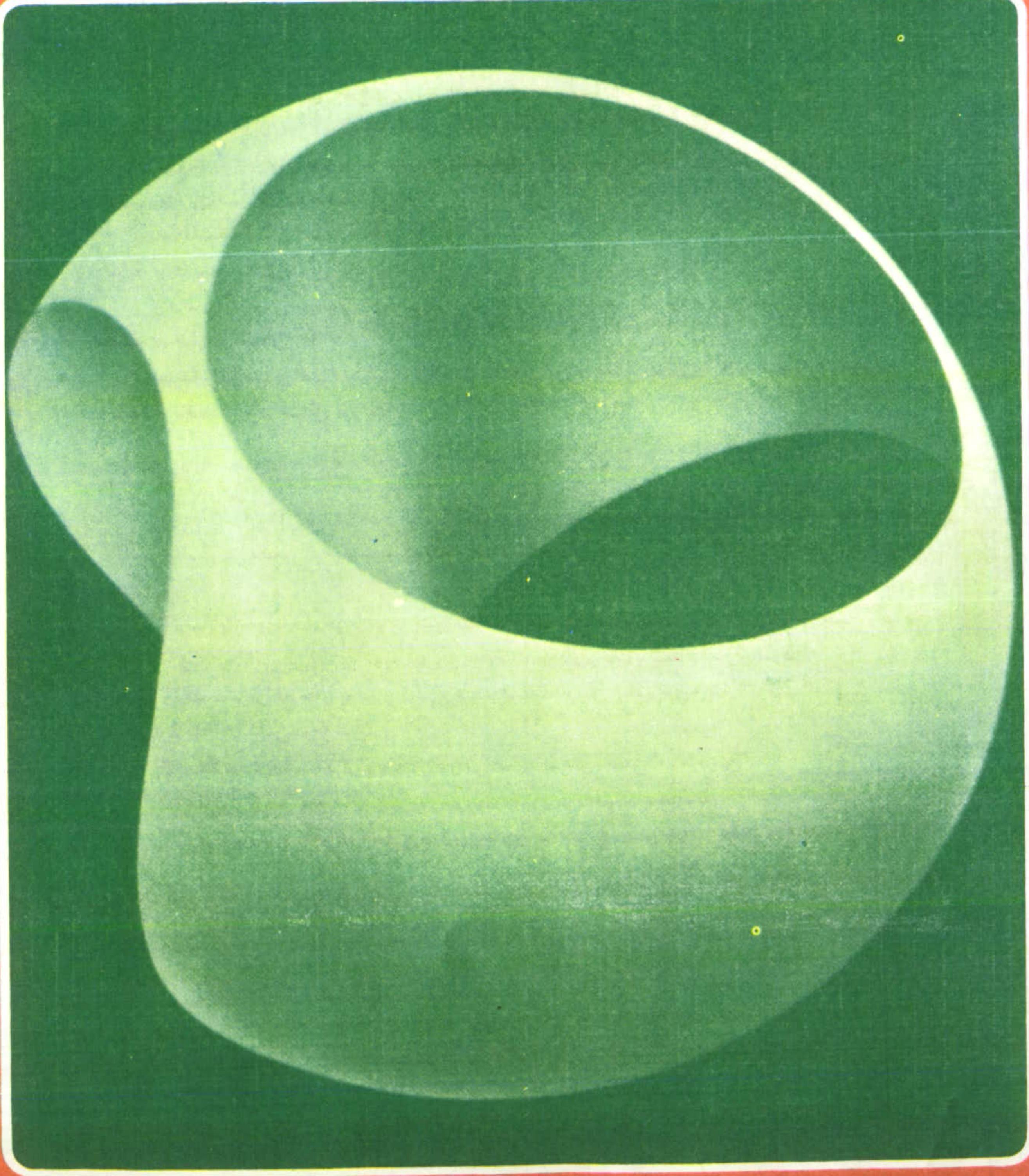
رشد آموزش ریاضی

سال ششم ـ پائیز۱۳۶۸ ـ شماره مسلسل ۲۳

بها: ۱۰۰ ریال



بسم‌الله الرحمن الرحیم

رشد آموزش ریاضی هر سه ماه یکبار از طرف سازمان پژوهش و برنامه‌ریزی آموزشی منتشر می‌شود هدف از انتشار این مجله اعتلای دانش ریاضی دانش‌آموزان، دبیران و دانشجویان دانشگاهها و مراکز تربیت معلّم است. علاوه بر این ایجاد ارتباط متقابل بین معلّمین ریاضی و دفتر تحقیقات، به منظور تبادل تجارب، ارائه روشهای جدید آموزش ریاضی، معرفی جنبه‌های تاریخی، فلسفی، کاربردی ریاضیات در سطح پیش دانشگاهی است هیأت تحریریه از مشارکت و همکاری همهٔ علاقه‌مندان بویژه دبیران و دانشجویان و دانش‌آموزان در ارائه مقالاتی در زمینه‌های زیر استقبال می‌کند:

الف) آموزش ریاضی (طرح و بررسی آموزش ریاضی، بویژه آموزش ریاضی در دوره‌های پیش دانشگاهی).

ب) تاریخ ریاضی (مشتمل بر سیر تحول مفاهیم ریاضی، شرح و احوال ریاضیدانان و کارهای علمی آنها، بویژه ریاضیدانان دورهٔ اسلامی).

ج) فلسفه ریاضی (تبیین مفاهیم ریاضی، ریاضیات چیست، بررسی مکاتب ریاضی، بررسی ارتباط تاریخ و فلسفه ریاضی).

ریاضی کاربردی (مشتمل بر مباحثی در زمینه‌های آنالیز عددی، کامپیوتر و برنامه‌ریزی، تحقیق در عملیات، آمار و احتمال).

د) سایر مباحث ریاضی (مشتمل بر مقالات مختلفی در زمینه‌های مختلف، ارائه راه‌حلهای مختلف برای مباحث ریاضی، ارائه مسائل نمونه).

رعایت نکات زیر در مورد مقالات ارسالی ضروری است:

۱) مقالات ارسالی باید در چهارچوب اهداف فوق و با سبکی مشابه با سبک مقالات چاپ شده در رشد ریاضی باشد و در سطحی عرضه شوند که ضمن داشتن محتوی مطلوب دارای کیفیت عرضه مطلوب هم باشند؛

۲) مقالات باید با خط خوانا (یا در صورت امکان ماشین شده) و به صورت یک سطر در میان و با در نظر گرفتن جای کافی در حاشیه تهیه شود و صفحات به طور دقیق شماره‌گذاری شود؛

۳) فهرست مراجع مقاله به طور کامل و در دو قسمت فارسی و خارجی و به ترتیب الفبایی و طبق استاندارد مقالات علمی درج شود؛

۴) مقالات ترجمه شده از زبانهای خارجی همراه با متن اصلی ارسال شود؛

۵) مقالات ارائه شده نباید قبلاً در نشریات کشور به چاپ رسیده باشد؛

۶) رد یا قبول و حک و اصلاح و ویراستاری مقالات به عهدهٔ هیأت تحریریه است.

رشد آموزش ریاضی

سال ششم - تابستان ۱۳۶۸ - شمارهٔ مسلسل ۲۳
نشریه گروه ریاضی دفتر تحقیقات و برنامه‌ریزی و تألیف کتب درسی. تلفن ۴ ـ ۸۳۹۲۶۱ داخلی (۵۲)
سردبیر : دکتر محمدحسن بیژن‌زاده
مدیر داخلی: میرزا جلیلی
مدیر فنی هنری و تولید: حسین فرامرزی نیکنام
صفحه‌آرا : محمد پریسای

مجله رشد آموزش ریاضی هر سه ماه یک بار به منظور اعتلای دانش دبیران و دانشجویان دانشگاهها و مراکز تربیت معلم و سایر دانش‌پژوهان در این رشته منتشر می‌شود. جهت ارتقاء کیفی آن نظرات ارزنده خود را به صندوق پستی تهران ۳۶۳ ـ ۱۵۸۵۵ ارسال فرمائید.

فهرست

پیشگفتار

در دنیای پرتکاپوی امروز نیاز به نشریاتی که بتوانند وسیله‌ای برای ارتباط افکار در سطح دانش‌آموزان و دبیران ریاضی کشور باشد بر هر کسی روشن و برای برخی از مفروضات است. به زعم نگارنده گذشت ۶ یا ۷ سال از عمر هر نشریه، گو اینکه فی‌نفسه امری دلگرم کننده است اما فی‌الواقع زمانی بس کوتاه است. امید ما بر آن است که این امانت که بیشتر به نهالی نو پا می‌ماند، هر چه بارورتر در اعماق زمانها به پیش رفته و به علاقمندان به ریاضیات این مرزوبوم و سازندگان آینده سپرده شود. به گمان ما هیچ نشریه‌ی علمی نباید در مسیر زمانه دستخوش توقف یا تعلل گردد. چه بسیارند مجلات و سازمانهای انتشاراتی در پهنای کرهٔ خاکی که عمری ۱۰۰ ساله و یا بیشتر از آن دارند. لیکن ادامهٔ مستمر و طولانی این کار، مستلزم برنامه‌ریزی حساب شده، همکاری و همیاری همهٔ کسانی که به نحوی با ریاضیات سروکار دارند، و بررسی نقاط قوت و ضعف مجله بدون هیچ تعارفی، حداقل برای دست‌اندرکاران مجله، می‌باشد.

مجله رشد آموزش ریاضی در عین حال که باید آینه فعالیتهای آموزش ریاضی در سطح کشور باشد در جهت اعتلای این رشته از معارف بشری نقشی مهم بر عهده دارد. گو اینکه

بقیه در صفحه ۳۷

قضیهٔ آخر فرما

دکتر علیرضا جمالی

۱. مقدمه

قضیهٔ فرما این حکم را بیان می‌کند که معادلهٔ

$$(*) \quad x^n+y^n=z^n \qquad (n > ۲),$$

در مجموعهٔ اعداد صحیح مثبت دارای جواب نیست. اثبات امتناع $x^۴+y^۴=z^۴$ چنانکه در مبحث ۵ خواهیم دید ساده است. بنابراین وقتی که n مضرب ۴ باشد معادلهٔ (*) ممتنع است؛ زیرا با فرض $n=۴k$، $X=x^k$، $Y=y^k$ و $Z=z^k$ معلوم می‌شود $X^۴+Y^۴=Z^۴$، که ممتنع است. به طریق مشابه، اگر امتناع معادلهٔ (*) به‌ازاء $n=m$ ثابت شود آنگاه امتناع آن به ازاء همهٔ مضارب m ثابت خواهد شد. چون هر $n(>۲)$ یا مضرب ۴ است یا اینکه مضربی از یك عدد اول فرد است. برای اثبات قضیهٔ فرما کافی است حالتهائی که n مضارب اعداد اول فردند ثابت شوند.

حالت $n=۳$ چندان مشکل نیست ولی نسبتاً طولانی است. در حالات $n=۵$ و $n=۷$ مشکلات بیشتر است ولی بازهم قضیه با روشهای مقدماتی ثابت می‌شود. کومر[1] با به کاربستن تئوری توانای تجزیهٔ ایده‌آلی خود، که در ۱۸۴۰ بنیاد نهاد، قضیه را بـه ازاء جمیع اعداد اول کوچکتر از ۱۰۰ غیر از ۳۷، ۵۹ و ۶۷ یکباره ثابت کرد. قضیهٔ کومر چنین است:

بنابرآنکه p یك عدد اول فرد باشد، شرط کافی برآنکه قضیهٔ آخر فرما به ازاء $n=p$ برقرار باشدآن است که p صورت اعداد برنولی[2] $B_۲$، $B_۴$، ...، $B_{p-۳}$ را عاد نکند.

از سال ۱۸۵۰ کوششهای فراوانی برای اثبات شرایط کافی بیشتر بـه عمل آمده است. از طرفی این شرایط جامع، و از طرف دیگر مأیوس‌کننده‌اند. از این معنی جامع‌اند کـه همهٔ

حالات $n(<۱۰^{۵})$ را دربر میگیرند و از این بابت مایوس کننده‌اند که هیچ شرط کافی برای این قضیه که متضمن اثبات آن به ازاء تعدادی نامتناهی از اعداد اول باشد پیدا نشده است. بنابراین، درحال حاضر این قضیه در موقعیتی است که نه آن‌را می‌توان ثابت کرد و نه اینکه باطل‌دانست. زیرا از طرفی صحت آن در حوزهٔ محاسبه ثابت شده است و از طرف دیگر سقم آن به ازاء **همه** اعداد اول از مرتبه‌ای به بعد معلوم نشده است.

در این مقاله ضمن بحث مختصری راجع به منشأ تاریخی این قضیه، حالت $n=۲$ درنظرخواهیم گرفت وجمیع جوابهای $x^{۲}+y^{۲}=z^{۲}$ را به دست خواهیم داد. این حالت هم از این جنبه که منشأ قضیهٔ آخر فرما بوده است قابل تأمل است وهم اینکه در اثبات امتناع (*) در حالت $n=۴$ به کار خواهد رفت. برای حالات $n=۳$، $n=۵$ و $n=۷$ می‌توان به مأخذ مقالهٔ حاضر رجوع کرد [قسمت یادداشتها را ملاحظه کنید].

۲. فرما و قضیهٔ آخر وی

هنگامی که پیردو فرما[۳] در ۱۶۶۵ درگذشت یکی از مشهورترین ریاضیدانان اروپا بود. درحال حاضر نام وی تقریباً مترادف با تئوری اعداد است ولی در عصر وی چنین نبود زیرا در آن عصر کار وی در زمینهٔ تئوری اعداد کاری انقلابی و جلوتر از زمان خویش بود. بدین سبب به ارزش کارهایش در این زمینه توجه کمتری شد و شهرت عمدهٔ وی از طریق تحقیقاتی کسب شد که در سایر رشته‌ها به عمل آورد. این تحقیقات مشتمل بودند بر کار مهمی که درکشف هندسهٔ تحلیلی، مستقل از دکارت، کرد ــ در تئوری مماسها، تربیع، و ماکزیمومها و مینیمومها ــ که مقدمهٔ حسابان[۴] بودند ــ و در اپتیك ریاضی ــ که آن را با کشف اینکه قانون انکسار از اصل کمترین زمان استنتاج می‌شود توسعه داد.

دوامر شگفت‌انگیز در مورد فرما به‌عنوان ریاضیدان وجود دارد. ابتدا اینکه وی اساساً ریاضیدان نبود بلکه در اصل قانوندان بود. در طی زندگی کامل خود مناصب عالی قضائی را در تولوز داشت و کار ریاضی را به عنوان مشغولیتی فرعی انجام می‌داد. ثانیاً وی هیچ کاری را در زمینه ریاضی منتشر نکرد[۵]. اشتهار وی از مکاتباتش با سایر محققان و نیز از تعدادی مقالهٔ دستنوشته ناشی شد. بارها به وی اصرار شد که تحقیقاتش را منتشر کند ولی وی به دلائلی که تشریح نشده است از چاپ مقالاتش امتناع کرد و بسیاری از کشفیاتش به ویژه در تئوری اعداد هرگز چاپ نشد. اینکه فرما از انتشار کارهایش امتناع می‌کرد شاید این بود که می‌پنداشت با این کار بزودی فراموش خواهد شد؛ زیرا پس‌از مرگش کسی در صدد جمع آوری نامه‌ها و مقالاتش برنخواهدآمد. پس‌از مرگش این کار را ساموئل، پسرش، به عهده گرفت. ساموئل دوفرما علاوه برنامه‌های حقوقی و مقالاتی از مکاتبات فرما با سایر افراد، به نامه‌ها وکتابهای پدرش نیزسرزد و بدین‌ترتیب بودکه «قضیهٔ آخر» منتشر شد.

کتابی که فرما درتئوری اعداد اساساً از آن متأثر شد، کتاب **حساب** دیوفانتوس[۶] بود. که از نوکشف و مختصراً به لاتین ترجمه شده بود. ساموئل دریافت که پدرش حواشی چندی برنسخهٔ خود (ترجمهٔ باشه[۷]) نوشته است. وی در حین انتشار کارهای پدرش ابتدا چاپ جدیدی ازدیوفانتوس باشه را منتشر ساخت که دارای‌ضمیمه‌ای مشتمل برحواشی‌پدرش بود. مسألهٔ[۸] کتاب II دیوفانتوس چنین‌است«عددی مفروض مربع‌کامل‌است؛ آن را به صورت حاصلجمع دو مربع دیگر بنویسید.» فرما در حاشیهٔ کتاب راجع به این مسأله به لاتین متذکر می‌شودکه 'از طرف دیگر، نوشتن یك مکعب به صورت حاصلجمع دو مکعب، یا یك قوهٔ چهارم بصورت حاصلجمع دو قوهٔ چهارم، یا بطورکلی، نوشتن هرعددکه به شکل قوه‌ای بزرگتر از ۲ است به صورت حاصلجمع دو قوهٔ مشابه ممتنع است. من برهانی واقعاً شگفت‌انگیز برای‌آن دارم که این حاشیه تنگتر ازآن است که درآن بگنجد.' و بدین‌ترتیب این حکم ساده که «به ازاء هر $n(>۲)$ صحیح معادلهٔ $x^n+y^n=z^n$ ممتنع است» به **قضیهٔ آخر فرما** مشهور شد. درصورتی‌که فرما برهانی برای‌آن داشت، واقعاً «شگفت‌انگیز» بود. زیرا در عرض سیصد سال پس‌از فرما هیچ‌کس نتوانسته است برهانی برای‌آن بیاورد. مسأله این است که‌گرچه با پیشرفتی چشمگیر حکم فرما تا هزاران قوه با موفقیت ثابت شده است باوجود این بسیاری از ریاضیدانان نامی در حل‌آن ناموفق مانده‌اند. در حال حاضر معلوم نیست این حکم صحیح است یا نه.

وجه تسمیهٔ «قضیهٔ آخر فرما» مبهم است. معلوم نیست فرما در چه دورانی از زندگی این حاشیه را برکتاب دیوفانتوس نوشته است. معمولاً چنین فرض می‌شودکه وی در دوره‌ای که مشغول مطالعهٔ این‌کتاب بوده است حاشیهٔ مذکور را آورده

است، یعنی در دهۀ ۱۶۳۰ سه دهه قبل‌از فوتش و مطمئناً این آخرین قضیۀ وی نبوده است. به احتمال زیاد این وجه تسمیه از این امر ناشی می‌شود که از میان قضایای ثابت نشده‌ای که فرما ذکر کرده است این آخرین آنها بوده است. وی در نامه‌هایش به سایر ریاضیدانان قضایا و مسائل مبارز طلب را بارها ذکر کرده است ولی این را تنها در یکجا ذکر می‌کند؛ آن هم درحاشیه بر مسألۀ دیوفانتوس. ابولهولی برای ارعاب نسل آینده!

چون **حساب** دیوفانتوس منحصراً با اعداد منطق سروکار دارد. نا گفته پیدا است که منظور فرما این بود که اعداد منطقی مانند x، y، و z موجود نیستند بطوری که $x^n+y^n=z^n$، که در آن $n > ۲$. درصورتی که اعداد اصم را درکارآوریم آنگاه به‌ازاء هر زوج ازاعداد مانند x و y بسادگی می‌توان جوابی با قرار دادن $z=\sqrt[n]{x^n+y^n}$ به دست‌آورد. توضیح اینکه اگر معادلۀ (*) جواب منطق داشته باشد بدیهی است که جواب صحیح هم خواهد داشت. اثبات این سهل است: فرض کنیم اعداد منطق x، y، و z در(*) صدق کنند. عدد d را کوچکترین مضرب مشترك مخرجهای کسور x، y، و z می‌گیریم؛ دراین‌صورت xd، yd، و zd اعدادی صحیح‌اندو

$$(xd)^n+(yd)^n=(x^n+y^n)d^n=(zd)^n.$$

بعلاوه، هم دیوفانتوس و هم فرما هردو با اعداد صحیح مثبت سروکار داشتند. اعداد منفی و ۰ هنوز در عصر فرما با تردید تلقی می‌شدند ـ بنابراین حالت بدیهی $x=۰$ یا $y=۰$ از بحث خارج می‌شود (به عنوان مثال $۲^۵+۰^۵=۲^۵$ با قضیۀ فرما متناقض نخواهد بود). خلاصه، صورت قضیۀ آخر فرما بدین گونه بیان می‌شود که با فرض $n > ۲$ معادلۀ $x^n+y^n=z^n$ در مجموعۀ اعداد صحیح مثبت ممتنع است؛ به عبارت دیگر اعداد صحیح مثبتی مانند x، y و z موجود نیستند بطوری که $x^n+y^n=z^n$.

امروزه به سایر کارهای ریاضی فرما کمتر توجه می‌شود؛ نه بدین سبب که از اهمیت کمتری برخورد دارند بلکه از این حیث که این تئوریها با زبان و نماد ریاضی کنونی به سادگی قابل شرح و فهم‌اند. از طرف دیگر شهرت جاودانی فرما در زمینۀ تئوری اعداد تنها به سبب قضیۀ آخر وی نیست بلکه به جهت سایر کشفیاتی است که وی در این زمینه به عمل آورده است.

بنظر می‌رسد که در میان همۀ کارهای باقیمانده از فرما در تئوری اعداد تنها یك برهان موجود است. این برهان حکم خاصی است که فرما چندین بارآن را در مکاتباتش ذکر کرده است ولی برهانی برای‌آن ارائه نداده است؛ در همه موارد برهان‌آن را به مخاطبان خود محول کرده است. برهان این حکم مانند قضیۀ آخر وی به توسط پسرش ساموئل در همان نسخۀ مذکور دیوفانتوس پیدا شد. فرما غالباً در مکاتباتش خاطرنشان می‌سازد که وی علاقه‌ای به محو کارهایش ندارد زیرا معتقد است که پیشرفت دانش بستگی به‌کوششهای عده‌ای محقق و همکاری‌آنان دارد و اینکه وی حاضر است روشهای خود را به افرادی که طالب‌آنند توضیح دهد. کلماتی که از حرف به عمل در نمی‌آیند! بسیاری از نامه‌های فرما حاکی از این است که وی حاضر نبوده است روشهای خود را در اختیارسایرین قرار دهد. باید گفت وی مانند همۀ ریاضیدانان معاصرخود حسود، پرده‌پوش، واهل رقابت بوده است. حکمی که فرما برهان‌آن را می‌دهد چنین است. **مساحت یك مثلث قائم‌الزاویه نمی‌تواند مربع کامل باشد.** البته بدین معنی است که مساحت یك مثلث قائم‌الزاویۀ **منطق** نمی‌تواند مربع کامل **یك عدد منطق** باشد. مطابق معمول منشأ این مسأله بازهم کتاب **حساب** دیوفانتوس است. در واقع کتاب **حساب** دیوفانتوس متضمن چندین مسأله راجع به یافتن مثلثهای فیثاغورسی (مبحث ۳) است که در شرایط متعددی مربوط به مساحاتشان صدق می‌کنند. برهان فرما برای مسألۀ مذکور بسیار ظریف و زیباست و همین تنها برهان موجود از وی حالت $n=۴$ قضیۀ آخر را نیز ثابت می‌کند. (توضیح اینکه حالت $n=۴$ مستقل از این حکم ثابت خواهد شد.)

۳. مثلثها و سه تائیهای فیثاغورسی

حساب دیوفانتوس که قضیۀ فرما ازآن متأثر است به مسألۀ قدیمی ریاضی «نوشتن یك مربع کامل به صورت حاصلجمع دومربع‌کامل» می‌پردازد. جوابی ازاین مسأله $۳^۲+۴^۲=۵^۲$ است. درواقع مسألۀ دیوفانتوس به‌مسألۀ یافتن همه سه‌تائیهائی مانند (x, y, z) که $x^۲+y^۲=z^۲$ برمی گردد. وقتی مسأله بدین‌صورت مطرح می‌شود ارتباط‌آن با قضیۀ فیثاغورس معلوم می‌شود. مثلاً از قضیۀ فیثاغورس معلوم می‌شود که مثلثی با طول اضلاع ۳، ۴ و ۵ یك مثلث قائم‌الزاویه است. بطورکلی، هر سه‌تائی مانند (x, y, z) از اعداد صحیح مثبت که $x^۲+y^۲=z^۲$، یك مثلث قائم‌الزاویه را با طول اضلاع x، y و z مشخص می‌کند. ازاینجا، مسألۀ دیوفانتوس بطور هندسی چنین بیان می‌شود «مطلوب است تعیین جمیع

مثلثهای قائم‌الزاویه با طول اضلاع صحیح». به موجب این تعبیر هندسی هر سه‌تائی مانند (x, y, z) از اعداد صحیح مثبت که $x^۲+y^۲=z^۲$، یك سه‌تائی فیثاغورسی نامیده می‌شود. سه‌تائی (۳, ۴, ۵) متداولترین مثال است. مثال دیگر (۵, ۱۲, ۱۳) است. مسألهٔ دیوفانتوس یافتن همهٔ سه‌تائیهای فیثاغورسی است. این مسأله قرنها قبل از دیوفانتوس (در حدود ۲۵۰ ب. م.) به وسیلهٔ اقلیدس (در حدود ۳۰۰ ق. م.) در **اصول** کتاب x (لم ۱ بین دوحکم ۲۸ و ۲۹) مطرح شد. اخیراً برطبق یکی از کشفیات مهم باستانشناسی معلوم شده است که این مسأله هزاران سال قبل از اقلیدس به‌توسط بابلیهای باستانی مورد مطالعه‌قرار گرفته‌است. این کشف مشتمل بر جدولی به خط میخی از سه‌تائیهای فیثاغورسی است که ۱۵۰۰ سال قبل از میلاد به وسیلهٔ بابلیها فراهم آمده است. در این جدول سه‌تائی (۳, ۴, ۵) مندرج است؛ علاوه بر سه‌تائیهای دیگر سه‌تائی نظیر (۴۹۶۱, ۶۴۸۰, ۸۱۶۱) در آن آمده است این سه‌تائی نشان می‌دهد که آنان از روشی غیر از روش کوشش و خطا استفاده می‌کرده‌اند. از این روش اطلاعی در دست نیست. به علاوه هنوز نمی‌دانیم که مقصود آنان از تعیین این سه‌تائیها چه بوده است. بنابر عقیدهٔ نویگبر[8] شاید اهمیت هندسی سه‌تائیهای فیثاغورسی بر آنان مکشوف بوده است[9].

ذیلاً هدف ما تعیین همهٔ سه‌تائیهای فیثاغورسی است. ایدهٔ اصلی یافتن این سه‌تائیها از دیوفانتوس است. این روش در ریاضیات کلاسیك یونانی به روش **تحلیلی** موسوم است. ذیلاً اصطلاحات و علامات متداول ریاضی را برای حل این مسأله به کار خواهیم برد. ضمناً بعد از این همه‌جا مقصود از عدد، عدد صحیح مثبت خواهد بود.

فرض کنیم که (x, y, z) یك سه‌تائی فیثاغورسی باشد. عدد d را بزرگترین مقسوم‌علیه مشترك x، y و z می‌گیریم و فرض می‌کنیم که $a=\frac{x}{d}$، $b=\frac{y}{d}$ و $c=\frac{z}{d}$. در این صورت از تساوی $x^۲+y^۲=z^۲$ معلوم می‌شود که $a^۲+b^۲=c^۲$. یعنی (a, b, c) یك سه‌تائی فیثاغورسی است. در اینجا ملاحظه می‌شود که سه عدد a، b و c نسبت به هم اولند (عامل مشترك بزرگتر از ۱ ندارند). این گونه سه‌تائیهای فیثاغورسی را **اولیه** خواهیم نامید. اینك واضح است که مسألهٔ پیدا کردن همهٔ سه‌تائیهای فیثاغورسی به تعیین همه سه‌تائیهای فیثاغورسی اولیه برمی‌گردد.

حال فرض می‌کنیم که (x, y, z) یك سه‌تائی فیثاغورسی اولیهٔ دلخواه باشد. ابتدا ثابت می‌کنیم که x، y و z دوبدو نسبت به هم اولند. به عنوان مثال، فرض کنیم که $d > ۱$ عامل مشترك x و y باشد. در این صورت از تساوی $x^۲+y^۲=z^۲$ نتیجه می‌شود که $d|z$؛ و این متناقض با اولیهٔ بودن (x, y, z) است. بنابراین، از میان x، y، و z حداقل دوتای آنها فردند. بعلاوه، هر سه درعین‌حال فرد نمی‌توانند باشند؛ زیرا خواهیم داشت: فرد = فرد + فرد، که ممتنع است. پس تنها یکی از آنها زوج است. گوئیم z نمی‌تواند زوج باشد. در غیر این صورت، با فرض $z=۲k$، و اینکه $x=۲n+۱$ و $y=۲m+۱$، با استفاده از تساوی $x^۲+y^۲=z^۲$ خواهیم داشت:

$$۴n'+۴m'+۲=۴k'$$

که ممتنع است. بنابراین z فرد و x و y دارای زوجیت متفاوتند، یعنی یکی زوج است و دیگری فرد. بدون آنکه به کلیت استدلال خللی وارد شود، فرض می‌کنیم x زوج و y فرد باشد (z فرد است). اینك تساوی $x^۲+y^۲=z^۲$ را به صورت $x^۲=z^۲-y^۲$ می‌نویسیم. از اینجا

$$x^۲=(z-y)(z+y)$$

چون x، z+y و z−y جملگی زوجند، اعدادی مانند u، ν، و w هست بطوری که $x=۲u$، $z+y=۲\nu$، و $z-y=۲w$، داریم $(۲u)^۲=(۲\nu)(۲w)$ یا $u^۲=\nu w$. بعلاوه ν و w نسبت به هم اولند؛ زیرا هر عدد بزرگتر از یك که هردو را عادکند باید هم $\nu+w(=z)$ را عادکند و هم $\nu-w(=y)$ که ممکن نیست (y و z نسبت به هم اولند). حال گوئیم چون حاصلضرب دو عدد متباین ν و w مربع کامل است پس هم ν مربع کامل است و هم w (به موجب قضیهٔ یکتائی تجزیه به عوامل اول). فرض کنیم که $\nu=r^۲$، $w=s^۲$. از اینجا،

$$z=\nu+w=r^۲+s^۲$$

$$y=\nu-w=r^۲-s^۲$$

از تساویهای فوق معلوم می‌شود که $r > s$ و اعداد r و s دارای زوجیت متفاوتند (زیرا y و z هر دو فردند)، بعلاوه x به سادگی برحسب r و s نوشته می‌شود:

$$x^۲=z^۲-y^۲=r^۴+۲r^۲s^۲+s^۴-r^۴$$
$$+۲r^۲s^۲-s^۴=۴r^۲s^۲=(۲rs)^۲$$

$$x=۲rs.$$

بطور خلاصه، به ازاء هر سه‌تائی فیثاغورسی اولیه مانند

(x, y, z) دو عدد متباین مانند r و s موجودند بطوری که $r > s$، اعداد r و s دارای زوجیت متفاوتند، و

$$x = ۲rs$$
$$y = r^۲ + s^۲$$
$$z = r^۲ - s^۲.$$

بالعکس، هر زوج از اعداد مانند (r, s) باخواص (۱) $r > s$، (۲) r و s نسبت به هم اولند، و (۳) r و s دارای زوجیت متفاوتند، سه‌تائی فیثاغورسی اولیهٔ $(۲rs، r^۲ - s^۲, r^۲ + s^۲)$ را معین می کند.

جدول زیر همه سه‌تائیهای فیثاغورسی اولیه را به ازاء rهای نا بیشتر از ۸ به دست می‌دهد:

r	s	x	y	z
۲	۱	۴	۳	۵
۳	۲	۱۲	۵	۱۳
۴	۱	۸	۱۵	۱۷
۴	۳	۲۴	۷	۲۵
۵	۲	۲۰	۲۱	۲۹
۵	۴	۴۰	۹	۴۱
۶	۱	۱۲	۳۵	۳۷
۶	۵	۶۰	۱۱	۶۱
۷	۲	۲۸	۴۵	۵۳
۷	۴	۵۶	۳۳	۶۵
۷	۶	۸۴	۱۳	۸۵
۸	۱	۱۶	۶۳	۶۵
۸	۳	۴۸	۵۵	۷۳
۸	۵	۸۰	۳۹	۸۹
۸	۷	۱۱۲	۱۵	۱۱۳

۴. روش نزول نامتناهی فرما

روش نزول نامتناهی[۱۰] را فرما ابداع کرد و این ابداعی بود که وی بیش از حد بدان می بالید. در نامه‌ای طولانی که در اواخر عمرش تحریر شده است وی کشفیات خود را در تئوری اعداد خلاصه کرد و متذکر شد که این روش را در همهٔ برهانهایش به کار برده است. بطور خلاصه، این روش ثابت می کند که هیچ عدد صحیح مثبت واجد فلان خواص نیست. برای اینکار ثابت می‌شود که اگر عددی واجد این خواص باشد آنگاه همین خواص را عددی کوچکتر از آن واجد است. بدین ترتیب رشته‌ای از اعداد صحیح مثبت که اکیداً نزول می کند به دست می آید که ممتنع است.

به عنوان مثال، استدلالی را که در قسمت آخر بخش ۳ به کار رفت درنظر می گیریم؛ یعنی اینکه اگر **حاصلضرب دو عدد متباین ν و w مربع کامل باشد آنگاه هر دو مربع کاملند.** اینك برای اثبات این حکم از روش نزول نامتناهی استفاده می کنیم. فرض کنیم که دو عدد متباین ν و w چنان باشند که νw مربع کامل باشد ولی ν مربع کامل نباشد. بنابراین، $\nu \neq ۱$ و بالنتیجه ν دارای عامل اولی مانند p است. فرض کنیم که $\nu = pk$ و $\nu w = u^۲$. ازاینکه $p|u^۲$ نتیجه می‌شود که $p|u$. از اینجا $u = pm$. چون $u^۲ = \nu w$، خواهیم داشت $kw = pm^۲$، بنابراین $p|kw$. پس $p|k$ یا $p|w$. چون ν و w متباینند، $p \nmid w$؛ و بالنتیجه $p|k$. فرض می کنیم که $k = p\nu'$، از $kw = pm^۲$ معلوم می‌شود که $\nu' w = m^۲$. چون $\nu = pk = p^۲\nu'$، هر عامل ν' یك عامل ν هم هست؛ بنابراین ν' و w متباینند. بعلاوه ν' مربع کامل نیست؛ زیرا در غیر این صورت از تساوی $\nu = p^۲\nu'$ معلوم می‌شود که ν مربع کامل است که متناقض با فرض اصلی است. خلاصه، ν' و w دارای همان خواصی اند که ν و w واجد آن بودند یعنی ν' و w متباینند، $\nu' w$ مربع کامل است، و ν' مربع کامل نیست. بعلاوه $\nu > \nu'$. با استدلال مشابه (درمورد ν' و w) عددی مانند ν'' $(\nu' >)$ یافت می‌شود بطوری که زوج ν'' و w واجد همان خاصیت مذکورند. با تکرار این استدلال رشته‌ای اکیداً نزولی ازاعداد صحیح مثبت مانند ... و ν''' و ν'' و ν' و ν به دست خواهد آمد که ممتنع است

$$(\nu > \nu' > \nu'' > \nu''' > \dots).$$

بطور خلاصه، روش نزول نامتناهی مبتنی براصل زیر است:

فرض کنیم از این فرض که عدد صحیح مثبت مفروضی واجد مجموعه‌ای از خواص مفروض است بتوان نتیجه گرفت که عددی کوچکتر با همان مجموعه از خواص موجود است. در این صورت هیچ عدد صحیح مثبت واجد این مجموعه از خواص نیست.

