ای در فضای d بعدی داریم که در فرض ابتدایی مساله صدق می‌کنند.

کتاب‌نامه

- [۱] نظریه اعداد، رویا بهشتی زواره، مریم میرزاخانی. انتشارات فاطمی.
- [2] Jiri Matousek, thirty-three miniatures: mathematical and algorithmic applications of linear algebra.
- [3] KOMAL, Mathematical and Physical Journal for High Schools.



نگاهی موزون به نامساوی

۱.۵ مقدمه

در این مقاله سعی کردم، یکی از نامساوی‌های جالب و به نسبت پر کاربرد را بررسی کنم و دید کلی‌ای از آن را به نمایش بگذارم. احتمالاً نام نامساوی میانگین حسابی-هندسی تا کنون به گوشتان خورده، اما در اینجا قرار است نسخه پیشرفته‌تر و متفاوت‌تری از آن را ببینیم؛ یعنی نامساوی میانگین حسابی-هندسی وزن‌دار. برای درک بهتر در ابتدا چند سوال را به عنوان مثال حل کردم و در آخر شما را با تعدادی تمرین زیبا تنها گذاشتم. در نهایت جا دارد تشکر ویژه‌ای از آقای شایان غلامی عزیز بکنم که ایده اصلی این مقاله را دادند؛ قطعاً بدون کمک‌های ایشان، این مقاله خالی از مشکل نبود.

۲.۵ قضیه میانگین حسابی-هندسی وزن دار

۱.۲.۵ گزاره

فرض کنید $a_1, \dots, a_n \in \mathbb{R}^+$ و همچنین $\alpha_1, \dots, \alpha_n \in \mathbb{R}^+$ به طوری که $\alpha_1 + \dots + \alpha_n = 1$ آنگاه داریم:

$$a_1 \alpha_1 + \dots + a_n \alpha_n \geq a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}.$$

راه حل.^۱ برای تابع $f(x) = -\ln x$ داریم $f'(x) = -\frac{1}{x}$ و $f''(x) = \frac{1}{x^2}$ ، یعنی $f''(x) > 0$ به ازای هر $x \in (0, \infty)$. بنابراین، نتیجه می‌گیریم که تابع f در بازه $(0, \infty)$ یک تابع محدب است. حال فرض کنید $a_i \in (0, \infty)$ به ازای $i = 1, 2, \dots, n$ و $\alpha_i \in [0, 1]$ به ازای $i = 1, 2, \dots, n$ اعدادی دلخواه هستند به طوری که $\alpha_1 + \alpha_2 + \dots + \alpha_n = 1$. با استفاده از نامساوی ین‌سن نتیجه می‌گیریم که:

$$\begin{aligned} -\ln \left(\sum_{i=1}^n \alpha_i a_i \right) &= f \left(\sum_{i=1}^n \alpha_i a_i \right) \leq \sum_{i=1}^n \alpha_i f(a_i) = -\sum_{i=1}^n \alpha_i \ln a_i \\ \iff -\ln(a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n) &\leq -\alpha_1 \ln a_1 - \alpha_2 \ln a_2 - \dots - \alpha_n \ln a_n \\ \iff \alpha_1 \ln a_1 + \alpha_2 \ln a_2 + \dots + \alpha_n \ln a_n &\leq \ln(a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n) \\ \iff \ln(a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}) &\leq \ln(a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n) \\ \iff a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n} &\leq a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n \end{aligned}$$

^۱ به دلیل استفاده از نامساوی ین‌سن در برخی از سوالات، صورت این قضیه را در صفحه بعد بیان کردیم تا تمام پیش‌نیازهای مورد نیاز برای حل مسائل این مقاله داشته باشید.

۳.۵ نامساوی ین سن

گزاره ۱.۳.۵

فرض کنید $f : (a, b) \rightarrow \mathbb{R}$ یک تابع محدب در بازه (a, b) باشد. فرض کنید $n \in \mathbb{N}$ و $\alpha_1, \alpha_2, \dots, \alpha_n \in (0, 1)$ اعدادی حقیقی باشند به طوری که $\alpha_1 + \alpha_2 + \dots + \alpha_n = 1$ آنگاه برای هر $x_1, x_2, \dots, x_n \in (a, b)$ داریم:

$$f\left(\sum_{i=1}^n \alpha_i x_i\right) \leq \sum_{i=1}^n \alpha_i f(x_i),$$

نتیجہ ۱.۳.۵

بنابراین، داریم:

$$f(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) \leq \alpha_1 f(x_1) + \alpha_2 f(x_2) + \cdots + \alpha_n f(x_n).$$

اثبات این قضیه به عهده خواننده واگذار می‌شود. برای راهنمایی، سعی کنید با استقرا این قضیه را ثابت کنید.

۴.۵ آشنایی بیشتر

۱. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $abc = 1$. ثابت کنید که:

$$a^{b+c}b^{c+a}c^{a+b} < 1$$

اثبات: طبق نامساوی میانگین حسابی-هندسی وزن دار داریم:

$$1 \geq \frac{\mathfrak{r}}{a+b+c} = \frac{a^{\frac{1}{a}} + b^{\frac{1}{b}} + c^{\frac{1}{c}}}{a+b+c} = \sum_{cyc} \left(\frac{a}{a+b+c} \right)^{\frac{1}{a}} \geq \sqrt[a+b+c]{1} = \sqrt[a+b+c]{a^{b+c} b^{a+c} c^{a+b}}$$

۲. (USAMO ۱۹۷۴) $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $\sum_{cyc} a = 3$. ثابت کنید که:

$$a^b b^c c^a \leq 1.$$

اثبات ۱: با استفاده از نامساوی میانگین حسابی-هندسی وزن دار، داریم:

$$(a^a b^b c^c)^{\frac{1}{a+b+c}} \geq \frac{a+b+c}{\frac{a}{a} + \frac{b}{b} + \frac{c}{c}} = \frac{a+b+c}{3}$$

سپس با استفاده از نامساوی میانگین حسابی-هندسی برای a, b, c داریم:

$$\frac{a+b+c}{3} \geq (abc)^{\frac{1}{3}}$$

با ترکیب این دو نتیجه می‌گیریم:

$$(a^a b^b c^c)^{\frac{1}{a+b+c}} \geq \frac{a+b+c}{3} \geq (abc)^{\frac{1}{3}}$$

بنابراین $a^a b^b c^c \geq (abc)^{\frac{a+b+c}{3}}$ در نتیجه اثبات کامل شد.

اثبات ۲: باید نامساوی زیر را اثبات کنیم:

$$\begin{aligned} a^a b^b c^c &\geq (abc)^{\frac{a+b+c}{3}} \\ \iff a \ln a + b \ln b + c \ln c &\geq \left(\frac{a+b+c}{3} \right) (\ln a + \ln b + \ln c). \\ \iff 3 \left(\frac{1}{3} a \ln a + \frac{1}{3} b \ln b + \frac{1}{3} c \ln c \right) &\geq \left(\frac{a+b+c}{3} \right) (\ln a + \ln b + \ln c). \end{aligned}$$

حال، فرض می‌کنیم که:

$$f(x) = x \ln(x).$$

چون:

$$f''(x) = \frac{1}{x} > 0 \quad \forall x \in (0, \infty).$$

از آنجا که $f(x)$ محدب است به ازای $\forall x \in (0, \infty)$ ، طبق نامساوی ینسن، داریم:

$$\begin{aligned} 3 \left(\frac{1}{3} f(a) + \frac{1}{3} f(b) + \frac{1}{3} f(c) \right) &= 3 \left(\frac{1}{3} a \ln a + \frac{1}{3} b \ln b + \frac{1}{3} c \ln c \right) \\ &\geq 3 \left(\left(\frac{a+b+c}{3} \right) \ln \left(\frac{a+b+c}{3} \right) \right) \geq (a+b+c) \ln \left(\sqrt[3]{abc} \right) = \frac{(a+b+c)}{3} \ln(abc). \end{aligned}$$

۳. (ELMO ۲۰۱۳) اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $\sum_{cyc} \sqrt[n]{a} = \sum_{cyc} a$ ثابت کنید که:

$$\prod_{cyc} a^a \geq 1.$$

اثبات ۱: طبق نامساوی میانگین حسابی-هندسی وزن دار، داریم:

$$1 = \sum_{cyc} \frac{a}{a+b+c} \cdot a^{-\frac{a}{a+b+c}} \geq (a^a b^b c^c)^{-\frac{a+b+c}{a+b+c}}$$

از این رو چون $a^a b^b c^c \geq 1$ اثبات کامل می‌شود.

اثبات ۲: فرض کنید $x^y = a$, $y^z = b$, $z^x = c$. بنابراین:

$$\begin{aligned} \sum x^{y^{x^y}} &\geq 1 \\ \iff \sum x^{x^y} &\geq 1 \\ \iff \sum x^y \ln x &\geq 0 \\ \Rightarrow \sum x^y \ln x &\geq \sum \frac{x^y}{e} - \frac{x}{e} = 0. \end{aligned}$$

در نتیجه اثبات کامل شد.