۵. حالت $n = ۴$ قضیهٔ آخر فرما

برای اثبات قضیهٔ آخر فرما در حالت $n = ۴$ از مطالب دو بخش قبل استفاده خواهیم کرد.

فرض کنیم که x، y، و z چنان باشند که $x^۴+y^۴=z^۴$. مانند قبل می‌توان فرض کرد که x، y، و z نسبت به‌هم اولند، وحتی اینکه دوبدو متباینند. بنابراین، $(x^۲, y^۲, z^۲)$ یك سه‌تائی فیثاغورسی اولیه است. بدون آنکه به‌کلیت استدلال خللی وارد شود، می‌توان نوشت

$$x^۲=۲rs$$

$$y^۲=r^۲-s^۲$$

$$z^۲=r^۲+s^۲$$

که درآن r و s متباینند و زوجیت متفاوت دارند، ونیز $r > s$. رابطهٔ دوم را چنین می‌توان نوشت: $y^۲+s^۲=r^۲$. از اینجا نتیجه می‌شود که (y, s, r) یك سه‌تائی فیثاغورسی اولیه است (r و s متباینند). بنابراین r فرد است و s زوج؛ بالنتیجه

$$s=۲ab$$

$$y=a^۲-b^۲$$

$$r=a^۲+b^۲,$$

که درآن a و b متباینند و زوجیت متفاوت دارند و $a > b > ۰$. بنابراین،

$$x^۲=۲rs=۴ab(a^۲+b^۲).$$

تساوی اخیر نشان می‌هدکه $ab(a^۲+b^۲)$ مربع کامل است. چون ab و $a^۲+b^۲$ نسبت به هم اولند (چرا؟)، به موجب آنچه‌که گفته شد، معلوم می‌شودکه ab و $a^۲+b^۲$ هردو مربع کامل‌اند. اما از اینکه ab مربع کامل است و a و b متباینند، a و b هر دو باید مربع کامل باشند. فرض کنیم که $a=X^۲$، $b=Y^۲$. از اینجا $X^۴+Y^۴=a^۲+b^۲$. چون $a^۲+b^۲$ مربع کامل است، نتیجه می‌شودکه $X^۴+Y^۴$ مربع کامل است. بعلاوه معلوم است که

$$X^۴+Y^۴=a^۲+b^۲=r < r^۲+s^۲$$
$$=z^۲ < z^۴=x^۴+y^۴.$$

خلاصه، از فرض اینکه $x^۴+y^۴$ مربع کامل است[۱۱] نتیجه گرفتیم که اعدادی مانند X و Y موجودندکه $X^۴+Y^۴$ مربع‌کامل است و $X^۴+Y^۴ < x^۴+y^۴$. حال اصل نزول نامتناهی را به کار می‌بندیم.

یادداشتها:

۱. E. E. Kummer

۲. اعداد برنولی چنین تعریف می‌شوند:

$$B_۰=۱$$

$$B_n=-\frac{۱}{n+۱}\Big[B_۰+(n+۱)B_۱+\cdots$$
$$+\binom{n+۱}{k}B_k+\cdots+\frac{n(n+۱)}{۲}B_{n-۱}\Big].$$

نخستین ۶ عدد برنولی عبارتنداز ۱ ، $\frac{۱}{۶}$ ، ۰ ، $-\frac{۱}{۳۰}$ ، ۰. اویلر مقادیر B_n را به ازاء همه nهای نابیشتر از ۳۰ محاسبه کرد. ثابت می‌شود که به ازاء هر $n(>۱)$ فرد، $B_n=۰$.

۳. Pierre de Fermat

۴. Calculus

۵. در اینجا یك استثناء کوچك وجود دارد. وی به یکی از همکارانش اجازه داد که کارکم‌اهمیتی از او را در ضمیمهٔ کتابش (۱۶۶۰) بدون امضاء منتشر کند.

۶. Diophantus' Arithmetic

۷. Bachet

۸. Neugebauer

۹. ضمناً مراجعه کنید به مقالات **گفتاری در باب منشأ و مبدأ ریاضیات و ریاضیات در عهد باستان** نوشتهٔ دکتر محمدقاسم وحیدی، مندرج در شماره‌های ۱ و ۲ مجلهٔ رشدآموزش ریاضی (۱۳۶۳).

۱۰. The method of infinite descent

۱۱. فرض اصلی ما این بود که $x^۴+y^۴=z^۴$. از ابتدا می‌توان فرض کردکه $Z=z^۲$ و استدلال را با تساوی $x^۴+y^۴=Z^۲$ شروع کرد.

مقالهٔ حاضر عمدتاً ازکتاب زیر اقتباس شده است:

Harold M. Edwards, Fermat's Last Theorem, A genetic Introduction to algebraic number theory, Springer – Verlag (1977).

درسهایی از هندسه (٦)

قطب و قطبی در مقاطع مخروطی

تنظیم از: حسین غیور

۱ـ تعریف و تعیین قطب و قطبی نسبت به دایره و دو خط متقاطع یا موازی را درشماره‌های قبل با روش هندسی دیده‌ایم اینك می‌خواهیم این مسأله را با روش تحلیلی در بارهٔ مقاطع مخروطی تعمیم دهیم، تا مسألهٔ قطب و قطبی در بارهٔ منحنی‌های درجه دوم در حدود متوسطه گفته شده باشد. ابتدا مسأله را از دایره شروع می‌کنیم و سعی می‌کنیم روش اثبات در بارهٔ بیضی و هذلولی و سهمی شبیه‌آن باشد، گو اینکه در بارهٔ هذلولی نیاز به دستگاههای غیر توافقی پیدا می‌شود که خوشبختانه قبلاً در مقاله‌های درسهای از هندسه راجع به‌آن صحبت شده است.

لازم به یادآوری است که برای این کار راهی با روش هندسی در کتاب بازآموزی و باز شناخت هندسه به‌کمك تبدیل قطبی معکوس و قضایای‌آن و استفاده از قضیه پاسکال در شش ضلعی محاط در مقاطع مخروطی و متفرعات‌آن، آمده است که برای‌طرح در مجله مناسبت ندارد. علاقه مندان می‌توانند به‌آن کتاب رجوع کنند. اینك مطلب را با تعریف قطر و دو قطر مزدوج در مقاطع مخروطی، و طرح دستگاهی که محورهای‌آن منطبق بر دوقطر مزدوج است، و تعیین معادله مقاطع مخروطی در این دستگاهها، شروع می‌کنیم.

قضیه ـ در مقاطع مخروطی مرکزدار (بیضی،هذلولی) مکان هندسی وسط وترهای موازی روی خطی است که از مرکز آن می‌گذرد و در سهمی روی خطی موازی با محور آن است که با قبول اصل دزارگ، از مرکز آن که نقطه بینهایت محور آن است می‌گذرد.

برهان.

الف ـ بیضی ـ بیضی به معادلهٔ $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ را با خط $Ax+By+m=0$ که درآن A و B ثابت و m متغیر است قطع و x و y مختصات وتر حاصل را تعیین می‌کنیم.

$$\left(\frac{B^2}{a^2}+\frac{A^2}{b^2}\right)X^2+2\frac{Am}{b^2}X+\frac{m^2}{b^2}-B^2=0$$

$$M\left(X=\frac{\frac{-Am}{b^2}}{\frac{B^2}{a^2}+\frac{A^2}{b^2}}\quad,\quad Y=\frac{\frac{-Bm}{a^2}}{\frac{B^2}{a^2}+\frac{A^2}{b^2}}\right)$$

از حذف m بین دو رابطهٔ فوق نتیجه می‌شود

$$Y=\frac{Bb^2}{Aa^2}X$$

معادلهٔ بالا قطری از بیضی است که ضریب زاویهٔ‌آن

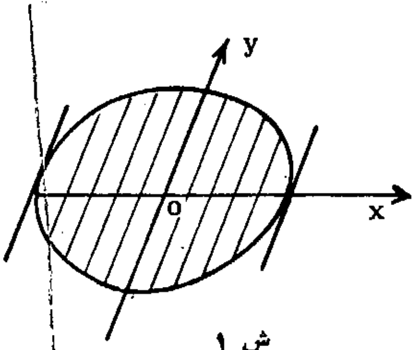
$$\lambda=\frac{B}{A}\cdot\frac{b^2}{a^2}$$

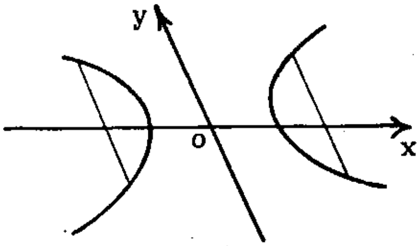
ضریب زاویهٔ قطرموازی با وترها $\lambda'=-\frac{A}{B}$ است. بین ضریب زاویه‌ها این رابطه برقرار است.

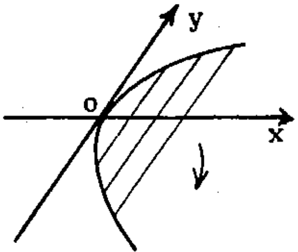
$$\lambda\lambda'=-\frac{b^2}{a^2}$$

خطی‌که از مرکز بیضی موازی با خط $Ax+By+m=0$ رسم می‌شود از تقاطع با بیضی قطری پدید می‌آورد که به موجب رابطهٔ $\lambda\lambda'=-\frac{b^2}{a^2}$ مزدوج قطر دیگر است به عبارت دیگر دو خط به معادلهٔ $y=\lambda x$ و $y=\lambda' x$ که به موجب

تساوی اخیر هر خط مکان هندسی وسط وترهای موازی با دیگری است دو قطر مزدوج نامیده می‌شود.


ش ۱


ش ۲


ش ۳

۲ـ تعریف قطر درمقاطع مخروطی ـ قطر مکان هندسی وسط وترهای موازی و خطی است که از مرکز مقطع مخروطی می‌گذرد.

ب ـ هذلولی ـ در هذلولی با عملیاتی مشابه معادلهٔ مکان وسط وترها چنین می‌شود

$$Y = \frac{-Bb^2}{Aa^2} X$$

در اینجا نیز بین ضریب زاویه قطر وسط وترها و قطر موازی با وترها این رابطه برقرار است

$$\lambda\lambda' = \frac{-Bb^2}{Aa^2} \cdot \frac{-A}{B} = \frac{b^2}{a^2}$$

یعنی قطر موازی با وترها و قطر مکان وسطهای وترها مزدوج یکدیگرند.

ج ـ سهمی ـ در سهمی از دستگاه

$$\left| \begin{array}{l} Y^2 = 2PX \\ AX + BY + m = 0 \end{array} \right.$$

نتیجه می‌شود

$$A^2X^2 - 2(PB^2 - Am)X + m^2 = 0$$

اگر X و Y مختصات وسط وتر باشد

$$\left| \begin{array}{l} X = \frac{PB^2 - Am}{A^2} \\ Y = -\frac{BP}{A} \end{array} \right.$$

پس مکان وسط وتر خط موازی با محور سهمی $Y = \frac{-B}{A} P$ یعنی همهٔ قطرهای سهمی موازی با محور آن می‌باشند.

۳ـ معادلهٔ بیضی و هذلولی و سهمی نسبت به محورهای منطبق بر قطرهای مزدوج. خواص قطرهای مزدوج که شرح آن گذشت به ما امکان می‌دهد که معادلهٔ بیضی و هذلولی را نسبت به دستگاه مایلی که محورهای آن منطبق بر دو قطر مزدوج است به دست آوریم.

الف ـ بیضی ـ اگر Ox و Oy منطبق بر دو قطر مزدوج باشند با توجه به اینکه با تغییر محورهای مختصات از دستگاه قائم به این دستگاه درجهٔ معادله منحنی تغییر نمی‌کند. معادلهٔ بیضی در این دستگاه نیز درجهٔ دوم است به موجب خواص دو قطر مزدوج که در شمارهٔ قبل ذکر کردیم اگر X را به $-X$ تبدیل کنیم و Y را تغییر ندهیم معادله تغییر نمی‌کند پس درجهٔ X در معادله زوج است و همینطور اگر Y به $-Y$ تبدیل کنیم و X را تغییر ندهیم معادله تغییر نمی‌کند پس درجهٔ Y نیز زوج است. پس معادلهٔ بیضی در این دستگاه به صورت زیر در می‌آید

$$AX^2 + By^2 + C = 0$$

چون منحنی را با محور Ox قطع کنیم

$$X^2 = -\frac{C}{A} = a_1^2 \quad (OA' = OA = a_1)$$

چون منحنی را با محور Oy قطع کنیم

$$Y^2 = -\frac{C}{B} = b_1^2 \quad (OB' = OB = b_1)$$

A و B را از دو رابطهٔ اخیر برحسب a_1 و b_1 به دست می‌آوریم و در معادلهٔ بیضی می‌بریم این معادله به‌دست می‌آید

$$\frac{x^۲}{a_۱^۲}+\frac{y^۲}{b_۱^۲}=۱$$

ب - هذلولی - برای اینک معادلهٔ هذلولی را نسبت به دستگاه منطبق بر قطرهای مزدوج به دست آوریم قضیهٔ زیر را به عنوان مقدمه ذکر می‌کنیم.

قضیه - در هذلولی هر دو قطر مزوج با مجانبها دستگاه توافقی تشکیل می‌دهند ضریب زاویه مجانبها عبارت است از $\frac{b}{a}$ ، $\frac{-b}{a}$ و ضریب زاویهٔ قطرهای مزدوج $-\frac{Bb^۲}{Aa^۲}$ و $-\frac{A}{B}$ بنابراین نسبت غیر توافقی چهار ضریب زاویه عبارت است از

$$\left(-\frac{Bb^۲}{Aa^۲},\frac{-A}{B},\frac{b}{a},\frac{-b}{a}\right)$$

$$=\frac{\frac{b}{a}+\frac{Bb^۲}{Aa^۲}}{\frac{-b}{a}+\frac{Bb^۲}{Aa^۲}}:\frac{\frac{b}{a}+\frac{A}{B}}{\frac{-b}{a}+\frac{A}{B}}$$

$$\left(-\frac{Bb^۲}{Aa^۲},-\frac{A}{B},\frac{b}{a},\frac{-b}{a}\right)=-۱$$

یعنی مجانبهای هذلولی و قطرهای مزدوج دستگاه توافقی تشکیل می‌دهند وتنها یکی از قطرهای مزدوج هذلولی را قطع می‌کنند.

نظیر آنچه در بیضی گفتیم معادلهٔ هذلولی در دستگاه مایل چنین است

$$Ax^۲+By^۲+C=۰$$

اگر فرض‌کنیم محور Ox هذلولی را قطع می‌کند

$$x^۲=-\frac{C}{A}=a_۱^۲\ (OA=OA'=a_۱)$$

و چون به فرض محور Ox هذلولی را قطع می‌کند محور Oy آن را قطع نمی‌کند

$$y^۲=-\frac{C}{B}=-b_۱^۲$$

A و B را از دو رابطهٔ اخیر در معادلهٔ هذلولی می‌بریم نتیجه می‌شود

$$\frac{x^۲}{a_۱^۲}-\frac{y^۲}{b_۱^۲}=۱$$

در سهمی مبدأ مختصات را نقطه‌ای از سهمی و محور طولها را خطی‌که ازآن نقطه موازی و هم جهت با محور سهمی رسم می‌شود و محور عرضها را مماس بر سهمی اختیار می‌کنیم در اینجا نیز اگر y را به $-y$ تبدیل‌کنیم و x را تغییر ندهیم معادلـه تغییر نمی‌کند. و مبدأ مختصات روی منحنی است پس معادله به صورت زیر است

$$Ax^۲+By^۲+Cx=۰$$

چـون Ox تنها سهمی را در یـك نقطه (مبدأ) قطع مـی‌کند $A=۰$ پس معادله سهمی چنین است

$$y^۲=-\frac{C}{B}x$$

می‌توان $-\frac{C}{B}=۲P_۱$ فرض‌کرد و معادله را به این شکل در آورد $Y^۲=۲P_۱X$.

یادآوری - اگر محورهای مختصات را منطبق بر مجانبهای هذلولی اختیارکنیم چون در تغییر محورها از دستگاه قائم به این دستگاه درجهٔ منحنی تغییر نمی‌کند بعلاوه خط موازی با مجانبها فقط هذلولی‌را دریك نقطه قطع می‌کند معادله هذلولی از صورت کلی

$$Ax^۲+۲Bxy+Cy^۲+۲Dx+۲Ey+F=۰$$

$$Ax^۲+۲Dx+F=۰\qquad A=۰$$

خط موازی با محور xها و yها منحنی را در یك نقطه قطع می‌کند

$$Cy^۲+۲Ey+F=۰\qquad C=۰$$

چون محورهـای مختصات منحنی را قطع نمی‌کند $D=۰$ و $E=۰$ می‌شود

$$۲Bxy+F=۰$$

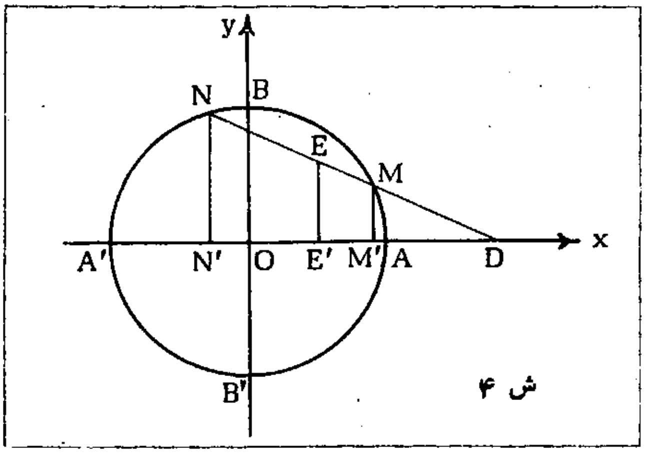
$$\boxed{xy=K}$$

۴ـ تعیین معادلـهٔ قطبی نقطهٔ مفروض نسبت بـه متقاطـع مخروطی است.

الف. دایره ـ تعیین قطبی D نسبت به دایره در دستگـاه قائم.

از D ناطعی رسم مـی‌کنیم تا دایره را در M و N قطع کند، E مزدوج توافقی D را نسبت به M و N تعیین می‌کنیم و M'، N' و E' تصویرهای قائم M، N و E را روی محور

Ox تعیین می‌کنیم



ش ۴

$$(DE'M'N') = (DEMN) = -۱$$

$$\frac{DM'}{DN'} : \frac{E'M'}{E'N'} = -۱ \implies$$

$$\frac{m'-d}{n'-d} : \frac{m'-C'}{n'-C'}$$

$$(۱) \quad e' = \frac{d(m'+n') - ۲m'n'}{۲d - (m'+n')}$$

برای تعیین مختصات M و N فرض می‌کنیم (q, p) پارامتر هاوی خط d باشد با معادلهٔ خط ومعادلهٔ دایره دستگاه زیر را تشکیل می‌دهیم

$$\left| \begin{array}{l} \frac{x-d}{p} = \frac{y}{q} \implies \\ y = \frac{q}{p}(x-d) = \lambda(x-d) \\ x^۲ + y^۲ = R^۲ \\ \qquad (۱+\lambda^۲)x^۲ - ۲\lambda^۲dx + \lambda^۲d^۲ - R^۲ = ۰ \end{array} \right.$$

رابطه بین ضرایب و ریشه‌ها

$$(۲) \quad x' + x'' = m' + n' = \frac{۲\lambda^۲d}{۱+\lambda^۲}$$

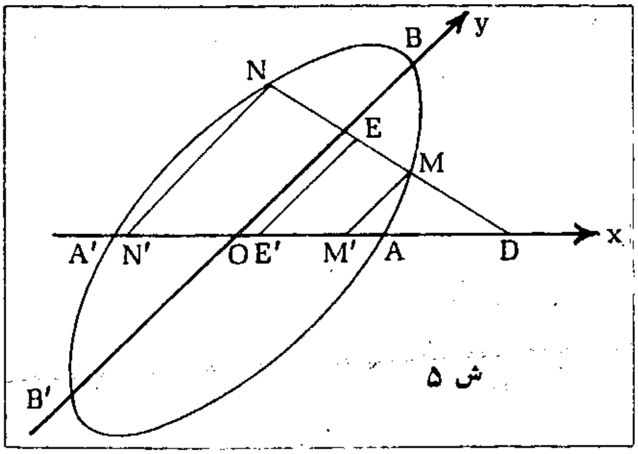
$$(۳) \quad x'x'' = m'n' = d^۲$$

بین سه معادلهٔ (۱)، (۲) و (۳) m'+n' و m'n' را حذف می‌کنیم نتیجه می‌شود

$$e' = -d \implies OA^۲ = OA'^۲ = OD \cdot OE'$$

E' مزدوج توافقی D نسبت بـه A و A' و خط E'E قطبی D نسبت به دایره است.

ب ـ تعیین قطبی نقطه در دستگاهی که محورهای آن منطبق بر دو قطر مزدوج از بیضی باشد. از D(d, ۰) قاطعی رسم می‌کنیم تا بیضی را در M و N قطع کند و E مزدوج توافقی D را نسبت به M و N مشخص می‌کنیم.



ش ۵

نقطه‌های M، N و E را به موازات محور Oy در سه نقطه M'، N' و E' تصویر می‌کنیم

$$(DE'M'N') = (DEMN) = -۱$$

$$\frac{DM'}{DN'} : \frac{E'M'}{E'N'} = -۱ \implies$$

$$\frac{m'-d}{n'-d} : \frac{m'-C'}{n'-C'} = -۱$$

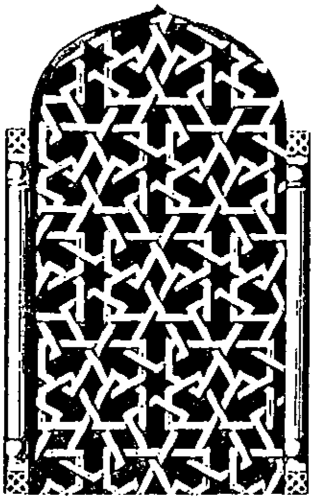
$$(۱) \quad e' = \frac{d(m'+n') - ۲m'n'}{۲d - (m'+n')}$$

معادلهٔ خط DMN را با پارامترهای هادی (p, q) با معادلهٔ بیضی در یك دستگاه می‌نویسیم

$$\left| \begin{array}{l} \frac{x-d}{p} = \frac{y}{q} \implies \\ y = \frac{q}{p}(x-d) = \lambda(x-d) \quad \left(\frac{q}{p} = \lambda\right) \\ \frac{x^۲}{a^۲} + \frac{y^۲}{b^۲} = ۱ \\ \qquad (\lambda^۲a^۲+b^۲)x^۲ - ۲\lambda^۲a^۲dx \\ \qquad\qquad + \lambda^۲a^۲d^۲ - a^۲b^۲ = ۰ \end{array} \right.$$

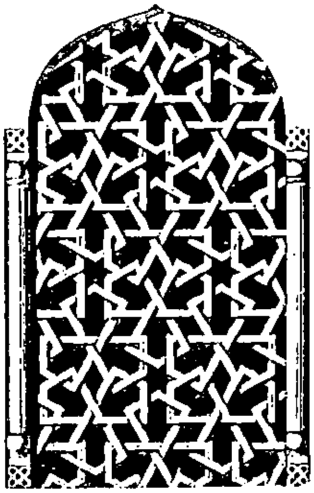
روابط بین ضرایب و ریشه‌ها را می‌نویسیم

بقیه در صفحه ۳۶



ریاضیات دورهٔ اسلامی

(۹)



دکتر محمدقاسم وحیدی اصل

محمدباقربن محمدحسین بن محمد باقر یزدی در شرحی به زبان عربی که در سال ۱۱۰۶ هجری قمری بر کتاب *عیون الحساب* جدّش ملامحمدباقر زین‌العابدین یزدی از ریاضیدانان دورهٔ اسلامی (که احتمالاً کمی پیش از سال ۱۰۶۹ هجری درگذشته) نوشته است، درضمن مطلبی دربارهٔ مساحت سطوح مستوی به محاسبهٔ عدد π در اروپا اشاره کرده است. ابوالقاسم قربانی، مورخ ریاضی، به استناد همین نوشته حدود دوره‌ای از تاریخ ریاضیات را که «دورهٔ اسلامی» نامیده می‌شود، از زمان خوارزمی در سدهٔ دوّم هجری تا زمان تألیف کتاب *عیون الحساب* می‌داند. زیرا از این به بعد ریاضیدانان ایرانی از کارهای ریاضی اروپائیان آگاهی پیدا کرده بودند و به قول قربانی دیگر نمی‌توان آثار آنان را از تأثیر کارهای اروپائیان در رشتهٔ ریاضی مبرّی و مستقل دانست و نوشته‌های آنان را متعلق به دورهٔ اسلامی به حساب آورد. ناگفته نماند که از پایان این دوره یعنی از قرن یازدهم هجری به بعد ریاضیدانان قابل ذکری که قابل مقایسه با ریاضیدانان دورهٔ اسلامی باشد، به عرصه نیامد.

آخرین ریاضیدان طرازاوّل دورهٔ اسلامی جمشیدبن مسعود بن محمود طبیب کاشانی ملقب به غیاث‌الدین است. اطلاعاتی که دربارهٔ زندگی او موجود است، پراکنده و بعضاً ضد و نقیض است. اولین تاریخ معلوم از زندگی او دوازدهم ذیحجهٔ ۸۰۸ هجری است که دراین تاریخ، بنابر آنچه در کتاب *زیج خاقانی* نوشته، کسوفی را در کاشان رصد کرده است. به گفته کندی[1]، در ۱۹ رمضان ۸۳۲ هجری در خارج شهر سمرقند درگذشته است. ترتیب گاهشناختی آثاری که کاشانی به فارسی و عربی نوشته کاملاً معین نیست، ولی وی گاهی تاریخ و محل دقیق اتمام آنها را می‌دهد. مثلاً *سلم السماء*، رساله‌ای دربارهٔ فواصل و اندازه‌های اجسام آسمانی، را که به وزیری به نام کمال‌الدین محمود اهدا کرده، در ۲۱ رمضان سال ۸۰۹ به پایان رسانیده است. همچنین کتاب مختصر در علم هیأت را به فارسی در سال ۸۱۳ نوشته و به سلطان جلال‌الدین امیرزاده اسکندر بهادرخان اهدا کرده است. در سال ۸۱۶، کاشانی زیج خاقانی را به اتمام رسانده و آن را به الغ بیگ تقدیم کرده است. در سال ۸۱۸ رسالهٔ مختصر شرح‌آلات رصد را به فارسی نوشته و آن را به سلطان اسکندر اهدا کرده است. تقریباً در همین زمان، یعنی در دهم ذیحجهٔ سال ۸۱۸ هجری، کاشانی کتاب *نزهة الحدائق* را به پایان رسانیده است. کاشانی آلتی نجومی به نام *طبق المناطق* اختراع کرده بود و این کتاب در چگونگی آن آلت نجومی و روش به کاربردن آن نوشته شده است.

کاشانی، بنا به رسم آن ادوار، با اهدای کتابهای خود به سلاطین و اعیان درصدد برآمد که به امنیت مالی دست یابد. گرچه کاشانی حرفه‌ای دیگر، یعنی طبابت، داشته ولی آرزو داشته است که در نجوم و ریاضیات به کار بپردازد. بعد از مدتها سرگردانی، سرانجام موقعیت مستحکم و قابل احترامی در دربار الغ بیگ، که خود عالمی بزرگ و حامی علم و دانش بود، پیدا نمود.

الغ بیگ بین سالهای ۸۲۱ـ ۸۲۴ هجری قمری، مدرسه و خانقاهی درسمرقند بنا کرد. پس از پایان یافتن ساختمان مدرسه، الغ بیگ فرمان بنای رصدخانه‌ای را در سمرقند صادر کرد و نظر به احتیاجی که به غیاث الدین جمشید در ساختن رصدخانه داشت، او علمای دیگری مانند قاصر زاده رومی و معین الدین کاشی را به سمرقند، که در آن زمان یکی از مراکز مهم علمی بود، فراخواند.

کاشانی در سمرقند فعالانه به مطالعهٔ

ریاضی و نجومی خود ادامه داد و سهم بزرگی در سازماندهی رصدخانه، تجهیز آن با بهترین آلات نجومی و تهیهٔ زیج الغ بیگ ایفا نمود که این زیج بعد از فوت او (کاشانی) به اتمام رسید. کاشانی در بین دانشمندانی که در خدمت الغ بیگ بودند، بالاترین مقام را داشت. در این ارتباط، خواندمیر در *حبیب السیر* می‌نویسد: «... و در سنهٔ ۸۲۴ آن خسرو بی مانند (الغ بیگ) در وسط بلدهٔ فاخرهٔ سمرقند مدرسهٔ رفیع و خانقاهی منیع بنا نموده و به اتمام رسانید وبسیاری از مزارع و قری و مستغلات فواید انتها بر آن بقاع و قف گردانید. و همچنین فرمان داد استادکاران در آن بلدهٔ فردوس نشان رصدی بنیان نهادند و بطلمیوس ثانی مولاناغیاث‌الدین جمشید و جامع کمالات انسانی معین‌الدین کاشی در ترتیب آن بنا سعی و اهتمام دادند.»

خود کاشانی شرح کاملی از زندگی علمی سمرقند را در نامه‌ای بدون تاریخ به پدرش می‌دهد. این نامه درزمانی که ساختمان رصدخانه شروع شده بود، نوشته شده است. استاد محیط طباطبایی این نامه را برای اولین بار در ایران، در سال ۱۳۱۹ هجری شمسی به چاپ رسانیده است. کاشانی در این نامه دانایی و استعداد ریاضی الغ بیگ، و بویژه توانایی او را در انجام محاسبات ذهنی دشوار بسیار ستوده است. او دراین نامه فعالیتهای علمی الغ بیگ را هم توصیف می‌کند و در یک مورد او را سرپرست رصدخانه می‌خواند. در نتیجه نظر سوتر[۲] که کاشانی را اولین سرپرست رصدخانه و جانشین او را قاضی زادهٔ رومی می‌داند، بسیار تردید آمیز به نظر می‌رسد. از طرف دیگر، کاشانی از حدود شصت همکار علمی الغ بیگ با تحقیر یاد می‌کند، گرچه قاضی زادهٔ رومی را «عالمترین آنها» می‌داند. با اشاره به مجالس علمی که هرچندروز یک بار در حضور الغ بیگ تشکیل و به وسیلهٔ خود او اداره می‌شد، کاشانی نمونه‌هایی از مسائل نجومی را که در آنجا مطرح می‌شدند، برمی‌شمارد. در دو مورد او بر قاضی زادهٔ رومی تفوق جسته است؛ در یک مورد قاضی زاده تعبیر نادرستی از برهانی در *قانون* مسعودی ابوریحان داده بوده و در یک مورد او قادر به حل مشکلی در ارتباط با مسأله تعیین اینکه سطح معینی واقعاً مسطح است یا نه نبوده است. با این حال روابط او با قاضی زاده صمیمانه بوده است. کاشانی با رضایت فراوان از ستایش الغ بیگ از او، که برخی از دوستانش بر او نقل کرده بودند، به پدرش می‌نویسد «از تحسین‌های حضرت سلطنت پناهی آن است که هیچ هفته نگذرد که بعضی از دوستان به این بنده نرسانند که بندگی حضرت سلطنت پناهی امشب یا امروز چنین و چنان نکته‌ها فرمودند امثال اینها: مستحضر است، بغایت خوب می‌داند و ازهمه این بهتر می‌داند و از قاضی (منظور قاضی زادهٔ رومی) مستحضرتر و پرمایه‌تر است و دراین فن پرذهن‌تر، چیزی که او به ده روز مشکل درمی‌یابد، مولانا غیاث‌الدین برفور یادر روز درمی‌یابد. جمیع اقسام این فن را می‌داند...» این نامه و مدارک دیگر کاشانی را به عنوان نزدیکترین همکار و مشاور الغ بیگ مشخص می‌کند. الغ بیگ ظاهراً بی‌توجهی کاشانی را به رسوم دربار تحمل می‌کرده امّا به گفتهٔ امین احمدرازی در تذکرهٔ *هفت اقلیم*. «... و چون مولانا (غیاث‌الدین جمشید) در آداب و رسوم خدمت پادشاهان بسیار عاری افتاده بود، هر آینه آنچه آداب و روش ملازمت بوده باشد از او به وقوع نمی‌پیوست، و جناب میرزا (الغ بیگ) از این رهگذر همواره مکدر بوده اظهار آزردگی می‌فرمود، امّا بنابرآنکه معاملهٔ زیج بی وجود مولانا سمت اختتام نمی‌پذیرفت؛ بالضروره در تجرع سخن تلخ مولانا صابر بودهٔ همیشه بر زبان می‌آورده که این مهّم کی صورت انصرام یابد تا من از اطوار و گفتار ناهنجار مولانا جمشید خلاص شوم. و بعضی *فوت مولانا را از جانب میرزا الغ بیگ می‌دانند*.»

کاشانی مهمترین آثار خود را در سمرقند به وجود آورد. در اواسط شعبان سال ۸۲۷ *رسالهٔ محیطیّه* را که شاهکاری در فنون محاسبه است و به محاسبهٔ ۲π تا ۱۶ رقم اعشاری منجر می‌شود، به پایان رسانید. در سوم جمادی الاولی ۸۳۰ ه.ق. کتاب *مفتاح الحساب* را که به الغ‌بیگ اهدا شده به اتمام رسانید. تاریخ اتمام سومین شاهکار او، *رسالهٔ وتر و جیب*، که در آن Sin۱° را با همان دقت که π را محاسبه کرده بوده، حساب می‌کند، معلوم نیست. ظاهراً او کمی قبل از زمان مرگش روی این اثر به کار پرداخته است. بنابر بعضی منابع این رساله در زمان فوت کاشانی نیمه تمام بوده و قاضی‌زادهٔ رومی آن را به پایان رسانیده است. ابوالقاسم قربانی با ارائه دلائلی این ادعا را رد می‌کند. کاشانی ظاهراً این روش محاسبهٔ Sin۱° را قبل از اتمام *مفتاح الحساب* تکمیل کرده بوده است؛ زیرا در مقدمهٔ این کتاب با ارائه فهرستی از آثار قبلی‌اش، به رسالهٔ وتر و جیب اشاره می‌کند.

چنانکه گفتیم، کاشانی در تألیف *زیج الغ‌بیگ* (زیج گورکانی = زیج جدید سلطانی) شرکت داشت. بخش نظری مقدماتی زیج در زمان حیات کاشانی تألیف شده و او آن را از فارسی به عربی ترجمه کرد.

مشهورترین اثر کاشانی در ریاضیات مفتاح *الحساب* است که یک دایرة المعارف واقعی از ریاضیات مقدماتی است و برای طیف وسیعی از محصلین نوشته شده است. این کتاب همچنین نیازهای محاسبه کنندگان اعم از منجمین، زمینسنجان، معماران، منشی‌ها، و بازرگانان را در نظر داشته است. از نظر غنای محتویات آن و از لحاظ به کارگیری‌روشهای حسابی و جبری در حل مسائل گوناگون، از جمله مسائل هندسی، و بالاخره از لحاظ وضوح و زیبایی بیان آن، این کتاب درسی

حجیم یکی از بهترین آثار سده‌های میانی است. کتاب همچنین گواه بارزی بر وقوف علمی مؤلف و توانایی آموزشی اوست. مفتاح الحساب به دلیل کیفیت ممتازش، کراراً رونویسی شده و برای صدها سال به عنوان کتاب دستی محاسبات مورد استفاده قرار گرفته است. عنوان کتاب (مفتاح=کلید) نشان می‌دهد که کاشانی حساب را کلید حل هرگونه مسأله‌ای که قابل تحویل به حساب باشد، تلقی می‌کرده و آن را «علم قواعد یافتن مجهولات عددی به کمک کمیتهای نظیر» تعریف کرده است. مفتاح به پنج فصل تقسیم شده و مقدمه‌ای در پیشاپیش آنها آمده است. عنوان این مقاله‌ها چنین‌اند: «در حساب عددهای صحیح با ارقام هندسی»، «حساب کسر»، «در طریق حساب منجمان»، «در مساحت»، «در استخراج مجهولات به وسیلهٔ جبر و مقابله و حظاین و غیره». این کتاب مشتمل بر مسائل جالب متعدد و مثالهای عددی دقیقاً تحلیل شده است.

در مقالهٔ اوّل *مفتاح الحساب*، کاشانی یک روش کلّی را برای استخراج ریشه‌های اعداد صحیح بتفصیل شرح می‌دهد. جزء صحیح این ریشه به کمک آنچه امروزه روش روفینی[۳] ـ هورنر[۴] نامیده می‌شود، به دست می‌آید. اگر ریشه اصم باشد، $a^n + ra + ۱$ (a, n, a و r اعداد صحیح)، جزء کسری ریشه مطابق با فرمول تقریبی ـــــ محاسبه می‌شود. خود کاشانی کلیهٔ قواعد محاسبه را در قالب کلمات بیان می‌کند، و جبر او همواره لفظی است. در رابطه با این مطالب، کاشانی قاعده‌ای کلّی برای بتوان رسانیدن یک دو جمله‌ای به هر توان صحیح مثبت و قاعدهٔ جمعی برای تعیین ضرایب دو جمله‌ای می‌دهد؛ و مثلث موسوم به مثلث پاسکال را (به ازای $n=9$) می‌سازد. این روشها قبلاً در *جامع الحساب بالتخت و التراب* (حساب به کمک تخته و غبار) خواجه نصیرالدین طوسی ارائه شده‌اند. امکان دارد که الاقل بخشی از این روشها را خیام ابداع کرده باشد. تأثیر ریاضیات چینی را هم نمی‌توان نادیده انگاشت [۴].

اهمّ مطالب فصلهای دوم و سوّم، اصول کسرهای اعشاری است که توسط کاشانی قبلاً در *رسالهٔ محیطیّه* به کار رفته است. این اولین باری نیست که کسرهای اعشاری در کتب ریاضی دورهٔ اسلامی ظاهر می‌شود. این کسرها قبلاً در کتاب *الفصول فی الحساب الهندی* تألیف ابوالحسن احمدبن ابراهیم اقلیدسی (که در سال ۳۴۱ هجری در دمشق می‌زیسته و بیشتر از این از اصول احوال شخصی او نمی‌دانیم) و مقالهٔ *فیما یحتاج الیه من الحساب الهندی فی صناعة النجوم* تألیف کوشیاربن لبان گیلانی (ریاضیدان و منجم ایرانی نیمهٔ دوّم قرن چهارم)، کتاب *شمارنامهٔ* حاسب طبری و «*کتاب المقنع فی الحساب الهندی*» تألیف ابوالحسن علی بن احمد نسوی (هر دو ریاضیدان ایرانی قرن پنجم) دیده می‌شوند و ریاضیدانان چینی هم گاهی آنها را به کار برده‌اند. امّا تنها کاشانی است که کسرهای اعشاری را به روش منظم معرفی می‌کند و قصدش ایجاد دستگاهی از کسرهاست که در آن (مانند دستگاه شصتگانی) کلیهٔ اعمال را بتوان به همان روالی که در مورد اعداد صحیح عمل می‌شود، به جا آورد. این دستگاه مبتنی بر شمارش دهدهی مرسوم در آن زمان بوده و بنابراین برای کلیهٔ کسانی که با حساب شصتگانی منجمین آشنا نبوده‌اند، قابل وصول بوده است. به قول خود کاشانی «... خواستیم که آن کسرها را به ارقام هندی تحویل کنیم تا محاسبی که حساب منجمان را نمی‌داند در حساب در نماند...» [۳]. اعمال با کسرهای متناهی به تفصیل شرح داده شده‌اند، ولی کاشانی به خاصیّت تناوب اشاره نمی‌کند. در نیمهٔ دوّم قرن پانزدهم میلادی و در قرن شانزدهم کسرهای اعشاری کاشانی در ترکیه رواج یافتند که این کار احتمالاً از طریق علی قوشچی (ریاضیدان ایرانی متوفی به سال ۸۷۹) بوده که در سمرقند با کاشانی همکاری داشته و بعد از قتل الغ بیگ و سقوط امپراطوری بیزانس، در قسطنطنیّه اقامت کرده بود. این کسرها همچنین در یک مجموعهٔ بیزانسی مجهول المؤلف مربوط به قرن پانزدهم که در سال ۱۵۶۲ به وین آورده شد، ظاهر می‌شوند. امکان دارد که افکار کاشانی در انتشار کسرهای اعشاری در اروپا تأثیر داشته باشد. در کتابهای تاریخ ریاضیات اختراع کسرهای اعشاری را معمولاً به سیمون استوین[5] بلژیکی (قرن شانزدهم)، بورگی[۶] سویسی (قرن شانزدهم) و فرانسوا ویت فرانسوی[۷] (قرن شانزدهم) و عده‌ای دیگر نسبت می‌دهند. [۱].

بزرگترین دستاورد کاشانی *رسالهٔ محیطیّه* و *رسالهٔ وتروجیب* هستند که هر دو در ارتباط مستقیم با پژوهشهای نجومی و بخصوص در رابطه با نیازهای روزافزون به جدولهای مثلثاتی دقیق نوشته شده‌اند.

در ابتدای *رسالهٔ محیطیّه* کاشانی خاطرنشان می‌کند که کلیّهٔ مقادیر تقریبی نسبت محیط دایره به قطر آن، یعنی عدد π، که توسط پیشینیان او محاسبه شده باعث خطای (مطلق) بسیار بزرگی در محیط و حتّی خطای بزرگتری در محاسبهٔ مساحتهای دایره‌های بزرگ می‌شوند. کاشانی مسألهٔ محاسبهٔ دقیقتر این نسبت را با دقتی خارج از نیازهای عملی منجمین برحسب استاندارد معمول آن زمان که اندازهٔ عالم مرئی یا «کره ستارگان ثابت» بود، پیش رو نهاد. برای این منظور او، نظیر قطب‌الدّین شیرازی منجم ایرانی قرن هفتم، فرض کرد که شعاع این کره ۷۰۰۷۳/۵ برابر قطر زمین است. در واقع مسأله‌ای که کاشانی مطرح کرد، محاسبهٔ π با چنان دقّتی بود که خطای محیط وقتی که شعاع ۶۰۰،۰۰۰ برابر قطر زمین باشد، از ضخامت یک موی اسب تجاوز نکند! کاشانی واحدهای اندازه‌گیری

زیر را مورد استفاده قرار داد.

۱۲۰۰۰ ذراع = ۱ فرسنگ (تقریباً شش کیلومتر)

۲۴ اصبع = ۱ ذراع

۶ برابر عرض یک دانه جو = ۱ اصبع (انگشت)

۶ برابر ضخامت موی اسب = ضخامت جو

محیط دایرهٔ عظیمهٔ زمین ۸۰۰۰ فرسنگ تصور می‌شد و لذا کاشانی قصد داشت که π را چنان حساب کند که خطا بیشتر از ۱۵×۱۰^{-۱۷} نباشد.

روش کاشانی بر محاسبهٔ محیطهای چند ضلعیهای محاطی و محیطی مبتنی است. این همان روش ارشمیدس است ولی شیوهٔ عمل تا حدی با روش ارشمیدس متفاوت است. کلیهٔ محاسبات در شمارش شصتگانی برای دایره‌ای به شعاع ۶۰ انجام می‌شوند. قضیه اساسی کاشانی، با نمادهای امروزی، به شرح زیر است: در دایره‌ای به شعاع r،

$$r(۲r + \mathrm{Crd}\,\alpha^\circ) = \mathrm{Crd}^۲(\alpha^\circ + \frac{۱۸۰^\circ - \alpha^\circ}{۲})$$

که در آن $\mathrm{Crd}\,\alpha^\circ$ طول وتر مقابل به کمان α° $(\alpha^\circ < ۱۸۰^\circ)$ است. بنابراین کاشانی در اینجا «مثلثات وترها» و نه خود خطوط مثلثاتی را به کار می‌گیرد. اگر $\alpha = ۲\varphi$ و $d = ۲$، در این صورت قضیهٔ کاشانی را می‌توان به زبان مثلثاتی به صورت:

$$\sin(۴۵^\circ + \frac{\varphi^\circ}{۲}) = \sqrt{\frac{۱ + \sin\varphi^\circ}{۲}}$$

نوشت که بعداً در آثار لامبرت[۱] (۱۷۷۰ میلادی) دیده می‌شود. طول وتر ۶۰° برابر r است و لذا می‌توان به کمک این قضیه وترهای

$$C_۱, C_۲, C_۳, \dots$$

مربوط به کمانهای

۱۲۰°، ۱۵۰°، ۱۶۵°، ...

را حساب کرد. در حالت کلّی وتر C_n از کمان

$$\alpha_n^\circ = ۱۸۰^\circ - \frac{۳۶۰^\circ}{۳۰۲^n}$$

برابر $c_n = \sqrt{r(۲r + c_{n-۱})}$ خواهد بود. با معلوم بودن وتر C_n، می‌توانیم مطابق قضیهٔ فیثاغورس، ضلع $a_n = \sqrt{d^۲ - c_n^۲}$ مربوطه را که ضالع ۳۰۲^n ضلعی منتظم محاطی است، حساب کنیم. ضلع b_n چند ضلعی محیطی نظیر به وسیلهٔ تناسب $b_n : a_n = r : h$ تعیین می‌شود که در آن h سهم (فاصلهٔ عمودی بین مرکز و ضلع چند ضلعی) چند ضلعی محاطی است. کاشانی در بخش سوم رساله‌اش محقق می‌دارد که دقت مطلوب در مورد چند ضلعی منتظم:

$$۳۰۲^{۲۸} = ۸۰۵,۳۰۶,۳۶۸$$

ضلع داشته باشد.

کاشانی سپس کار محاسبهٔ وترها را در بیست و هشت سال جدول مبسوط پی می‌گیرد و درستی استخراج جذر را با مجذور کردن و با طرح ۵۹ به ۵۹ (مانند طرح ۹ به ۹ در شمارش اعشاری) امتحان می‌کند. می‌توان وترهای c_n و اضلاع a_n را با نمادهای کنونی با فرمولهای

$$c_n = r\sqrt{۲ + \sqrt{۲ + \dots + \sqrt{۲ + \sqrt{۳}}}}$$

و

$$a_n = r\sqrt{۲ - \sqrt{۲ + \dots + \sqrt{۲ + \sqrt{۳}}}}$$

که در آن عدهٔ رادیکالها برابر با n است، بیان کرد. در فصل ششم کتاب، کاشانی با ضرب $a_{۲۸}$ در $۳۰۲^{۲۸}$ محیط $P_{۲۸}$ چند ضلعی ۳×۲^{۲۸} ضلعی و سپس محیط $P_{۲۸}$ چند ضلعی منتظم محیطی نظیر را حساب می‌کند. سرانجام بهترین مقدار تقریبی برای $۲\pi r$ را میانگین حسابی $\frac{P_{۲۸}+P_{۲۸}}{۲}$ اختیار می‌کند که مقدار آن در دستگاه شصتگانی به ازای $r = ۱$ برابر است با

۴۶، ۵۱، ۳۴، ۱، ۲۸، ۵۹، ۱۶، ۶

که همهٔ ارقام درست هستند. کاشانی در فصل هشتم کتابش این مقدار را به دستگاه اعشاری برمی‌گرداند:

$$۲\pi = ۶/۲۸۳۱۸۵۳۰۷۱۷۹۵۸۶۵$$

که تا ۱۶ رقم اعشاری درست است. این نتیجهٔ فوق‌العاده بر کلیه محاسبات قبلی π به مراتب پیشی جست. تقریب اعشاری $\pi \approxeq ۳/۱۴$ متناظر با کرانهای مشهور $۳\frac{۱۰}{۷۱} < \pi < ۳\frac{۱}{۷}$ که به توسط ارشمیدس به دست آمده است؛ بطلمیوس مقدار ۳، ۸، ۳۰ ($\approxeq ۳/۱۴۱۶۶$) را در دستگاه شصتگانی به کار برد و نتایج پیشینیان کاشانی در کشورهای اسلامی بهتر از این نبودند. دقیقترین مقدار π که قبل از کاشانی به وسیلهٔ ریاضیدان چینی، تسوچانگ چی[۹] (قرن پنجم میلادی) به دست آمده است، تنها تا ۶ رقم اعشاری درست بود. در اروپا در سال ۱۵۹۷ میلادی وان رومن[۱۰] با محاسبهٔ π تا ۱۵ رقم اعشاری درست به نتیجهٔ کاشانی نزدیک شد، بعداً لودلف وان کوله[۱۱] π را تا بیست و سپس تا سی و دو رقم اعشار محاسبه کرد (که در سال ۱۶۲۵ به چاپ رسید.)

کاشانی در رسالهٔ وتر و جیب مقدار $\sin ۱^\circ$ را تا ۱۷ رقم درست شصتگانی محاسبه می‌کند؛ بهترین نتیجه پیش از او، با چهار رقم درست، در قرن چهارم به وسیلهٔ ابوالوفای بوزجانی و ابن یونس (ریاضیدان مصری متوفی به سال ۳۹۹) به دست آمد. کاشانی معادلهٔ تثلیث زاویه را که همان $px = q + x^۳$ باشد، به دست آورد. در کشورهای اسلامی با معادلهٔ تثلیث از قرن یازدهم آشنا بودند؛ معادله‌ای از این نوع به طور تقریبی به وسیلهٔ ابوریحان بیرونی برای تعیین ضلع یک نه ضلعی منتظم حل شده بود، امّا روش ابوریحان دقیقاً معلوم نیست. کاشانی یک روش ابداعی برای حل تقریبی این معادله پیشنهاد کرد که می‌توان آن را به بیان امروزی چنین توصیف کرد: فرض کنید که معادلهٔ

$$x = \frac{q + x^۳}{p}$$

دارای ریشهٔ مثبت کوچکی مانند x باشد؛ در تقریب اوّل $x_۱ = \frac{q}{p}$؛ در تقریب دوّم $x_۲ = \frac{q+x^۳}{p}$، در تقریب سوّم $x_۳ = \frac{q + x^۳}{p}$؛ و به طور کلّی

$$x_۰ = ۰ \quad \text{و} \quad x_n = \frac{q + x_{n-۱}^۳}{p}$$

اختیار می‌کنیم. می‌توان ثابت کرد که چنین روندی در همسایگی مقادیر n به طوری که $۱>$ $r < \frac{۳x^۲}{p}$، همگراست. کاشانی شیوه‌ای نسبتاً متفاوت را به کار برد: وی $x_۱$ را با تقسیم q بر p به عنوان اولین رقم شصتگانی ریشهٔ مطلوب پیدا کرد، سپس به جای خود تقریبهای

$$x_۲, x_۳, \dots$$

مقادیر تصحیح شدهٔ نظیر، یعنی ارقام شصتگانی متوالی x را پیداکرد. نقطهٔ شروع محاسبهٔ کاشانی مقدار sin۳۰° بود که می‌توان آن را با اعمال مقدماتی از وتر ۷۲° (ضلع پنج ضلعی منتظم محاطی) وتر ۶۰° پیداکرد (نگاه کنید به [۱]، صفحهٔ ۱۹۵)sin۱° وقتی شعاع ۶۰ باشد به عنوان ریشه‌ای از معادلهٔ

$$x = \frac{۹۰۰\ \sin ۳^\circ + x^۳}{۴۵\times ۶۰}$$

به دست می‌آید. مقدار sin۱° در دستگاه شصتگانی برای دایره‌ای به شعاع ۶۰ برابر است با

۱۷، ۲۶، ۱۶، ۴۴، ۱۴، ۱۱، ۴۳، ۴۹، ۱؛۲

و مقدار کسر نظیر برای دایره‌ای به شعاع ۱ برابر است با

۰/۰۱۷۴۵۲۴۰۶۴۳۷۷۲۸۳۵۷۱

کلیهٔ ارقام در هر مورد با مقدار واقعی تطبیق دارند.

روش کاشانی در حل عددی معادلهٔ تثلیث، که صورتهای دیگری از آن به وسیله الغ بیگ، قاضی زادهٔ رومی، و نوه‌اش محمودبن محمّد میریم حلبی (که در ترکیه اقامت داشت) مستلزم تعداد اعمال نسبتاً کمی است و میزان دقت تقریب را در هر مرحله از محاسبه نشان می‌دهد و بدون تردید می‌توان آن را یکی از بهترین دستاوردهای سده‌های میانی دانست. ه. هانکل[12] نوشته است که این روش «در ظرافت و زیبایی از هیچیک از روشهای تقریب که بعد از ویت در غرب کشف شدند، چیزي کم و کسر ندارد». امّا کلیهٔ این کشفیات کاشانی مدتها در اروپا ناشناخته بودند و تنها در قرن نوزدهم و بیستم میلادی بود که به وسیلهٔ مورخینی چون سدیو[13]، هانکل، لوکی[14]، و کندی مورد مطالعه قرار گرفتند.

به طوری که در بالا دیدیم کاشانی تألیفات متعددی هم در نجوم دارد که اهم آنها عبارت‌اند از زیج خاقانی (در تکمیل زیج ایلخانی)، رسالهٔ *سلم السماء*، کتاب *نزهة الحدائق*، رسالهٔ در شرح آلات رصد، و چند رسالهٔ دیگر که برای آشنایی بیشتر با این آثار و مندرجات و اهمیت آنها خواننده را به [۳] ارجاع می‌دهیم.

امّا جنبه‌ای از شخصیت کاشانی که در کتابهای تاریخ ریاضیات (و حتی کاشانی نامه اثر ابوالقاسم قربانی که شرحی عالی از زندگی و کارهای کاشانی است) از نظر دورمانده، این است که غیاث‌الدین جمشید کاشانی در ساختن ماشینهای حساب بر بلزپاسکال[15]، که او را اولین مخترع ماشین حساب می‌دانند، مقدم بوده است. در سال ۱۹۸۴ میلادی بنیاد علوم ایالات متحدهٔ امریکا کمیته‌ای را برای بررسی وضع ریاضیات در آن کشور تشکیل داد. ریاست این کمیته با ادوارد دیوید[16] بود و نتیجهٔ بررسیهای این کمیته به «گزارش دیوید» معروف شده است. ترجمهٔ یکی از پیوستهای این گزارش در مجلهٔ نشر ریاضی به چاپ رسیده است. در این گزارش می‌خوانیم: «... در قرن پانزدهم غیاث‌الدین جمشید کاشانی ریاضیدان ایرانی ماشین حسابی را برای محاسبهٔ خسوفهای ماه، و ماشین حساب دیگری را برای تجسم و نمایاندن موضع ستارگان ساخت...».

امّا دریغ که وقتی این ستارهٔ قدر اوّل آسمان ریاضیات و نجوم مشرق زمین غروب می‌کند، جای خالی او را کسی در این سوی عالم پر نمی‌کند و ریاضیات (و علوم به طور کلی) بسرعت رو به افول می‌گذارد تا آنجا که در زمان تأسیس دارالفنون، امیرکبیر ریاضیدانان خارجی را بناگزیر برای تدریس و تألیف کتب ریاضی (یا درواقع ترجمه کتب ریاضی مرسوم در اروپا) به ایران دعوت می‌کند! علل این افول باید دقیقاً بررسی و یافته‌های آن نصب العین ما باشد. باشد تا دانشگاههای ما یک بار دیگر محیطی برای پژوهشهای علمی درجه اوّل و سرورندهٔ خواندمیها، ابن سیناها، بیرونیها، و... و کاشانیها باشد، انشاءاله. و بررسی مختصر ریاضیات دورهٔ اسلامی را به همینجا به پایان می‌بریم.

پانوشتها:

1) Kennedy
2) Suter
3) Ruffini
4) Horner
5) Simon Stevin
6) Bürgi
7) Francois viete
8) Lambert
9) Tsu chung-chin
10) Van Roomen
11) Ludolph Van Ceulen
12) Hankel
13) Sedillot
14) Luckey
15) Blaise pascal
16) Edward David

مراجع:

۱) ایوز، هاورد، *آشنایی با تاریخ ریاضیات*، ترجمهٔ محمدقاسم وحیدی اصل، مرکز نشر دانشگاهی، تهران، ۱۳۶۳.

۲) قربانی، ابوالقاسم، *زندگینامهٔ ریاضیدانان دورهٔ اسلامی*، مرکز نشر دانشگاهی، تهران، ۱۳۶۵

۳) ـــ، ـــ، *کاشانی نامه*، انتشارات دانشگاه تهران، تهران، ۱۳۵۰.

۴) وحیدی اصل، محمدقاسم، *ریاضیات دورهٔ اسلامی (۷)*، رشد آموزش ریاضی شمارهٔ مسلسل ۱۹-۲۰، تهران، ۱۳۶۷.

۵) جفی، آرتور، *صورتبندی نظم عالم: نقش ریاضیات*، ترجمهٔ بهرام معلمی، *نشر ریاضی* سال ۱، شمارهٔ ۱، فروردین ۱۳۶۷

6) Dictionary of Scientific Biography.

مقالهٔ کاشانی در این فرهنگ، به قلم یوشکویچ و روزنفلد، تقریباً به طور کامل ترجمه شده و رئوس اصلی نوشتار بالا را تشکیل می‌دهد.

مباحث ریاضی در مبحث رمزنگاری

کاربردهایی از نظریه اعداد در طراحی سیستم‌های رمز

گروه ریاضی‌کاربردی
بخش طرحها و تحقیقات ـ جهاد دانشگاهی
دانشگاه صنعتی شریف

۱) مقدمه. موضوع ارتباطات و ارسال پیام از نقطه‌ای به نقطه دیگر مسأله است که از هزاران سال پیش مطرح بوده است و غالباً نیز هدف اصلی این بوده است که یک پیام با سرعت هر چه بیشتر و با صرف هزینه‌ای کمتر مخابره شود. در این بین حالاتی وجود دارد که محتوای پیام تا حدودی محرمانه بوده است. با این موارد به نحو خاصی برخورد می‌شود و هم اینک نیز افراد بسیاری در این مقوله مشغول به فعالیت می‌باشند تا بتوانند از محتوای یک پیام خاص به نهایت درجه حراست نمایند. البته میزان دقت در پاسداری از محتوای یک پیام نیز متفاوت است و برحسب آنکه این محتوا تا چه اندازه محرمانه باشد می‌بایست روشهای متفاوتی جهت ارسال آنها برگزیده شود.

هرگاه بخواهیم پیامی را به گونه‌ای محرمانه به اطلاع دیگری برسانیم اولین راهی که به نظر می‌رسد این است که از قاصد استفاده کنیم. این روش در موارد خاص می‌تواند کارساز باشد، لیکن در صورت زیاد بودن پیامها، عملاً پرخرج و غیرعملی خواهد بود. راه دیگری که به نظر مفید می‌آید آنست که قبل از مخابره یا ارسال پیام الفاظ آن را به صورتی تغییر دهیم که محتوای آن بسادگی از ظاهرش مشخص نشود. این روش اساس مبحث رمزنویسی و رمزگشایی را تشکیل می‌دهد و هدف از طرح سیستم‌هایی که این منظور را برآورده می‌کنند (CIPHER SYSTEM) این است که این تبدیل و مخابره به روشی انجام گیرد که تا حد ممکن بیگانگان از محتوای پیام مطلع نشوند. دانش و در واقع هنری که جهت طراحی چنین سیستم‌هایی به کار می‌رود رمزنگاری (CRYPTOGRAPHY) نامیده می‌شود.

مبحث رمزنگاری از نخستین روزهای پیدایش خود تاکنون مراحل مختلفی را پشت سر گذاشته است. در اولین مراحل با وسایل ساده‌ای چون کاغذ و قلم حروف پیام را تغییر داده، ظاهر متن ارسالی را دگرگون می‌ساختند. این مرحله از سیر تکامل رمزنگاری، که تا قبل از اختراع ماشین‌های الکترومکانیکی ادامه داشت، به کمک وسایل مکانیکی خاصی نیاز مخابره و ارسال پیامهای سری برآورده می‌شد که به دلیل محدود بودن روشهای موجود، طرف مقابل و یا به تعبیر دیگر «دشمن» اغلب به سادگی می‌توانست الگوریتم به کار گرفته شده در طرح این قبیل وسایل را شناسایی نموده و در جهت شکستن رمزهای ارسالی حرکت نماید. در دومین مرحله پیشرفت این مبحث، که از آغاز قرن بیستم تا اواخر ۱۹۵۰ را در می‌گیرد، ماشین‌های مکانیکی و الکترومکانیکی پیچیده‌ای به کار گرفته شدند که اغلب آنها در جریان جنگ جهانی دوم طراحی گشتند. در طرح این قبیل دستگاهها اطلاع نه چندان عمیقی از مباحث ریاضی، همچون حساب همنهشتی‌ها، نظریه اعداد، مختصری از جبر خطی و آمار می‌توانست کافی باشد. مقاله شانون (C.E. Shannon) در اواخر دهه ۱۹۴۰، که جایگاه خاصی برای ریاضی در مبحث رمزنگاری بیان می‌نمود، و پیدایش لوازم الکترونیکی کوچک در دهه ۱۹۶۰، مرحله جدیدی را در پیشرفت این مقوله موجب شدند و مباحثی را مطرح کردند که نتیجه آنها طرح دستگاههایی گردید که می‌توانند محتوای اطلاعات را تا حد بسیار بالایی سری نگهدارند.

۲) تقسیم‌بندی سیستم‌های موجود، از سال ۱۹۷۶، پس از مقاله‌ای که دیفی (W. Diffe) و هلمن (M. Hellman) ارائه نمودند، یک تقسیم‌بندی کلی در بین سیستم‌های رمز بصورت تفکیک سیستم‌ها به سیستم‌های با کلید محرمانه (SECRET Key) و سیستم‌های با کلید عمومی (PUBLIC KEY) مطرح گردید. [۱] علی‌الاصول یک سیستم رمز بین دو نقطه فرستنده و گیرنده ایجاد ارتباط می‌کند و طبیعی است که در این نقاط اطلاعات مشترکی به نام کلید سیستم وجود داشته باشد. سیستم‌هایی که تمامی اطلاعات کلیدی آنها محرمانه باشند، سیستم‌های با کلید محرمانه و سیستم‌هایی که بخشی از این اطلاعات محرمانه و بخش دیگر علنی باشند سیستم‌های با کلید عمومی خوانده می‌شوند. طراحان سیستم‌های رمز بسته به نیازهایی که به ایشان ارجاع می‌شود، سیستم موردنظر خود را در یکی از این طبقات جای می‌دهند. پس از طرح یک سیستم نحوه پیاده‌سازی آن پیش می‌آید که در این مورد نیز رمزهای مختلف به دو دسته مشخص تقسیم می‌شوند. در دسته اول که به رمزهای پاره‌ای (BLOCK CIPHER) معروف می‌باشند، متن اصلی به قطعات یا پاره‌هایی تقسیم شده و بر روی قطعات متوالی یک پردازش مشخص صورت می‌گیرد. در رمزهای دسته دوم بر روی قطعات متوالی پردازش‌های متفاوتی صورت می‌گیرد که به همین خاطر نیز به آنها رمزهای جاری (STREAM CIPHER) اطلاق می‌شود. نقش و جایگاه مباحث مختلف ریاضی در چگونگی انجام این پردازش‌ها

نمایان می‌شود. در اینجا به ذکر دو مثال از رمزهای پاره‌ای و جاری پرداخته و پس از آن به تأکید خاص مقاله در مورد کاربردهایی از نظریه اعداد در طراحی سیستم‌های رمز که در واقع شیوه‌ای خاص در انجام پردازش‌های فوق‌الذکر است می‌پردازیم.

مثال ۱. فرض می‌کنیم $P \geqslant ۲$ یک عدد اول باشد، در این صورت هر عنصر مخالف صفر از مجموعه:

$Z_p = \{۰ ، ۱ ،۲ ، ... ،p - ۱\}$، که در واقع یک هیأت می‌باشد، دارای یک معکوس حسابی در هنگ p خواهد بود. این ویژگی بیان قضیه زیر را که ابزار لازم در طراحی سیستم رمز پاره‌ای موردنظر را فراهم خواهد ساخت میسر می‌سازد.

قضیه ۱. اگر $A = [aij]$ یک ماتریس $S×S$ از عناصر Z_p باشد بطوریکه $p \nmid \det A$، آنگاه A در هیئت Z_p وارون‌پذیر خواهد بود. طریقه ساختن معکوس نیز بصورت زیر می‌باشد:

$$A^{-۱} \equiv (\det A)^{-۱} [\overset{*}{A}ij]^{T} \qquad (\text{هنگ } p)$$

که در آن Aij^{*} هم عامل‌های متناظر با عناصر aij می‌باشند.

تعداد الفبای زبان فارسی را با اضافه نمودن ارقام ۰ تا ۹ و یک علامت اضافی، برای مثال علامت فضای خالی (SPACE)، به ۴۳ افزایش می‌دهیم. حال با انتخاب یک ماتریس وارون‌پذیر $S×S$ مانند A به عنوان کلید و تقسیم متن اصلی به قطعات S حرفی (با اضافه نمودن حداکثر $S - ۱$ حرف دلخواه) عمل رمز را انجام می‌دهیم. برای این کار ماتریس کلید را در بردار عددی معادل هر قطعه ضرب نموده و بردارهای جدیدی به دست می‌آوریم. معادل حرفی این بردارها رمز شده متن اصلی را نشان می‌دهند. برای کشف رمز نیز کافی است ماتریس $A^{-۱}$ را در بردار عددی معادل قطعات رمز شده ضرب نمائیم.

مثال ۲. برای تشریح این مثال نخست به مفهوم مولد اعداد تصادفی اشاره می‌کنیم. به طورکلی هر فرایندی که در مقاطع متوالی خود منجر به انتخاب تصادفی اعدادی از یک مجموعه متناهی شود یک مولد اعداد تصادفی نامیده می‌شود. گذشته از فرآیندهای کاملاً فیزیکی که نهایتاً اعداد کاملاً تصادفی نیز تولید می‌کنند فرآیندهایی وجود دارند که براساس قواعد مشخص ریاضی استوار شده‌اند. اعداد تولید شده توسط این فرآیندها، به جهت تبعیت از یک نظم معین، کاملاً تصادفی نمی‌باشند ولیکن خواصی را دارا هستند که به موجب همین خواص به آنها اعداد شبه تصادفی گفته می‌شود. در این مثال ابتدا نمونه‌ای از این مولدها را طراحی کرده و سپس سیستم رمز جاری موردنظر را ارائه می‌کنیم. در ابتدا تعاریف و قضایایی از نظریه اعداد را یادآور می‌شویم. [۲]

تعریف ۱. برای عدد صحیح n، تابع $\varphi(n)$ که تابع اویلر نامیده می‌شود به صورت زیر تعریف می‌گردد:

$$\varphi(n)\ \#\ \left\{mez^{+}\ \backslash m<n ,(m,n) = ۱\right\}$$

که در آن (m و n) نشان دهنده بزرگترین مقسوم علیه مشترک m و n بوده و نماد#به معنای تعداد عناصر مجموعه می‌باشد.

تعریف ۲. عدد a را که نسبت به n اول باشد در نظر می‌گیرم، $(a \text{ و } n) = ۱$. به کوچکترین عدد صحیح مثبتی مانند K که در رابطه $a^k \equiv ۱$ (در هنگ n) صدق کند، مرتبه a در هنگ n گفته می‌شود.

قضیه ۲. فرض می‌کنیم مرتبه عدد a در هنگ n برابر با k باشد، در این صورت

a ،$a^۲$ ،$a^۳$ و ... و a^k

در هنگ n با یکدیگر همنهشت نخواهد بود.

تعریف ۳. هرگاه a و n نسبت به هم اول و مرتبه a در هنگ n برابر با $\varphi(n)$ باشد، در آن صورت a را یک ریشه اولیه عدد n می‌نامند.

قضیه ۳. ریشه اولیه تنها برای اعداد ۲، ۴ و اعدادی به صورت p^k و $۲p^k$ موجود می‌باشد (p یک عدد اول و k عدد صحیح). اعداد دیگری که به این چهار صورت نباشند فاقد ریشه اولیه خواهند بود.

قضیه ۴. اگر n دارای ریشه اولیه‌ای باشد، در آن صورت تعداد کل ریشه‌های اولیه آن دقیقاً با $(\varphi\varphi(n))$ خواهد بود.

از جمع تعاریف و قضایای فوق به نکته‌ای می‌رسیم که تصویری از یک مولد اعداد تصادفی را به دست می‌دهد. در واقع این نکته بیان می‌کند که اگر p یک عدد اول و r ریشه اولیه‌ای برای آن باشد در آن صورت اعداد

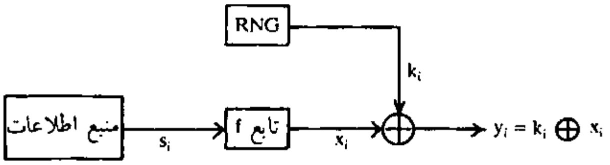
r و $r^۲$ و $r^۳$ و...و $r^{p-۱}$

$(p - ۱)$ عدد متمایز خواهند بود که در هنگ p با یکدیگر همنهشت نمی‌باشند. به عبارت دیگر این اعداد یک جایگشت شبه تصادفی از مجموعه $\{۱ \text{ و } ۲ \text{ و } ۳ \text{ و } ... \text{ و } p - ۱\}$ را نتیجه می‌دهند. برای تولید اعداد توسط مولدی که براساس قاعده فوق استوار باشد کافی است یک عدد اول مناسب p و ریشه اولیه دلخواهی از آن به عنوان مقادیر اولیه انتخاب شوند (این مقادیر را غالباً دانه‌های مولد می‌خوانند) و سپس این ریشه به توانهای ۰ تا $p - ۱$ برسد. محاسبه نتایج در هنگ p اعداد شبه تصادفی موردنظر را نتیجه خواهد داد. به عنوان مثال، با انتخاب $p = ۷$ و ریشه اولیه $r = ۳$، برای دنباله (✱) خواهیم داشت:

۳ و ۲ و ۶ و ۴ و ۵ و ۱

بدین ترتیب به مولدی می‌رسیم که در یک محدوده مشخص می‌تواند اعداد شبه تصادفی تولید کند. البته برای استفاده عملی از این مولد لازم است نکاتی چند مورد توجه قرار بگیرند. این نکات عمدتاً مربوط به اعمال روشهایی در جهت بالا بردن دوره تناوب دنباله و افزایش پیچیدگی آن می‌باشند که در این مقاله به آنها پرداخته نمی‌شود.

در مثالی که شرح خواهیم داد یک مولد اعداد تصادفی: (RANDOM NUMBER GENERATOR) RNG به کار رفته است. این مولد را می‌توان صورت تعمیم یافته‌ای از مولدی که شرح داده شد تصور نمود. حال به بیان سیستم موردنظر می‌پردازیم. نمودار ترسیمی این سیستم به شرح زیر می‌باشد:



در این سیستم طول قطعات متن اصلی را به اندازه یک حرف در نظر می‌گیریم. فرض می‌کنیم مولد RNG دنباله‌ای تصادفی از اعداد مجموعه {۴۳...، ۳، ۲، ۱} را تولید کند. برای انتساب اعداد به حروف الفبای ۴۳ حرفی زبان فارسی تابع یک به یک $f{:}L \longrightarrow z_{۴۳}$ را قرارداد می‌کنیم که در آن L الفبای زبان می‌باشد. برای رمز نمودن حرف s_i نخست مقدار $x_i=f(s_i)$ را به دست آورده و با عدد تولید شده k_i جمع می‌کنیم. محاسبه حاصل در هنگ ۴۳ مقدار y_i را نتیجه خواهد داد که با تعیین $f^{-1}(y_i)$ رمز شده حرف s_i به دست می‌آید. برقراری رابطه $x_i = y_i \oplus (۴۳ - k_i)$ طریقه کشف رمز این سیستم را روشن می‌سازد.