تعمیم: برای هر مجموعه‌ای از اعداد حقیقی و مثبت a_i به طوری که $\sum_{cyc} a_i^{p_1} = \sum_{cyc} a_i^{p_2}$ که در آن $p_1 > p_2$ است، آنگاه، داریم:

$$\prod_{cyc} a_i^{a_i^{p_1}} \geq 1.$$

۴. (ELMO SL ۲۰۱۸) اعداد $abcxyz \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$. ثابت کنید که:

$$a^x + b^y + c^z \geq \frac{4abcxyz}{(x+y+z-3)^2}.$$

اثبات: در این راه حل دو بار از ناسمادی میانگین حسابی-هندسی وزن دار استفاده می‌کنیم:

$$\begin{aligned} a^x + b^y + c^z &= xyz \left(\frac{1}{x} \cdot \frac{a^x}{yz} + \frac{1}{y} \cdot \frac{a^y}{zx} + \frac{1}{z} \cdot \frac{a^z}{xy} \right) \\ &\geq xyz \left(\frac{a^x}{yz} \right)^{\frac{1}{x}} \left(\frac{a^y}{zx} \right)^{\frac{1}{y}} \left(\frac{a^z}{xy} \right)^{\frac{1}{z}} \\ &= \frac{abcxyz}{(yz)^{\frac{1}{x}} (zx)^{\frac{1}{y}} (xy)^{\frac{1}{z}}} \\ &= \frac{abcxyz}{\left(x^{\frac{1}{yz}} y^{\frac{1}{xz}} z^{\frac{1}{xy}} y^{\frac{1}{zx}} z^{\frac{1}{xy}} x^{\frac{1}{yz}} \right)^{\frac{1}{x}}} \\ &\geq \frac{abcxyz}{\left(\frac{x}{yz} + \frac{y}{xz} + \frac{z}{xy} + \frac{y}{zx} + \frac{z}{xy} + \frac{x}{yz} \right)^{\frac{1}{x}}} \\ &= \frac{4abcxyz}{\left(\frac{x^{\frac{1}{yz}} y^{\frac{1}{xz}} + y^{\frac{1}{xz}} z^{\frac{1}{xy}} + z^{\frac{1}{xy}} x^{\frac{1}{yz}} + x^{\frac{1}{yz}} y^{\frac{1}{xz}} + y^{\frac{1}{xz}} z^{\frac{1}{xy}} + z^{\frac{1}{xy}} x^{\frac{1}{yz}} \right)^{\frac{1}{x}}} \\ &= \frac{4abcxyz}{\left(\frac{x^{\frac{1}{yz}} y^{\frac{1}{xz}} + y^{\frac{1}{xz}} z^{\frac{1}{xy}} + z^{\frac{1}{xy}} x^{\frac{1}{yz}} + x^{\frac{1}{yz}} y^{\frac{1}{xz}} + y^{\frac{1}{xz}} z^{\frac{1}{xy}} + z^{\frac{1}{xy}} x^{\frac{1}{yz}} - 3 \right)^{\frac{1}{x}}} \\ &= \frac{4abcxyz}{\left(\frac{(x+y+z)(xy+yz+zx)}{xyz} - 3 \right)^{\frac{1}{x}}} \\ &= \frac{4abcxyz}{(x+y+z-3)^2}. \end{aligned}$$

۵. (IMO ۲۰۲۰) اعداد حقیقی a, b, c, d به گونه‌ای هستند که $a \geq b \geq c \geq d > 0$ و $a + b + c + d = 1$. ثابت کنید که:

$$(a + 2b + 3c + 4d)a^a b^b c^c d^d < 1$$

اثبات: با استفاده از نامساوی میانگین حسابی-هندسی وزن دار داریم:

$$a^a b^b c^c d^d \leq \sum_{cyc} \frac{a}{a+b+c+d} \cdot a = a^2 + b^2 + c^2 + d^2.$$

در نتیجه، کافی است که ثابت کنیم:

$$(a^2 + b^2 + c^2 + d^2)(a + 2b + 3c + 4d) \leq 1 = (a + b + c + d)^2.$$

هر دو طرف را باز می‌کنیم تا به شکل زیر برسیم:

$$\begin{array}{cccccccc} +a^3 & +b^3a & +c^3a & +d^3a & +a^3 & +2b^3a & +3c^3a & +3d^3a \\ +2a^3b & +2b^3 & +2bc^3 & +2d^3b & +2a^3b & +b^3 & +2bc^3 & +2d^3b \\ +2a^3c & +2b^3c & +3c^3 & +3d^3c & +2a^3c & +2b^3c & +c^3 & +3d^3c \\ +4a^3d & +4b^3d & +4c^3d & +4d^3 & +2a^3d & +2b^3d & +3c^3d & +d^3 \\ & & & & +6abc & +6bcd & +6cda & +6dab \end{array} <$$

به بیان دیگر، باید ثابت کنیم که:

$$\begin{array}{cccccccc} +b^3 & +2c^3 & +a^3d & +b^3d & +2b^3a & +2c^3a & +2d^3a & +a^3b \\ +c^3d & +3d^3 & & & +bc^3 & +d^3b & +6abc & +6bcd \\ & & & & +6cda & +6dab & & \end{array} <$$

این نتیجه حاصل می‌شود چون:

$$2b^3a \geq b^3 + b^3d$$

$$2c^3a \geq 2c^3$$

$$2d^3a \geq 2d^3$$

$$a^3b \geq a^3d$$

$$bc^3 \geq c^3d$$

$$d^3b \geq d^3$$

$$\text{و } 6(abc + bcd + cda + dab) > 0$$

۵.۵ تمارین برای تسلط بیشتر

۱. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید، ثابت کنید که:

$$\frac{ab(a^{\frac{1}{2}} + b^{\frac{1}{2}})}{a + b} \geq \sqrt[2]{a^{\frac{1}{2}} b^{\frac{1}{2}}}.$$

۲. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $\sum_{cyc} a = 1$ ثابت کنید که:

$$\prod_{cyc} a^a + \prod_{cyc} a^b + \prod_{cyc} a^c \leq 1.$$

۳. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید، ثابت کنید که:

$$\prod_{cyc} a^a \geq \prod_{cyc} a^b.$$

۴. فرض کنید $n \geq 3$ یک عدد صحیح باشد، اعداد $x_1, x_2, \dots, x_n \in \mathbb{R}^+$ در نظر بگیرید به طوری که،

$$x_1 + x_2 + \dots + x_n = 1$$

$$x_1^{1-x_2} + x_2^{1-x_3} + \dots + x_{n-1}^{1-x_n} + x_n^{1-x_1} < 2.$$

۵. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید، ثابت کنید که:

$$\prod_{cyc} (a + b - c)^a \leq \prod_{cyc} a^a.$$

۶. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید، ثابت کنید که:

$$\left(\frac{\sum_{cyc} a}{3} \right) \sum_{cyc} a \geq \prod_{cyc} a^b.$$

۷. اعداد $a, b, c, p, q, r \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $\sum_{cyc} p = 1$ ثابت کنید که:

$$\sum_{cyc} a \geq \sum_{cyc} a^p + b^q + c^r.$$

۸. اعداد $a, b, c \in \mathbb{R}^+$ را در نظر بگیرید به طوری که $\sum_{cyc} \frac{1}{a} = 1$ ثابت کنید که:

$$\sum_{cyc} a^{abc} \geq 27 \sum_{cyc} ab.$$



روش‌های احتمالاتی

۱.۶ مقدمه و تعاریف

در مدرسه با مفهوم احتمال هم‌شانس آشنا شده‌اید، مثل پرتاب تاس یا انداختن یک سکه سالم. در این نوع پدیده‌ها مجموعه‌ای از اتفاقات داریم که با احتمال برابر رخ می‌دهند. حال به دنبال این هستیم که بدانیم چقدر احتمال دارد یک عضو این مجموعه عضو یک زیرمجموعه مشخص باشد، به عنوان مثال چقدر احتمال دارد که نتیجه پرتاب یک تاس عضو زیرمجموعه اعداد فرد باشد. پاسخ همان فرمول تعداد حالات مطلوب تقسیم بر کل حالات است. در بعضی موارد همه اتفاقات هم‌شانس نیستند، مثلاً سکه‌ی دست‌کاری شده‌ای را در نظر بگیرید که احتمال شیر آمدن آن بیشتر از خط آمدن است. بیان ریاضی این موضوع چنین است که مجموعه

$$\{x_1, x_2, \dots, x_n\}$$

از اتفاقات ممکن داریم، که آن را فضای حالات می‌نامند، و به نوعی به این اتفاقات اعداد $p(x_1), p(x_2), \dots, p(x_n)$ را نسبت داده‌ایم که $p(x_i)$ احتمال رخ دادن واقعه x_i باشد. از آن جا که از بین این اتفاقات حتماً یکی رخ می‌دهد باید داشته باشیم: $\sum_{i=1}^n p(x_i) = 1$. در این حالت برای حساب کردن احتمال این که یک عضو مجموعه در یک زیرمجموعه مشخص آمده باشد باید احتمال اعضای آن زیرمجموعه را با هم جمع زد. توجه به موضوع ساده زیر گاهی در حل مسائل راهگشاست.

گزاره ۱.۱.۶

اگر احتمال این که عضوی در یک زیرمجموعه مشخص وجود داشته باشد، ناصفر باشد، قطعاً آن زیرمجموعه ناتهی است.

روش استفاده به این صورت است که گاهی برای اثبات این که موجودی با خاصیت مطلوب مساله وجود دارد ثابت می‌کنیم که اگر موجود را به تصادف انتخاب کنیم با احتمال مثبتی خاصیت مطلوب را داراست. یک ابزار مهم در محاسبه احتمال، احتمال شرطی است که به ما امکان می‌دهد مسائل پیچیده را به مسائل ساده‌تر بشکنیم. احتمال شرطی به صورت زیر تعریف می‌شود

$$p(a|b) = \frac{p(A \cap b)}{p(b)}$$

خاصیت مهمی که احتمال شرطی را سودمند می‌کند این است که اگر زیرمجموعه‌های $b_1, b_2, \dots, b_k$ افزایی از فضای حالات به ما بدهند خواهیم داشت:

$$p(a) = \sum_{i=1}^k p(a|b_i)p(b_i)$$

حال فرض کنید ما در حال انجام یک بازی هستیم و مثلاً اگر عدد رو شده تاس فرد باشد، مقدار مشخصی پول برنده

می‌شویم. یک سوال طبیعی این است که اگر این بازی را به دفعات تکرار کنیم به طور میانگین چقدر پول برنده خواهیم شد. این موضوع جدا از حل مسائل ریاضی در دنیای واقعی هم دارای اهمیت است. به عنوان مثال فرض کنید برای شرکت در بازی شما لازم باشد یک ورودی پرداخت کنید، اگر میانگین برد شما در بازی از ورودیه خیلی کمتر باشد، آیا منطقی است در آن بازی شرکت کنید؟

روش مدل کردن ریاضی مساله بالا مفهومی است به عنوان متغیر تصادفی. فرض کنید یک مجموعه داریم که هر عضو آن به احتمال مشخصی اتفاق می‌افتد. یک متغیر تصادفی تابعی از این مجموعه به اعداد حقیقی است.