هر چند تفکیک کامل سیستم‌ها به سیستم‌های با کلید محرمانه و سیستم‌های با کلید عمومی همواره امکان‌پذیر نیست، چرا که می‌توان ترکیبی از این دو سیستم را نیز به عنوان یک سیستم واحد طراحی نمود، ولیکن بیان یک تقسیم‌بندی موضوعی چندان دور از واقعیت نمی‌باشد. این تقسیم‌بندی جایگاه ویژه‌ای را برای نظریه اعداد در سیستم‌های با کلید عمومی نشان داده و در مقابل به نقش موثر جبر در طرح اصولی سیستم‌های با کلید محرمانه اشاره می‌کند.

۳) طراحی سیستم‌های رمز ـ بنا به گفته شانون، مسأله طراحی یک رمز خوب با یافتن مسائل مشکل معادل می‌باشد. به عبارت دیگر می‌بایست رمز را به گونه‌ای طراحی کرد که شکستن آن با حل یک مسئله ریاضی گیج‌کننده معادل باشد. شمار بسیار زیادی از این مسائل را می‌توان در میان قانونمندی‌های حاکم بر اعداد جستجو کرد و دقیقاً به همین خاطر است که نظریه اعداد به عنوان یکی از نظریه‌های مبنای علم رمزنگاری مطرح شده است. نظریه پیچیدگی، نظریه اطلاعات و جبر نظریه‌های دیگر مبنا در این مقوله می‌باشند.

در تقسیم‌بندی رمزها به دو دسته جاری و پاره‌ای بیان شد که قطعات متوالی متن اصلی موردپردازش‌هایی قرار گرفته و نهایتاً قطعاتی از متن رمز را تولید می‌کنند. این پردازش‌ها چیزی جز اعمال توابع ریاضی نمی‌باشند. اما اینکه این توابع چه ویژگی‌هایی می‌بایست داشته باشند در تعریف زیر تا حدودی روشن شده است. [۳]

تعریف ۴. تابع $f{:}A \longrightarrow B$ را یک تابع یکطرفی (One-Way function) گوینده هرگاه به ازای هر $x \epsilon A$ محاسبه $f(x)$ به سهولت انجام شود ولی محاسبه $f^{-1}(y)$، برای هر $y \epsilon f(A)$، بسیار مشکل باشد.

برای اینکه تصویر روشنی از این تعریف ارائه شده باشد، به انگاره دیفی، هلمن و پاولیگ (s.pohlig) توجه می‌کنیم [۳]. در مقالات نوشته شده توسط این افراد، تابع زیر به عنوان یک تابع یکطرفی معرفی شده است:

$$f(x) \equiv \alpha^x \ (\text{p هنگ})$$

که در آن {۱ ـ p،... و ۱ و ۰} $x\epsilon$، p یک عدد اول بسیار بزرگ ویژه و α یک ریشه اولیه p می‌باشد. با توجه به الگوریتم‌های بسیار کارآیی که برای محاسبه تابع نمایی در یک هنگ معین طرح شده است، برای مثال «الگوریتم مربع‌سازی و ضرب»، می‌بایست پذیرفت که محاسبه $f(x)$ برای هر مقدار x از z_p بسیار ساده می‌باشد. توجه داریم که α بدین جهت ریشه اولیه اختیار شده است که یک به یک بودن تابع حفظ شده و در نتیجه بتوان از محاسبه تابع معکوس صحبت نمود. بنابراین محاسبه معکوس $f(x)=\alpha^x=y$ (در هنگ p) به معنای تعیین لگاریتم گسسته $f^{-1}(g) = \mathrm{Log}_\alpha g$ (در هنگ p) خواهد بود. با استفاده از مطالب مندرج در مرجع شماره [۴]، این نتیجه به دست می‌آید که چنانچه: ۱ ـ p دارای یک عامل اول بزرگ باشد، حتی اگر بهترین الگوریتم‌های موجود را بکار ببریم، محاسبه لگاریتم در z_p بسیار دشوار خواهد بود.

طرح این تابع، با تمام سادگی ظاهری آن، حرکتی انقلابی در حل مسأله توزیع کلیدهای محرمانه سیستم‌های رمز بوده است. در بخشهای قبلی اشاره شد که در سیستم‌های رمز با کلید محرمانه اطلاعات محرمانه‌ای بین فرستنده و گیرنده مشترک می‌باشد. توزیع محرمانه این اطلاعات در بین اعضای یک شبکه اطلاع‌رسانی امر پیچیده و حساسی است که با کمک توابع یکطرفی براحتی انجام میشود. فرض می‌کنیم در فرستنده عدد تصادفی k_i تولید شده و مقدار $\alpha^{ki}=y_i$ (در هنگ p) برای گیرنده فرستاده میشود. در همین هنگام مقدار تصادفی k_j در گیرنده تولید شده و مقدار $\alpha^{kj}\equiv y_j$ (در هنگ p) برای فرستنده ارسال میشود. دو مقدار $z_{ij}\equiv y_j^{ki}$ و $z_{ji}\equiv y_i^{kj}$ (در هنگ p) مقادیری خواهند بود که بطور همزمان در فرستنده و گیرنده محاسبه می‌شوند. برای این مقادیر داریم:

$$z_{ij}\ \ y_j^{ki} \equiv (\alpha^{ki})^{ki} \equiv \alpha^{kjki} \equiv \alpha^{kikj} \equiv (\alpha^{ki})^{kj} \equiv y_i^{kj} \equiv z_{ji} \ (\text{pهنگ})$$

که نشان می‌دهد اطلاعات مشترک کلیدی (همانند z_{ij}) می‌توانند بر روی کانالهای آزاد به گونه‌ای محرمانه مبادله شوند.

به این ترتیب درمی‌یابیم که هر مفهومی از ریاضیات که به نوعی با ویژگی توابع یکطرفی قابل انطباق باشد می‌تواند در طراحی

سیستم‌های رمز به‌کار گرفته شود. مثال زیر که به مسئله کوله‌پشتی (Knapsack Problem) معروف می‌باشد نمونه بارزی از ادعای فوق محسوب می‌گردد.

مثال ۳ ــ بردار کلیدی زیر را در نظر می‌گیریم:

$$A = (a_{۱} \text{ و } a_{۲} ,...., a_n)$$

صورت رقمی متن اصلی را به صورت n تایی مرتب

$$X = (x_{۱} \text{ و } x_{۲} \text{ و... و } x_n)$$

در نظر گرفته و متن رمز را با استفاده از ضرب داخلی بردارهای A و X به دست می‌آوریم:

$$Y = A.X$$

در واقع y حاصلجمع عناصر زیر مجموعه‌ای از A می‌باشد که محاسبه آن به سادگی انجام میشود. ولیکن با کمی دقت متوجه می‌شویم که محاسبه تابع معکوس در این مورد چندان ساده نمی‌باشد. در حالت کلی، روش معمول برای محاسبه تابع معکوس اینست که تمامی ۲^n حالت X مورد بررسی قرار بگیرند.

سؤالی که در اینجا مطرح می‌شود اینست که آیا تابع مثال فوق قابلیت اجرایی لازم برای طرح یک سیستم رمز را دارا می‌باشد یا خیر؟ پاسخ به این سؤال به طور ضمنی در بیان تعریف زیر ارائه می‌شود. [۳]

تعریف ۵. تابع $f_z:A_z \longrightarrow B_z$ را یک تابع یکطرفی دریچه‌ای (Trapdoor one-way function) گویند هرگاه:

۱ ــ با فرض معلوم بودن z، براحتی بتوان الگوریتم‌های E_z و D_z را، به ترتیب، برای محاسبه ساده f_z و $f_z^{-۱}$ بدست آورد.

۲ ــ چنانچه z مشخص نباشد، محاسبه $f_z^{-۱}(y)$ برای هر $y \in f_z(A_z)$، حتی با آگاهی از الگوریتم رمز E_z، بسیار مشکل باشد.

برای تصریح در تعریف فوق، به مثال زیر که نوع ساده مسئله کوله‌پشتی می‌باشد توجه می‌کنیم. [۵]

مثال ۴. در مورد بردار کلیدی مثال (۳) فرض می‌کنیم داشته باشیم:

$$a_i > \Sigma a_j$$

به عبارت دیگر فرض می‌کنیم این بردار دارای خاصیت فوق صعودی باشد. واضح است که

$$y \geqslant a_n \text{ اگر و فقط اگر } x_n = ۱$$

براحتی دیده می‌شود که اگر بردار A دارای خاصیت فوق صعودی باشد، X بسادگی محاسبه خواهد شد. حال برای طرح یک سیستم رمز بر اساس ویژگی بردار A و مفهوم توابع یکطرفی دریچه‌ای، به طریق زیر عمل می‌کنیم.

ــ عدد u را چنان انتخاب می‌کنیم که داشته باشیم

$$u > ۲a_n > \Sigma a_i$$

ــ عدد w را که نسبت به u اول باشد انتخاب کرده و معکوس حسابی آن در هنگ u، یعنی $w^{-۱}$، را محاسبه می‌کنیم.

ــ بردار A' را که عناصر آن بر طبق رابطه

$$a'_i = w \times a_i \ (\text{هنگ } u)$$

محاسبه می‌شود به دست می‌آوریم.

بردار A که بدین طریق حاصل میشود خاصیت فوق صعودی نداشته و لذا می‌توان به طرح یک مسأله مشکل کوله‌پشتی اندیشید. در عمل برای تابع رمز خواهیم داشت:

$$E_{u,w} = A.x = y' \ (\text{هنگ } u)$$

با استفاده از اطلاعات اضافه‌ای که u و w در اختیار می‌گذارند (اطلاعات دریچه‌ای) براحتی می‌توان الگوریتم کشف $D_{u,w}$ را به حل یک مسئله ساده کوله‌پشتی تبدیل نمود. داریم،

$$y \equiv w^{-۱}\ y' \ (\text{هنگ } u)$$
$$\equiv w^{-۱}\ (A.x) \ (\text{هنگ } u)$$
$$\equiv w^{-۱}\ (wA).x$$
$$\equiv (w^{-۱}w)\ A.x \ (\text{هنگ } u)$$
$$\equiv A.x$$

و چون بردار A دارای خاصیت فوق صعودی می‌باشد براحتی خواهیم توانست بردار مجهول x را محاسبه نمائیم.

آنچه در این مثال قابل توجه است نقش u و w می‌باشد. در واقع اگر این اطلاعات در مثال وارد نمی‌شدند عملاً امکان استفاده از یک مسأله مشکل کوله‌پشتی در طراحی یک سیستم رمز وجود نمی‌داشت.

۴) سیستم‌های رمز با کلید عمومی. با دقت در مثال (۴) به نمونه‌ای از این سیستم‌ها دست می‌یابیم. در این مثال می‌توان بردار A را یک کلید عمومی محسوب نمود که تمامی اعضای شبکه مخابراتی از آن مطلع می‌باشند. بردار A و مقادیر u و $w^{-۱}$ کلیدهای محرمانه این سیستم می‌باشند. سیستم رمز کوله‌پشتی را می‌توان یک سیستم رمز با کلید عمومی تلقی نمود که می‌تواند برای انجام مقاصد خاصی بکار گرفته شود. توضیحی که خواهد آمد کاربردهای ویژه سیستم‌های رمز با کلید عمومی را روشن می‌سازد. فرض کنید در یک موضع نظامی قرار داشته باشیم و قرار باشد اطلاعات محرمانه از منابع متعدد گزارش‌دهی به مقر فرماندهی رسانیده شود. طبیعی است که این محدودیت‌ها در سیستم اعمال شود: ۱ ــ هیچیک از منابع گزارش‌دهی از اطلاعات منابع دیگر آگاهی نداشته باشند؛ ۲ ــ هیچ فرد غیر مجازی امکان دسترسی به اطلاعات گزارش شده از منابع را نداشته باشد. در طراحی این سیستم لازم داریم که از مقر فرماندهی یک کلید عمومی

بین منابع گزارش‌دهی توزیع شود، هر یک از این منابع تنها بتوانند به رمز گزارشات بپردازند و کلید عمومی قابلیت کشف گزارشات منابع دیگررا نداشته‌باشد. در اینجا بصورت گام به گام به‌طرح‌سیستم‌دیگری با این‌خصوصیات می‌پردازیم.نخست‌قضیه اویلر را یادآوری می‌کنیم:

قضیه ۵. هرگاه $(x \text{ و } m) = ۱$ باشد، خواهیم داشت:

$$x^{\varphi(m)} \equiv ۱ \ (\text{هنگ } m)$$

گام اول ــ دو عدد اول متمایز p و q را انتخاب کرده و قرار می‌دهیم $m = pq$. این اعداد می‌بایست بسیار بزرگ باشند (حداقل در حدود $۱۰^{۲۰۰}$). p و q محرمانه خواهند بود.

گام دوم ــ مقدار $\varphi(m) = (p - ۱)(q - ۱)$ را محاسبه می‌کنیم. این مقدار نیز محرمانه می‌باشد.

گام سوم ــ عددی مانند sk را که نسبت به $\varphi(m)$ اول باشد بدست می‌آوریم، $(sk \text{ و } \varphi(m)) = ۱$. مقدار sk در این سیستم نقش کلید محرمانه را خواهد داشت.

گام چهارم ــ معکوس حسابی sk را در هنگ $\varphi(m)$ بدست آورده و آنرا pk می‌نامیم. بین sk و pk که کلید عمومی سیستم خواهد بود رابطه زیر برقرار می‌باشد:

$$sk.\,pk = k\varphi(m) + ۱$$

گام پنجم ــ تعریف توابع رمز و کشف:

تابع رمز	$E(x) \equiv x^{pk} \equiv y \quad (\text{هنگ } m)$
تابع کشف	$D(y) \equiv y^{sk} \equiv (x^{pk})^{sk} \equiv x^{pk.sk} \ (\text{هنگ } m)$

سؤال: آیا رابطه $D(E(x)) = x$ برقرار است؟ چنانچه پاسخ این سئوال مثبت باشد منظور اصلی از طرح یک سیستم با کلید عمومی برآورده خواهد شد. چرا که در اینصورت منابع گزارش دهی فوق الذکر می‌توانند از کلید pk استفاده کرده و در مقر فرماندهی نیز برای کشف رمز تمامی گزارشات از کلید محرمانه sk استفاده می‌شود.

قبل از آنکه به پاسخ سئوال بپردازیم لازم است یک محدودیت اساسی بر روی x اعمال کنیم و آن اینکه برای یک به یک بودن تابع کشف‌رمزلزوماً بایدداشته‌باشیم: $x \in \{۰،۱،۲، \dots، m - ۱\}$ در اینجا برای پاسخ‌به سئوال‌طرح شده‌فوق حالتهای‌سه گانه زیر را در نظرمی‌گیریم.

۱ ــ حالت اول. $x = o$، در این صورت رابطه مورد نظر به طور بدیهی برقرار می‌باشد.

۲ ــ حالت دوم. داشته باشیم $(x \text{ و } m) = ۱$، در اینصورت طبق قضیه اویلر خواهیم داشت:

$$x^{\varphi(m)} \equiv ۱ \ (\text{هنگ } m)$$

و از آنجا با توجه به اینکه می‌توان طرفین یک همنهشتی را به توان رسانید، به رابطه زیر می‌رسیم:

$$x^{k\varphi(m)} \equiv ۱ \ (\text{هنگ } m)$$

که با ضرب طرفین در x نتیجه مطلوب حاصل می‌شود:

$$x^{k\varphi(m)+۱} \equiv x \ (\text{هنگ } m) \text{ نتیجه می‌دهد } x^{pk.sk} \equiv x \ (\text{هنگ } m)$$

۳ ــ حالت سوم. x و m نسبت به هم اول نباشند. برای مثال فرض می‌کنیم $(x \text{ و } m) = p$ که در این صورت خواهیم داشت $x = cp$. با توجه به اینکه x از m کوچکتر می‌باشد نتیجه $(x \text{ و } q) = ۱$ براحتی بدست می‌آید. مجدداً از قضیه اویلر استفاده می‌کنیم:

$$x^{\varphi(q)} \equiv ۱ \ (\text{هنگ } q)$$

طرفین این همنهشتی را به توان $k(p - ۱)$ می‌رسانیم

$$x^{k(p-۱)\varphi(q)} \equiv ۱ \ (\text{هنگ } q)$$

که از آنجا خواهیم داشت.

$$x^{k\varphi(m)} + nq = ۱$$

با ضرب طرفین در x بدست می‌آوریم

$$x^{k\varphi(m)+۱} + nqx = x$$

و در نتیجه

$$x^{k\varphi(m)+۱} + nq(cp) = x$$

$$x^{k\varphi(m)+۱} + nc(pq) = x \Longrightarrow x^{k\varphi(m)+۱} \equiv x \ (\text{هنگ } m)$$

$$\Longrightarrow x^{pk.sk} \equiv x \ (\text{هنگ } m)$$

به این ترتیب مثبت بودن جواب سئوال به اثبات می‌رسد.

سیستمی که بدین صورت ساخته شد به سیستم RSA معروف می‌باشد که در سال ۱۹۷۸ ارائه شده است [۶]. البته این سیستم در اصل به شیوه دیگری مورد استفاده قرار می‌گیرد. قوت و استحکام این سیستم به دشواری تجزیه اعداد مربوط می‌باشد. در واقع تاکنون هیچ راه دیگری برای شکستن این سیستم به جز تجزیه m پیشنهاد نشده است. البته یک راه دیگر نیز وجود دارد و آن محاسبه $\varphi(m)$ می‌باشد، چرا که با معلوم بودن $\varphi(m)$ و pk، مقدار محرمانه sk براحتی محاسبه خواهد شد. ولیکن واقعیت این است که بدست آوردن $\varphi(m)$ از نقطه نظرمحاسباتی‌باتجزیه‌عددmمعادل‌می‌باشدزیرا،بافرض $p>q$داریم:

$$\begin{cases} p + q = m - \varphi(m) + ۱ \\ q - p = \sqrt{(p+q)^{۲} - ۴m} \end{cases}$$

و از این دستگاه p و q براحتی به دست می‌آیند. در واقع اگر $\varphi(m)$ محاسبه شود مانند این است که تجزیه شده است.

با توجه به این مطلب که تجزیه عددی در حدود $۱۰^{۲۰۰}$ (که حداقل اندازه اعداد اول p و q برای ایمن بودن سیستم RSA می‌باشد) بر روی کامپیوتر CRAY-1 در حدود ۵۵۰۰۰۰ سال وقت نیاز دارد، براساس سریعترین الگوریتم تجزیه اعداد موجود: Pomeranc's quadratic sieve، تقریباً می‌توان مطمئن بود که تا طرح یک الگوریتم تجزیه بسیار پیشرفته‌تر این سیستم ایمنی مورد نیاز را تامین خواهد کرد. [۳]

بقیه در صفحه ۳۷

چرا آنها را خواندم

ترجمه: دکتر علیرضا جمالی
دانشگاه تربیت معلم

جورج پولیا

برخی از گفتارهای ذیل به طور تحت اللفظی نقل‌قول یا ترجمه شده‌اند، و بعضی دیگر تفسیر (ترجمهٔ آزاد، خلاصه، ...) شده یا به بیان نودر آمده‌اند. [ازعلامت [ ] به منظور بیان نکات مندرج در این نقل‌قولها و اشارات ملحوظ در آنها استفاده شده است]. تلاش کرده‌ام که غرض اصلی مؤلفین بیش از حد تحریف نشود. در هر صورت، **چوآنها را خواندم**، در تنویر افکار من بس مفید واقع شدند. امیدست در خوانندگان نیز مؤثر واقع شوند.

۱ـ ایده‌ها باید در ذهن متعلم متولد شوند، و معلم صرفاً باید نقش یک قابله را داشته باشد.

سقراط

۲ـ دموکریت اولین کسی بود که به بیان حکمی پرداخت بدون آنکه به برهان آن نایل شود [فقط آن‌را حدس زد]؛ بدین اعتبار نباید سهم او را اندک دانست ... روشی که من بکار بستم اثباتی واقعی بدست نداد [فقط یک پیشنهاد، یک حدس بود... معهذا] پیش‌بینی می‌کنم که این روش برای کشف سایر قضیه‌هائی که هنوز با آنها مواجه نشده‌ام، به‌توسط ریاضیدانی که در عصر حاضر زندگی می‌کنند یا آنانی که هنوز متولد نشده‌اند، بکار گرفته خواهد شد.

ارشمیدس

[ابتدا حدس بزن سپس ثابت کن ـ راه و رسم این است.]

۳ـ شهود ادراک یک ذهن دقیق است؛ بقدری واضح، روشن و بی‌زحمت است که نمی‌توان در مدرک شک کرد.

دکارت

[زیبائی در ریاضیات دیدن واقعیت‌ها بی هیچ‌کوشش است.]

۴ـ زنجیرهائی که منطقیون می‌پندارند که به توسط آن قادر به‌کنترل ذهن بشرند برای من ارزش چندانی ندارند.

دکارت

[منطق خوبی که در آن زمان یا مکان نامناسب بکار گرفته شود، ممکن است بدترین دشمن برای یک تعلیم خوب باشد.]

۵ـ هیچ چیز مهمتر از پی بردن به سرچشمه‌های ابداعات نیست که به عقیدهٔ من، از خود آنها جالبتر است.

لایبنیتز

۶ـ ریاضیات علمی است که بهترین مجال را جهت مداقه کار ذهن فراهم می‌کند... [و] دارای این مزیت است که با پرورش آن می‌توان عادت یک روش استدلال را تحصیل نمود که بعداً می‌تواند در مطالعهٔ هر موضوع، و نیز به عنوان راهنمائی در پی‌گیری مسائل زندگی بکار گرفته شود.

کندورسه

[در اظهار نظر نسبت به کارهای اویلر.]

۷ـ بنابراین همهٔ معرفت بشری با شهود آغاز می‌شود، و از آنجا به ادراک منجر شده، و به ایده ختم می‌شود.

کانت

[آموختن با فعل و عمل و ادراک حسی شروع می‌شود و از آنجا به عبارت و مفاهیم منجر می‌شود، و باید به عادت عقلانی مطلوب منتهی شود.]

۸ـ تعلیم خوب چیست؟ دادن فرصت به متعلم که چیزها را خودکشف کند.

هربرت اسپنسر

۹ـ موضوع دقت ریاضی تصدیق و مشروعیت دادن به نتایج شهود است، و هرگز هدف دیگری برای آن در بین نبوده است،

ج.آدامار

۱۰ـ اگر اقلیدس در برانگیختن ذوق عهد شباب شما دچار شکست شود، در این صورت به عنوان یک متفکر دانشمندزاده نشده‌اید.

آلبرت اینشتین

گزارش از آموزش و آموزش ریاضی در شوروی

اطلاعات زیر، در مسافرت اخیر آقای میرزا جلیلی به شوروی، ضمن صحبت با رئیس دپارتمان ریاضی انستیوی تحقیقاتی و برنامه‌ریزی وزارت آموزش و پرورش آن کشور به دست آمده است. هیات تحریریه مجله جهت اطلاع برنامه‌ریزان و سایر علاقمندان به‌آموزش ریاضی اقدام به نشر آن نموده است.

میرزا جلیلی

در شوروی دانش‌آموزان از سن ۶ سالگی در مدرسه پذیرفته می‌شوند. (از ۷ سالگی نیز می‌توانند شروع کنند) دورهٔ دبستان برای آنهایی که از ۶ سالگی شروع می‌کنند ۴ سال و برای کسانی که ۷ از سالگی آغاز می‌کنند ۳ سال است (یکسال دورهٔ آمادگی و مقدماتی است). در دبستان تأکید روی خواندن و نوشتن، مقدمات ریاضی و اطلات عمومی ساده و متناسب با سن بچه‌هاست. دانش‌آموزان ۶ روز در هفته به مدرسه می‌روند و ۴ ساعت در روز درس می‌خوانند. عدهٔ دانش‌آموزان در یك کلاس ۳۰ نفر و حقوق معلم ۱۵۰ تا ۲۰۰ روبل در ماه است. دانش‌آموزان بعد از پایان دبستان وارد مرحله اول دبیرستان می‌شوند که دورهٔ آن ۵ سال است (از کلاس ۵ تا ۹). در این دورهٔ دروس اصلی و کلی آموزش داده می‌شود و همهٔ بچه‌ها همهٔ دروس را می‌خونند. در این مقطع دانش‌آموزان ۶ روز در هفته و ۵ ساعت در روز به‌کلاس می‌روند (۳۰ ساعت در هفته) و ۶ ساعت در هفته ریاضی تدریس می‌شود (قرار است درآینده روزهای مدرسه از ۶ روز به ۵ روز در هفته تقلیل پیدا کند).

درکلاسهای ۵ و ۶ ریاضیات در یك کتاب حساب و حساب جبری و مقدمات هندسه‌آموزش داده می‌شود. درکلاسهای ۷، ۸ و ۹ دو درس ریاضی دارند.

جبر ۴ ساعت در هفته.
هندسه ۲ ساعت در هفته.

تحصیلات تا پایان کلاس ۹ اجباری است.

در مرحله دوم دبیرستان، یعنی سالهای ۱۰ و ۱۱ بچه‌ها وارد مدارس خاص می‌شوند که رشته‌های مختلف دارند:

۱ـ رشته ریاضی و فیزیك.
۲ـ رشته فنی.
۳ـ رشته شیمی و بیولوژی.
۴ـ رشته علوم انسانی.
۵ـ رشته حرفه‌ای.

در رشته ریاضی وفیزیك در هفته ۸ تا ۹ ساعت ریاضی و ۶ ساعت فیزیك می‌خوانند حجم و ساعات دروس دیگر مثل شیمی، بیولوژی، ادبیات، زبان، ... کمتر است. دانش‌آموزان ۶ روز در هفته به مدرسه می‌روند و روزی ۶ ساعت (۳۶ ساعت در هفته) درس می‌خوانند (قبلاً در کلاسهای ۱۰ و ۱۱ نیز تقسیم‌بندی نبوده و همهٔ بچه‌ها دروس کلی و عمومی می‌خوانده‌اند. اخیراً برنامه وکتابهای آنها عوض شده است.

رشته ریاضی وفیزیك

درسها درسالهای ۱۰ و ۱۱ عبارتنداز: آنالیز ریاضی ۴ ساعت، جبر ۲ ساعت، و هندسه ۲ ساعت در هفته.

آمار و احتمال قبلاً جز برنامه نبوده است ولی قرار است که جز برنامه گذاشته شود در این رشته اصولاً ریاضیات سنتی آموزش داده می‌شود و هندسه همان هندسه اقلیدسی است. مختصری از منطق و مجموعه‌ها در حد نیاز در درس جبر آموزش داده می‌شود (گفته شد که در شوروی در دهه ۸۰ـ ۷۰ ریاضی جدید وارد مدارس شد ولی مخالفینی داشت. لذا در دهۀ ۹۰ـ ۸۰ ریاضی جدید را حذف یا خیلی مختصر کردند). در مورد آموزش کامپیوتر، گفته شد که دانش‌آموزان هفته‌ای ۳ ساعت برنامه‌کارگاه دارند که افرادی که علاقمند باشند درکارگاههای مجهز به‌کامپیوتر با اصول برنامه‌ریزی آشنا می‌شوند بعضی مدارس هم خود تشکیلات کامپیوتری دارند. اگر عده دانش‌آموزان ورود به رشته ریاضی زیاد باشد با مصاحبه انتخاب بعمل می‌آید. ورود دانش‌آموزان به دانشکده‌های مخصوص ریاضی و فیزیك که آکادمیست‌های شوروی را تربیت می‌کند بسیار مشکل و شانس ورود به‌آنها برای این دانش‌آموزان $\frac{1}{8}$ است در صورتی که شانس ورود همین دانش‌آموزان به انستیتوهای فنی و تکنولژی که مهندس تربیت می‌کند $\frac{1}{2}$ است. کسانی که بعداز دبیرستان در

رشته مورد علاقه خود در تحصیلات عالی پذیرفته نشوند به دنبال کار می‌روند و هر سال‌کار برای‌آنها امتیازی برای ورود به دانشگاه خواهد بود. انستیوهای عالی شبانه هم وجود داردکه دانشجو روزکار می‌کند و شب درس می‌خواند. در حال حاضر، استفاده ازکامپیوتر، به طور گسترده، به عنوان یك وسیله کمك آموزشی تحت بررسی و مطالعه است. در عین‌حال بعضی‌از مدارس از کامپیوتر به‌عنوان یك وسیله کمك آموزشی بهره می گیرند.

در پاسخ در مورد ریاضی کاربردی و تأکیدی که اکنون در کشورهای غربی روی آن دارند گفته شد که سعی می‌شود کاربرد هر مطلب ریاضی بلافاصله در دنبال‌آن مطلب در همان کتاب آورده شود. به عبارت دیگر بعداز آموزش هر مبحث ریاضی کوشش بر این است که کاربردآن مبحث نیز عنوان گردد.

مثلثات درس مستقلی نیست و مطالب مورد نیاز درکتاب جبر آورده می‌شود. آموزش هندسه ازکلاس ۷ شروع می‌شود وتا آخرکلاس ۱۱ ادامه دارد وفقط هندسه اقلیدسی آموزش داده می‌شو.

دانش‌آموزانی که در رشته ریاضی تحصیل می‌کنند معمولاً به ریاضی علاقمندند و درآموزش به‌آنها مشکلی وجود ندارد .

از نظر دبیر ریاضی واجد شرایط نیز کمبودی وجود ندارد بلکه برعکس برای هر ۲ پست دبیری ۳ نفر متقاضی وجود دارد.

معلمین ریاضی دبیرستانها اکثراً مرد هستندکه بیشتر مورد قبول جامعه است برخلاف ابتدایی و مرحلهٔ اول دبیرستان که معلمین‌اکثراً زن هستند (در دبستان همه زن هستند). وزارت آموزش و پرورش شوروی توجه خاص به تربیت معلم ریاضی دارد و اعتقاد بر این است که معلم خوب است که جهت تحصیلی و مسیر زندگی دانش‌آموز را تعیین می‌کند.

رشته فنی:

درشوروی بعد از رشته‌ریاضی فیزیك، رشته فنی مورد توجه خانواده‌هاو دانش‌آموزان است در این رشته به دانش‌آموزان اطلاعات فنی برای‌آمادگی ورود به انستیتوهای فنی‌و تکنولوژی،که مهندس تربیت می کند، می‌دهد دورهٔ این‌انستیتوه‌ها ۵ سال است.

رشته شیمی و بیولوژی:

در این‌رشته تأکید روی همین دو درس است علاوه براین دانش‌آموزان هفته‌ای ۴ساعت ریاضی و۳ ساعت فیزیك وبعضی دروس دیگرنیزمی‌خوانند فارغ‌التحصیلان این‌رشته‌ها درقسمتهای پزشکی ورشته‌های وابسته ادامه تحصیل می‌دهند.

رشته علوم انسانی:

دانش‌آموزان این رشته برای ادامه تحصیل دررشته‌های، فلسفه، منطق، ادبیات، موسیقی، تاریخ ونظایر آن‌آماده می‌شوند.

رشته حرفه‌ای:

در این رشته کارگران با یك تخصص خاص برای ورود به بازار کار تربیت می‌شوند جنبه‌های تئوری و علمی این‌رشته ضعیف و جنبه عملی‌آن بیشتر است کسانی که گواهی رشته حرفه‌ای می گیرند زودتر جذب بازار کار می‌شوند.

امتحانات:

در پایان‌کلاس نهم، دانش‌آموزان یك امتحان نهائی از تمام دروس خوانده شده دارند و همچنین در پایان‌کلاس ۱۱ یك امتحان نهائی دیگر دارندکه در هر دو امتحان‌گواهی مخصوص به دانش‌آموزان داده می‌شود. روی نحوهٔ برگزاری امتحانات درشوروی بحث و گفتگو است و ممکن است نحوهٔ امتحانات درآینده عوض شود.

دبیرستانهای ویژه:

ازقدیم‌الایام، در شوروی برای تربیت دانش‌آموزان تیز هوش دبیرستانهای خاص وجود داشته است. بعضی ازآنها قدیمی و دارای تاریخ مخصوص خود می‌باشند. تعداد این مدارس درمسکو تاچند سال پیش۷ تا بوده است ولی‌اکنون بیشتر شده است. این نوع دبیرستانهادرشهرهای بزرگ شوروی و بیشتر در قسمتهای اروپائی وجود دارند. درمسکو دبیرستان شماره ۴۳، به علت وجود یك دبیر بسیار عالی‌درآنجا، شهرت خاص دارد. دانش‌آموزان ازکلاس هفتم باکنکور وارد این دبیرستانها می‌شوند درهر دبیرستان ۲۰۰ نفر دانش‌آموز تحصیل می کنند وکلاسها کم جمعیت می‌باشد. در این دبیرستانها ریاضیات سنگین و غیرکلاسیك (نسبت به برنامهٔ دبیرستانی) آموزش داده می‌شود دبیران و اساتید با دانش‌آموزان زیاد کار میکنند. ریاضی‌جدید، جبرخطی، نظریه‌اعداد برنامه‌ریزی خطی، و هندسه‌های نا اقلیدس علاوه‌بر ریاضیات سنتی‌آموزش داده می‌شود.

آنچه تحت عنوان ریاضیات دبیرستان به‌انگلیسی ترجمه می‌شود ریاضیات مربوط به همین دبیرستانهاست. دانش‌آموزان این دبیرستانها وارد تحصیلات نظری و آکادمی دانشگاهها می‌شوند. محققین شوروی عموماً از همین دبیرستانها فارغ‌التحصیل شده‌اند. والدین روشنفکر

بسیار علاقمندندکه بچه‌هایشان در این مدارس قبول شوند.

برنامه ریزی و تألیف:

برنامه ریزی و تألیف کتب درسی دانش‌آموزان شوروی در انستیتوی تحقیقاتی وزارت آموزش و پرورش انجام می گردد برنامه ریزان و مؤلفین در ضمن کار خود به طورمداوم با معلمین ودانش‌آموزان در تماس هستند. در برنامه ریزی همیشه این سئوال‌ها مطرح است که آیا مطالب تنظیم شده برای دانش‌آموزان قابل فهم است؟ آیا مطالب مفیداست؟ آیا معلمین قادرهستند این برنامه را پیاده کنند؟ آیا در این برنامه ریزی نارسائیهای گذشته رفع شده است؟ درنتیجه برنامه ریز ومؤلف ناگزیر است در طول پیشرفت برنامه ریزی و تألیف قدم به قدم با دانش‌آموزان و معلمین در تماس وتبادل نظر باشد. برنامهٔ ریاضی دبیرستانهای معمولی در حد قوه دانش‌آموزان متوسط تنظیم می‌شود وتأکید بر تمرین و تکلیف شب دارد. مطالب ریاضی این مدارس مطالبی سنتی، کلیدی، مفهومی وغیرمعمائی می‌باشد. آنها معتقدند که قوه درک اکثریت دانش‌آموزان متوسطه برای مفاهیم مجرد ریاضی ضعیف است لذا سعی می‌شودکه مطالب در سطح دبیرستانهای عمومی بیشتر جنبهٔ تکنیکی و محاسباتی و عملی داشته باشد.

یک کتاب جدید التألیف جبر و یك کتاب هندسه برای سال ۷ چاپ ۱۹۸۹ وسیلهٔ مؤلفین به عنوان نمونهٔ ارائه مطالب ریاضی در دبیرستان در اختیار ما قرار گرفت.

المپیاد ریاضی در شوروی:

روز پنجشنبه ۶ مهرماه ۶۸ با آقای شاریگین که‌از کارگردانان مسابقات ریاضی شوروی است و خود در دبیرستانهای ویژه تدریس می کند ملاقاتی صورت گرفت ایشان برای دانش‌آموزانی که برای المپیاد ریاضی آماده می‌شوند مسائل هندسه طرح و تهیه می کنداو طراح یکی از سوالات هندسه المپیادکوبا بوده است ایشان توضیح دادندکه در شوروی چند نوع مسابقه المپیاد برگزار می کنیم.

۱ـ در سطح شهر.

۲ـ در سطح جمهوری.

۳ـ در سطح کشور.

در بهار هر سال، مسابقات کشوری انجام می گردد سئوالات همراه با نماینده از مسکو به جمهوریها اعزام می گردد. پس از برگزاری امتحان، اوراق در مسکو تصحیح می‌شود در این مسابقات ۲۰ نفر از دانش‌آموزان ممتاز ریاضی کشور انتخاب می‌شوند. در طول یکسال مسائل و تکلیف خانه برای آنها فرستاده می‌شود و در زمستان امتحان دیگری در محل مرکز جمهوریها از آنها به‌عمل می آیدواز بین آنها ۸نفرانتخاب می‌شوند در فاصلهٔ زمستان تا خرداد ماه مجدداً برای این عده مسائل و تکلیف خانه فرستاده می‌شودکه باید حل کنند و در خرداد ماه یك کلاس یك ماهه برای آنها دائر می گرددکه در طول دوره یکروز درس و یکروز امتحان دارند بنابراین دراین مدت ۱۰تا۱۴ بار ازاین دانش‌آموزان امتحان به عمل می‌آید (در هر جلسه، یك درس امتحان می گیرند). ۶ نفری که مجموع نمرات امتحانشان بیشتر است برای المپیاد بین‌المللی همان سال انتخاب می‌شوند. باید توضیح دادکه دانش‌آموزان المپیاد ازمیان دانش‌آموزان دبیرستانهای ویژه انتخاب می‌شوند.

ایشان توضیح دادندکه مسابقات داخلی ما هم تقریباً جنبهٔ بین‌المللی پیدا کرده و دانش‌آموزان کشورهای دنیا به طور غیر حضوری در این مسابقات شرکت می کنند. سئوالات این مسابقات در مجلهٔ «کوانت» چاپ می‌شود.

ایشان اضافه کردندکه عده‌ای از ریاضیدانان شوروی با مسابقات المپیاد ریاضی با سبك فعلی موافق نیستند زیرا معتقدند:

الف ـ مسائل المپیاد ریاضی محدود بوده ودر نتیجه فکر دانش‌آموزان به این مسائل محدود می‌شود و تصور می‌کنندکه همه ریاضی همین است در نتیجه این خطر وجود داردکه روند موجود به ظهور نوابغ ریاضی لطمه بزند.

ب ـ برای دانش‌آموزان متوسط و خوب هم مسائل مشکل و ناامیدکننده است این دانش‌آموزان اگر با این مسائل مواجه نمی‌شدند ممکن بود روزی یك محقق ریاضی شوند ولی با برخورد با این مسائل ممکن است ریاضی به ذائقه آنها خوش نیاید و تغییر مسیر بدهندکه این خود یك ناکامی برای ریاضی است.

در حال حاضر یك پیشنهاد این است که مسابقه دهندگان المپیاد ریاضی به دو دسته تقسیم شوند به یك دسته مسائل مشکلتر و متنوع‌تر از آنچه‌آلان در المپیاد بین‌المللی مطرح است داده شود و به دسته دیگر مسائل‌آسانتر از مسائل فعلی با این برنامه شاید خطرات احتمالی ذکرشده تقلیل پیدا نماید.

آقای شاریگین یك کتاب مسائل هندسه فضایی که خودشان تألیف کرده بودند و به زبان انگلیسی ترجمه شده بود به دانش‌آموزان المپیاد ایران هدیه کردند وآدرس خود را در اختیار ما قرار دادند که برای کسب اطلاعات بیشتر و احیاناً تهیه منابع وکتب مفید با ایشان مکاتبه بعمل آید.

●

دایره‌های محاطی درونی[۱]

ترجمهٔ: محمود نصیری

مطالعه اجـزاء «مهم» مثلث نظیر میانـه، ارتفـاع و نیمساز زوایا توجه افـراد بسیاری با سلیقه‌هـا و موقعیت‌هـای فکری متفاوت را به خود جلب کـرده است کـه نتایج بسیاری را به همراه داشته است.

تعداد قابل توجهی از این نتایج مربوط بـه نامساوی‌ها در مثلث است که در بین آنها مجموعه‌های [۱] و مطالعات اصولی [۳] می‌باشد.

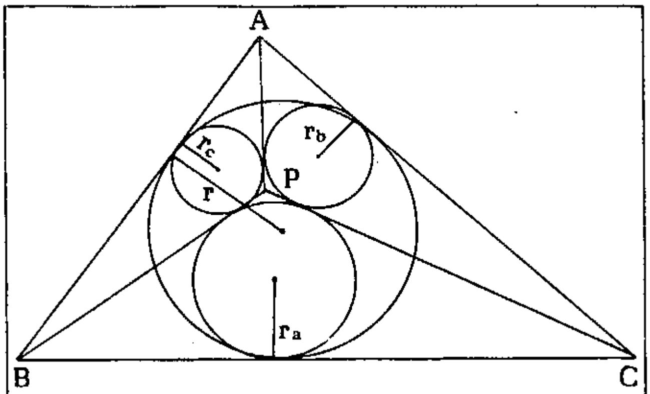
به نظر می‌رسد که همه این‌ها فقط در ارتباط با مثلث هستند. در این مقالـه مثلثی مـانند ABC را درنظر گـرفته و برخی نامساوی‌هـا و نتایج مربوط بـه‌آنها را در مورد دایره‌هـای محاطی داخلی مثلثهای جزئی مثلث ABC معرفی می‌کنیم.

شاید خواننده راه جدیدی برای این برهانها پیدا کند.

مثلث ABC و نقطه P را در داخل یـا روی‌آن درنظر مـی‌گیریم و فرض مـی‌کنیم r_a، r_b و r_c بترتیب شعاعهای دایره‌هـای محاطی داخلی مثلثهای PBC، PCA و PAB بـاشند. اگـر a، b، c و r اضلاع و شعاع دایره محاطی داخلی مثلث ABC باشند می‌خواهیم رابطه‌ای بین $r_a+r_b+r_c$ و a، b، c و r به دست آوریم.

قضیه ۱. با توجه به تعریفات فوق،

$$(۱)\quad r \leqslant r_a+r_b+r_c < \min(a,\ b,\ c)$$



(شکل ۱)

قبل‌از اثبات قضیه ۱ لم زیرا ثابت می‌کنیم.

لم. فرض‌کنیم P_a نقطه‌ای روی ضلع BC ازمثلث ABC باشد. و r، $r_{۲}$ و $r_{۳}$ به ترتیب شعاعهای دایره‌هـای محاطی داخلی مثلثهای ABC، P_aCA و P_aBA باشند.

اگـر h_a ارتفاع نظیر ضلع a از مثلث ABC بـاشد، آنگاه

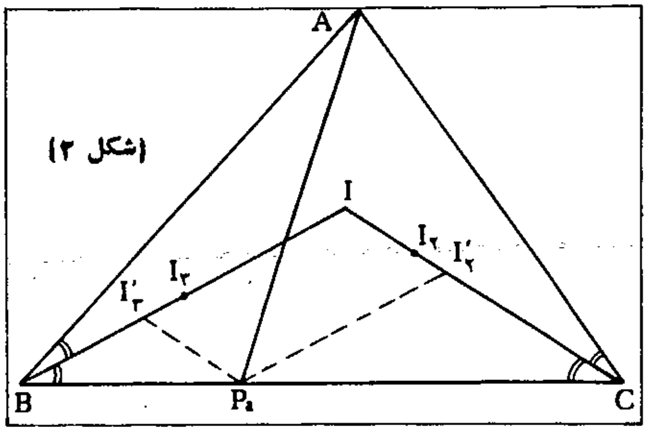
$$(۲)\quad r \leqslant r_{۲}+r_{۳} < h_a$$

و تساوی در سمت چپ وقتی برقرار است‌کـه P_a منطبق بر B یا C باشد.

---

[۱] Incircles Within

اثبات. فرض مـی‌کنیم I، $I_۲$، $I_۳$ بـه ترتیب مرکزهـای دایره‌های محاطی داخلی مثلثهای ABC، P_aCA و P_aBA باشند (شکل ۲) فرض می‌کنیم خطهائی‌که از P_a به موازات BI و CI رسم مـی‌شوند بترتیب پاره خطهای CI و BI را در نقاط $I'_۲$ و $I'_۳$ قطع‌کنند.


(شکل ۲)

چـون $P_aI_۳$ نیمساز خـارجـی زاویـه AP_aB از مثلث P_aCA و $P_aI'_۳$ مـوازی IC است، نقطه $I'_۳$ بین B و $I_۳$ قرار دارد، و به همین ترتیب، $I'_۲$ نیز بین C و $I_۲$ قرار دارد.

اگر فاصله‌های نقاط I و $I_۲$ و $I_۳$ و $I'_۲$ و $I'_۳$ را از BC بترتیب بـــه r و $r_۲$ و $r_۳$ و $r'_۲$ و $r'_۳$ نشان دهیم. در متوازی‌الاضلاع $P_aI'_۲II'_۳$ داریم.

$$r=r'_۲+r'_۳ \leqslant r_۲+r_۳$$

(هر خط که از یك رأس متوازی‌اضلاع و در خارج‌آن‌رسم شود فاصله رأس مقابل‌آن از این خط برابر است با مجموع فواصل دو رأس دیگر از این خط. مترجم).

بنابراین سمت چپ رابطه (۲) ثابت شد.

برای اثبات طرف دیگر، از این واقعیت استفاده مـی‌کنیم کـه در یك مثلث دلخواه، قطر دایره محاطی داخلی از هـر ارتفاع مثلث‌کوچکتر است.

$$(S=rp \implies a_ih_i=۲rp>۲ra_i$$
$$\implies h_i>۲r$$

p نصف محیط مثلث و a_i و $h_i(i=۱,۲,۳)$ ضلع و ارتفاع نظیرآن می‌باشند. مترجم.)

در نتیجه،

$$r_۲+r_۳=\frac{۱}{۲}(۲r_۲+۲r_۳)$$
$$<\frac{۱}{۲}(h_a+h_a)=h_a$$

که سمت راست نامساوی (۲) را ثابت می‌کند.

اکنون ما می‌توانیم قضیه ۱ را ثابت‌کنیم.

اگر P نقطه‌ای داخل مثلث ABC باشد، AP را امتداد می‌دهیم تا ضلع BC را در P_a قطع‌کند.

در غیر این‌صورت فرض می‌کنیم P روی BC قرار دارد و $P=P_a$ و اثبات مانندآن است‌که بیان شد.

فـرض‌کنیم $J_۲$ و $J_۳$ مرکزهـای دایره‌های محاطی داخلی مثلثهای PAC و PAB بـاشد (شکـل ۳). همچین فـرض می‌کنیم خطهائی‌کـــه از P به موازات $P_aI_۲$ و $P_aI_۳$ رسم مـی‌شوند خطهای $AI_۲$ و $AI_۳$ را در نقاط $J'_۲$ و $J'_۳$ قطع کنند،

مانند بحثی‌که در اثبات لم بیان شد، $J'_۲$ بین A، $J_۲$ و $J'_۳$ بین A، $J_۳$ قرار دارند.

فاصله‌های $I_۲$ و $I_۳$ را از AP_a به $r_۲$ و $r_۳$ و فاصله‌های $J'_۲$ و $J'_۳$ را از AP_a به $r'_۲$ و $r'_۳$ نشان می‌دهیم و

$$PP_a=y \quad و \quad PA=x$$

فرض می‌کنیم، داریم:

$$\frac{r'_۲}{r_۲}=\frac{AJ'_۲}{AI_۲}=\frac{AP}{AP_a}=\frac{x}{x+y}=\frac{r'_۳}{r_۳}$$

که ازآن به دست می‌آید:

$$r'_۲+r'_۳=\frac{x}{x+y}(r_۲+r_۳)$$

چون r_b و r_c فاصله‌های $J_۲$، $J_۳$ از PA می‌باشند داریم:

$$r_b \geqslant r'_۲ \quad و \quad r_c \geqslant r'_۳$$

بنابراین.

$$r_b+r_c \geqslant r'_۲+r'_۳=\frac{x}{x+y}(r_۲+r_۳)$$

و با توجه به لم فوق‌که $r_۲+r_۳ \geqslant r$، داریم:

$$(۳)\quad r_b+r_c \geqslant \frac{x}{x+y} r$$

اکنون مساحت و نصف محیط مثلثهـای ABC و PBC را بترتیب بـه S، S_a و l، l_a نشان می‌دهیم آنگاه $S=rl$ و $S_a=r_a l'$. بنابراین،

$$r_a=\frac{S_a}{l'}=\frac{S_a}{S}\cdot\frac{S}{l'}=\frac{S_a}{S}\cdot\frac{l}{l'}\, r$$

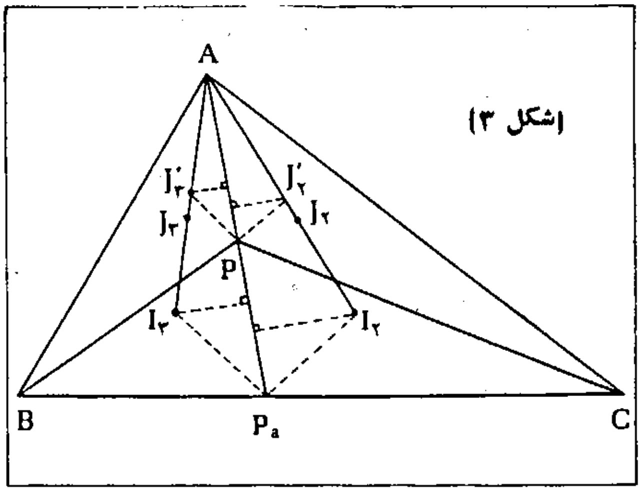
$$=\frac{y}{x+y}\cdot\frac{a+b+c}{a+PB+PC}\, r$$

$$\geqslant\frac{y}{x+y}\cdot ۱\cdot r=\frac{y}{x+y}\, r$$

لذا $r_a \geqslant \frac{y}{x+y} r$ و با توجه به رابطه (۳)

$$r_a+r_b+r_c \geqslant \frac{y}{x+y} r+\frac{x}{x+y} r=r$$

حالا بـرای اثبات طـرف راست نـامساوی (۱)، شعاعهـای دایره‌هـای محاطی داخلـی مثلثهای PP_aC و PP_aB را بـه $t_{۲}$ و $t_{۳}$ نشان می‌دهیم و فرض می‌کنیم $h'_{۲}$ و $h'_{۳}$ ارتفاعهای رأسهای C و B مثلثهای PP_aC و PP_aB باشند. با به کار بردن لمی کـــــه ثابت شد در هر یك از مثلثهای PBC و ABP_a و ACP_a سه نامساوی زیر را داریم.



(شکل ۳)

$$r_a \leqslant t_{۲}+t_{۳}$$

$$t_{۲}+r_b < h'_{۲}$$

$$t_{۳}+r_c < h'_{۳}$$

از جمع نامساوی‌های فوق داریم.

$$r_a+r_b+r_c < h'_{۳}+h'_{۲} \leqslant a.$$

چـون سمت چپ این نـامساوی نسبت به a و b و c متقارن است لذا.

$$r_a+r_b+r_c < \min(a,\ b,\ c)$$

به دست آید که این اثبات قضیه ۱ را کامل می‌کند.

جالب است کـه می‌توانیم نامساوی‌های مشابه دیگری کـه نسبت به r_a و r_b و r_c متقارن هستند به دست بیاوریم.

باید توجه کنیم که تساوی طرف چپ رابطه(۱) وقتی برقرار است که P منطبق بریکی از رأسهای مثلث ABC شود.

بـا ضرب مقداری ثابت در $\min(a, b, c)$ نمی‌تـوان طرف راست نامساوی (۱) را طوری اصلاح کرد کـه تساوی برقرار شود. (هر مثلث باریکی درنظر بگیریم شامل مثلثهای جزء باریکتری است).

اگـر چه لمی کـه ثابت شد یك نامساوی بین شعاع دایـرۀ محاطی داخلی مثلث و شعاعهای دایره‌هـای محاطی دو مثلث دیگری که داخل ABC هستند وارتفاع مثلث برقرار می‌کند. نتیجه زیـر این کمیتها را در یك معادلـه قرار می‌دهد. بعلاوه چند ساختمان زیبای هندسی را نیز ممکن می‌سازد.

قضیه ۲. فرض مـــی‌کنیم P نقطه‌ای روی ضلع BC از مثلث ABC بـاشد. و r، $r_{۲}$ و $r_{۳}$ بـــه ترتیب شعاعهای دایره‌هـای محاطی داخلی مثلثهای ABC، ACP و ABP باشند. آنگاه

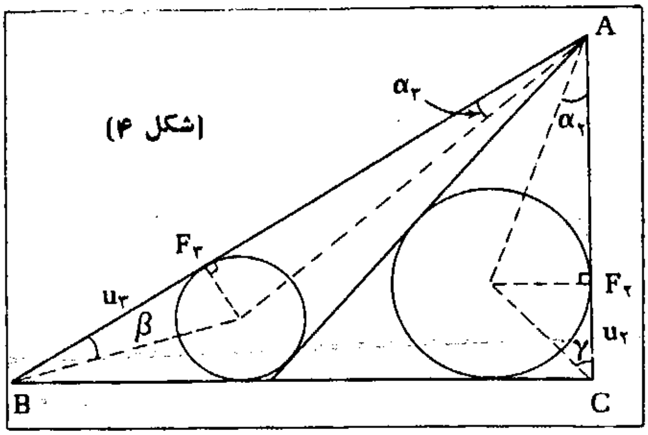
$$\frac{۱}{r_{۲}}+\frac{۱}{r_{۳}}-\frac{r}{r_{۲}r_{۳}}=\frac{۲}{h_a}$$

که h_a ارتفاع رأس A از مثلث ABC است.

اثبات. فرض کنیم a، b، c اضلاع و ۲α، ۲β، ۲γ زوایا، p نصف محیط، R شعاع دایـره محیطـی و S مساحت مثلث ABC بـاشند (شکل ۴) همچنین فرض مـی کنیم دایره‌هـای محاطـی داخلـی مثلثهـای ACP و ABP بترتیب در نقاط $F_{۲}$ و $F_{۳}$ بر اضلاع AC و AB مماس باشند و

$$BF_۳=u_۳ \quad \text{و} \quad CF_۲=u_۲$$

انتخاب می‌کنیم. اگر زوایای CAP و BAP، $۲\alpha_۲$ و $۲\alpha_۳$ باشند، داریم،


(شکل ۴)

$$\mathrm{cotg}\,\alpha=\mathrm{cotg}(\alpha_۲+\alpha_۳)=\frac{\mathrm{cotg}\,\alpha_۲\,\mathrm{cotg}\,\alpha_۳-۱}{\mathrm{cotg}\,\alpha_۲+\mathrm{cotg}\,\alpha_۳}$$

که معادل است با،

$$\mathrm{cotg}\,\alpha(\mathrm{cotg}\,\alpha_۲+\mathrm{cotg}\,\alpha_۳)=\mathrm{cotg}\,\alpha_۲\,\mathrm{cotg}\,\alpha_۳-۱ \tag{۵}$$

چون

$$\mathrm{cotg}\,\alpha_۲=\frac{b-u_۲}{r_۲}=\frac{b}{r_۲}-\mathrm{cotg}\,\gamma.$$

$$\mathrm{cotg}\,\alpha_۳=\frac{c-u_۳}{r_۳}=\frac{c}{r_۳}-\mathrm{cotg}\,\beta.$$

با جای‌گذاری در رابطه (۵) داریم،

$$\mathrm{cotg}\,\alpha\left(\frac{b}{r_۲}+\frac{c}{r_۳}-\mathrm{cotg}\,\gamma-\mathrm{cotg}\,\beta\right)=\left(\frac{b}{r_۲}-\mathrm{cotg}\,\gamma\right)\left(\frac{c}{r_۳}-\mathrm{cotg}\,\beta\right)-۱$$

که پس‌از ضرب و دسته‌بندی به دست می‌آید،

$$\frac{b}{r_۲}(\mathrm{cotg}\,\alpha+\mathrm{cotg}\,\beta)+\frac{c}{r_۳}(\mathrm{cotg}\,\alpha+\mathrm{cotg}\,\gamma)-\frac{bc}{r_۲r_۳}=\mathrm{cotg}\,\alpha\,\mathrm{cotg}\,\beta+\mathrm{cotg}\,\alpha\,\mathrm{cotg}\,\gamma+\mathrm{cotg}\,\gamma\,\mathrm{cotg}\,\beta-۱. \tag{۶}$$

اکنون هر یك از دو طرف رابطه (۶) را ساده می‌کنیم در مورد طرف چپ می‌دانیم در هر مثلث

$$r\,\mathrm{cotg}\,\alpha+r\,\mathrm{cotg}\,\beta=c.$$

و

$$r\,\mathrm{cotg}\,\alpha+r\,\mathrm{cotg}\,\gamma=b$$

یا،

$$\begin{cases}\mathrm{cotg}\,\alpha+\mathrm{cotg}\,\gamma=\dfrac{b}{r}\\[2ex]\mathrm{cotg}\,\alpha+\mathrm{cotg}\,\beta=\dfrac{c}{r}\end{cases} \tag{۷}$$

برای طرف راست، با به کار بردن علامت مجموع دوری می‌توان آنرا به‌صورت $\Sigma\mathrm{cotg}\,\beta\,\mathrm{cotg}\,\gamma-۱$ نوشت. بنابراین.

$$\Sigma\mathrm{cotg}\,\beta\,\mathrm{cotg}\,\gamma=\Sigma\frac{(p-b)(p-c)}{r\cdot r} \tag{۸}$$

$$=\frac{۱}{r^۲}\Sigma[p^۲-(b+c)p+bc]$$

$$=\frac{۱}{r^۲}[-p^۲+\Sigma bc].$$

حال اگر دو طرف رابطه هرون را به توان دو برسانیم

$$pr=\sqrt{p(p-a)(p-b)(p-c)}$$

یا

$$pr^۲=(p-a)(p-b)(p-c)$$
$$=p^۳-۲p\cdot p^۲+p\Sigma bc-abc$$

و برای محاسبه Σbc:

$$\Sigma bc=p^۲+r^۲+\frac{abc}{p}=p^۲+r^۲ \tag{۹}$$
$$+\frac{۲S\cdot ۲R}{p}=p^۲+r^۲+۴rR.$$

با جای‌گذاری رابطه (۹) در رابطه (۸) داریم.

$$\Sigma\mathrm{cotg}\,\beta\,\mathrm{cotg}\,\gamma=۱+\frac{۴R}{r}. \tag{۱۰}$$

با جای‌گذاری رابطه‌های (۷) و (۱۰) در رابطه (۶)، به‌دست می‌آید.

$$(۱۱)\quad \frac{bc}{r_۲ r}+\frac{bc}{r_۳ r}-\frac{bc}{r_۲ r_۳}=\frac{۴R}{r}$$

با تقسیم طرفین رابطه (۱۱) بر $\frac{bc}{r}$ و به کاربردن نسبتهائی در مثلث سرانجام چنین داریم.

$$\frac{۱}{r_۲}+\frac{۱}{r_۳}-\frac{r}{r_۲ r_۳}=\frac{۴R}{bc}=\frac{۴aR}{abc}$$

$$=\frac{۴aR}{۴SR}$$

$$=\frac{a}{S}=\frac{۲}{h_a}$$

(ذیلاً اثبات دیگری به غیر از این اثبات برای قضیه فوق ارائه می‌دهیم.

برای طرف راست با توجه به قانون تانژانتها در مثلث،

$$cotg\,\frac{A}{۲}=cotg\alpha=\sqrt{\frac{p(p-a)}{(p-b)(p-c)}}$$

داریم.

$$cotg\alpha cotg\beta+cotg\alpha cotg\gamma+cotg\gamma cotg\beta-۱=\frac{p}{p-c}+\frac{p}{p-b}+\frac{p}{p-a}-۱=$$

$$=\frac{p(p-a)(p-b)+p(p-a)(p-c)+p(p-b)(p-c)-(p-a)(p-b)(p-c)}{(p-a)(p-b)(p-c)}$$

$$=\frac{p(p-a)(۲p-b-c)+(p-b)(p-c)(p-p+a)}{(p-a)(p-b)(p-c)}$$

$$=\frac{a(p^۲-pa+p^۲-pb-pc+bc)}{\frac{S^۲}{p}}=\frac{pabc}{S^۲}=\frac{۲pabc}{S\cdot ah_a}=\frac{۲bc}{rh_a}$$

بنابراین رابطه (۶) به صورت زیر نوشته می‌شود.

$$\frac{bc}{r_۲ r}+\frac{bc}{r_۳ r}-\frac{bc}{r_۲ r_۳}=\frac{۲bc}{rh_a}.$$

که با تقسیم دو طرف این رابطه بر bc و سپس ضرب‌آن در r داریم

$$\frac{۱}{r_۲}+\frac{۱}{r_۳}-\frac{r}{r_۲ r_۳}=\frac{۲}{h_a}$$

که اثبات قضیه تمام است، مترجم).

اکنون کاربردی از رابطه (۴) را درحل مسأله زیر می‌بینیم.

مسأله. تنها با به کار بردن خط‌کش و پرگار خط AP را در مثلث ABC چنان رسم کنید که دایره‌های محاطی داخلی دو مثلث ABP و ACP مساوی شوند:

حل. اگر در رابطه (۴)، $r_۲=r_۳$ قرار دهیم، داریم

$$\frac{۲}{r_۲}-\frac{r}{r_۲^۲}=\frac{۲}{h_a}\implies ۲r_۲^۲-۲h_a r_۲+rh_a=۰$$

که از حل این معادله برحسب $r_۲$ به دست می‌آید،

$$r_۲=\frac{۱}{۲}\left(h_a-\sqrt{h_a(h_a-۲r)}\right)$$

طریقه رسم به صورت زیر است. (شکل ۵)

۱) دایرهٔ Γ را به قطر ارتفاع AD رسم می‌کنیم.

۲) به موازات ضلع BC از مثلث ABC، مماسی بر دایره محاطی داخلی این مثلث رسم می‌کنیم تا دایرهٔ Γ را در نقاط E و F قطع کند.

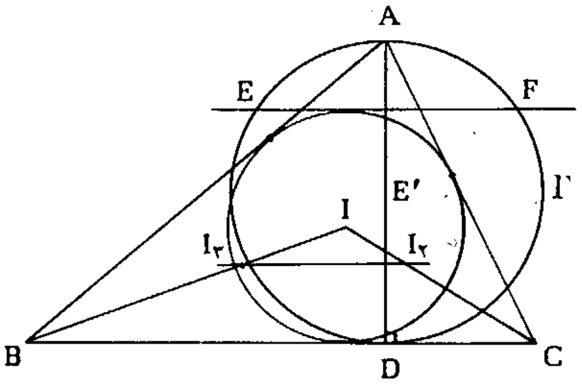
۳) پاره خط AE′ را روی AD و برابر AE رسم

می‌کنیم. در این صورت

$$DE' = ۲r_{۲} = ۲r_{۳}$$

۴) عمود منصف DE'، نیمسازهـای زوایای B و C را در نقاط $I_{۳}$ و $I_{۲}$ قطع می‌کندکـه مرکزهای این دو دایره، به شعاعهای مساوی می‌باشند.

۵) این دو دایره را کـه به شعاع $r_{۲}$ می‌باشند رسم‌کرده، مماس مشترکی‌ازآنها را که از A می‌گذرد رسم می‌کنیم محل تلاقی‌آن با BC نقطه مطلوب P است.



(شکل ۵)

یك نتیجه غیر منتظره رابطه (۴) در قضیه زیر است‌که‌آن‌را قضیه پنج دایره می‌نامیم.

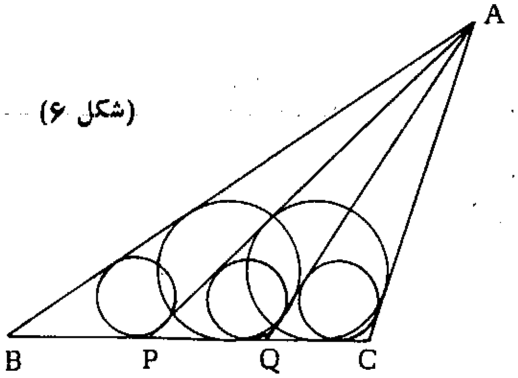
قضیه ۳. فرض‌کنیم P و Q دو نقطه روی ضلع BC از مثلث ABC باشندکـــه بترتیب B، P، Q، C قرار گـرفته باشند. اگردایره‌های محاطی داخلی مثلثهای ABP، APQ، AQC مساوی باشندآنگاه دایره‌هـای محاطی داخلی مثلثهای ABQ و APC نیز مساویند.

اثبات. فرض مـی‌کنیم r شعاع مشترك سه دایـره مساوی باشند. شعاعهای دایره‌هـای محاطی داخلی مثلثهای ABQ و APC را $r_{۲}$ و $r_{۳}$ می‌نامیم(شکل ۶) رابطه (۴) را دراین‌دو مثلث به کار می‌بریم، در نتیجه.

$$\frac{۲}{r}-\frac{r_{۱}}{r^{۲}}=\frac{۲}{h_a} \quad و \quad \frac{۲}{r}-\frac{r_{۲}}{r^{۲}}=\frac{۲}{h_a}$$

و بنابراین $r_{۱} = r_{۲}$

اثبات هندسی از قضیه پنج دایره را بـه عهده خوانندگـان می‌گذاریم.



(شکل ۶)

مرجع

MATHEMATICS MAGAZINE VoL. 59, NO. 2, APRIL 1986.

[1] O. Bottema. et al., Geometric Inequalities. Wolters – Noordhof Publishing. Groningen. 1969.

[2] H. S. M. Coxeter. Introduction to Geometry. 2nd ed.: John Wiley & Sons 1969.

[3] N. D. Kazarinoff. Geometric Inequalities. MAA New Mathematical Library no. 4,1961.

مسائل ویژه دانش‌آموزان

تهیه و تنظیم: محمود نصیری

درخواست مکرر دبیران و دانش‌آموزان، در مورد اینکه مسائلی صرفاً درسطح کلاس درس و امتحانات مدارس در مجله رشد آموزش ریاضی مطرح شود، اخیراً مورد تصویب هیأت تحریریه مجله قرار گرفته است. وازاین شماره درج این مسائل شروع شده است ازعموم همکاران محترم دبیر و دانش‌آموزان عزیز انتظار داردکه مسائل جالب و غیرتکراری وحتی‌المقدور قابل درج در مجله، به نام خودشان به دفترمجله ارسال دارند ضمناً تقاضادارد این مسائل‌را باراه‌حل ارسال دارند. معهذاچون اینگونه مسائل عموماً کلاسیك هستند مجله از درج راه حل آنها خودداری خواهد کرد. قبلاً از همکاری شما تشکر می‌کنیم **مسائل ویژه دانش‌آموزان سال‌های اول و دوم نظری است.**

۱. هرگاه در یك تصاعد حسابی t_n جمله nام و S_n مجموع n جمله اول باشد مجموع‌های زیر را پیدا کنید

الف) $$A=\frac{S_۱}{t_۱+۲S_۱}+\frac{S_۱+S_۲}{۲t_۱+۲S_۲}+\cdots+\frac{S_۱+S_۲+\cdots+S_n}{nt_۱+۲S_n}$$

ب) $$B=\frac{S_p}{t_p+t_۱}+\frac{S_{p+۱}}{t_p+t_۲}+\cdots+\frac{S_{p+n}}{t_p+t_{n+۱}}$$

ج) $$C=\frac{S_۱}{۱}+\frac{S_۲}{۲}+\cdots+\frac{S_{۲n}}{۲n}$$

(فرستنده. محمدآذرتاش دبیر دبیرستانهای تهران)

۲. معادله $۲۶^{\log x}-۲۴^{\log x}=x$ را حل کنید.

(فرستنده. محمد مهدی‌امینی دانش‌آموز از قرچك ورامین)

۳. کسر $\frac{a+a^۲+\cdots+a^n}{a^{-۱}+a^{-۲}+\cdots+a^{-n}}$ را ساده کنید.

(فرستنده. کوروش کریمی از مشهد)

۴. اگر α و β ریشه‌های معادله

$$x^۲-۲x-۷=۰$$

باشند حاصل عبارت

$$A=(\alpha-۲)^{-۳}+(\beta-۲)^{-۳}$$

را پیدا کنید.

۵. زاویه $\widehat{xoy}$ مفروض است قطعه خط MN را متکی بر دو ضلع زاویه طوری رسم کنیدکه $MN=l$ و مساحت مثلث OMN مقدار معلوم S باشد.

۶. چهار دایره در نقاط A، B، C و D دو به دو برهم مماسند ثابت‌کنید چهارضلعی ABCD محاطی است.

۷. از مثلثی اضلاع b و c در دست است و می‌دانیم $\angle B=۳\angle C$ مثلث را رسم کنید.

۸. مجموع زیر را خساب کنید.

$$S_n=\frac{۱}{۲^۰}+\frac{۲}{۲^۱}+\frac{۳}{۲^۲}+\cdots+\frac{n+۱}{۲^n}$$

۹. هرگاه از نقطه O داخل مثلث ABC به سه رأس A، B و C وصل کرده امتداد دهیم تا اضلاع مقابل به این رأسها را به ترتیب در $A_۱$، $B_۱$ و $C_۱$ قطع کند ثابت کنید

$$\frac{OA}{OA_۱}+\frac{OB}{OB_۱}+\frac{OC}{OC_۱}\geqslant ۶$$

(فرستنده مسائل ۸ و ۹: مجید صادقی دیپلمه از اصفهان)

۱۰. مثلث ABC را با معلومات زیر رسم کنید،

$AB+AC=l$ و $BC=a$ و $CH=h_c$

مجموع دو ضلع و ضلع سوم و ارتفاع وارد بر ضلع c.

۱۱. اگر $a\geqslant ۰$، $b\geqslant ۰$ و $c\geqslant ۰$ ثابت کنید

$$\frac{a+b+c}{۳}\leqslant\sqrt{\frac{a^۲+b^۲+c^۲}{۳}}$$

۱۲. تساوی زیر را ثابت کنید.

$$\sqrt[4]{6a(5+2\sqrt{6})}\sqrt{3\sqrt{2a}-2\sqrt{3a}}=\sqrt{6a}$$

۱۳. نامعادله زیر را حل کنید

$$\left|\frac{x^2-3x+2}{x^2+3x+2}\right|>1$$

۱۴. نامعادله زیر را حل کنید

$$\log_{\frac{\sqrt{3}}{2}}(2^{x+2}-4^x)\geqslant -2$$

۱۵. بدون استفاده ازجدول ثابت کنید $\cos 36^\circ > tg 36^\circ$.

مسائل ویژه دانش‌آموزان سالهای سوم وچهارم دبیرستان.