مثال ۱.۱.۶

فرض کنید مجموعه ما تمام حالات ممکن یک سکه در صد بار پرتاب باشد و X را تابعی تعریف کنید که به یک حالت تعداد سکه‌های رو آمده را نسبت می‌دهد. این تابع مثالی از یک متغیر تصادفی است. می‌توان متغیر تصادفی X_i را این گونه تعریف کرد که اگر سکه i ام شیر آمده باشد مقدار یک و در غیر این صورت مقدار صفر بگیرد. در این صورت خواهیم داشت $X = \sum_{i=1}^{100} X_i$

مثال ۲.۱.۶

مجموعه تمام رئوس یک گراف را در نظر بگیرید و فرض کنید احتمال انتخاب تمام رئوس برابر باشد. متغیر Y که به هر راس درجه آن را نسبت می‌دهد مثالی از یک متغیر تصادفی است.

حال به مساله میانگین پول‌های برنده شده برگردیم. به طور ریاضی این موضوع را امید ریاضی می‌نامند.

تعریف ۱.۱.۶

اگر $X: M \rightarrow \mathbb{R}$ یک متغیر تصادفی باشد امید ریاضی X را بصورت زیر تعریف می‌کنیم:

$$E(X) = \sum_{m \in M} p(m)X(m)$$

امید ریاضی خاصیت ساده ولی مفیدی دارد که می‌توان آن را به سادگی چک کرد، داریم $E(X + Y) = E(X) + E(Y)$. امید ریاضی نوع میانگین وزن دار است و بنابراین در خاصیت ساده زیر صدق می‌کند که در حل برخی مسائل مفید است.

گزاره ۲.۱.۶

همواره عضو m از فضای حالات وجود دارد که $X(m) \geq E(X)$

امید ریاضی خواص مهم دیگری هم دارد که در این مقاله به آن نخواهیم پرداخت، از جمله همان شهود ما که اگر یک متغیر تصادفی را به تعداد زیاد تکرار کنیم و از آن میانگین بگیریم به احتمال بالا مقداری نزدیک به امید ریاضی به دست خواهیم آورد یا این که مقدار یک متغیر تصادفی به احتمال زیادی در حوالی امید ریاضی آن متغیر است.

۲.۶ کاربرد احتمال در حل مسائل

در این بخش قصد داریم چند مساله جالب را به کمک گزاره‌های ساده بالا ثابت کنیم. ابتدا از کاربردی از ساده‌ترین گزاره شروع کنیم، اگر احتمال تمام حالات ممکن را با هم جمع کنیم حاصل برابر یک خواهد بود.

مساله ۱.۲.۶ (لنینگراد ۱۹۸۷)

مجموعه‌های $A_1, A_2, \dots, A_s$ زیرمجموعه‌هایی از $\{1, 2, \dots, m\}$ هستند که هیچ کدام زیرمجموعه دیگری نیست و تعداد اعضای A_i برابر a_i است. ثابت کنید

$$\sum \frac{1}{\binom{M}{a_i}} \leq 1$$

راه حل. برای اثبات این مساله، به تصادف یک جایگشت از اعداد $\{1, 2, \dots, m\}$ انتخاب کنید. بنا بر تقارن، احتمال این که a_i جمله ابتدایی این جایگشت اعضای مجموعه A_i باشند برابر است با

$$\frac{1}{\binom{M}{a_i}}$$

توجه کنید که دو اتفاق از این جنس نمی‌توانند همزمان رخ دهند زیرا هیچ A_i ای زیرمجموعه A_j دیگری نیست، پس جمع احتمال این اتفاقات از یک کمتر یا مساوی است که همان خواسته مساله است.

حال ببینید می‌توانید مساله زیر را حل کنید:

مساله ۲.۲.۶ (لیست کوتاه جهانی ۲۰۰۶)

فرض کنید S مجموعه‌ای متناهی از نقاط در صفحه است که هیچ سه تایی هم خط نیستند، برای هر چندضلعی محدب P برای $a(P)$ ، $b(P)$ را برابر تعداد رئوس چندضلعی و $c(P)$ را برابر تعداد رئوس S خارج چندضلعی تعریف کنید. (فرض کنید پاره خط یک چندضلعی محدب دو راسی، نقطه یک چندضلعی محدب یک راسی و تهی یک چندضلعی محدب صفر راسی است). ثابت کنید

$$\sum x^{a(P)} (1-x)^{b(P)} = 1$$

حال اجازه دهید به سراغ ایده ۲.۱.۶ برویم.

خوب است قبل از خواندن پاسخ خودتان کمی روی مساله زیر فکر کنید.

مساله ۳.۲.۶

یک جدول 100×100 داریم، اعداد یک تا ۱۰۰ را طوری در این جدول نوشته‌ایم که همه اعداد به تعداد یکسان آمده‌اند. ثابت کنید یک سطر یا ستون هست که در آن حداقل ده عدد متمایز آمده است.

راه حل. متغیر تصادفی X را تعریف کنید که به یک سطر یا ستون تعداد اعداد متمایز آن را نسبت دهد. هم چنین متغیر X_i را تعریف کنید که به هر سطر یا ستون عدد یک را نسبت می‌دهد اگر i در آن سطر یا ستون آمده باشد و در غیر این

صورت عدد صفر را نسبت می‌دهد. داریم $X = X_1 + X_2 + \dots + X_{1600}$ بنابراین $E(X) = \sum E(X_i)$. از طرفی E_i بیشتر است از نسبت تعداد سطر و ستون‌هایی که i در آن آمده به کل سطرها و ستون‌ها و بنابراین حداقل برابر ۱۰ است. بنابراین داریم $E(X) \geq \frac{1600 \times 10}{1600} = 10$

حال مساله‌ای سخت‌تر ببینید.

مساله ۴.۲.۶ (روسیه ۱۹۹۶)

مجلس روسیه ۱۶۰۰ عضو دارد و ۱۶۰۰۰ کمیته ۸۰ نفری در آن وجود دارد. ثابت کنید دو کمیته وجود دارند که چهار عضو مشترک دارند.

راه حل. متغیر تصادفی X را در نظر بگیرید که به دو کمیته تصادفی، تعداد اعضای مشترک آن دو کمیته را نسبت می‌دهد. هم‌چنین متغیر تصادفی X_i را متغیری تعریف کنید که $X_i = 1$ اگر نفر i - ام عضو مشترک این دو کمیته باشد و در غیر این صورت $X_i = 0$. واضح است که

$$X = X_1 + X_2 + \dots + X_{1600}$$

بنابراین $E(X) = \sum E(X_i)$. از طرفی $E(X_i)$ برابر است با نسبت تعداد جفت کمیته‌هایی است که شامل i باشند به کل جفت کمیته‌ها، اگر این فرد در n_i کمیته عضو باشد $E(X_i) = \frac{\binom{n_i}{2}}{\binom{16000}{2}}$. چیزی که در مورد n_i ها می‌دانیم این است که جمعشان برابر است با 16000×80 پس داریم

$$\begin{aligned} E(X) &= \frac{1}{\binom{16000}{2}} \left(\binom{n_1}{2} + \binom{n_2}{2} + \dots + \binom{n_{16000}}{2} \right) > \frac{1600}{\binom{16000}{2}} \left(\frac{n_1 + n_2 + \dots + n_{16000}}{2} \right) \\ &= \frac{1600}{\binom{16000}{2}} \binom{800}{2} > 3 \end{aligned}$$

در این مساله بالا از این نابرابری معروف اثبات کردیم که اگر $\sum n_i$ ثابت باشد، $\sum \binom{n_i}{2}$ ها وقتی کمینه است که n_i ها برابر باشند.

حال خودتان سعی کنید با این ایده دو مساله زیر را حل کنید.

مساله ۵.۲.۶ (انتخاب تیم ۲۰۰۸ ایران)

۷۷۹ تیم در یک لیگ والیبال شرکت کرده‌اند. هر دو تیمی دقیقاً یک بار با هم بازی می‌کنند. ثابت کنید زیر مجموعه‌های هفت عضوی A, B از تیم‌ها پیدا می‌شود که هر تیم A هر تیم B را برده باشد.

مساله ۶.۲.۶ (لیست کوتاه جهانی ۹۹)

فرض کنید یک مجموعه n عضوی از باقی‌مانده‌ها به پیمانه n^2 داریم. ثابت کنید مجموعه n عضوی از باقی‌مانده‌ها همچون B وجود دارد که حداقل نصف باقی‌مانده‌ها به فرم

$$a + b, a \in A, b \in B$$

باشند.

حال بگذارید سراغ سوالاتی برویم که دید احتمالاتی حتی کمک بیشتری به حل آن‌ها بکند.

مساله ۷.۲.۶ (روسیه ۱۹۹۹)

تعدادی پسر و مرد داریم که هر پسر حداقل با یک استاد مرد دسته داده است و برعکس و هیچ دو پسر یا دو مردی با هم دست نداده‌اند. ثابت کنید زیرمجموعه‌ای وجود دارد که حاقل نیمی از افراد جمع را داشته باشد و هر پسری از این زیرمجموعه با فرد مرد در این زیرمجموعه دست داده باشد.

راه حل. مجموعه تصادفی زیر را تشکیل دهید، طوری که هر مرد را به احتمال $1/2$ انتخاب کنید و سپس هر پسری که با فرد تا از مردهای انتخاب شده دست داده باشد به مجموعه اضافه کنید. ادعا می‌کنیم هر فردی با احتمال $1/2$ در این مجموعه آمده است، در مورد مردها که این موضوع واضح است، اگر یک پسر با a مرد دست داده باشد احتمال این که در این مجموعه بیاید برابر است به احتمال این که تعداد فردی از این a مرد در مجموعه انتخاب شده باشند. به بیان دیگر برابر است با احتمال این که در a بار پرتاب یک سکه، فرد بار شیر بیاید. استدلال شمارشی ساده‌ای نتیجه می‌دهد که این احتمال برابر $1/2$ است، پس هر فرد به احتمال $1/2$ در این مجموعه آمده است پس امید ریاضی تعداد اعضای این مجموعه به اندازه نصف افراد است و کار تمام است.

مساله ۸.۲.۶

فرض کنید فرض کنید در یک جمع n ، نفره دوستی یک رابطه دو طرفه است و میانگین تعداد دوستان یک فرد در این جمع برابر است با d . ثابت کنید برای هر $k \leq d$ می‌توان زیرمجموعه‌ای با حداقل $\frac{kn}{d+1}$ عضو از آن انتخاب کرد که هیچ $k+1$ نفری در این زیرمجموعه دودو با هم دوست نباشند.

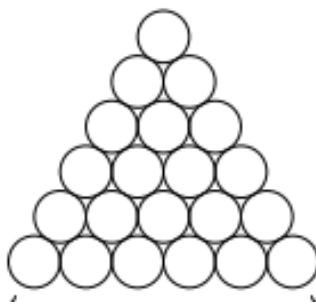
راه حل. مساله را با گراف مدل کنید. ابتدا یک جایگشت تصادفی از راس‌ها انتخاب کنید، به ترتیب جلو بروید و هر راسی که حکم را به هم نمی‌زند اضافه کنید. مثل مسائل قبلی متغیر تصادفی X را تعریف کنید که به هر جایگشت اندازه مجموعه درست‌شده با این الگوریتم را نسبت دهد و متغیرهای X_i که بسته به این که راس i ام در این جایگشت عضو مجموعه بوده یا نه صفر یا یکند.

راس v را در نظر بگیرید و فرض کنید ترتیب این راس و رؤوس متصل به آن در جایگشت $v_1, v_2, \dots, v_{d_v+1}$ باشد. اگر v در بین $v_1, v_2, \dots, v_k$ باشد اضافه کردن آن قطعاً گراف کامل $k+1$ راسی ایجاد نمی‌کند چرا که درجه راس v حداکثر برابر k خواهد بود پس

$$E(X) > \sum \frac{k}{d_v+1} > \frac{nk}{d+1}$$

مساله ۹.۲.۶ (ساده شده سوال پنج جهانی ۲۰۲۳)

فرض کنید n یک عدد طبیعی باشد. تعداد $\frac{n(n+1)}{2}$ دایره را روی هم چیده‌ایم. یک مسیر نینجا مسیری است که از دایره بالا شروع می‌شود و هر مرحله به یکی از دو دایره زیری می‌رود ثابت کنید اگر از هر سطر یک دایره قرمز شود همواره می‌توان یک مسیر نینجا یافت که از $l n n$ دایره قرمز بگذرد.



شکل ۱. ساده شده جهانی!

راه حل. یک مسیر تصادفی انتخاب کنید. امید ریاضی تعداد خانه‌های قرمز این مسیر را مشاهده می‌کنیم. در سطر i امید ریاضی تعداد خانه‌های قرمزی که مسیر از آن می‌گذرد $1/i$ است پس به خاطر جمع بودن امید ریاضی، امید ریاضی کل تعداد خانه‌ها برابر است با $\sum \frac{1}{i} \approx l n n$.

مساله ۱۰.۲.۶

هر طور یک گراف n راسی را با $m > 5n$ یال را روی صفحه رسم کنیم حداقل $\frac{4m^2}{243n^2}$ تقاطع بین یال‌ها خواهیم داشت

راه حل. برای یک گراف فرض کنید $cr(G)$ حداقل تعداد تقاطع‌های ممکن در روش‌های مختلف کشیدن G باشد. گراف G را با $cr(G)$ تقاطع رسم کنید و هر راس G را به احتمال p انتخاب کنید که زیرگراف G_p از G بدست آید. اگر $X(G_p)$ تعداد تقاطع‌های گراف G_p در این کشیدن خاص باشد داریم $X(G_p) \geq cr(G_p)$ مساله ترکیبیاتی معروف و نه چندان سختی است که تعداد تقاطع‌های یک گراف با v راس و e یال حداقل $3v - e$ است. بنابراین

$$X(G_p) > e(G_p) - 3v(G_p)$$

از دو طرف امید ریاضی بگیرید. هر تقاطع G به احتمال p^4 در G_p ظاهر می‌شود بنابراین $E(X(G_p)) = p^4 cr(G)$. پس داریم

$$p^4 cr(G) > p^2 m - 3pn$$

با انتخاب $p = \frac{2}{9}$ حکم مورد نظر ثابت می‌شود.

۳.۶ مسائلی برای فکر کردن

مساله ۱.۳.۶

هر گراف m راسی یک زیرگراف دوبخشی القایی با $m/2$ یال دارد.

مساله ۲.۳.۶

فرض کنید $R(s)$ کوچکترین عددی باشد که هر طور یال‌های گراف کامل $R(s)$ عضوی را با رنگ‌های قرمز و آبی رنگ کنیم یک زیرگراف s راسی کامل قرمز یا آبی داشته باشیم. ثابت کنید $R(s) > 2^{\frac{s}{2}}$

مساله ۳.۳.۶

فرض کنید $p, q > 0$ اعدادی حقیقی‌اند که $p + q = 1$ ثابت کنید

$$(1 - p^m)^n + (1 - q^n)^m \geq 1$$

مساله ۴.۳.۶ (لیست کوتاه جهانی ۸۷)

ثابت کنید می‌توان مجموعه $\{1, 2, \dots, 1987\}$ را با چهار رنگ رنگ کرد طوری که هیچ تصاعد حسابی به طول ده و تکرنگ وجود نداشته باشد.

مساله ۵.۳.۶ (لیست کوتاه جهانی ۸۹)

به هر راس یک گراف دوبخشی $\log_2 n + 1$ رنگ نسبت داده‌ایم. ثابت کنید می‌توان برای هر راس یک رنگ انتخاب کرد طوری که هیچ دو راس مجاور هم‌رنگ نباشند.

مساله ۶.۳.۶ (مرحله دو آمریکا ۲۰۱۶)

فرض کنید ۱۳۶ زوج مرتب از اعداد حقیقی روی تخته نوشته شده است طوری که از بین (k, k) و $(-k, -k)$ حداکثر یکی ظاهر شود. علی تعدادی از اعداد نوشته شده را پاک می‌کند، طوری که جمع هیچ دو عدد پاک‌شده‌ای صفر نشود. سپس علی به اندازه تعداد زوج‌های مرتبی که عددی از آن پاک شده باشد امتیاز می‌گیرد. حداکثر امتیازی که علی می‌تواند از گرفتن آن مطمئن باشد چقدر است؟

مساله ۷.۳.۶ (سوئد ۲۰۱۰)

شهری n شهروند دارد، هر دو نفر حداقل یک دوست مشترک دارند. ثابت کنید $\frac{n}{3}$ نفر هستند که هر فردی از آن‌ها حداقل یک دوست بین خودشان دارد. آیا می‌توانید کران بهتری ارائه دهید؟

مساله ۸.۳.۶

آمنه و باران قصد دارند تنیس بازی کنند. آمنه در هر دستی که سرویس می‌زند به احتمال شصت درصد برنده می‌شود و آمنه در هر دستی که سرویس می‌زند به احتمال پنجاه درصد. هر کسی دوازده پیروزی به دست بیاورد برنده بازی می‌شود. کدام روش سرویس زدن برای آمنه بهتر است این که یکی در میان سرویس بزنند یا هر کسی که برنده شد سرویس بعدی را بزنند.

مساله ۹.۳.۶ (روسیه ۲۰۲۴)

در یک کشور $n > 100$ شهر وجود دارند که در ابتدا جاده‌ای بین آن‌ها نیست. دولت دیار کفر هزینه احداث هر جاده را عددی تصادفی بین یک تا $\frac{n(n-1)}{4}$ تتر اعلام می‌کند. شهردار هر شهر ارزان‌ترین جاده از بین $n-1$ جاده ممکن را انتخاب می‌کند و آن را احداث می‌کند. امید ریاضی تعداد مولفه‌های همبندی را بدست آورید.

مساله ۱۰.۳.۶ (لیست کوتاه جهانی ۱۹۸۶)

فرض کنید n, k اعدادی طبیعی اند و n نقطه در صفحه داریم طوری که هیچ دو نقطه‌ای هم خط نیستند و برای هر نقطه‌ای حداقل k نقطه با فاصله برابر از آن وجود دارند. ثابت کنید $\frac{1}{4} + \sqrt{2n} \leq$.

مساله ۱۱.۳.۶ (لیست کوتاه جهانی ۱۹۸۹)

فرض کنید n نقطه در صفحه داریم که فاصله‌هایشان دو بده متمایز است و r تا از پاره‌خط‌های بین این نقاط را قرمز کرده‌ایم. اگر $m = \lceil \frac{2r}{n} \rceil$ ثابت کنید مسیر قرمز رنگی با m پاره‌خط وجود دارد که طول پاره‌خط‌ها صعودی باشد.

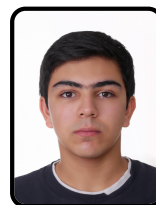
مساله ۱۲.۳.۶

ثابت کنید اگر تمام یال‌های یک گراف کامل n عضوی را با تعدادی گراف دوبخشی بیوشانیم جمع تعداد رئوس این گراف‌های دوبخشی حداقل $n \log_2 n$ هست.

مساله ۱۳.۳.۶

اگر $A = A_1 \times A_2 \times \dots \times A_n$ که A_i ها مجموعه‌هایی متناهی هستند، یک آجر ضرب زیرمجموعه‌ای است که از ضرب زیرمجموعه‌های سره A_i ها بدست آید. ثابت کنید A را نمی‌توان با کمتر از 2^n آجر پوشاند.

ما در عصر جدید بسر می‌بریم
عصر جدید
عصر قاطعیت تردید
عصری که در آن هیچ اصلی جز اصل احتمال یقینی نیست
عصر پیش‌بینی هوا
از هر طرف که باد بوزد...
اما
من بی تو حتی یک لحظه احتمال ندارم
چشمان تو عین‌الیقین من
قاطعیت نگاه تو دین من است
من بی تو ناگزیرم
من بی نام ناگزیر تو می‌میرم
-- قیصر امین‌پور



زیگموندی

۱.۷ مقدمه

۱.۱.۷ چکیده

در این مقاله قصد داریم کاربرد دسته‌ای از چندجمله‌ای‌ها به نام چندجمله‌ای‌های دایره بر^۱ را در نظریه اعداد بررسی کنیم. ابتدا مقداری مطالب نظری خواهیم گفت و سپس قضیه زیگموندی را بررسی می‌کنیم و در نهایت با این قضیه چندین سوال المپیاد را حل می‌کنیم.