۱۶. در بین مثلثهای بـا قاعده معلوم AB و طـول ارتفاع ثابت CH آن را پیدا کنید که شعاع دایره محیطی آن مینیمم است.

۱۷. ثابت کنید که معادله $x^6+y^6-z^6=1972$ دارای جواب صحیح نمی‌باشد.

۱۸. از نقطه M داخـل مثلث ABC سه عمود برسه ضلع رسم کرده و طولهای آنها را x، y و z می‌نامیم. اگر S مساحت و a، b و c سه ضلع مثلث باشند، ثابت کنید

$$x^2+y^2+z^2\geqslant\frac{4S^2}{a^2+b^2+c^2}$$

۱۹. ثابت کنید در هر مثلث

$$\frac{1}{(p-a)^2}+\frac{1}{(p-b)^2}+\frac{1}{(p-c)^2}\geqslant\frac{1}{r^2}$$

که r شعاع دایره محاطی داخلی و p نصف محیط است.

۲۰. عددی پیدا کنید که برابر با $\frac{1}{3}$ مجموع مکعبات رقم‌هایش باشد.

۲۱. اگر (G, o) یك گروه باشد که به‌ازای هر a و b ∈ G، $(a\,o\,b)^2=a^2\,o\,b^2$ ثابت کنید که G آبلی است.

۲۲. مطلوب است محاسبه حدهـای ذیل (N مجموعه اعداد طبیعی و $n\in N$)

a) $\lim\limits_{n\to\infty}(\sin\pi\sqrt{n^2+1})$

b) $\lim\limits_{n\to\infty}\sin^2(\pi\sqrt{n^2+n})$

c) $\lim\limits_{n\to+\infty}\sqrt[n]{\frac{3^n+5^n+7^n}{3}}$

۲۳. فرض کنیم تابع f به ازای هر x دارای مشتق دوم و

$$f''(x)+f(x)=0 \quad و \quad f(0)=f'(0)=0$$

باشند در این صورت تابع f را پیدا کنید.

۲۴. نمودار تابع $f(x)=x|x|\sqrt{1-x}$ را رسم کنید.

۲۵. اگر عدد $5a+3b$ بر ۷ بخش‌پذیر باشد، ثابت کنید عدد $6a^2+17ab+10b^2$ بر ۴۹ بخش‌پذیر است.

۲۶. به استقراء ثابت کنید:

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

۲۷. ثابت کنید اگر

$$\vec{a}\cdot\vec{b}=\vec{a}\cdot\vec{c} \quad و \quad \vec{a}\wedge\vec{b}=\vec{a}\wedge\vec{c}$$

آنگاه $\vec{b}=\vec{c}$.

۲۸. دو دایره متقاطع به مرکزهای O و O′ و به شعاعهای R و R′ مفروضند قاطعهائی این دو دایره را قطع مـی‌کنند. دایره به مرکز O را در A و B و دایره به مرکز O′ را در C و D به‌طوری که ABCD تقسیم توافقی است مکان هندسی وسطهای وترهای AB و CD را پیدا کنید.

۲۹. نمودار تابع $f(x)=\frac{\sin x}{x}$ را رسم کنید.

۳۰. ثابت کنید

$$(a>0)\quad\int_0^a x^3f(x^2)dx=\frac{1}{2}\int_0^{a^2}xf(x)dx$$

بقیه از صفحهٔ ۱۳

$$(۲)\quad x'+x''=m'+n'=\frac{۲\lambda^۲a^۲d^۲}{\alpha^۲a^۲+d^۲}$$

$$(۳)\quad x'x''=m'n'=\frac{\lambda^۲a^۲d^۲-a^۲b^۲}{\lambda^۲a^۲+b^۲}$$

بین معادله‌های (۱)، (۲) و (۳) $m'+n'$ و $m'n'$ را حذف می‌کنیم نتیجه می‌دهد

$$c'=\frac{a^۲}{d}$$

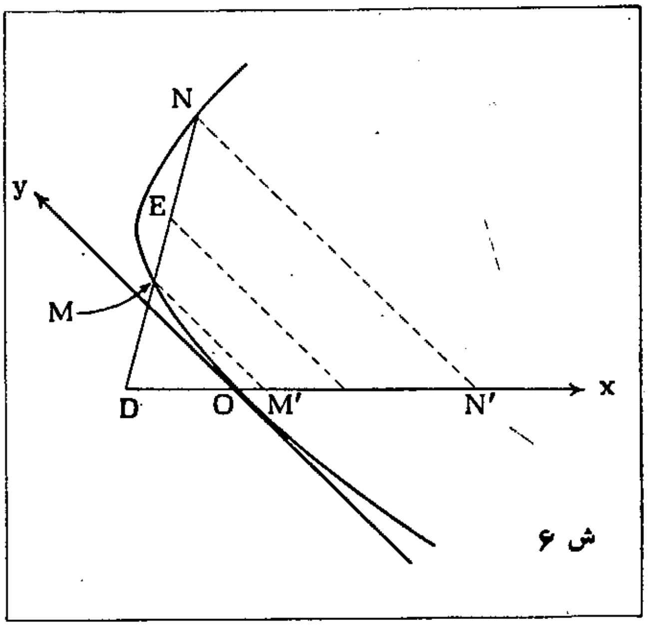
یا

$$OA'^۲=OA^۲=OD\cdot OE'$$

یعنی E' مزدوج توافقی D نسبت بـه A و A' و در نتیجه EE' قطبی نقطه D نسبت به بیضی است.

ج ـ راجع بـه هذلولی با همین حروف عمل کنید به نتیجه می‌رسید.

د ـ معادله سهمی در دستگاه xOy، $y^۲=۲Px$، $OD=d$ و $D(d,۰)$.



ش ۶

E مزدوج توافقی D نسبت بـه M، N و M'، N' و E' تصاویر M، N و E در دستگاه xOy است.

E مزدوج توافقی D نسبت به M و N است و

$$OM'=m' \text{ و } OE'=e' \text{ و } ON'=n'$$

می‌خواهیم معادلهٔ مکان هندسی نقطه E را تعیین کنیم آنگاه کـه خط DM در حول O تغییر امتداد می‌دهد یعنی قطبی نقطهٔ D را نسبت به سهمی تعیین کنیم

$$(DE'M'N')=(DEMN)=-۱$$

$$\frac{DM'}{DN'}:\frac{EM'}{EN'}=-۱\quad\Longrightarrow$$

$$(۱)\quad e'=\frac{۲m'n'-d(m'+n')}{(m'+n')-۲d}$$

$$\left|\begin{array}{l} y^۲=۲Px \\ \dfrac{x-d}{p}=\dfrac{y}{q} \qquad \Longrightarrow \\ \qquad q^۲x^۲-۲(dq^۲+Pp^۲)+d^۲q^۲=۰ \end{array}\right.$$

$$(۲)\quad x'+x''=m'+n'=\frac{۳(dq^۲+Pp^۲)}{q^۲}$$

$$(۳)\quad x'x''=m'n'=d^۲$$

بین تساوی‌های (۱)، (۲) و (۳) $m'+n'$ و $m'n'$ را حذف می‌کنیم

$$e'=-d$$

$$OE'=-OD$$

تبصره ـ محورهـای منطبق بر دو قطر مـزدوج را در سال ۱۳۲۵ از درس هندسه تحلیلی جناب آقـای دکتر وحیدی یاد گرفتیم، که اشاره کرد در این دستگاه معادلهٔ بیضی و هذلولی و سهمی را میتوان بـه شکل ساده‌ای کـه در متوسطه دیده‌اید ثابت کرد.

من بعداً در هیچ کتاب داخلی و خارجی اثری راجع به‌این موضوع پیدا نکردم سالها بعد که در دانشگاه تربیت معلم هندسه تحلیلی درس می‌دادم در کتاب هندسه تحلیلی کـه تألیف کـردم این مطلب را در یـك فصل نـوشتم. اخیراً در تهیه مقالات درسهایی ازهندسه که برای مجله رشد می‌نویسیم به فکرم رسید کـه قطب و قطبی را دربارهٔ مقاطع مخروطی در این دستگـاه پیاده کنم. بعداز یك هفته کار درآن بـه نتیجهٔ جالبی رسیدم و آن این است که قطب و قطبی در این دستگاه عیناً مانند دایره پیاده مـی‌شود این مطلب را از هیچ کتاب و مقاله‌ای استفاده نکرده‌ام.

بقیه از صفحهٔ ۲۳

۵ ـ نتیجه‌گیری و ملاحظات. هر چند قانونمندی‌های متعددی را می‌توان برای کاربرد در طراحی سیستم‌های رمز پیشنهاد نمود و لیکن واقعیت این است که در عمل تعداد معدودی از آنها می‌توانند بکار گرفته شوند. دلیل این امر ضرورت انطباق آنها با تعاریف ارائه شده برای توابع یکطرفی می‌باشد. نکته دیگری که در تعریف و طراحی یک سیستم رمز می‌بایست در نظر گرفته شود تحقیق روشهای شکستن آن سیستم می‌باشد. طراحان سیستم‌های مشهور امروزی وقت بسیاری را در بررسی این روشها مصروف داشته‌اند و محققین دیگری نیز به پیروی از ایشان، و یا دقیقاً به منظور شکستن سیستم‌های طرح شده، در این زمینه‌ها به مطالعه پرداخته‌اند که بعضاً نیز به نتایج ارزنده‌ای نایل شده‌اند.[۷]. به عنوان مثال، بدنبال ارائه سیستم رمز، RSA، خطوط مشخصی در زمینه تحقیقات کاربردی نظریه اعداد پدیدار شد. یافتن الگوریتم موثر برای تجزیه اعداد بزرگ، دست‌یابی به روشهایی برای آزمون اول بودن اعداد و محاسبه لگاریتم گسسته در هیأتهای متناهی عناوین برخی از این خطوط می‌باشند. نتایج فعالیت‌های متعدد در این زمینه‌ها شمار قابل توجه الگوریتم‌هایی می‌باشد که تاکنون ارائه شده‌اند. البته در این میان افرادی نیز بوده‌اند که از محدوده نظریه اعداد فراتر رفته و با استمداد از مباحث شاخه‌های دیگر ریاضیات سعی در حل مسائل فوق الذکر نموده‌اند. سعی و تلاش در این خصوص گذشته از آنکه به ظهور نتایج جدید و الگوریتم‌های کاراتر می‌انجامد، این امید را نیز می‌تواند در پی داشته باشد که سیستم‌های نوینی در آینده رمز نگاری طراحی شوند

مراجع :

1 – W. Oiffe and M. Hellman, "New direction in cryptography" IEEE Trans. Inform. Teory, Vol. IT – 22, PP. 472, 1976

2 – D.M. BURTON, Elementary Number theory theory, Allyn and Bacon, Inc. 1980.

3 – Advanced tecology Seminars, "Cryptography, Fundamentals and applications", 1987.

4 – S. Pohlig and M.Hellman, "An Improved algorithm for computing logarithm over GF (P) and its cryptographic Significance." IEEE Trans. Inform. Theory, Vol. II – 24, PP. 110, 1978.

5 – R. C. Mercle and M.E. Hellman, "Hiding "Hiding information and signature in Trapdoor Knapsacks," IEEE Trans inform. Theory, Vol IR – 24, 24, No. 5. 1978.

6 – R.Rivest, A. Shamir and L. Adleman, "A method for obtaining digital Signatures and public Key Crypto systems, "commun. ACM. Vol. 21, No. 2, PP. 120 – 126, Feb. 1978.

7 – Taher Elgamal, "A Public – Key Crypto System and Signature Scheme based on discrete Logarithms, " IEEE Trans. Inform. Theory, Vol. IT – 31, No. 4, July 1985.

بقیه از صفحهٔ ۳

در نظامهای پیشرفته آموزش نقش معلم و دبیر در اشاعه صحیح هر شاخه از علوم نقشی اساسی و کلیدی است، معهذا وجود وسایل و منابع کمك آموزشی از جمله نشریاتی که بتواند به عنوان تریبونی برای ارائه شیوه درتفکر ریاضی، استراتژیهای حل مساله، تاریخ وفلسفه ریاضی، مسائل برنامه‌ریزی و تالیف و نظایر آن بکار آید از ضروریات هرکار فرهنگی است.

به استناد سخنی از رسول اکرم ﷺ که میفرماید «کل مولود یولد علی الفطره» باید وسائل و امکاناتی فراهم کنیم تا استعدادهایی که به صورت فطری دربچه‌ها و دانش‌آموزان است از قوه به فعل در آمده و فرصت شکوفایی پیدا کند تا همه افراد در مسیر ترقی و تعالی قرار گیرند و هم جامعه از استعدادهای خدادادی خود بهره مندگردد. هرچه این وسایل مهیاتر، متنوعتر، و حساب شده‌تر باشند این شکوفایی بیشتر و درخشندتر خواهد بود. هدفمان نباید صرفاً آموزش باشد، بلکه باید بیشتر به القاء شیوه‌ی درست تفکر،کشف مسائل و مدلهای جدیدریاضی، تقویت قوه خلاقیت در بچه‌ها بپردازیم و به عبارتی بهتر است چگونه یاد گرفتن را یاد بدهیم. این هنر ظریف و بدیعی است تقریباً بیشتر طرحها و ابتکاراتی‌که پیرامون برنامه‌ریزی آموزشی در دهه‌های اخیر به وقوع پیوسته منبعث از آن است. در این راستا، مجله رشد ریاضی هر تجربه‌ای را که صادقانه در جهت اعتلای فکری، برداشتن گامی به جلو، و یا بهبود روش در آموزش و فراگیری ریاضیات ارائه شود ارج می‌نهد و از همهٔ معلمین، دبیران و دانشگاهیان محترم، دانش‌آموزان و دانشجویان عزیز انتظار دارد. تا با ارائه تجربیات آموزشی خود ما را یاری کنند..

سردبیر

چند رابطه مثلثاتی

$$(۱)\quad \sin(A_{۱}+A_{۲}+\cdots+A_{n}) = S_{۱}-S_{۳}+S_{۵}-\cdots$$

$$(۲)\quad \cos(A_{۱}+A_{۲}+\cdots+A_{n}) = S_{۰}-S_{۲}+S_{۴}-\cdots$$

S_r مجموع حاصلضربهای ازسینوسهای r زاویه وکسینوسهای n − r زاویه است. مثلاً،

$$S_{۰}=\cos A_{۱}\cos A_{۲}\cdots\cos A_{n}$$

$$S_{۱}=\sin A_{۱}\sin A_{۲}\cdots\cos A_{n}+\cos A_{۱}\cos A_{۲}\cdots\cos A_{n}+\cdots$$

برهان بـه استقراء است. فرض‌کنید (۱) و (۲) بـه ازاء n برقرار باشد، داریم.

$$\begin{aligned}\sin(A_{۱}+A_{۲}+\cdots+A_{n}+A_{n+۱})&=\\ \sin(A_{۱}+A_{۲}+\cdots+A_{n})&\cos A_{n+۱}\\ +\cos(A_{۱}+A_{۲}+\cdots+A_{n})&\sin A_{n+۱}\\ =(S_{۱}-S_{۳}+S_{۵}-\cdots)&\cos A_{n+۱}\\ +(S_{۰}-S_{۲}+\cdots)&\sin A_{n+۱}\end{aligned}$$

فرض‌کنید S'_r مجموع حاصلضربهای از سینوسهای r زاویه از $A_{۱}$، $A_{۲}$، ...، $A_{n+۱}$ وکسینوسهای n + ۱ − r زاویه است. مثلاً

$$S'_{۱}=S_{۱}\cos A_{n+۱}+S_{۰}\sin A_{n+۱}$$

$$S'_{۳}=S_{۳}\cos A_{n+۱}+S_{۲}\sin A_{n+۱}$$

$$S'_{۵}=S_{۵}\cos A_{n+۱}+S_{۴}\sin A_{n+۱}$$

پس

$$\sin(A_{۱}+A_{۲}+\cdots+A_{n+۱}) = S'_{۱}-S'_{۳}+S'_{۵}-\cdots$$

به همین ترتیب

$$\cos(A_{۱}+A_{۲}+\cdots+A_{n+۱}) = S'_{۰}-S'_{۲}+S'_{۴}-\cdots$$

همچنین داریم

$$\sin(A_{۱}+A_{۲}+\cdots+A_{n})=\cos A_{۱}\cos A_{۲}\cdots \cos A_{n}(t_{۱}-t_{۳}+t_{۵}-\cdots)$$

$$\cos(A_{۱}+A_{۲}+\cdots+A_{n})=\cos A_{۱}\cos A_{۲}\cdots \cos A_{n}(۱-t_{۲}+t_{۴}-\cdots)$$

t_r مجموع حـاصلضربهای r بـه r از $tgA_{۱}$، ...، tgA_{n} است. پس

$$(۳)\quad tg(A_{۱}+A_{۲}+\cdots+A_{n}) = \frac{t_{۲}-t_{۳}+t_{۵}-\cdots}{۱-t_{۲}+t_{۴}-\cdots}$$

تبصره. فرمول (۳) را هم می‌توان مستقیماً به استقراء ثابت کرد.

نتیجه.

$$(۴)\; tg(nA)=\frac{n\,tgA-\binom{n}{۳}tg^{۳}A+\binom{n}{۵}tg^{۵}A-\cdots}{۱-\binom{n}{۲}tg^{۲}A+\binom{n}{۴}tg^{۴}A-\cdots}$$

مثلاً،

$$tg۳A=\frac{۳tgA-tg^{۳}A}{۱-۳tg^{۲}A}$$

یعنی برای محاسبه فرمول (۴) می‌توان بسط $(۱+tgA)^n$ را نوشت و توانهای فرد را با علامت یك در میان مثبت و منفی در صورت و جملات بـا توانهای زوج را با علامت یك در میان مثبت و منفی در مخرج نوشت.

اثبات شرکتپذیری جمع متقارن مجموعه‌ها به روشی ساده

علی مقدس
دبیر دبیرستانهای اصفهان

تعریف. ترکیب دو گزاره با یاءمانعةالجمع فقط و فقط وقتی درست است که فقط یکی از دو گزاره راست باشد و با علامت $p \veebar q$ نشان می‌دهیم پس داریم

p	q	$p \veebar q$
t	t	F
t	F	t
F	t	t
F	F	F

به‌کمك جدول زیر معلوم است که ترکیب‌گزاره‌ها با یاءمانعةالجمع شرکپذیر است

p	q	r	$p \veebar q$	$(p \veebar q) \veebar r$	$q \veebar r$	$p \veebar (q \veebar r)$
t	t	t	F	t	F	t
t	t	F	F	F	t	F
t	F	t	t	F	t	F
t	F	F	t	t	F	t
F	t	t	t	F	F	F
F	t	F	t	t	t	t
F	F	t	F	t	t	t
F	F	F	F	F	F	F

از ستون پنجم و ستون هفتم بسادگی معلوم می‌شود که:

$$p \veebar (q \veebar r) \equiv (p \veebar q) \veebar r$$

تعریف. تفاضل متقارن دو مجموعه را که با $A\Delta B$ نشان می‌دهیم برحسب تعریف چنین است:

$$A\Delta B = (A-B)\cup(B-A)$$

$$\begin{aligned} &= \{x | x \in (A-B) \vee x \in (B-A)\} \\ &= \{x | (x \in A \wedge x \notin B) \\ &\vee (x \in B \wedge x \notin A)\} \\ &= \{x | x \in A \veebar x \in B\} \end{aligned}$$

قضیه. تفاضل متقارن مجموعه‌ها شرکتپذیر است.

برهان. داریم

$$\begin{aligned} A\Delta(B\Delta C) &= \{x | x \in A \veebar x \in B\Delta C\} \\ &= \{x | x \in A \veebar (x \in B \veebar x \in C)\} \end{aligned}$$

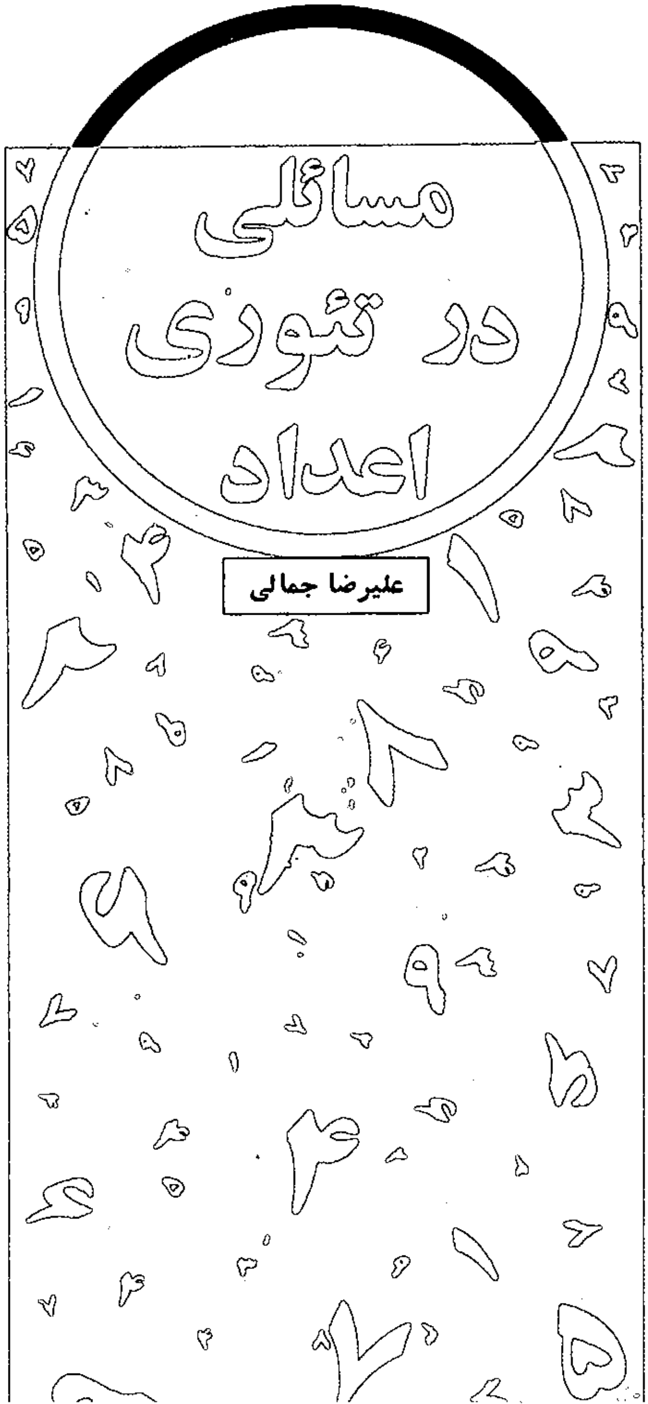
و با توجه به شرکتپذیری یاءمانعةالجمع

$$\begin{aligned} A\Delta(B\Delta C) &= \{x | (x \in A \veebar x \in B) \veebar x \in C\} \\ &= (A\Delta B)\Delta C \Rightarrow A\Delta(B\Delta C) \\ &= (A\Delta B)\Delta C \end{aligned}$$

●

ریاضیات ملکهٔ علوم است و
حساب ملکهٔ ریاضیات

گاوس



علیرضا جمالی

مقدمه

مقالهٔ حاضر را ابتدا با چند مسألهٔ مقدماتی از نظریهٔ اعداد شروع مـی‌کنیم؛ سپس ضمن طرح چند مسألهٔ تاریخی به بحث مختصری راجع به تولید اعدادِ اول می‌پردازیم.

۱ـ آلگوریتم اقلیدس و قضیهٔ لامه

موضوع را با آلگوریتم اقلیدس آغاز می‌کنیم. این کارهم از جنبهٔ تاریخی مدخل خوبی است و هم حاکی از احترام ما نسبت به متفکرین گذشته است. این آلگوریتم ساده که پیش ما بـه طریقهٔ نردبانی موسوم است، فـرآیند ساده‌ای است کـه بـزرگترین مقسوم‌علیه مشترك دو عدد را به دست می‌دهد. دو عدد ۱۵۶ و ۵۶ را درنظر می‌گیریم. روش مذکور کـه عدد ۱۴ به دست خواهد داد چنین است:

$$۱۵۴=۲\times ۵۶+۴۲$$
$$۵۶=۱\times ۴۲+۱۴$$
$$۴۲=۳\times ۱۴$$

یا

۳	۱	۲	
۱۴	۴۲	۵۶	۱۵۴
	۰	۱۴	۴۲

سؤال در مورد تعداد مراحل این فرآیند است. گابریل لامه[1]، ریاضیدانان فرانسوی، در ۱۸۸۴ ثابت کرد که

تعداد مـراحل درآلگـوریتم اقلیدس هرگـز از ۵ برابر تعداد ارقام عدد کوچکتر تجاوز نمی‌کند.

از برهان لامه اطلاعی نداریم ولـی برهان زیبائی در سال ۱۹۲۴ به توسط ه. گروسمن[2] ارائه شد. عین همین برهان را مـی‌توان درکتاب برجستهٔ سیرپینسکی[3] (نظریهٔ اعداد) یافت [۱۰]. (ضمناً به [۴] صفحهٔ ۱۵۹ مراجعه کنید.)

این برهان گرچه ساده و مقدماتی است واردآن نمی‌شویم و همچنان موضوع را بـا بررسی از خواص اعداد طبیعی دنبال می‌کنیم.

۲ـ سه مسأله از ترکیبات نظریه اعداد

درشمارهٔ ۴ مجلهٔ رشد ریاضی مقاله‌ای تحت عنوان «بستائی

یك عدد اول در یك عدد طبیعی» درج شد [۳]، در این مقاله دستوری که بزرگترین قوهٔ یك عدد اول مانند p را در n! به دست می‌دهد چنین است (قضیهٔ ۵):

$$(*) \quad h=[n/p]+[n/p^{۲}+[n/p^{۳}]+\cdots$$

که در آن [x] یعنی جزء صحیح x. مثلاً بزرگترین قوهٔ ۲ در عدد !۴۷ عبارت است از

$$\begin{aligned} h&=[۴۷/۲]+[۴۷/۲^{۲}]+[۴۷/۲^{۳}] \\ &+[۴۷/۲^{۴}]+[۴۷/۲^{۵}] \\ &=۲۳+۱۱+۵+۲+۱ \\ &=۴۲. \end{aligned}$$

اینك آماده‌ایم که خاصیت جالبی را در مورد عدد طبیعی دلخواه n بیان کنیم. فرض کنیم که g تعداد ارقام ۱ باشد که در نمایش عدد n در مبنای ۲ ظاهر می‌شوند. به عنوان مثال g مذکور در مورد عدد ۴۷ عبارت است از ۵ (زیرا، $(۴۷)_{۲}=۱۰۱۱۱۱$). در اینجا ملاحظه می‌شود که $۴۷=۴۲+۵$. همواره چنین است. یعنی به ازاء هر عدد طبیعی n داریم

$$g+h=n.$$

این نتیجه زیبا از لژاندر[۴] (۱۸۳۳ — ۱۷۵۲) فرانسوی است و اثبات آن هم با توجه به (*) و اینکه

$$n=a_{0}+a_{1}\cdot ۲+a_{2}\cdot ۲^{۲}+\cdots+a_{k}\cdot ۲^{k}$$

یعنی

$$(n)_{۲}=b_{k}a_{k-1}\cdots a_{1}a_{0}$$

بسیار ساده است[۵].

مسألهٔ دیگری را مطرح می‌کنیم. دو باره n را یك عدد طبیعی می‌گیریم، و g را به همان صورت قبل تعریف می‌کنیم. اینك ضرایب دو جمله‌ای $\binom{n}{r}$ را که در بسط $(۱+x)^{n}$ ظاهر می‌شوند درنظر می‌گیریم. این ضرایب سطر nام مثلث حسابی پاسکال را تشکیل می‌دهند. مسأله بدیع این است:

به ازاء هر n تعداد ضرایب $\binom{n}{r}$ واقع در سطر nام که فردند مساوی است با ۲^{g} طرح زیر این حکم را به ازاء هر n که $۱ \leqslant n \leqslant ۸$ نشان می‌دهد.

۲^{g}	g	n در مبنای ۲	مثلث پاسکال	n
۱	۰	۰	۱	۰
۲	۱	۱	۱ ۱	۱
۲	۱	۱۰	۱ ۲ ۱	۲
۴	۲	۱۱	۱ ۳ ۳ ۱	۳
۲	۱	۱۰۰	۱ ۴ ۶ ۴ ۱	۴
۴	۲	۱۰۱	۱ ۵ ۱۰ ۱۰ ۵ ۱	۵
۴	۲	۱۱۰	۱ ۶ ۱۵ ۲۰ ۱۵ ۶ ۱	۶
۸	۳	۱۱۱	۱ ۷ ۲۱ ۳۵ ۳۵ ۲۱ ۷ ۱	۷
۲	۱	۱۰۰۰	۱ ۸ ۲۸ ۵۶ ۷۰ ۵۶ ۲۸ ۸ ۱	۸

n\	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹
۰	۱																			
۱			۱	۱																
۲					۱	(۲)	۱													
۳							۱	(۳)	(۳)	۱										
۴									۱	(۴)	۶	(۴)	۱							
۵											۱	(۵)	(۱۰)	(۱۰)	(۵)	۱				
۶													۱	(۶)	۱۵	۲۰	۱۵	(۶)	۱	
۷															۱	(۷)	(۲۱)	(۳۵)	(۳۵)	(۲۱)
۸																	۱	(۸)	۲۸	(۵۶)
۹																				(۹)

برهان این برخلاف برهان حکم قبل پیچیده است. خواستاران می‌توانند به [۷] مراجعه کنند.

در مسأله سوم پای اعداد اول به میان می‌کشیم و غربال دیگری برای بیختن اعداد اول وضع می‌کنیم. این غربال غیراز غربال معروف به اراتستن[۶] است و ارتباط زیبائی با مثلث پاسکال دارد. ابتدا جدولی به صورت زیر را درنظر می‌گیریم و به ازاء هر n، $n+۱$ درایهٔ سطر nام مثلث پاسکال را (مطابق طرح زیر) در سطر nام و ستونهای $۲n$ تا با $۳n$ درج می‌کنیم.

اینك همهٔ اعداد تا یك واقع در سطر nام راکه به n قابل قسمت‌اند با علامت دایره مشخص می‌کنیم. در این صورت،

شرط لازم و کافی برای‌آنکه عدد طبیعی k اول باشد آن است‌که همهٔ اعداد تا یك واقع در سطر kام با علامت دایره مشخص شوند.

برهان این حکم مقدماتی است؛ [۸] را ملاحظه کنید.

هرجا صحبت از خواص اعداد طبیعی می‌شود، ناچار اعداد اول مطرح می‌شوند. چنانکه در مقدمه گفتیم مبحثی از این مقاله را به اعداد اول اختصاص خواهیم داد. ذیلاً وارد مبحث دیگری می‌شویم.

۳ـ یك رشتهٔ جالب از اعداد

برای آماده کردن ذهن از عدد ۲۵۲۰ شروع می‌کنیم و رشتهٔ زیر را می‌سازیم:

$$۲۵۲۰ \text{ و } ۲۵, ۱۱, ۱۲, ۸, ۷, ۸, ۷, \cdots$$

هر جملهٔ رشتهٔ فوق چنین حاصل می‌شود: همهٔ عوامل اول جملهٔ پیش را با احتساب بستائی [= مرتبهٔ تکرار]آنها به دست آورده و حاصلجمع آنها را با ۱ جمع می‌کنیم. مثلاً،

$$۲۵۲۰ = ۲^۳ \times ۳^۲ \times ۵ \times ۷;$$

بنابراین، جملهٔ دوم عبارت است از

$$۱ + ۳ \times ۲ + ۲ \times ۳ + ۵ + ۷ = ۲۵$$

همچنین چون $۵^۲ = ۲۵$، داریم $۱۱ = ۵ \times ۲ + ۱$ که جملهٔ سوم است. بطورکلی، با فرض $n = p_۱^{a_۱} p_۲^{a_۲} \cdots p_k^{a_k}$ تالی n راکه با $f(n)$ نشان خواهیم داد چنین‌تعریف می‌کنیم:

$$f(n) = ۱ + a_۱p_۱ + a_۲p_۲ + \cdots + a_kp_k.$$

چون $f(۷) = ۸$ و $f(۸) = ۷$، ملاحظه می‌شود که رشتهٔ فوق از مرتبه‌ای به بعد نوسانی است. مسأله این است:

به ازاء هر n، از مرتبه‌ای به بعد، جملات ۷ و ۸ در رشته

$$n, f(n), (f(n)), \cdots$$

تکرار می‌شوند.

برای اینکه خوانندگان توانائی خود را در حل مسائل نظریهٔ اعداد آزمایش کنند از ذکر برهان کامل آن خودداری می‌کنیم. راهنمائی‌های زیر به حل مسأله منجر خواهد شد.

(آ) به استقراء ثابت‌کنیدکه به ازاء هر عدد مرکب n که $n \neq ۸$، $f(n) \leqslant n - ۲$؛

(ب) به ازاء هرعدد n که $n > ۶$، $f(n) > ۶$ (حالتی را که n دارای عامل اول تا کمتر از ۷ است‌کنار بگذارید و سپس برهان به طریقهٔ حالات را به کار ببندید).

۴ـ فرما و اعداد مصور

معرفی اعداد مصور (یا اعداد چند ضلعی) به فیثاغورس و پیروان وی برمی‌گردد. آنان با معرفی این اعداد حساب را با هندسه مرتبط ساختند. تصور می‌شودکه خوانندگان با این اعداد و تاریخچهٔ آن‌آشنائی دارند. در شمارهٔ ۳ مجله رشد ریاضی در مبحث مربوط به ریاضیات یونانی به نقش فیثاغوریان در مطالعهٔ علمی اعداد صحیح، یعنی مبدأ نظریهٔ اعداد، اشاره شده است [۵]. ذیلاً اعداد مصور را بطور هندسی نمایش می‌دهیم و سپس قضیهٔ فرما را بدون اثبات ذکر خواهیم‌کرد:

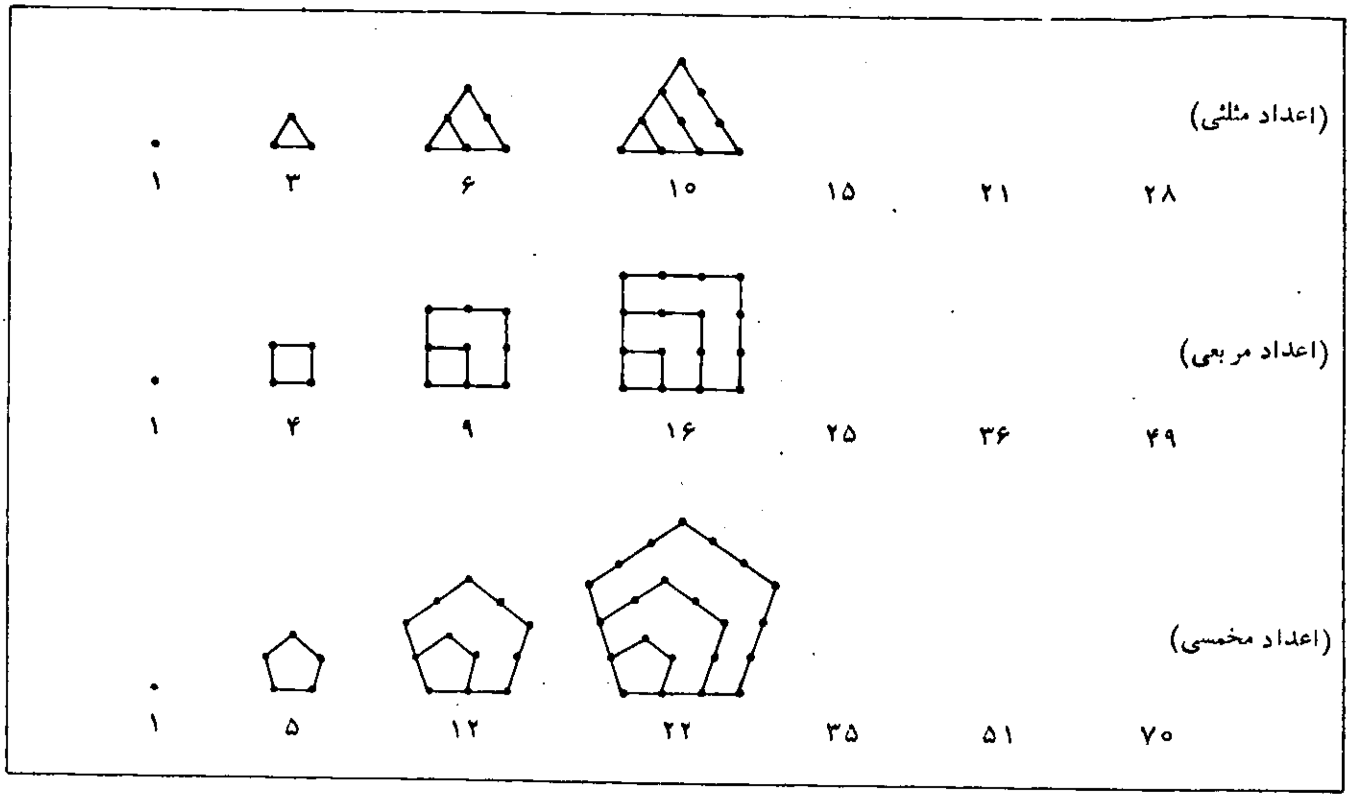
قضیهٔ فرما چنین است:

هر عدد مثلثی است، یا حاصلجمع دو یا سه عدد مثلثی است؛

هر عدد مربعی است، یا حاصلجمع دو، سه، یا چهار عدد مربعی است؛

هر عدد مخمسی است یا حاصلجمع دو، سه، چهار، یا پنج عدد مخمسی است؛ و غیره.

بسیار بجا بودکه در اینجا قدری راجع به فرما و نقش وی در نظریهٔ اعداد اشاره می‌کردیم. این کار را به‌آتیه موکول می‌کنیم. ذیلاً، بعضی‌از خواص مقدماتی اعداد مثلثی را به صورت تمرین فهرست می‌کنیم. این مسائل جملگی در شماره‌های مختلف مجلهٔ AMM مندرج‌اند[۷]. یقیناًدوستداران نظریه از اعدادآنها را بسادگی حل خواهندکرد.



(آ) هر مربع کامل فرد در مبنای ۸ به یك ختم می‌شود. بنابر آنکه از این ۱ صرفنظر شود، عدد باقیمانده مثلثی است.

(ب) در مبنای ۹، هر عدد که ارقامش منحصر به ۱ باشد یك عدد مثلثی است.

(پ) مجموعهٔ اعداد مثلثی که مربع کامل‌اند نامتناهی است.

(ت) تفاضل مربعات دو عدد مثلثی متوالی مکعب کامل است.

(ث) ازآخرین ارقام اعداد مثلثی عدد

N = ۰٫۱۳۶۰۵۱۸ ...

را می‌سازیم. N گویا است یا اصم؟

(ج) آیا می‌توان یك دنباله نامتناهی از اعداد مثلثی با این خاصیت استخراج کرد که حاصلجمع n جملهٔ اول‌آن خود یك عدد مثلثی (مربعی) باشد.

۵- یك قضیهٔ قدیمی چینی و فرما

فرما در نامه‌ای به برنارد فرنیکل دوبسی[۸] قضیهٔ زیر را بدون اثبات ذکر کرد.

اگر p یك عدد اول باشدآنگاه به ازاء هر عدد صحیح مانند a عدد $a^p - a$ بر p قابل قسمت است.

فرما ادعا کرد که برهانی برای‌آن دارد ولی در نامه‌اش ذکری از آن نکرد. اولین برهان‌آن را اویلر صد سال بعد منتشر کرد. درعین‌حال شواهدی در دست است که لایبنیتز هم آن‌را درحدود ۱۶۸۳ ثابت کرده است. این قضیه درکتابهای مقدماتی نظریهٔ اعداد به قضیهٔ کوچك فرما مشهور است و برهانهای متعددی برای‌آن اقامه شده است. برهان مقدماتی آن به استقراء با به کار بردن دستور دو جمله‌ای است. برهان دیگرآن به وسیلهٔ نظریهٔ همنشتیها صورت می‌گیرد [۲].

اینك a را مساوی با ۲ می‌گیریم. قضیهٔ فرما می‌گوید که اگر p اول باشد، $۲^p - ۲$ بر p قابل قسمت است. طرح عکس این حکم طبیعی است. یعنی اینکه:

اگر عدد طبیعی $۲^n - ۲$ بر n قابل قسمت باشد، آیا n اول است؟

چینیها این حکم را به ازاء nهای مختلف بررسی کردند و در ۲۵۰۰ سال پیش به این نتیجه رسیدند که پاسخ «مثبت» است. محاسبات جدید نشان داد که به ازاء nهای ($n > ۱$) کوچکتر از ۳۰۰ تنها آن nهائی $۲^n - ۲$ را عاد می‌کنند که اولند. بسادگی معلوم می‌شود که قضیهٔ (در اصل حکم) چینی نادرست است. عدد $n = ۳۴۱$ مثال نقض را به دست می‌دهد. درواقع $۳۴۱ | ۲^{۳۴۱} - ۲$ و $۳۴۱ = ۳۱ \times ۱۱$. قابلیت

قسمت از این حکم ساده نتیجه می‌شود که $x-y|x^m-y^n$. داریم،

$$۲^{۳۴۱}-۲=۲(۲^{۳۴۰}-۱)=۲[(۲^{۱۰})^{۳۴}-۱]$$
$$=۲[(۲^{۱۰}-۱)(\cdots)]=۲[(۱۰۲۳)(\cdots)]$$
$$=۲[۳(۳۴۱)(\cdots)].$$

گرچه حکم چینی باطل شد ولی منشأ تعریف اعدادی جدید درنظریهٔ اعداد شد. اعدادی مانند $n(>۱)$ را که اول نیستند ولی $۲^n-۲$ را عاد می‌کنند **اعداد شبه اول** می‌نامند. در سال ۱۹۲۶ ب. پوله[9] جدولی از اعداد شبه اول خود را تا ۵۰ میلیون منتشر کرد، ودر ۱۹۳۸ این جدول را تا ۱۰۰ میلیون توسعه داد. از این‌رو اعداد شبه اول به **اعداد پوله** موسوم شد. اینك سؤالهای متعددی برای‌خواننده پیش می‌آید. ابتدا اینکه‌آیا مجموعهٔ اعداد شبه اول نامتناهی است؟ جواب برمی‌گردد به اینکه به ازاء هر عدد شبه اول فرد مانند $n(>۱)$ عدد $۲^n-۱$ یك عدد شبه اول (فرد) است (ثابت کنید). بنابراین همین عدد شبه اول فرد ۳۴۱ منجر به تعدادی نامتناهی از چنین اعداد خواهد شد. مسأله بعد این است‌که آیا عدد شبه اول زوج وجود دارد؟ د. ه. لمر[10] در ۱۹۵۰ عدد ۱۶۱۰۳۸ راکشف‌کرد. گرچه این‌کشف به‌سختی انجام گرفت ولی اثبات شبه اول بودن‌آن کار ساده‌ای است: عدد مزبور را به عوامل اول تجزیه می‌کنیم. داریم

$$۱۶۱۰۳۸=۲\times۷۳\times۱۱۰۳$$

چون

$$۲^{۱۶۱۰۳۸}-۲=۲(۲^{۱۶۱۰۳۷}-۱)$$

کافی است نشان دهیم که ۷۳ و ۱۱۰۳ عدد $۲^{۱۶۱۰۲۷}-۱$ را عاد می‌کنند. از اینکه

$$۱۶۱۰۳۷=۳^۲\times۲۹\times۶۱۷$$
$$۲^{۱۶۱۰۳۷}-۱=(۲^۹)^{۲۹\times۶۱۷}-۱$$
$$=(۲^۹-۱)(\cdots)=۵۱۱(\cdots)$$
$$=۷(۷۳)(\cdots);$$

یعنی عدد واقع درطرف چپ تساوی به ۷۳ قابل قسمت است. به طریق مشابه

$$۲^{۱۶۱۰۳۷}-۱=(۲^{۲۹})^{۹\times۶۱۷}-۱$$
$$=(۲^{۲۹}-۱)(\cdots)$$
$$=۱۱۰۳(۴۸۶۷۳۷)(\cdots),$$

یعنی ۱۱۰۴ هم این عدد را عاد می‌کند. چون ۷۳ و ۱۱۰۳ هردو اولند، حاصلضرب‌آنها هم $۲^{۱۶۱۰۲۷}-۱$ را عاد می‌کند. بنابراین ۱۶۱۰۳۸ یك عدد شبه اول زوج است. بیگر[11] در ۱۹۵۱ ثابت‌کردکه مجموعهٔ اعداد شبه اول زوج نامتناهی است. برای تعمیمی از اعداد شبه اول و نیز اعداد پوله به [۸] (فصلهای ۱۰ و ۱۳) مراجعه‌کنید. (ضمناً [۴] را هم ملاحظه‌کنید.)

۶ـ اعداد اول و حدس گولدباخ[12]

یکی از مهمترین مسائل مربوط به نظریهٔ اعداد حدس گولد باخ است. گولدباخ، ریاضیدان‌آلمانی، در ۱۷۴۲ طی نامه‌ای به اویلر مسأله زیر را پیشنهاد می‌کند.

هر عدد زوج نا کمتر از ۴ حاصلجمع دو عدد اول است.

به عنوان مثال $۴=۲+۲$، $۶=۳+۳$، $۸=۳+۵$، $۱۰=۷+۳=+۵+۵$ و $۱۲=۵+۷$.

صحبت و سقم این حدس درحال حاضر معلوم نیست. کوششهای فراوان سالهای اخیر تنها منجر به این شده است‌که این حدس **احتمالاً** درست است. حال سؤال این است‌که چرا ریاضیدانان‌آن را احتمالاً درست می‌دانند درحالی‌که اثباتی برای‌آن ندارند.

ابتدا اینکه‌حدس مذکور به ازاء جمیع اعداد زوج بزرگتر از ۶ وکوچکتر از ۳۳×۱۰^۶ امتحان شده است. در واقع این اعداد نه تنها حاصلجمع دوعدد اول فردند، بلکه، حاصلجمع دو عدد اول فرد متمایزند. ولی معلوم است‌که با امتحان چندین هزار حالت نمی‌توان حکم کلی کرد. از اینجا تنها می‌توان حکم به صحت احتمالی‌آن کرد. در این مورد مثالی می‌آوریم. می‌دانیم که مجموعهٔ اعداد اول فرد را می‌توان به دومجموعه ازاعداد به‌صورت $۴n+۱$ و به صورت $۴n+۳$ افرازکرد. فرض‌کنیم $\pi_1(x)$ عدهٔ همهٔ اعداد اول به صورت $۴n+۱$ باشدکه از x نابیشترند و به طریق مشابه $\pi_2(x)$ عدهٔ همهٔ اعداد اول به صورت $۴n+۳$ می‌گیریم که از x نابیشترند. معلوم شده است‌که مجموعهٔ اعداد اول از هردو نامتناهی است. به محاسبه معلوم می‌شودکه به ازاء هر x که $x<۲۶۸۶۱$، $\pi_1(x)\leqslant\pi_2(x)$؛ ولی ج. لیچ[13] در ۱۹۵۷ نشان دادکه به ازاء $x=۲۶۸۶۱$،

$$\pi_1(x)=۱۴۷۳ \quad \text{و} \quad \pi_2(x)=۱۴۷۲$$

بنابراین نامساوی معکوس شد. در ۱۹۱۴ لیتلورد[14] ثابت

کـرد کـه بینهایت بـار $\pi_۱(x) < \pi_۲(x)$ و بینهایت بار $\pi_۲(x) < \pi_۱(x)$. خلاصه اینکه این گـونه حدسها دربارهٔ اعداد اول همیشه صحیح نیستند ولـو اینکه بـه محاسبه چندین هـزار حالت امتحان شده بـاشد. اینك برگردیم بر موضوع اصلی؛ اینکه حدس گـولدباخ به ازاء همهٔ اعداد زوج کوچکتر از ۳۳×۱۰^{۶} محقق شده است نمی‌تـواند دال بر صحت آن باشد، بلکه تنها به عنوان شاهد کوچکی است بر له آن.

دلیل بعدی اینکه ریاضیدانان موفق به اثبات قضایائی شده‌اند که تا حدودی شبیه به حدس گولدباخ است. به عنوان مثال در ۱۹۳۰ ریاضیدان روسی شنیرلمان[۱۵] ثابت کرد که **عددی مانند M هست به طوری کـه هر عدد طبیعی n از مرتبه‌ای ببعد حاصلجمع منتها M عدد اول است؛**

$$n=p_۱+p_۲+\cdots+p_M$$ (n بقدرکافی بزرگ).

اگـر می‌دانستیم کـه M مساوی بـا ۲ است آنگاه همین قضیه حدس گولدباخ را به ازاء همهٔ nهای زوج بقدر کافی بزرگ ثابت مـی‌کـرد. در ۱۹۵۶ ریاضیدان چینی ین ون ـ لین[۱۶] ثابت کرد که $M \leqslant ۱۸$. یعنی هر عدد، مانند n، از مرتبه‌ای ببعد حـاصلجمع منتها ۱۸ عدد اول است. نتیجهٔ شنیرلمان به عنوان گـام بزرگی در جهت صحت حدس گـولدباخ محسوب مـی‌شود. این در واقع اولین پیشرفت اساسی بود کـه ۲۰۰ سال اخیر صورت گرفت. گام دیگری در این زمینه در ۱۹۳۷ به وسیلهٔ ریاضیدان دیگر روسی برداشته شد. وینوگرادوف[۱۷] ثابت کرد که

از مرتبه‌ای ببعد، هر عدد فرد n حاصلجمع سه عدد اول است؛

$$n=p_۱+p_۲+p_۳$$ (n بقدرکافی بزرگ، n فرد).

در واقع، این حکم به ازاء همهٔ nهـای فرد بزرگتر از $۳^{۳^{۱۵}}$ درست است. در حال حاضر این محکمترین شاهد بر له حدس گـولدباخ بوده است. توضیح اینکه بسادگـی معلوم می‌شود که قضیهٔ وینوگرادوف نتیجهٔ حکم گولدباخ است. یعنی اگـر حدس گولدباخ راست باشد، دراین صورت قضیهٔ وینوگرادوف ازآن نتیجه خواهد شد. کار شگرف وینوگـرادوف این بود که وی قضیهٔ خود را مستقل از حدس گـولدباخ مستقیماً ثابت کرد. متأسفانه تاکنون کسی نتوانسته است عکس این کار انجام دهد یعنی اینکه با اثبات حکم گولدباخ قضیهٔ وینوگرادوف را ازآن نتیجه‌گیرد. بازهـم گواه دیگـری مبنی برصحت حدس گولدباخ: رنی[۱۸] ریاضیدان مجاری، در ۱۹۴۸ ثابت کرد که **Mی هست بطوری کـه به ازاء هر عدد n زوج بقدرکافی بزرگ، $n=p+A$، کـه درآن، F یك عدد اول است و A منتها M عامل اول دارد.**

حال اگـر می‌دانستیم کـه $M=۱$، درآن صورت صحت حدس گولدباخ به ازاء nهای بقدر کافی بزرگ نتیجه می‌شد. وینوگرادوف و ا. ا. بوشتاب[۱۹] در ۱۹۶۵ ثابت کردند کـه $M \leqslant ۳$ و چن جنیگ ـ رون[۲۰]، در ۱۹۶۶، ثابت کرد کـه $M \leqslant ۲$. (اطلاعات ارزندهٔ فوق را از مقدمهٔ تاریخی کتاب [۶] نقل کرده‌ایم.)

این مبحث را باکلمه‌ای از سیرپینسکـی بـه پایان می‌بریم. وی وقتی گفته است: «... اینکه دانش ما راجع به اعداد مترقی است صرفاً از بابت معلومـات قبلی بـا در مـورد آنها نیست، بلکه پـی برده‌ایم چـه چیزهائـی را هنوز در مـورد آنهـا نمی‌دانیم ...»

۷ـ اعداد اول و تولید آنها

ازجملهٔ مسائل تاریخی نظریه اعداد یـافتن دستوری بوده است کـه همهٔ اعداد اول را به دست دهد. در سال ۱۷۷۲، اویلر خاطرنشان ساخت که بسجملهٔ

$$f(x)=x^۲+x+۴۱$$

به ازاء هـر x طبیعی کـه $۰ \leqslant x \leqslant ۳۹$ یك عدد اول را به دست می‌دهد. چون $f(x-۱)=f(-x)$،

$$f(۰)=f(-۱) \text{ و } f(۱)=f(-۲)$$

و

$$f(۲)=f(-۳) \text{ و } \ldots$$

بنابراین معلوم مـی‌شود کـه $f(x)$ به ازاء هر x صحیح کـه $-۴۰ \leqslant x \leqslant -۱$ نیز اول است. نتیجه اینکـه $x^۲+x+۴۱$ بـه ازاء ۸۰ عـدد صحیح متوالـی −۴۰، −۳۹، ...، ۳۸، ۳۹ اول است. اینك بسجملهٔ زیـر را در نظر می‌گیریم:

$$f(x-۴۰)=x^۲-۷۹x+۱۶۰۱.$$

این بسجمله هشتاد عدد اول را به ازاء ۰، ۱، ۲، ...، ۷۹ به دست می‌دهد. درحال‌حاضر این طولانی‌ترین رشته از اعداد صحیح است که یك بسجملهٔ درجه دوم به ازاء جمل آن منحصراً اعداد اول را تولید می‌کند. (تابع $x^۲-۲۹۹۹x+۲۲۴۸۵۴۱$ نیز ۸۰ عدد اول را بـه ازاء ۱۴۶۰، ۱۴۶۱، ...، ۱۵۳۹ تولید می‌کند). دیگر بسجملهٔ $۶x^۲+۶x+۳۱$ است که به

ازاء ۰، ۱، ...، ۲۸ اول است. بسجملهٔ $۲x^{۲}+۲۹$ وضع بهتری دارد: ۵۷ عدد اول متوالی را به ازاء ۲۸ −، ۲۷ −، ...، ۲۸ به‌دست می‌دهد. بنابراین، بسجملهٔ اویلر در میان بسجمله‌های درجهٔ دوم مشابه بمراتب بهتر است. بعلاوه، خواص دیگری هم دارد. به عنوان مثال، $f(x)$ به جز وقتی که $x = ۴۰$ و $x = -۴۱$ هرگز مربع کامل نیست. همچنین، $f(x)$ به هیچ عددی بین ۱ و ۴۱ قابل قسمت نیست.

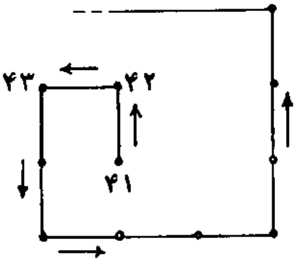
اعداد اولی که از بسجملهٔ اویلر حاصل می‌شوند، درطرحی که ذیلاً توصیف خواهد شد، به طرز جالبی آشکار می‌شوند.

رشتهٔ اعداد طبیعی متوالی زیر را

$$۴۱, ۴۲, ۴۳, \dots, ۱۶۸۱$$

دریك طرح مربعی به صورت حلزونی می‌نویسیم (طرح زیر). در این صورت، اعداد اول حاصل از بسجملهٔ اویلر، به ازاء xهای بین ۰ و ۴۰ درقطر اصلی این طرح مربعی ظاهرخواهند شد؛

.	۶۶	۶۷	۶۸	۶۹	۷۰	**۷۱**
.	۶۵	۵۰	۵۱	۵۲	**۵۳**	۷۲
.	۶۴	۴۹	۴۲	**۴۳**	۵۴	.
.	۶۳	۴۸	**۴۱**	۴۴	۵۵	.
.	۶۲	**۴۷**	۴۶	۴۵	۵۶	.
.	**۶۱**	۶۰	۵۹	۵۸	۵۷	.
۸۳	.	.	.	.	.	.



این نکته را **اولام**[۲۱] و دیگران در مورد بسجمله‌های درجهٔ دوم که اعداد اول را به دست می‌دهند متذکر شده‌اند.

اطلاعات اندکی در مورد بسجملهٔ اویلر در دست است. ولی در عین حال نتایج مختصر اما جالبی ازآن به دست آمده است.

حال بسجملهٔ $f(x)=x^{۲}+x+m$ را درنظر می گیریم که درآن m يك عدد طبیعی است. بعضی‌از ریاضیدانها عدد طبیعی m را **خوشبخت** می‌خوانند درصورتی که مقادیر بسجملهٔ $f(-x)$ به ازاء مقادیر ۰، ۱، ...، $m-۱$ از x اول باشد[۲۲]. برای‌آنکه عدد طبیعی m خوشبخت باشد لازم است که m اول باشد. با توجه به تذکرات فوق، ۴۱ خوشبخت است. همچنین به سادگی ملاحظه می‌شود که اعداد ۲، ۳، ۵، ۱۱ و ۱۷ خوشبخت‌اند. درسال ۱۹۳۳، د. ه. لمر ثابت کرد که در بسجملهٔ $x^{۲}+x+m$، که درآن $m > ۴۱$، عدد m درصورتی خوشبخت خواهد بود که بزرگتر از $۱\frac{۱}{۴}$ بیلیون باشد. در سال ۱۹۳۴ ثابت شد که حتی در قلمرو اعداد بزرگ هم بیش يك چنین mی نمی‌تواند موجود باشد. بالاخره در ۱۹۶۰ با يك برهان مشکل ثابت شد که هیچ mی موجود نیست. بنابراین، اعداد خوشبخت منحصر به همان شش عدد مذکور است.

معلوم شده است که به ازاء هر n، بسجمله‌ای با ضرایب صحیح از درجهٔ n موجود است که به ازاء ۰، ۱، ۲، ...، n اعداد اول را به دست می‌دهد.

گولدباخ درسال ۱۷۵۲ ثابت کرد که هیچ بسجمله برحسب x با ضرایب صحیح وجود ندارد که به ازاء هر x مقادیر اول را به‌دست دهد (حتی به ازاء xهای بقدر کافی بزرگ). تذکر می‌دهیم که تابع $f(x)=x$ بالبداهه همهٔ اعداد اول را به ازاء xهائی طبیعی تولید می‌کند؛ اما، هیچ بسجمله از درجهٔ ۲ و بالاتر برحسب x، که به ازاء تعدادی نامتناهی از xهای طبیعی اعداد اول را تولیدکند، در دست نیست.

دیریکله[۲۳] در ۱۸۳۷ حکم زیر را ثابت کرد.

اگر اعداد طبیعی a و b نسبت به هم اول باشندآنگاه بسجملهٔ اول $ax+b$ يك تعداد نامتناهی از اعداد اول را به دست می‌دهد[۲۴].

این نتیجه به قضیهٔ دیریکله دربارهٔ وجود اعداد اول دریك تصاعد حسابی موسوم است. برای اثبات این حکم دیریکله از حوزهٔ اعداد صحیح خارج شد و ابزارآنالیز مانند حد و اتصال را به کارگرفت. با این کاروی مبدع شاخهٔ جدیدی از نظریه اعداد شد که به نظریه تحلیلی اعداد موسوم است. همانگونه‌که توضیح دادیم وجود بسجملهٔ درجهٔ دومی مانند $ax^{۲}+bx+c$ $(a \neq ۰)$ که تعداد نامتناهی از اعداد اول را به‌دست دهد معلوم نیست؛ در عین‌حال دیریکله روش تحلیلی قوی خود را به کارگرفت و ثابت کرد که درصورتی‌که اعداد a، $۲b$ و c عامل اول مشترکی نداشته باشند، بسجملهٔ درجهٔ دوم $ax^{۲}+۲bxy+cy^{۲}$ برحسب دومتغیر x و y يك تعداد

نامتناهی از اعداد اول را به دست می‌دهد وقتی که x و y در مجموعهٔ اعداد طبیعی تغییر کنند. در سال ۱۹۶۳ بردیئین[۲۵] ثابت کرد که تابع $f(x, y)=x^۲+y^۲+۱$ یك تعداد نامتناهی از اعداد اول به ازاء زوجهای صحیحی (x, y) می‌دهد. همچنین، معلوم شده است که یك تعداد نامتناهی از اعداد اول به هریك از صورتهای $x^۲+y^۲$ و $x^۲+y^۲+z^۲+۱$ موجودند. از توابع بسجمله‌ای که بگذریم به تابعی می‌رسیم که مقادیر اول را بینهایت بار می‌گیرد. میلز[۲۶] ثابت کرد که

عددی حقیقی مانند k هست بطوری که به ازاء هر n طبیعی عدد $[k^{(۳^n)}]$ یك عدد اول است. ($[x]$ یعنی جزء صحیح x). میلز تنها وجود k را ثابت کرد و مقدارش هنوز معلوم نیست.

ذیلاً هدف ما معرفی تابع ساده‌ای مانند $f(x, y)$ با مقادیر اول است که هر عدد اول فرد را درست یك‌بار بگیرد. برای انجام این کار ابتدا قضیهٔ ویلسون[۲۷] را که مورد نیاز است می‌آوریم. این قضیه شرط و لازم و کافیی را برای آنکه یك عدد اول باشد بیان می‌کند. صورت قضیه چنین است:

شرط لازم و کافی برای آنکه عدد p اول باشد آن است که p عدد $(p-۱)!+۱$ را عاد کند.

برای برهان این قضیه می‌توانید به کتابهای مقدماتی نظریه اعداد مراجعه کنید (ضمناً یك طرف این قضیه در شمارهٔ دوم مجله رشد ریاضی ثابت شده است [۲]). پیش از آنکه به معرفی تابع $f(x, y)$ و ارتباط آن با قضیهٔ ویلسون بپردازیم بی‌مناسبت نیست که در مورد قضیهٔ اخیر بحث مختصری داشته باشیم. این قضیه تقریباً ۳۰۰ سال پیش به وسیلهٔ لایبنیز طرح شد و اولین بار به توسط لاگرانژ در ۱۰۰ سال پیش ثابت شد. ویلسون هرگز این قضیه را ثابت نکرد وی فقط آن را پیشنهاد کرد. حالا خواهید پرسید چگونه این قضیه به قضیهٔ ویلسون مشهور شد.

در واقع، ادوارد وارینگ[۲۸] بود که در نوشته‌ای قضیهٔ مذکور را به سرجان ویلسون نسبت داد زیرا قبلاً ویلسون راجع به آن با وی گفتگو کرده بود. به هرحال داستان هرچه باشد، قضیه از این نظر که شرط لازم و کافی در مورد اولیت یك عدد بیان می‌کند حائز اهمیت است. برگردیم به موضوع اصلی و آن اینکه

تابع

$$f(x, y)=\frac{y-۱}{۲}\{|B^۲-۱|-(B^۲-۱)\}+۲,$$

که در آن،

$$B=x(y+۱)-(y!+۱)$$

x و y طبیعی‌اند، تابعی است با مقادیر اول. این تابع همهٔ اعداد اول را می‌گیرد و هر عدد فرد اول را درست یك‌بار به دست می‌دهد.

برهان. به ازاء هر x و y طبیعی $B^۲$ یك عدد صحیح نامنفی است. بنابراین، (آ) $B^۲ \geqslant ۱$، یا (ب) $B^۲=۰$.

(آ) $B^۲ \geqslant ۱$. از اینجا $B^۲-۱ \geqslant ۰$، و داریم

$$|B^۲-۱|=B^۲-۱$$

بنابراین $f(x, y)=۲$.

(ب) $B^۲=۰$. در این حالت داریم

$$f(x, y)=\frac{y-۱}{۲}[\,|-۱|-(-۱)\,]+۲$$

$$=\frac{y-۱}{۲}[۱+۱]+۲=y+۱.$$

چون $B^۲=۰$ ، $B=۰$. مطابق تعریف B،

$$x(y+۱)-(y!+۱)=۰$$

یا

$$x(y+۱)=y!+۱$$

یعنی $y!+۱$ بر $y+۱$ قابل قسمت است. به موجب قضیهٔ ویلسون، $y+۱$ اول است. بنابراین، به ازاء هر x و y طبیعی، $f(x, y)$ اول است.

ابتدا توضیح می‌دهیم که $f(۱, ۱)=۲$. اینك فرض کنیم که p یك عدد اول فرد دلخواه باشد. فرض می‌کنیم که

$$x=\frac{۱}{p}[(p-۱)!+۱] \;\text{و}\; y=p-۱.$$

(بنابر قضیهٔ ویلسون x صحیح است). نشان می‌دهیم که

$$f(x, y)=p$$

به موجب تعریف x و y،

$$p=y+۱ \;\text{و}\; xp=(p-۱)!+۱$$

بنابراین

$$x(y+۱)=xp=(p-۱)!+۱=y!+۱$$

از اینجا $B=۰$ و

$$f(x, y)=y+۱=p$$

بنابراین $f(x, y)$ همهٔ اعداد اول را می‌گیرد.

بقیه در صفحه ۵۷

مسائل شماره ۲۳

تنظیم از: ابراهیم دارابی

۱- عدد اول p را چنان تعیین کنید که $۷p+۱$ مکعب یك عدد طبیعی باشد.

۲- کلیه جوابهای صحیح معادله سیاله

$$۲xy-۶x-۵y=۷$$

را تعیین کنید.

۳- فرض کنید

$$X=\{۱, ۲, ۳, \cdots, ۱۰۰\}$$

عمل $*$ و o را در X چنین تعریف می‌کنیم:

$$a * b=\frac{۱}{۲}\,[a+b+|a-b|]$$

و

$$a\ o\ b=\frac{۱}{۲}\,[a+b-|a-b|]$$

الف) کدام یك از اصول موضوع گروه، تحت هریك از دو عمل o و $*$، برقرار است.

ب) ثابت کنید

$$a * b=\mathrm{Max}\{a, b\}$$

$$a\ o\ b=\min\{a, b\}$$

ج) جوابهای معادلات ذیل را در X به دست آورید.

$$(x * ۱۲)\ o\ ۷=۱۲$$

$$(x * ۱۲)\ o\ ۱۴=۱۳$$

$$(x * ۱۲)\ o\ ۱۴=۱۲$$

۴- بهرام و جواد و سعید، که متهم به تقلب در مواد غذایی هستند، به شرح ذیل در دادگاه شهادت داده‌اند:

بهرام؛ جواد مقصر است و سعید بی‌تقصیر است.

جواد؛ اگر بهرام مقصر است، سعید هم مقصر است.

سعید؛ من بی‌تقصیرم ولی حداقل یکی‌از بهرام و جواد مقصر است.

فرض کنید: A، یعنی بهرام بی‌تقصیراست و B، یعنی جواد بی‌تقصیر است و C، یعنی سعید بی‌تقصیر است.

الف) جدول مشترك ارزش سه شهادت را تنظیم کنید.

ب) اگر هر سه شاهد بی‌تقصیر باشند، کدام یك ازآنها شهادت دروغ داده‌اند.

ج) اگرآنکه مقصر است شهادت دروغ وآنکه بی‌تقصیر است شهادت راست داده باشد، مقصر کیست؟ و بی‌تقصیر کدام است؟

۵- فرض کنید که $f(x)$ یك چندجمله‌ای باکوچکترین درجه باشد به طوری‌که در دونقطه متمایز $x_۱$ و $x_۲$ داشته باشیم

$$f(x_۱)=a_۱ \quad و \quad f'(x_۱)=b_۱$$

و

$$f(x_۲)=a_۲ \quad و \quad f'(x_۲)=b_۲$$

الف) ضابطه چند جمله‌ای را برحسب a_i و b_i و x_i $(i=۱, ۲)$ به دست‌آورید.

ب) درحالتی‌که $x_۱=۱$ و $x_۲=۲$ و $a_i=b_i=x_i$ $(i=۱, ۲)$ ضابطه چند جمله‌ای را بنویسید.

۶- فرض کنید که f بربازه $[۰, ۱)$ تعریف شده باشد و در نقطه صفر از سمت راست پیوسته باشد. اگر تابع f، در هر نقطه x از بازه $[۰, ۱)$ در رابطه $f(x)=f(x^۲)$ صدق کند، ثابت‌کنید f براین بازه تابع ثابت است.

۷- در بین اعداد به فرم $|۵^l-۳۶^k|$ کوچکترین مقدار کدام است.؟ k و l اعداد طبیعی هستند.

۸- ارقام از ۱ تا ۹ را روی رئوس و اضلاع مثلثی طوری درج می‌کنیم که روی هر ضلع‌که شامل رئوس هم می‌شود، ۴ عدد با مجموع ۲۰ قرارگیرند. ارقامی را که در سه رأس مثلث قرار می‌گیرند، مشخص کنید.

۹- ثابت‌کنید بین اعداد n و $n+1$ و $n+2$ و ... n^3+n^2+n+2، به ازاء جمیع مقادیر n اعداد طبیعی از توان چهارم پیدا می‌شود.

۱۰- اگر در رشته اعداد $x_1, x_2, \ldots, x_n$ که در آن
$m \geqslant 3$ و $x \neq 0$

رابطه

$$(x_1^2+x_2^2+\cdots+x_{n-1}^2)(x_2^2+x_3^2+\cdots+x_n^2)$$
$$=(x_1x_2+x_2x_3+\cdots+x_{n-1}x_n)^2$$

برقرار باشد، ثابت‌کنید رشته اعداد مفروض تشکیل یك تصاعد هندسی می‌دهند.

۱۱- به ازاء چه مقداری از x، تابع

$$f(x)=|x-1|+|x-2|+\cdots+|x-1368|$$

به حداقل مقدار خود می‌رسد.

۱۲- ۱۹۸۷ نقطه متمایز در فضا مفروضند. ثابت‌کنید ازیکی از این نقاط می‌توان صفحه‌ای طوری رسم کرد که در هرطرف آن ۹۹۳ نقطه از این نقاط قرار داشته باشد.

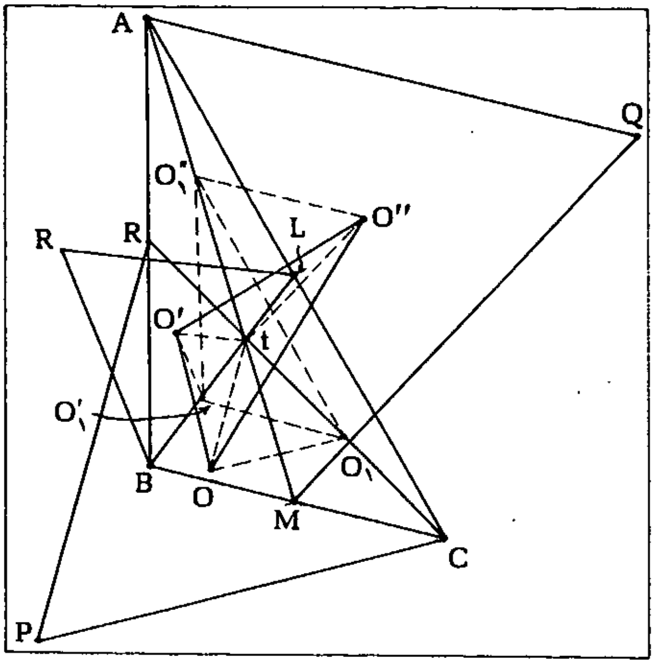
۱۳- روی یك صفحه ۱۰۰ نقطه موجود است. حداقل تعداد اوساط پاره خطهایی را پیدا کنیدکه انتهایشان این نقاط باشند.