۲.۱.۷ چرا؟

اگر تا حالا با اعداد مختلط کار کرده باشید احتمالاً درباره ریشه‌های واحد شنیدید و با آنها کار کرده‌اید. ω را ریشه سوم واحد تعریف کنید. می‌دانیم که ω و ω^2 و ۱ ریشه‌های چندجمله‌ای $x^3 - 1$ هستند. اما سوالی که پیش می‌آید این است که چندجمله‌ای مینیمال ریشه‌های سوم واحد چی هست؟ در واقع ۱ که ریشه بدیهی معادله قبلی بود، ریشه $x - 1$ است اما ω و ω^2 ریشه‌های $x^2 + x + 1$ اند و می‌دانیم این چندجمله‌ای در $\mathbb{Z}[x]$ تجزیه‌ناپذیر است، یعنی به صورت ضرب دو چندجمله‌ای ضریب صحیح نمی‌توان آن را نمایش داد. پس این چندجمله‌ای مینیمال ریشه‌های نابديهی سوم واحد است (چرا؟). همین کار را می‌توان برای ریشه‌های ۴ام واحد انجام داد و چندجمله‌ای مینیمال ریشه‌های نابديهی آن را (یعنی i و $-i$) ساخت که می‌شود $x^2 + 1$. سوالی که پیش می‌آید این است که چطور می‌توان این چندجمله‌ای‌ها را برای ریشه‌های n ام واحد ساخت؟ این چندجمله‌ای‌ها چه خواص دیگه‌ای دارند؟

تعریف ۱.۱.۷

عدد مختلط ω را ریشه n ام واحد می‌نامیم اگر $\omega^n = 1$.

تعریف ۲.۱.۷

عدد مختلط ω را ریشه اولیه n ام واحد می‌نامیم اگر $\omega^n = 1$ باشد و هیچ $r \in \mathbb{N}$ که $r < n$ وجود نداشته باشد که $\omega^r = 1$.

برای مثال i ریشه ۸ام واحد است، اما ریشه اولیه ۸ام واحد نیست؛ زیرا $i^4 = 1$.

۲.۷ چندجمله‌ای‌های دایره‌بر

۱.۲.۷ تعاریف

ریشه‌های واحد ϵ ام را در نظر بگیرید، چندجمله‌ای می‌خواهیم بسازیم که w_1^{ϵ} و w_2^{ϵ} ریشه‌های آن باشند اما w_3^{ϵ} و w_4^{ϵ} ریشه‌های آن نباشند. زیرا w_1^{ϵ} و w_2^{ϵ} ریشه‌های اولیه ϵ ام واحد هستند اما w_3^{ϵ} و w_4^{ϵ} دیگر ریشه اولیه نیستند؛ زیرا با رسیدن به توانی کوچکتر از ϵ (در اینجا ۲)، به یک تبدیل می‌شوند. و این ما را مجاب میکند که تعریف زیر را ارائه بدهیم.

تعریف ۱.۲.۷

چندجمله‌ای n ام دایره‌بر با نماد $\Phi_n(x)$ را به صورت زیر تعریف می‌کنیم:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \omega_n^k)$$

که در آن ω_n یک ریشه اولیه n ام واحد است.

در واقع این تعریف معادل با چندجمله‌ای تکین هست که مرتبه ریشه‌های آن دقیقاً n است (یعنی r ریشه این چندجمله‌ای است اگر و تنها اگر n کمترین عددی باشد که $r^n = 1$). برای مثال چند جمله اول از دنباله $\Phi_n(x)$ را آورده‌ایم:

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

...

در مرحله اول این چندجمله‌ای بدون معنی و منطق خاص و بی‌نظم به نظر می‌رسند اما مشخص می‌شود که پشت هر کدام معنای خاصی نهفته است!

۲.۲.۷ قضایای اولیه

گزاره ۱.۲.۷

برای هر $n \in \mathbb{N}$ ، درجه $\Phi_n(x)$ برابر با $\varphi(n)$ است.

راه‌حل. با توجه به تعریف این چندجمله‌ای اثبات گزاره بالا سخت نیست و به خواننده واگذار می‌شود.

گزاره ۲.۲.۷

برای هر $n \in \mathbb{N}$ ریشه‌های $\Phi_n(x)$ شامل تمام ریشه‌های اولیه n ام واحد است و از هر کدام از آن‌ها دقیقاً یکی در خود دارد (تکرر هر ریشه ۱ است).

گزاره ۳.۲.۷

برای هر $m, n \in \mathbb{N}$ که $m \neq n$ چندجمله‌ای‌های $\Phi_m(x)$ و $\Phi_n(x)$ ریشه مشترکی ندارند.

راه حل. اگر ω ریشه جفت این چندجمله‌ای‌ها باشد، یعنی هم ریشه اولیه n ام واحد است، هم ریشه اولیه m ام واحد. که با توجه به تعریف ریشه اولیه در تناقض است.

گزاره ۴.۲.۷

برای هر $n \in \mathbb{N}$ ، داریم که $x^n - 1 = \prod_{d|n} \Phi_d(x)$

راه حل. می‌دانیم که ریشه‌های چندجمله‌ای $x^n - 1 = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_n)$ همان ریشه‌های n ام واحد هستند که از هر کدام دقیقاً یکی داخل این چندجمله‌ای وجود دارد (چرا؟). حال هر کدام از این ریشه‌ها، یک ریشه d ام اولیه واحد است. که یعنی d کوچکترین عددی است که $\omega^d = 1$ با توجه به اینکه $\omega^n = 1$ نتیجه می‌گیریم که n بر d بخش‌پذیر است. پس اینگونه توانستیم ثابت کنیم ω که ریشه‌ای دلخواه در $x^n - 1$ است، ریشه $\Phi_d(x)$ نیز هست که $d | n$. از آن طرف مشخص است که چندجمله‌ای‌های عبارت سمت راست ریشه‌ای مشترک با هم ندارند؛ و ریشه هر کدام درون چندجمله‌ای سمت چپ هست (چرا؟). و اینگونه ثابت می‌شود که ریشه‌های دو طرف عبارت برابرند و از هر کدام از ریشه‌ها تکرر ۱ داریم. و حکم گزاره نتیجه می‌شود.

نتیجه ۱.۲.۷

برای هر $n \in \mathbb{R}$ داریم که $\sum_{d|n} \varphi(d) = n$

راه حل. درجات چندجمله‌ای‌های دو طرف را جمع بزنید!

گزاره ۵.۲.۷

برای هر $n \in \mathbb{R}$ داریم که $\Phi_n(x) \in \mathbb{Z}[x]$ ، یعنی که ضرایب $\Phi_n(x)$ صحیح‌اند.

راه حل. استقرا می‌زنیم، برای $\Phi_1(x) = x - 1$ گزاره درست است. حال فرض کنید به ازای هر $1 \leq k < n$ این حکم درست است. ثابت می‌کنیم $\Phi_n(x)$ نیز ضریب صحیح است. $P_n(x)$ را اینطور در نظر بگیرید:

$$P_n(x) = \prod_{d|n, d \neq n} \Phi_d(x)$$

طبق استقرا می‌دانیم که $P_n(x) \in \mathbb{Z}$ و همچنین تکیه است. پس می‌توان $x^n - 1$ را بر $P_n(x)$ تقسیم کرد یعنی $Q, R \in \mathbb{Z}$ وجود دارند طوری که

$$x^n - 1 = P_n(x).Q(x) + R(x)$$

طوری که $\deg R < \deg P_n$ یا $R = 0$. اگر حالت اول اتفاق بیفتد، در این صورت اگر تمام $n - \varphi(n)$ ریشه $P_n(x)$ را در معادله جایگذاری کنیم متوجه خواهیم شد که $R(x)$ حداقل $n - \varphi(n)$ ریشه دارد پس درجه‌اش هم حداقل $n - \varphi(n)$ است و این با این گزاره که $\deg R < \deg P_n$ تناقض دارد. پس $R = 0$ و طبق تعریف می‌دانیم که $x^n - 1 = P_n(x).\Phi_n(x)$ پس $Q(x) = \Phi_n(x) \in \mathbb{Z}[x]$ می‌دهد این نتیجه می‌دهد.

اکنون می‌دانیم که این چندجمله‌ای‌ها ضریب صحیح‌اند. احتمالاً مشتاق هستید تا اثبات تجزیه‌ناپذیر بودن آنها را بدانید. خب متأسفانه فعلاً ابزار و دانش کافی برای اثبات این قضیه را نداریم اما می‌توانیم آن را در حالت خاص $n = p$ حل کنیم!

گزاره ۶.۲.۷

به ازای هر p اول، چندجمله‌ای $\Phi_p(x)$ در $\mathbb{Z}[x]$ تجزیه‌ناپذیر است.

ابتدا لازم است تا لمی را بیان کنیم.

لم ۱.۲.۷ (محک آیزنشتاین)

فرض کنید $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ چندجمله‌ای در $\mathbb{Z}[x]$ باشد و p عددی اول باشد به طوری که

$$1. \quad \forall i, 0 \leq i \leq n-1: p \mid a_i$$

$$2. \quad p \nmid a_n$$

$$3. \quad p^2 \nmid a_0$$

در این صورت $P(x)$ در $\mathbb{Z}[x]$ تجزیه‌ناپذیر است.

اثبات این لم در این مقاله نمی‌گنجد اما می‌توانید اثبات آن را در فصل بخش پذیری در $\mathbb{Z}[x]$ کتاب نظریه‌اعداد نوشته دکتر مریم میرزاخانی و رویا بهشتی زواره بخوانید.

حال به اثبات برگردیم، برای اثبات این گزاره کفایت ثابت کنیم $\Phi_p(x+1)$ تجزیه‌ناپذیر است. دقت کنید که

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}$$

و این نیز طبق محک آیزنشتاین تجزیه‌ناپذیر است.

حال یک سوال بسیار جالب پیش می‌آید، تا آنجایی که مشاهده کردیم تمامی ضرایب $\Phi_n(x)$ ، $1, -1, 0$ بودند! آیا این درست است که برای هر $n \in \mathbb{N}$ ضرایب $\Phi_n(x)$ ، $1, -1, 0$ اند؟ جواب این سوال خیر است؛ اما شرط لازم و کافی برای n که $\Phi(n)$

فقط ضرایب ۰ و ۱- و ۱ داشته باشد چیست؟

پیشنهاد می‌کنم ابتدا مطالب بخش بعدی را بخوانید سپس روی این سوال فکر کنید اما می‌توانید با مطالبی که تا الان گفته شده است نیز به این سوال فکر کنید و خودتان را به چالش بکشید!

۳.۲.۷ رابطه‌ای مهم بین این چندجمله‌ای‌ها

در اینجا می‌خواهیم گزاره‌ای را ثابت کنیم که به ما در اثبات زیگموندی کمک می‌کند و روش جالبی برای محاسبه چندجمله‌ای‌های دایره‌بر ارائه می‌دهد.

گزاره ۷.۲.۷

فرض کنید $n \in \mathbb{N}$ و p عددی اول است. در این صورت

$$\begin{cases} \Phi_{np}(x) = \Phi_n(x^p) & p \mid n \\ \Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)} & p \nmid n \end{cases}$$

راه حل. ابتدا حالتی که $p \nmid n$ را ثابت می‌کنیم. طبق گزاره ۱.۲.۷ می‌دانیم درجه هر دو طرف برابر است پس کافی است ثابت کنیم هر ریشه pn ام اولیه واحد یک ریشه از سمت راست هم هست. برای این هم ω_{pn}^k را طوری که $\gcd(k, pn) = 1$ در نظر بگیرید که یک ریشه اولیه pn ام واحد است؛ و سپس این عدد را در سمت راست جایگذاری کنید. در این صورت مخرج سمت راست ۰ نمی‌شود (زیرا این عدد ریشه اولیه n ام واحد نیست که در $\Phi_n(x)$ صفر شود) اما $(\omega_{pn}^k)^p = \omega_{pn}^{pk}$ یک ریشه اولیه n ام واحد است (چرا؟). بنابراین ω_{pn}^k ریشه چندجمله‌ای $\Phi_n(x^p)$ خواهد شد و مقدار این چندجمله‌ای در این نقطه ۰ می‌شود. پس صورت کسر سمت راست ۰ است و حکم با توجه به برابری درجه این دو چندجمله‌ای ثابت می‌شود. حالت $p \mid n$ نیز کاملاً مشابه حل می‌شود.

نتیجه ۲.۲.۷

اگر n عددی فرد باشد در این صورت $\Phi_{pn}(x) = \Phi_n(-x)$

۳.۷ مرتبه!

۱.۳.۷ چند لم جالب

احتمالاً با مفهوم مرتبه در نظریه اعداد آشنا هستید و کاربرد آن را در مسائل المپیاد دیده‌اید. اگر دقت کنید تعریف چندجمله‌ای‌های دایره‌بر یا اصلاً خود ریشه‌های اولیه با مرتبه مرتبط هستند. در واقع ریشه‌های اولیه n ام واحد یعنی اعدادی در $\mathbb{C}$ که مرتبه‌شان n هست! سوال جالبی که پیش میاد این هست که آیا میشه این مبحث را به مرتبه روی $\mathbb{Z}_p$ مرتبط کرد؟ برای بررسی این اول به یه لم نیاز داریم.

لم ۱.۳.۷

فرض کنید که m و n ۲ عدد طبیعی اند طوری که $p \nmid mn$. در این صورت روی میدان $\mathbb{Z}_p$ می‌دانیم:

$$\gcd(\Phi_m(x), \Phi_n(x)) = 1$$

راه حل. می‌دانیم که $x^{mn} - 1$ ریشه تکراری ندارد (چون اگر داشته باشد و از آن مشتق بگیریم، این ریشه باید در مشتق آن نیز صدق کند که تناقض است) پس روی $\mathbb{Z}_p$ خالی از مربع هست. حال فرض کنید $\gcd(\Phi_m(x), \Phi_n(x)) = P(x)$ در این صورت چون $x^{mn} - 1 \mid \Phi_m(x) \cdot \Phi_n(x)$ پس $x^{mn} - 1 \mid P(x)^2$ و این با خالی از مربع بودن $x^{mn} - 1$ در تناقض است.

نتیجه ۱.۳.۷

اگر m و n دو عدد طبیعی باشند و p اول طوری که $p \nmid mn$ در این صورت به ازای یک $a \in \mathbb{Z}$ نمی‌تواند همزمان $\Phi_m(a)$ و $\Phi_n(a)$ را عاد کند.

حال با اثبات این لم می‌توانیم گزاره‌ای را ثابت کنیم که می‌توان آن را مهم ترین قضیه چندجمله‌ای‌های دایره‌بر نامید.

گزاره ۱.۳.۷

p عددی اول است، در این صورت به ازای هر $n \in \mathbb{N}$ و هر $a \in \mathbb{Z}$ که $\gcd(n, p) = 1$ داریم که

$$p \mid \Phi_n(a) \iff \text{ord}_p(a) = n$$

راه حل. استقرا می‌زنیم، مورد $n = 1$ بدیهی است. حال فرض کنید به ازای هر $k < n$ درست باشد. حال کافیت تا ثابت کنیم به ازای n نیز درست است. فرض کنید a طوری باشد که $\Phi_n(a) \equiv 0 \pmod{p}$. حال دقت کنید چون $a^n - 1 \mid \Phi_n(a)$ پس $a^n \equiv 1 \pmod{p}$. حال فرض کنید $\text{ord}_p(a) = k \neq n$ در این صورت طبق استقرا داریم که $\Phi_k(a) \equiv 0 \pmod{p}$ پس $\Phi_n(a) \equiv \Phi_k(a) \equiv 0 \pmod{p}$ و این با نتیجه ۱.۳.۷ در تناقض است. حال فرض کنید $\text{ord}_p(a) = n$ در این صورت یعنی $a^n - 1 \equiv 0 \pmod{p}$ و این a ریشه یک $\Phi_k(x)$ هست که $k \mid n$ اما طبق استقرا k نمی‌تواند از n کمتر باشد پس $k = n$ و گزاره ما ثابت می‌شود.

نتیجه ۲.۳.۷

از اینکه $\text{ord}_p(a) = n$ در بالا نتیجه می‌شود که $p - 1 \mid n$ پس $n \equiv 1 \pmod{p}$.

حال می‌خواهیم گزاره‌ای قوی و کاربردی را اثبات کنیم که در اثبات زیگموندی نیز به کمک ما می‌آید و به مرتبه هم مرتبط است.

گزاره ۲.۳.۷

فرض کنید $m \neq n \in \mathbb{N}$ و $h \in \mathbb{Z}$ در این صورت اگر $\gcd(\Phi_m(h), \Phi_n(h)) \neq 1$ آنگاه $\frac{m}{n} = p^k$ و

$$\gcd(\Phi_m(h), \Phi_n(h)) = p^z$$

به ازای یک k و z صحیح.

راه حل. فرض کنید $\Phi_m(x) \equiv \Phi_n(x) \pmod{p}$. حال $m = p^a b$ و $n = p^c d$ طوری که $p \nmid b, d$ حال طبق گزاره ۲.۲.۷ داریم که $\Phi_n(x) \equiv \Phi_d(x)^{p^{c-1}(p-1)} \pmod{p}$ و $\Phi_m(x) \equiv \Phi_b(x)^{p^{a-1}(p-1)} \pmod{p}$ چون داریم $p \nmid bd$ در صورتی که هر دو تا چندجمله‌ای $\Phi_n(x), \Phi_m(x)$ ریشه‌ای مانند r در $\mathbb{Z}_p$ داشته باشند باید $b = d$ که این نتیجه می‌دهد $\frac{m}{n}$ توانی از p است. سپس دقت کنید که $\frac{m}{n}$ در واقع توانی از هر عامل اولی از $\gcd(\Phi_m(h), \Phi_n(h))$ است پس نتیجه می‌شود که $\gcd(\Phi_m(h), \Phi_n(h)) = p^z$.

۲.۳.۷ حالتی از یک قضیه بزرگ

احتمالاً اسم دیریشله به گوشتان خورده است. این قضیه یکی از مهم ترین قضایایی است که راجع به اعداد اول داریم که بسیار کاربردی است و راه ما را برای حل خیلی از سوالات المپیاد هموار می‌کند. اثبات حالت کلی این قضیه بسیار کار سختی هست و در این مقاله نمی‌گنجد، اما با چیزهایی که دیدیم می‌توان حالت خاص آن را حل کرد.

گزاره ۳.۳.۷

به ازای هر $n \in \mathbb{N}$ بینهایت عدد اول مانند p وجود دارد طوری که $p \equiv 1 \pmod{n}$.

راه حل. طبق قضیه بسیار معروف شور می‌دانیم که به ازای هر $P(x) \in \mathbb{Z}[x]$ بینهایت p اول وجود دارد طوری که وجود داشته باشد a طوری که $p \mid P(a)$ حال این قضیه را روی چندجمله‌ای $\Phi_n(x)$ اعمال کنید و با توجه به نتیجه ۱.۳.۷ می‌فهمیم که بینهایت p اول وجود دارد که $p \equiv 1 \pmod{n}$.

۴.۷ زیگموندی

خب رسیدیم به چیزی که منتظرش بودید. اکنون ابزارهای لازم برا اثبات قضیه زیگموندی را داریم. البته این قضیه اثبات‌های دیگری هم دارد که خیلی پیچیده و غیر مقدماتی است و ما به آن‌ها نمی‌پردازیم.

گزاره ۱.۴.۷

فرض کنید $a, b, n \in \mathbb{N}$ و n بیشتر از ۱ باشند. در این صورت عامل اولی مانند q وجود دارد که $a^n \pm b^n$ را عاد کند اما به ازای هر $0 < k < n$ ، $q \nmid a^k \pm b^k$ به جز این ۲ تا حالت خاص:

$$۱. \quad n = 2, a = 2^s - 1, s \geq 2$$

$$۲. \quad n = 6, a = 2$$

در اینجا برای راحتی کار تنها حالت $b = -1$ را حل می‌کنیم اما اثبات حالت کلی نیز کاملاً مشابه است و می‌توانید به عنوان تمرین حالت کلی آن را ثابت کنید! در ابتدا ۲ لم مفید برای اثبات این قضیه بیان می‌کنیم.

لم ۱.۴.۷

فرض کنید a, n دو عدد صحیح بزرگتر از ۱ باشند و داشته باشیم که تمام عوامل اول $\Phi_n(a)$ ، n را عاد کنند. آنگاه داریم که $\Phi_n(a)$ یا مساوی است با ۲ یا مساوی است با یکی از عوامل اول n .

راه حل. فرض کنید $p \mid \Phi_n(a)$ چون ضریب ثابت $\Phi_n(a)$ برابر با یک است پس $\gcd(p, a) = 1$ حال فرض کنید $\text{ord}_p(a) = k$ حال طبق گزاره ۱.۳ می‌دانیم که $p \mid \Phi_k(a)$ و همچنین طبق گزاره ۲.۳.۷ داریم که $\frac{n}{k} = p^t$ به ازای یک t طبیعی (پس منطقاً $p \mid n$)، حال داریم که $\Phi_n(x) \cdot Q(x) = x^n - 1 = \Phi_n(x) \cdot Q(x)$ بدیهی است که $x^{\frac{n}{p}} - 1 \mid Q(x)$ حال لم دو خط می‌زنیم، طبق لم دو خط $v_p(a^n - 1) = v_p(a^{\frac{n}{p}} - 1) + 1$ (چون $k \mid \frac{n}{p}$ پس منطقاً $a^{\frac{n}{p}} - 1 \mid p$ و شرایط لم دو خط زدن را داریم) و اگر به جای x در معادله بالا a را جایگذاری کنید چون $a^{\frac{n}{p}} - 1 \mid Q(a)$ پس $\Phi_n(a)$ نهایت توان عامل p اش یک است و چون فرض کرده بودیم که $p \mid \Phi_n(a)$ پس $p \mid \Phi_n(a)$ حال فرض کنید $\Phi_n(a)$ دو تا عامل اول p, q داشته باشد. در این صورت $k_1 = \text{ord}_p(a)$ و $k_2 = \text{ord}_q(a)$ و اکنون داریم که $\frac{n}{p^{a_1}} \mid p - 1$ و $\frac{n}{q^{a_2}} \mid q - 1$ یعنی $q \mid p - 1$ و $p \mid q - 1$ که این یعنی $p = q$ پس $\Phi_n(a) = p$ طوری که $p \mid n$ فقط حالتی می‌ماند که $\Phi_n(a) \mid 2$ که در این حالت چون a باید فرد باشد پس $k = 1$ پس $n = 2^t$ که در این صورت $\Phi_n(a) = \Phi_{2^t}(a) = a^{2^{t-1}} + 1$ و این هم جز حالت $t = 1$ به پیمانه ۴ می‌شود ۲ پس دوباره $\Phi_n(a) = 2$ مگر اینکه $n = 2$ پس اثبات ما کامل شد.

لم ۲.۴.۷

فرض کنید $a, n > 1$ اعدادی طبیعی باشند. اگر $n = p^k \cdot r$ طوری که $p \nmid r$ در این صورت داریم که

$$\Phi_n(a) > (b^{p-2}(b-1))^{\varphi(r)}$$

که در اینجا $b = a^{p^{k-1}}$

راه حل. طبق گزاره ۲.۲.۷ داریم که $\Phi_n(a) = \frac{\Phi_r(b^p)}{\Phi_r(b)}$ حال می‌دانیم که $\Phi_r(b^p) > (b^p - 1)^{\varphi(r)}$ (به صورت کلی تر $|\Phi_n(x)| > |(x-1)|^{\varphi(n)}$ که اثبات آن ساده است) و همچنین به طریق مشابه $\Phi_r(b^p) < (b^p + 1)^{\varphi(r)}$ پس داریم که

$$\Phi_n(a) = \frac{\Phi_r(b^p)}{\Phi_r(b)} > \frac{(b^p - 1)^{\varphi(r)}}{(b^p + 1)^{\varphi(r)}} = \left(\frac{b^p - 1}{b^p + 1} \right)^{\varphi(r)}$$

و اکنون با استفاده از این نامساوی که $b^p - 1 > b^{p-2}(b^2 - 1)$ اثبات ما کامل می‌شود.

حال با این دو لم می‌توانیم اثباتی کوتاه برای زیگموندی ارائه بدهیم.

راه حل. اثبات حالات استثنا که چرا جواب نمی‌دهند ساده است. فرض کنید که $a^n - 1$ عامل اولی ندارد که در قبلی‌ها نیامده باشد، همچنین می‌دانیم که $x^n - 1 = \prod_{d \mid n} \Phi_d(a)$ پس داریم که به ازای هر $p \mid \Phi_n(a)$ وجود دارد d طوری که $p \mid \Phi_{\frac{n}{d}}(a)$ پس داریم که $p \mid a^{\frac{n}{d}} - 1$ و طبق لم دو خط می‌دانیم که $v_p(a^n - 1) = v_p(a^{\frac{n}{d}} - 1) + v_p(d)$ چون می‌دانیم که

$p \mid \Phi_n(a)$ پس قطعاً $v_p(a^{\frac{n}{d}} - 1) > v_p(a^n - 1)$ و این یعنی $v_p(d) \geq 1$ پس $p \mid d \mid n$ پس نتیجه گرفتیم که به ازای هر $p \mid \Phi_n(a)$ داریم که $p \mid a$ حال طبق لم ۱.۴ یا $n = 2$ یا $\Phi_n(a) = p$ طوری که $p \mid n$ حالت $n = 2$ ساده است و از آن گذر می‌کنیم. در حالت دوم اگر $n = p^k \cdot r$ باشد که $p \nmid r$ طبق لم ۲.۴ داریم که $p \mid (b^{p-2}(b-1))^{\varphi(r)}$ که در اینجا $b = a^{p^{k-1}}$ حال اگر $p > 5$ داریم که $b^{p-2} > p$ به ازای هر b طبیعی پس $p = 3$ حال نتیجه میگیریم $a = 2$ و $k = 1$ و $r = 1$ یا 2 که این به ما نتیجه می‌دهد $n = 3$ یا 6 که در حالت $n = 3$ کاملاً درست است و در حالت $n = 6$ هم که $a = 2$ استثنا بود پس به تناقض میرسیم که $a^n - 1$ حتماً عاملی دارد که در قبلی‌ها نبوده است.

۵.۷ مسائلی برای حل

بعد از اثبات قضیه زیگموندی و بررسی چندجمله‌ای‌های دایره‌بر زمان آن رسیده که با چیزهایی که گفتیم سوال‌های المپیادی حل کنیم. البته سوال‌های زیر ممکن هست راه‌هایی دیگر بدون استفاده از مطالب مقاله هم داشته باشند. امیدوارم از فکر کردن و حل کردن سوالات زیر لذت ببرید!

مساله ۱.۵.۷ (ژاپن)

تمام ۵ تایی‌های (a, n, p, q, r) از اعداد طبیعی را بیابید طوری که

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

مساله ۲.۵.۷ (بریتانیا)

ثابت کنید در دنباله زیر عدد اولی وجود ندارد

$$10001, 100010001, 1000100010001, \dots$$

مساله ۳.۵.۷

ثابت کنید بینهایت عدد طبیعی مانند n وجود دارد طوری که تمام عوامل اول $n^2 + n + 1$ کمتر مساوی $\sqrt{n}$ باشند.

مساله ۴.۵.۷ (IMO)

اگر p عددی اول باشد. ثابت کنید عدد اول دیگری مانند q وجود دارد طوری که به ازای هر $n \in \mathbb{N}$ داشته باشیم $q \nmid n^p - n$.

مساله ۵.۵.۷ (TST USA 2012 P4)

تمام $a, n \geq 1$ را بیابید طوری که به ازای هر عامل اولی مانند p که $p \mid a^n - 1$ وجود داشته باشد $m < n$ طوری که $p \mid a^m - 1$.

مساله ۶.۵.۷ (EMC Senior 2024 P1)

یک زوج مرتب از عددهای متمایز (a, b) را جادویی می‌نامیم اگر $ab + 1$ توانی از ۲ باشد. مجموعه S از اعداد طبیعی داده شده است. حداکثر تعداد دوتایی‌های جادویی در S چقدر است؟

مساله ۷.۵.۷ (China TST 2009, P3)

دنباله a_n از اعداد طبیعی را طوری تعریف می‌کنیم که به ازای هر $m, n \in \mathbb{N}$ ، $\gcd(a_m, a_n) = a_{\gcd(m, n)}$. ثابت کنید برای هر $n \in \mathbb{N}$

$$\prod_{d|n} a_d^{\mu(\frac{n}{d})} \in \mathbb{N}$$

که در اینجا منظور از $\mu(x)$ تابع موبیوس x است که به صورت زیر نمایش داده می‌شود

$$\mu(n) = \begin{cases} 1 & \exists p, p^2 \mid n \\ (-1)^k & \text{O.W.} \end{cases}$$

که در آن k برابر تعداد عوامل اول مختلف عدد n است.

مسائل کولموگروف

۱.۸ مقدمه

--علی پرتوفرد

سوالات کولموگروف خوب است. حل کنید.

۲.۸ سوالات

۱.۲.۸ روز اول

مساله ۱.۲.۸

آیا چندجمله‌ای‌های $P(x), Q(x), R(x)$ وجود دارند به طوری که

$$P(Q(x)) = (x-1)(x-3)(x-5)(x-7) \quad \text{و} \quad Q(R(x)) = (x-2)(x-4)(x-6)(x-8)$$

مساله ۲.۲.۸

یک «نمایش» از عدد صحیح مثبت n را به صورت یک عبارت به شکل زیر تعریف کنیم:

$$n = a_1 + a_2 + \dots + a_n$$

که در آن $a_1 \geq a_2 \geq \dots \geq a_n \geq 0$ اعداد صحیح هستند. ثابت کنید که برای $n \geq 3$ تعداد نمایش‌هایی که حداقل نیمی از اعداد ناصفر آن‌ها برابر با یک هستند، برابر با تعداد نمایش‌هایی است که در آن‌ها $a_2 = a_3$ است.

مساله ۳.۲.۸

تمام اعداد فرد n را بیابید که $(5^n - 1)(2^n - 1)$ مربع کامل عددی طبیعی باشد.

مساله ۴.۲.۸

چهارضلعی $ABCD$ درون دایره‌ای به مرکز O محاط شده است. پاره‌خط‌های AC و BD در نقطه P یکدیگر را قطع می‌کنند. امتدادهای CB و DA در نقطه Q یکدیگر را قطع می‌کنند. دایره محیطی مثلث APB ، پاره‌خط‌های AD و BC را به ترتیب در نقاط A_1 و B_1 برای دومین بار قطع می‌کند. دایره محیطی مثلث CPD ، پاره‌خط‌های B_1C و A_1D را به ترتیب در نقاط C_1 و D_1 برای دومین بار قطع می‌کند. ثابت کنید که خطوط A_1C_1 ، B_1D_1 و QO هم‌رس هستند.

مساله ۵.۲.۸

کوچکترین عدد C را بیابید که گزاره زیر برای آن درست باشد:
 گزاره. $n > 2$ عددی طبیعی و $a_1, a_2, \dots, a_n$ اعدادی مثبت هستند. قرار دهید $a_{n+k} = a_k$ برای هر k طبیعی. تعریف می‌کنیم $b_i = a_i + \max(a_{i+1}, a_{i+2})$. پس خواهیم داشت:

$$C \sum_{i=1}^n (a_i - a_{i+1})^{1000} \geq \sum_{i=1}^n (b_i - b_{i+1})^{1000}$$

مساله ۶.۲.۸

عدد اول p داده شده است، قرار دهید $n = p^2 + p + 1$. حال یک خانواده S از زیرمجموعه‌های $p + 1$ عضوی از مجموعه n عضوی X را در نظر بگیرید؛ به طوری که هیچ دو عضو S در دقیقاً یک عضو مشترک نباشند. حداکثر اندازه خانواده S را پیدا کنید.

مساله ۷.۲.۸

نیمسازهای AA_1, BB_1, CC_1 از مثلث مختلف‌الاضلاع ABC در نقطه I یکدیگر را قطع می‌کنند. دایره‌ی محاطی مثلث ABC ضلع BC را در نقطه A_2 لمس می‌کند. دایره ω_a از نقاط A_1, A_2 و میانه‌ی پاره خط AI عبور می‌کند. به طور مشابه، دو دایره ω_b و ω_c تعریف می‌شوند. ثابت کنید که مراکز دایره‌های ω_a, ω_b و ω_c روی یک خط راست قرار دارند.

مساله ۸.۲.۸

عدد طبیعی k مفروض است به طوری که $p = 4k + 1$ عددی اول است. اعداد صحیح $a_1, a_2, \dots, a_{4k+2}$ مفروض هستند به طوری که $|a_i| = i$ برای $i = 1, 2, \dots, 4k + 2$. برای هر $j = 1, 2, \dots, 4k + 2$ جمع زیر را در نظر بگیرید:

$$S_j = a_1^{2j-1} + a_2^{2j-1} + \dots + a_{4k+2}^{2j-1}$$

کمترین تعداد از عبارت‌های بالا را بیابید که هیچ کدام بر p بخش پذیر نباشند.

۲.۲.۸ روز دوم

مساله ۹.۲.۸

برای کدام اعداد طبیعی n می‌توان جایگشت $(b_1, b_2, \dots, b_n)$ از اعداد طبیعی را یافت طوری که باقی‌مانده ib_i بر n صفر یا یک باشد.

مساله ۱۰.۲.۸

اعداد طبیعی m, t داده شده‌اند یک ابرگراف داریم که درجه هیچ راسی از $2m$ تجاوز نمی‌کند و کوتاه‌ترین فاصله هر دو راسی t است. بین دو راس حداکثر چند مسیر به طول t می‌تواند وجود داشته باشد.

مساله ۱۱.۲.۸

فرض کنید $p = 2n + 1$. فرض کنید $\omega_1, \omega_2, \dots, \omega_n$ جایگشت‌هایی از اعداد یک تا p باشند طوری که هر گاه $ij = k$ یا $ij = p - k$ داشته باشیم $\sigma_i \circ \sigma_j = \sigma_k$. ثابت کنید همه این جایگشت‌ها توان‌هایی از یکی از جایگشت‌ها هستند.

مساله ۱۲.۲.۸

مجموعه فشردۀ K در فضا محدب است و حداقل یک نقطه غیر مرزی دارد. برای هر دو نقطه A, B روی مرز K صفحه‌ای وجود دارد که اشتراک آن با K دایره‌ای به وتر AB است. آیا درست است که K یک کره است؟

مساله ۱۳.۲.۸

آیا هزار مجموعه دوبه‌دو مجزا از اعداد طبیعی یافت می‌شوند که جمع اعضا و جمع معکوس اعضایشان مساوی باشد؟

مساله ۱۴.۲.۸

اعداد $z_1, \dots, z_k, w_1, \dots, w_k$ مختلط با نرم واحد هستند. ثابت کنید

$$\sqrt{k^2 - \left| \sum z_i w_i \right|^2} < \sqrt{k^2 - \left| \sum z_i \right|^2} + \sqrt{k^2 - \left| \sum w_i \right|^2}$$

مساله ۱۵.۲.۸

پنج ضلعی $P_1 P_2 P_3 P_4 P_5$ در دایره‌ای محاط شده است، به طوری که $P_5 = P_5$ و $P_6 = P_1$ تعریف شده‌اند. برای $k = 1, 2, 3, 4, 5$ مرکز دایره‌ی محاطی مثلث $P_{k-1} P_k P_{k+1}$ می‌باشد. معلوم است که پنج ضلعی $I_1 I_2 I_3 I_4 I_5$ نیز محاطی است. ثابت کنید که خطوط $P_1 I_1, P_2 I_2, P_3 I_3, P_4 I_4, P_5 I_5$ در یک نقطه یکدیگر را قطع می‌کنند.

مساله ۱۶.۲.۸

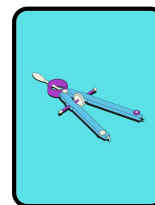
برای عدد داده شده $N > 1000$ دنباله‌های به طول N از اعداد $1, -1$. را در نظر بگیرید یک دنباله را بزرگ می‌گوییم هر گاه جمع هیچ چند جمله متوالی آن -100 نشود و آن را کوچک می‌گوییم اگر جمع هیچ چندجمله متوالی آن $100, 101$ نشود. ثابت کنید تعداد دنباله‌های کوچک و بزرگ برابر است.

مساله ۱۷.۲.۸

در داخل مثلث حاده‌الزاویه ABC که در آن $\angle A = 60^\circ$ است، نقطه‌ی متغیر P به گونه‌ای انتخاب می‌شود که $\angle BPC = 120^\circ$ باشد. نقاط P_B و P_C تصویرهای قرینه‌ی نقطه‌ی P نسبت به اضلاع AC و AB به ترتیب هستند. خطوط BP_B و CP_C در نقطه Q یکدیگر را قطع می‌کنند. ثابت کنید که دایره‌ی محیطی مثلث APQ از نقطه‌ای غیر از A که مستقل از انتخاب P است، عبور می‌کند.

مساله ۱۸.۲.۸

تعدادی فیل روی یک صفحه شطرنج 2025×2025 داریم که هیچ فیلی روی مرز نیست اما تمام خانه‌های مرز تهدید می‌شوند. ما کسیمم تعداد خانه‌هایی که توسط هیچ فیلی تهدید نمی‌شود را بیابید.



داستان سه سوال!

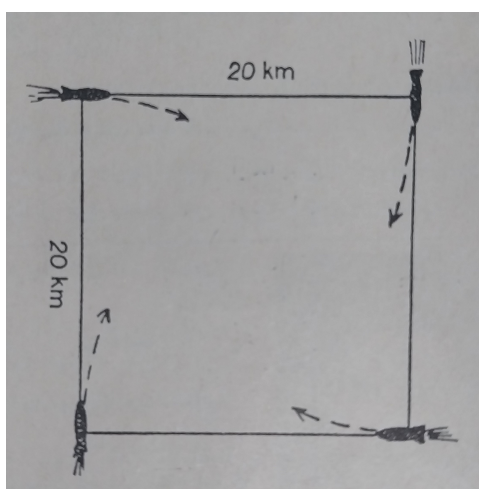
۱.۹ مقدمه

در این بخش تعدادی سوال بسیار زیبا برای شما عزیزان قرار گرفته است. مثل قرارهای قبلی مان، شما برای حل کردن آن‌ها و رسیدن به جوایز فوق‌نفیس پرگار، کافیت در طول سه ماه آینده حسابی روی آن‌ها فکر کنید و جواب پیشنهادی‌تان را به ایمیل pargarmagazine@gmail.com ارسال کنید. مشتاقانه، منتظر شکست شما در حل این سوالات هستیم. به هر حال جایزه به هر کسی که تعلق نمی‌گیرد.

۲.۹ مسائل

مساله ۱.۲.۹

روزی روزگاری در شهر شکرستان، در ۴ نقطه شهر مثل A, B, C و D که یک مربع به ضلع ۲۰ کیلومتر را تشکیل می‌دهند، ۴ موشک نقطه‌زن با سرعت‌های ۱ کیلومتر بر ساعت قرار داده شده بود. اما به دلیل اختلالات فنی، هر ۴ موشک همزمان پرتاب شدند. موشک A روی موشک B تنظیم شده بود، موشک B روی موشک C ، موشک C روی موشک D و در نهایت موشک D روی موشک A تنظیم شده بود. چند ثانیه طول می‌کشید که این ۴ موشک با هم برخورد کنند و همگی منفجر شوند؟



شکل ۱. چهار موشک

مساله ۲.۲.۹

تمامی چندجمله‌ای‌های $P(x)$ با ضرایب صحیح را بیابید به طوری که برای اعداد حقیقی دلخواه s و t ، اگر $P(s)$ و $P(t)$ هر دو صحیح باشند، نتیجه بشود که $P(st)$ نیز صحیح است.

مساله ۳.۲.۹

آیا روی هر خمی در صفحه نقطه‌ای وجود دارد که جفت مختصات آن نقطه گنگ یا جفت مختصاتش گویا باشد؟ خم را می‌توانید تابعی پیوسته از بازه $(0, 1)$ به نقاط صفحه در نظر بگیرید.



شکل ۲. موفق باشید!