۱۴- ثابت‌کنید در داخل دایره‌ای به شعاع واحد، نمی‌توان دو دایره را که مساحت هر یك ازآنها بیشتر از واحد است، بدون لغزاندن برروی هم جا داد.

۱۵- طول هریك از اضلاع شش ضلعی محدبی بیش‌از واحد است. آیا همواره می‌توان قطری ازآن را پیدا کردکه طول آن از ۲ بیشتر باشد؟

۱۶- بر سه میانه مثلث غیر مشخص ABC، مثلث متساوی‌الاضلاع استوار می‌کنیم (مطابق شکل ضمیمه) ثابت کنید. مثلثی‌که رئوس‌آن مراکز این سه مثلث متساوی‌الاضلاع است با مثلث ABC متشابه است.

(از: آرش رستگار).



۱۷- بین سه جمله‌ای‌های درجه دومی که ضریب x^2 درآنها برابر واحد باشد، سه جمله‌ای f را طوری پیداکنیدکه، برای آن، حداکثر مقدار $|f(x)|$ در فاصله $[-1, 1]$ دارای حداقل مقدار ممکن باشد.

۱۸- ثابت‌کنید

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{1}{k+m+1}$$
$$=\sum_{k=0}^{n}(-1)^k\binom{m}{k}\frac{1}{k+n+1}$$

(راهنمایی: $\frac{1}{k+m+1}=\int_0^1 t^{k+m}dt$)

۱۹- ثابت‌کنید اگر تابع

$$f(x)=\sin x+\cos ax$$

متناوب باشد، آنگاه a یك عددگویا است.

۲۰- ثابت‌های a و b را طوری تعیین‌کنیدکه

$$\lim_{x\to 0}\frac{1}{bx-\sin x}\int_0^x\frac{t^2dt}{\sqrt{a+t}}=1$$

حل
مسائل شماره ۲۱

تنظیم از: ابراهیم دارابی

مسأله ۱- فرض‌کنیم G گروهی از مرتبه n باشد. اگر به ازای هر مقسوم‌علیه n مانند d مجموعه

$$\{x\in G|x^d=۱\}$$

حداکثر d عضو داشته باشد، آنگاه G دوری است.

حل: فرض‌کنیم که d یك مقسوم‌علیه دلخواه n باشد. عده همهٔ اعضائی از G را که مرتبه‌آنها d است با $\nu(d)$ نشان می‌دهیم (ملاحظه‌کنید که در حالت‌کلی ممکن است $\nu(d)=۰$). حال معلوم است که

$$n=\sum_{d|n}\nu(d).$$

اینك فرض می‌کنیم که $x\in G$ عضوی از مرتبه d باشد. در این صورت هریك از جمل دنبالهٔ

$$۱, x, x^۲, \dots, x^{d-۱} \qquad (*)$$

در معادله $y^d=۱$ صدق می‌کند. چون این معادله، بنابه فرض، حداکثر d جواب دارد، بنابراین G غیراز جمل (*) (که دو به دو متمایزند) هیچ عضو دیگری ندارد که در معادله مذکور صدق‌کند. لذا اعضائی از G که مرتبه‌آنها d است فقط دربین جمل (*) است. چون تعداد این قبیل اعضا $\varphi(d)$ است، نتیجه می‌گیریم که،

$$\nu(d)=\begin{cases}\varphi(d) & \text{اگر G عضوی از مرتبه d داشته باشد،}\\ ۰ & \text{، در غیر این صورت}\end{cases}$$

[یادآوری می‌کنیم که $\varphi(d)$ عبارت است از عدهٔ اعداد طبیعی کوچکتر از d و متباین با آن.] اینك با توجه به رابطه

$$n=\sum_{d|n}\varphi(d)$$

به سادگی معلوم می‌شود که G باید عضوی از مرتبه d داشته باشد، زیرا در غیر این صورت، n مقسوم‌علیهی مانند d' دارد که $\nu(d')=۰$ و در نتیجه

$$n=\sum_{d|n}\nu(d)<\sum_{d|n}\varphi(d)=n$$

که یك تناقض است. حال گوئیم چون d مقسوم‌علیه دلخواهی از n انتخاب شده است، با انتخاب $d=n$ نتیجه می‌گیریم که G عضوی از مرتبهٔ n دارد. یعنی G دوری است.

مسأله ۲- فرض‌کنید که هریك از n ترکهٔ چوب به دو قسمت کوتاه و بلند شکسته می‌شوند. ۲n تکه چوب حاصل را دوتا دوتا به هم می‌چسبانیم تا n ترکه چوب جدید حاصل شود. مطلوب است احتمال اینکه:

الف) این n زوج به ترتیب اولیه چوبها قبل‌از شکستن آنها بهم چسبانده شوند.

ب) قطعات بلند، به قطعات کوتاه چسبانده شوند.

حل: **(الف)** - قطعه‌کوتاه ترکه iام را با S_i و قطعه بزرگتر را با L_i نشان می‌دهیم. پس n قطعهٔ چوب $i=۱, ۲, \dots, n$ و L_i و S_i داریم که می‌توانیم آنها را مثلاً در یك ردیف قرار دهیم و با شروع از یك سمت هر دو قطعه چوب مجاور را به هم بچسبانیم و ازآنها n ترکه چوب جدید بسازیم. در این صورت صور ممکن عبارت از تمام جایگشتهای ۲n شیء خواهد بود، یعنی

صور ممکن $=(۲n)!$

برای‌آنکه قطعه‌ها به ترتیب اصلی به هم متصل شوند، باید L_i درکنار S_i (در سمت چپ یا راست‌آن قرارگیرد. بنابراین به ازاء هر i، دو امکان از لحاظ قرارگرفتن قطعه L_i در سمت چپ یا راست‌آن وجود دارد و با درنظرگرفتن تمام جایگشتهای ممکن زوجهای (L_i, S_i)، که $n!$ است خواهیم داشت:

صور مساعد $=۲^n\cdot n!$

پس،

$$\text{احتمال مطلوب} = \frac{\text{صور مساعد}}{\text{صور ممکن}} = \frac{۲^n \cdot n!}{(۲n)!}$$

(ب) - مانند حالت (الف) عمل می‌کنیم به جز اینکه در این حالت چون هر قطعه L می‌تواند به هر قطعه S متصل شود، ۲n قطعه Lها. S را غیر متمایز می‌گیریم. در این صورت

$$\text{صور ممکن} = \frac{(۲n)!}{n!\,n!} = \binom{۲n}{n}$$

$$\text{صورت مساعد} = ۲^n$$

لذا،

$$\text{احتمال مطلوب} = \frac{۲^n}{\binom{۲n}{n}}\,.$$

مسأله ۳- دنباله متناهی $\{a_k\}_{k=۱}^{n}$ متشکل از اعداد $۱\,,\,۲\,,\,\cdots\,,\,n$ با ترتیب دلخواه است.

اگر n فرد باشد، ثابت کنید عدد،

$$(a_۱-۱)\,(a_۲-۲)\,\cdots\,(a_n-n)$$

زوج است.

حل: فرض کنیم که n عددی فرد باشد. عبارت زیر را درنظر می‌گیریم،

$$A=(a_۲-۱)\,(a_۳-۳)\,\cdots\,(a_n-n)$$

برای اثبات حکم کافی است ثابت کنیم که A زوج است. برای این منظور، ادعا می‌کنیم که حداقل یکی از عوامل A، لزوماً زوج است. زیرا هرگاه همه عوامل A فرد باشند آنگاه لازم می‌آید که $\frac{n-۱}{۲}$ عدد

$$a_۱\,,\,a_۳\,,\,\cdots\,,\,a_n$$

جملگی زوج باشند واین ممکن نیست، زیرا با توجه به فرض تعداد جمل زوج دنباله

$$a_۱\,,\,a_۲\,,\,\cdots\,,\,a_n$$

$\frac{n-۱}{۲}$ است.

مساله ۴- فرض کنیم تابع f در یك همسایگی صفر تا مرتبه $(k+۱)$ مشتق‌پذیر باشد و بعلاوه $f(۰)=۰$. ثابت کنید

$$\lim_{k\to ۰}\frac{d^k}{dx^k}\left(\frac{f(x)}{x}\right)=\frac{۱}{k+۱}\,f(۰)^{(k+۱)}$$

حل. چون $f(۰)=۰$، می‌توانیم چنین بنویسیم

$$\frac{f(x)}{x}=\int_۰^۱ f'(xt)dt$$

$$\frac{d^k}{dx^k}\left(\frac{f(x)}{x}\right)=\int_۰^۱ f^{(k+۱)}(xt)t^k dt$$

بنابراین

$$\lim\frac{d^k}{dx^k}\left(\frac{f(x)}{x}\right)=\int_۰^۱ f^{(k+۱)}(۰)t^k dt$$

$$=\frac{f^{(k+۱)}(۰)}{k+۱}$$

مسأله ۵- تعداد جمله‌های گویای $(\sqrt{۲}+\sqrt[۳]{۳})^{۱۰۰}$ را تعیین کنید.

جمله عمومی دو جمله‌ای نیوتن به صورت، $C_n^k a^{n-k}b^k$ نوشته می‌شود. دراینجا

$$a^{n-k}b^k=(\sqrt{۲})^{۱۰۰-k}(\sqrt[۳]{۳})^k$$

باید گویا بشود. بنابراین باید داشته باشیم،

$$(۱)\ \text{و}\ (۲)\quad \begin{cases} ۱۰۰-k=۲m \\ k=۳m' \end{cases}\qquad (m,\ m'\ \text{و}\ k\in N)$$

$$(۲)\ \text{و}\ (۱)\implies ۱۰۰=۲m+۳m'\quad(۴)$$

تعداد جوابهای صحیح معادله سیال تعداد جملات گنگ را مشخص می‌کند. از (۴) نتیجه می‌شود m' زوج است و $m'\leqslant ۳۲$ پس مقادیر قابل قبول برای m' عبارتند از:

$$۰\,,\,۲\,,\,۴\,,\,\cdots\,,\,۳۲$$

رشته اعداد بالا تشکیل تصاعد عددی با قدر نسبت ۲ می‌دهد که جمله اول آن صفر و جمله nام آن ۳۲ است پس داریم،

$$l\ =a+(n-۱)d$$

$$۳۴=۰+۲(n-۱) \Longrightarrow n=۱۸$$

مسأله ۶- سه مجذور کامل تعیین کنید که مجموع هریك، با حاصلضرب آنها مجذور کامل باشد.

حل. سه عدد $a^۲$ و $b^۲$ و $c^۲$ فرض می‌کنیم. بنا به فرض باید داشته باشیم،

$$a^۲+a^۲b^۲c^۲=k^۲ \qquad (k\in N)$$

$$a^۲(۱+b^۲c^۲)=k^۲$$

$$۱+b^۲c^۲=m^۲$$

$$۱=(m-bc)\,(m+bc)$$

$$\begin{cases} m-bc=۱ \\ m+bc=۱ \end{cases} \qquad \begin{cases} m-bc=-۱ \\ m+bc=-۱ \end{cases}$$

که در هرحالت تناقض حاصل می‌شود و مسأله جواب ندارد.

مسأله ۷- معادله زیر را حل کنید.

$$x^۲-۸[x]+۷=۰$$

حل ـ اگر x ریشه معادله مفروض باشد و $n=[x]$ از معادله نتیجه می‌شود

$$x^۲+۷=۸n$$

و ازآنجا $n\geqslant ۰$ در این حالت با استفاده از نامساوی $n\leqslant x<n+۱$ خواهیم داشت

$$n^۲+۷\leqslant x^۲+۷<(n+۱)^۲+۷$$
$$=n^۲+۲n+۸$$

با تبدیل $x^۲+۷$ به $۸n$ نامساوی زیر را برحسب n خواهیم داشت،

$$n^۲+۷\leqslant ۸n<n^۲+۲n+۸$$

ازحل $n^۲+۷\leqslant ۸n$ مقادیر قابل قبول n درفاصله $[۱, ۷]$ به دست می‌آید. و نامساوی $۸n<n^۲+۲n+۸$ به ازاء $n<۲$ و $n>۴$ برقرار می‌گردد. بنابراین یا

$$۴<n\leqslant ۷ \quad \text{و یا} \quad ۱\leqslant n<۲$$

و چون n عدد صحیحی است بنابراین مقادیر

$$n=۱,\ ۵,\ ۶,\ ۷$$

قابل قبولند. به ازاء این مقادیر n معادله به صورت زیر نوشته می‌شود

$$x^۲=۱,\ ۳۳,\ ۴۱,\ ۴۹$$

با امتحان‌کردن ریشه‌ها معلوم می‌شود ۷ و $\sqrt{۴۱}$ و $\sqrt{۳۳}$ و ۱ ریشه‌های معادله‌اند و ۷- و $-\sqrt{۴۱}$ و $-\sqrt{۳۳}$ و ۱- ریشه‌های خارجی معادله هستند.

مسأله ۸- اگر سه جمله‌ای درجه دوم

$$f(x)=ax^۲+bx+c$$

دارای ریشه‌های صحیح و k عدد طبیعی باشد مطلوب است تعیین تعداد اعداد طبیعی n بقسمی‌که f(n) بر k بخش‌پذیر باشد.

حل ـ اگر m ریشه صحیح f(x) باشد و برای اعداد صحیح p و q که متمایز با m می‌باشند مقادیر f(p) و f(q) بر k بخش‌پذیر باشند درآن صورت

$$ap^۲+bp+c\in Z$$

و

$$am^۲+bm+c=۰$$

و

$$aq^۲+bq+c\in Z$$

اعداد صحیح خواهند بود. بنابراین:

$$a(p^۲-m^۲)+b(p-m)\in Z$$

ازآنجا،

$$a(p+m)+b\in Q$$

و

$$a(q+m)+b\in Q$$

بنابراین،

$$a(p-q)\in Q \quad \text{و} \quad a\in Q \quad \text{و} \quad b\in Q$$

و

$$c=-am^۲-bm\in Q$$

با قرار دادن

$$a=\frac{r}{s} \quad \text{و} \quad b=\frac{t}{u} \quad \text{و} \quad c=\frac{v}{w}$$

$$g(x)=suwf(x)=ruwx^۲+tswx+sur$$

کثیرالجمله $g(x)$ ضرایب صحیح دارد. و برای هر $l\in z$

$$g(m+klsuw)=g(m+klsuw)-g(m)$$

به $klsuw$ بخش‌پذیر است پس به ازاء

$$n=m+klsuw$$

که درآن $l\in Z$ می‌باشد $g(n)$ بر $klsuw$ بخش‌پذیر است و درآن صورت $f(n)$ بر kl بخش‌پذیر می‌شود. به این ترتیب اگر لااقل دو عدد $m\neq n$ موجود باشدکه به ازاء آنها $f(n)$ بر k بخش‌پذیر باشد، درآن صورت از چنین nهایی بی‌شمار وجود خواهد داشت.

شگفتیهای اعداد

فرستنده:
رضا علاقه‌بندان ـ دانش‌آموز ـ بوشهر

$۶۳:۳=۶\times۳+۳$

$۹۵:۵=۹+۵+۵$

$۸۵-۶۳=۸+۵+۶+۳$

$۲۷۲+۱۶=(۲+۷)\times۲\times۱۶$

$\sqrt{۶۴}=۶+\sqrt{۴}$

$\sqrt{۶۷۲۴}=۶+۷۲+۴$

$\sqrt{۱۶۹}=\sqrt{۱۶}+۹$

$\sqrt{۱۱۸۸۱}=۱۱۸-۸-۱$

تاریخ پیدایش بعضی از علائم

آقای رضا علاقه‌بندان دانش‌آموز
سال چهارم ریاضی از بوشهر

تاریخ پیدایش بعضی‌از علائم ریاضی را از شماره ۳ مجله یکان اقتباس نموده و ارسال داشته‌اند. اصل مطالب توسط آقای فتح‌ا... زرگری تنظیم‌شده است. با توجه به‌جالب بودن این نکات تاریخی، ذیلاً این نمادها را می‌آوریم.

علامت	مفهوم	مبتکر	تاریخ
$\varphi(x)$, $f(x)$	تابع	برنویی، اویلر	۱۷۱۸، ۱۷۳۴
$d^n x$	دیفرانسیل	لایب نیتز	۱۶۷۵
$\int$	انتگرال	»	۱۶۷۵
$\frac{d}{dx}$	مشتق	لایب نیتز	۱۶۷۵
$f'(x)$, y'	مشتق	لاگرانژ	۱۷۷۰
$\int_a^b$	انتگرال معین	فوریه	۱۸۱۹
!	فاکتوریل	کرامپ	۱۸۰۸
$\lvert x\rvert$	قدرمطلق	وایرشتراس	۱۸۴۱
lim	حد	هامیلتن	۱۸۵۳
=	تساوی	رکورد	۱۵۵۷
$> <$	بزرگ، کوچك	هاریوت	۱۶۳۱
$\parallel$	توازی	اوترید	۱۶۷۷
$\perp$	تعامد	اریگون	۱۶۳۴
( )	پرانتز	کاروان، استیفل	۱۵۴۴، ۱۵۴۵
[ ]	کروشه	بامیلی، ویت	۱۵۵۰، ۱۵۹۳
{ }	آکولاد	ویت	۱۵۹۳

اسامی همکارانی شماره ۱۹ و ۲۰ و راه حل بوده

از کلیه این همکاران تشکر می‌کنیم و

تنظیم از: محمود نصیری

علی‌اکبر جاوید مهر دبیر ریاضی ساوه: ۱، ۲، ۳، ۴، ۶، ۱۷

همکار گرامی آقای جاوید مهر، از لطف شما نسبت به مجله و از همکاری صمیمانه شما تشکر می‌کنیم. امیدواریم موفق باشید، از مسائل ارسالی شما انشاءالله در شماره‌های آتیه استفاده خواهیم کرد.

فرامرز صابری دانش‌آموز تهران: ۱، ۲، ۳، ۴، ۶، ۷، ۸، ۱۰، ۱۳، ۱۴، ۱۵، ۱۶، ۲۰

محمد علی‌پور اسکندانی دانشجو تبریز: ۱، ۴، ۵، ۶، ۷، ۱۰، ۱۳، ۲۰

سامان سروشیان دانش‌آموز تهران: ۴، ۷، ۸

بیژن صفوی: از اظهار لطف شما نسبت به مجله تشکر می کنیم.

هما راستی دوم ریاضی مشهد: ۱، ۱۳

رضائی طباطبائی دانش‌آموز مشهد: شماره ۲۰، از ارسال مسائل تشکر می کنیم.

مجید وطنی دانش‌آموز کاشمر: ۱۶ ازشماره ۱۸ و ۱، ۱۳ شماره ۱۹ـ۲۰

رامین منوری دانشجو تهران: ۱، ۲، ۳، ۵، ۱۷

یزمان سوداگری دانش‌آموز تهران: ۱، ۷، ۱۰، ۱۳، ۲۰

امیر معطر تهرانی دانش‌آموز تهران: ۱، ۸ ـ

علی سلیمانی دانش‌آموز اصفهان: (۱) و ۱۳ و ۱ و ۲، ۹، ۱۵ از شمارهٔ ۱۸

محسن خلیلی‌دلشاد دانش‌آموز: ۱۳

مسعود طاهرخانی دانش‌آموز قزوین: ۷ و ۱۳ و ۱ از شماره ۱۸ از لطف شما متشکریم.

محمدحسین محسنی دبیر اندیمشك: ۱، ۶، ۱۰، ۱۳، ۱۴، ۱۶، ۱۷ از ارسال مسائل تشکر می‌کنیم.

بهرنگ نوحی، شهرام محسنی‌پور دانش‌آموزان تهران: ۱، ۲، ۴، ۶، ۷، ۱۰، ۱۳، ۱۴، ۱۶ و حل مسائل مسابقه دانش‌آموزی.

احمدرضا دیوسالار دانش‌آموز تهران: ۱ و ۱۶

فرشاد ماهوشی دانش‌آموز اصفهان: ۱

داودکریمی دانش‌آموز تهران: ۱، ۲، ۷، ۱۰، ۱۳، ۱۶، ۱۷

حسین‌زاده مرشدبیك دانشجو تهران: ۱، ۲، ۳، ۷، ۹، ۱۰، ۱۷

مهردادآقاجانی دانش‌آموز: ۴، ۱۴

داوید ربیب دانش‌آموز تهران: ۱

هادی هادی‌زاده نجف‌آباد: ۱، ۱۰، ۱۳، ۲۰

غلامرضا احمدنژاد رودسر دانش‌آموز: ۱، ۱۳

ج. ر. غفاری: ۱، ۳، ۱۰، ۱۶

فرزاد تبریزی دانش‌آموز بجنورد: ۱

پورنگ ابولمعصومی دانش‌آموزکرج: ۱۰، ۱۳

مهدی بوستانپور دانش‌آموز مشهد: ۱، ۴، ۶، ۱۰، ۱۷

سعید عرفانیان دانش‌آموز مشهد: ۱۴

ماهان غلامی تهران: ۱، ۲، ۳، ۴، ۵، ۷، ۹، ۱۰، ۱۷

فهمیه فروحی دانش‌آموز رشت: ۱، ۷، ۱۳، ۱۴

محمدرضا حاج سید جوادی دانش‌آموز تهران: ۱، ۱۳

که حل مسائل را فرستاده‌اند آنها صحیح است

امیدواریم بیش از این با ما همکاری کنند

احمدرضا شهیدی دانش‌آموز نجف‌آباد: ۴، ۱۳ مطالب شما در هئیت تحریریه مطرح گردید.

محمد ذاوری‌اردکان دبیر اردکان یزد: ۱۳، ۱۴، و ۱۵ از شماره ۱۸

علی‌آذر بر دانش‌آموز تهران: ۱، ۱۳

محمدرحیم دانشجو تهران: ۱، ۲، ۷، ۸، ۹، ۱۱ و ۱۲ و ۱۹ شمارهٔ ۱۸

محمدتقی رحمتی دانش‌آموز خمینی‌شهر اصفهان: ۷

محمد مهرپویا دانش‌آموز بجنورد: ۱، ۹، ۱۲ از ارسال مسائل تشکر می کنیم.

ایوب احمدپورپرویزیان دانشجو تبریز: ۱، ۳، ۵، ۱۰ شماره ۱۸ و ۱۳ شماره ۱۹ـ۲۰

محمد مهدی امینی دانش‌آموز ورامین: ۱، ۲ شماره ۱۸ و ۱ شماره ۱۹

ابوالحسن اسبکیان دانش‌آموز بابل: ۱، ۶، ۷، ۱۳، ۱۴

کورش‌کلانتززاده دانش‌آموز تهران: ۱، ۱۰، ۲۰

آرش اسلامی دانش‌آموز رشت: ۱۰، ۱۳

حسین پیرهادی دوم ریاضی تهران: ۱، ۱۳

حمید زارع‌دوست، کاشمر: ۹، ۱۷ شماره ۱۸ و ۱ و ۱۴ شماره ۱۹ـ۲۰

رضا الفتی‌صابر دانش‌آموز رشت: ۱، ۲، ۴، ۱۰، ۱۳، ۱۴، ۱۶

روح‌الله جهانی‌پور دانش‌آموز قم: ۱، ۳، ۴، ۵، ۶، ۷، ۹، ۱۳، ۱۵ نظم شما قابل تحسین است، موفق باشید.

آریا آریاپاد دانش‌آموز رشت: ۱۳ و مسأله ۲ شمارهٔ ۱۸

آرش صباحی‌فرد دانش‌آموز تهران: ۸

علیرضا حیدرپور دانش‌آموز رشت: ۱ شماره ۱۸

ارشك حمیدی دانش آموز تهران: ۱، ۶، ۱۳، ۱۴

محمدمهدی امینی دانش‌آموز قرچك ورامین: ۱، ۱۳، ۳، ازارسال مسائل تشکرمی کنیم ولی باید منابع آنها را ذکر کنید.

محمدرضا هریسی دانشجو تبریز: ۸

سید مهدی هاشمی دانش‌آموز قم: ۱، ۵

کورش‌کریمی دانشجو مشهد: راه‌حل شما صحیح است از ارسال مسائل تشکر مـی‌کنیم انشاءالله ازآنها استفاده خواهیم کرد.

کامبیز کاویانی تهران: ۱، ۴، ۷، ۳

شهرام محسنی‌پور دانش‌آموز سوم ریاضی تهران: از حل مسائل مرحله دوم مسابقه و بعضی مسائل شماره ۱۹ـ۲۰ تشکر می کنیم.

محمدمهدی کاوه‌یزدی یزد: از اظهار لطف شما نسبت بـه مجله تشکر می کنیم مسائل ۱، ۲ شماره ۱۸ صحیح است.

سراج روحی دانش‌آموزچالوس: صورت این تست اشتباه است نیازی بـه جمله اول نیست زیرا در هـر تصاعد عددی $a_1 = S_1$.

احمد جلالی دانشجو اهواز: شما بـرای تهیه سؤالات فوق لیسانس ریاضی می‌توانید به‌گروه ریاضی دانشگاه تهران مراجعه یا مکاتبه کنید.

مسیب بهرامی دانش‌آموز شهرضا: ازاظهارلطف شما نسبت به مجله تشکر می‌کنیم.

برادرانی که حل مسائل مجله شماره ۲۱ را برای ما فرستاده‌اند با درج شماره‌های مسائل آنها به قرار ذیل‌اند:

پیام ناصر طیوب سوم ریاضی از شیراز: ۲-۳-۷-۱۳
داریوش سعیدکیا و احمد رضا شیرزاد: ۲-۳-۷-۸-۹-۱۱-۱۲-۱۳
محسن بهپور دانش‌آموز بندرانزلی: ۷-۹-۱۱
شاهرخ مسعودی‌فر دانش‌آموز سوم ریاضی از اندیمشك: ۷-۱۸
غضنفر فدوی دانش‌آموز ریاضی از اندیمشك: ۱-۷
بهروز جوهری دبیر ریاضیات از اهواز: ۵-۷-۹-۱۵
افشین خاشعی دانش‌آموز دوم ریاضی: ۹-۱۳-۲۰-۳
مازیار صیامی چهارم ریاضی‌ازتهران: ۲-۷-۹-۱۳-۲۰
محمد چکینی چهارم ریاضی از تهران: ۴-۷-۹-۱۴-۱۸
فرشاد مهوشی سوم ریاضی: ۷-۹
حمیدرضا غفاری دانشجوی پزشکی: ۲-۳-۷-۹-۱۳
سعید صفری - سید علی میرفخرایی ازدبیرستان سجاد: ۲-۴-۷-۱۲-۱۳-۱۹
آرش صباحی‌فرد چهارم‌ریاضی‌ازتهران: ۳-۴-۶-۷-۱۰
مهدی امینی سوم ریاضی از قرچك ورامین: ۱۲-۱۷-۲۰
علی‌اکبر جاویدمهر دبیر ریاضی ساوه: ۳-۴-۶-۷-۹-۱۰-۱۱-۱۲-۱۳-۱۵-۲۰
فرزاد صداقتی سوم ریاضی از تهران: ۳-۷-۹-۱۲
محمد رمضانی سوم ریاضی از تهران: ۷
کامبیز کاویانی از تهران: ۲-۳-۷-۱۰-۲۰
مشکوة دانشجو از تهران: ۷-۹
هادی‌زاده از نجف‌آباد اصفهان: ۷
امیرحسین صبوری سوم ریاضی از مشهد: ۱۱-۱۲-۱۷-۲۰
یغما محمدیان‌روشن: ۷-۱۱

ابوالفضل جلیلو چهارم ریاضی تاکستان: ۷-۹-۱۹
فیروز بهنام‌فر از تهران: ۲-۹-۱۱-۱۳-۱۴-۱۶-۱۸-۲۰
فرهاد نادریان از باختران: ۳-۴-۷-۹-۱۲-۱۳-۱۶
مهدی نجفی‌خواه دانشجوی ریاضی دانشگاه علم وصنعت: ۲-۴-۷-۱۳-۱۴
رضا فرهی‌مقدم چهارم ریاضی ازکرمان: ۲-۴-۷-۱۸
پژمان سوداگری سوم ریاضی از تهران: ۲-۳-۷-۱۱-۱۶
ارژنگ حمیدی دوم ریاضی از تهران: ۷
حسین سیارنعیمی: ۳
بهرنگ نوحی دوم ریاضی از تهران - حل همه مسائل.
علی قاسمپور دانشجو از تبریز: ۷-۱۳
ابراهیم آشوری از اراك سلطان‌آباد: ۲-۱۷
آرتا آریاپاد: ۷-۹-۱۷-۱۸
سعید عرفانیان چهارم ریاضی از مشهد: ۷-۹
وحید آقایانی دانش‌آموز ازکرج: ۲-۹
محمدعلیپور اسکندایی دانشجو از تهـران: ۳-۴-۶-۷-۸-۹-۲-۱۸-۱۹
حجت اخوان‌آذری دانش‌آموز از رشت: ۷-۱۷-۲۰
مانی حمزیان سوم ریاضی از تهـران: ۲-۳-۷-۸-۱۰-۱۳-۱۸-۱۹
علیرضا صفری‌نژاد دانش‌آموز سوم ریاضی از بندرانزلی: ۷-۹-۱۱
عیسی پیله‌ور دانشجو از تهران: ۲-۳-۴-۶-۷-۹-۱۰-۱۱-۱۶-۱۷
حمید زارع‌دوست: ۲-۷

بقیه از صفحهٔ ۴۷

باقی می‌ماند اینکه ثابت‌کنیم f هر عدد اول فرد را درست یکبار مـی‌گیرد. اثبات این با توجه به توضیحات قبل آسان است و آن را به خواننده محول می‌کنیم.

تشکر:

در تنظیم این مقاله آقای جواد لالی نکات مفیدی را تذکر داده‌اند که بدینوسیله از ایشان تشکر می‌شود.

یادداشتها

۱. Gabriel Lame

۲. H. Grossman

۳. W. Sierpinski

۴. Adrin Legender

۵. حالت‌کلی این حکم با عدد اول p بجای ۲ چنین است؛ قضیه (لژندار)، اگـر p عددی اول بـاشد، و $S(n)$ مجموع ارقام عدد طبیعی n در شمار به مبنای p، آنگاه

$$(p-1)E(p, n)=n-S(n)$$

که درآن $E(p, n)$ به معنی بستائی p است در $n!$. (برای اثبات این حکم به [۴] صفحهٔ ۳۹۸ مراجعه‌کنید.)

۶. Erathostenes

۷. AMM را برای اختصار بجای American Mathematical Monthly اختیارکرده‌ایم.

۸. Bernard Frenide de Bessy

۹. P. Poulet

۱۰. D. H. Lehmer

۱۱. N. G. W. H. Beeger

۱۲. Christian Goldbach

۱۳. J. Leech

۱۴. T. E. Littlewood

۱۵. Schnirelmann

۱۶. Yin Wen – Lin

۱۷. I. M. Vinogradov

۱۸. Renyi

۱۹ A. A. Buhstab

۲۰. Chen Ting – Yun

۲۱. Ulam

۲۲. این تعریف را با اندکـی تغییر از [۴] صفحهٔ ۷۱۹ نقل کرده‌ایم.

۲۳. P. G. L. Dirichlet

۲۴. دربارهٔ فراوانی این قبیل اعداد اول در مجموعهٔ اعداد اول به [۱] مراجعه‌کنید.

۲۵. B. M. Bredihin

۲۶. W. H. Mills

۲۷. Sin John Wilson

۲۸. Edward Waring

مراجع

[۱]. جمالی، علیرضا، **دربارهٔ اعداد اول**، مجلهٔ رشدآمـوزش ریاضی، در سال اول ـ شمارهٔ ۳ (۱۳۶۳).

[۲]. شهریاری اردبیلی، رضا، **دو قضیهٔ مشهور در حساب‌عالی**، مجلهٔ رشدآموزش ریاضی، سال اول ـ شمارهٔ ۲ (۱۳۶۳).

[۳]. لالـی، جواد، **بستائی یك عدد اول در یك عدد طبیعی**، مجلهٔ رشدآموزش ریاضی، سال اول ـ شمارهٔ ۴ [۱۳۶۳[.

[۴]. مصاحب، غـلامحسین، **تئوری مقدماتی اعداد**، جلد دوم، انتشارات سروش، اسفند ۱۳۵۸.

[۵]. وحیدی، دکتر محمد قـاسم، **ریاضیات یونانی (۱)**، مجلهٔ رشدآموزش ریاضی، سال اول ـ شمارهٔ ۳ (۱۳۶۳).

[۶]. APostol ToM M., **Introduction To Analytic Number Theory**, Springer – Verlag (1976).

[۷]. N. J.Fine,**Binomial Cofficients modulo & prime**, AMM, 54(1947)589; See also AMM, 65 (1958) 368 (Probleme E1288).

[۸]. Honsberger Ross, **Mathematical Gems** (I, II), The Mathematical Association of America (1973, 1976).

[۹]. Honsberger Ross, **Mathematical Morsels**, The Mathematical Association of America (1978).

[۱۰]. W. Sierpinski, **Theory of Numbers**, Wars Zawa (1964) 21–22.

پاسخ به نامه‌های رسیده

تنظیم از: ابراهیم دارابی

برادر جلال گلباغی دبیر دبیرستانهای رشت، مقاله شما درباره خطوط مثلثات را دریافت کردیم متأسفانه چون منبع مقاله را درج نکرده‌اید، نتوانستیم اقدامی بکنیم.

برادر حسین سیارنعیمی چهارم ریاضی. سعی کنید مسائل جالب‌تر با ذکر منابع برای ما بفرستید.

برادر محمدچکینی چهارم ریاضی. اشکال شما در مورد حل مسأله مشتق‌ازآنجا ناشی می‌شود که طبق‌فرض تنها $f'(x) = 0$ است و حال‌آنکه شما مشتق‌های بعدی را هم صفر گرفته‌اید.

در چهارضلعی‌های به اضلاع معلوم که مساحت ماکزیمم داشته باشد ... است.

برادر کاوه پیروزرام دوم ریاضی از شیراز: اثبات عکس قضیه تالس شما درست است.

برادر رحیم باقری سوم ریاضی از تهران، حل مسائل ارسالی شما را دریافت کردیم در حل مسائل بیشتر دقت کنید. مسائل شما برای درج در مجله هم به دست ما رسیده است.

برادر ارژنگ حمیدی دوم ریاضی از تهران، از تبریک شما به مناسبت ششمین سال انتشار مجله صمیمانه سپاسگزاریم.

برادر صدرالدین ابوترابی چهارم ریاضی ازتهران، مسائل شما را دریافت کردیم ازلطف شما متشکریم. زیبایی‌های اعداد شما منبع نداشت بنابراین قابل‌چاپ نبود. مسائل ارسالی شما هم درکتاب مرحوم مصاحب بنوعی وجود دارد.

برادر بهرنگ نوحی دوم ریاضی ازتهران، مسائل خودتان را مستقیماً به مجله بفرستید.

برادر محمدتقی رحمتی‌اندامی دانش‌آموز از خمینی‌شهر: شماره‌های قبلی مجله در فرصت مناسب چاپ خواهد شد. در مورد شماره‌های بعدی جوینده یابنده است!.

برادر علی‌اکبر جاویدمهر دبیر ریاضی ساوه، از خاصیت‌های شگفت‌آور ۷ و ۹ از برادر عارف سید نجفی درصورت لزوم استفاده خواهد شد.

برادر امیرحسین صبوری سوم ریاضی از مشهد، هردو نامه شما را دریافت کردیم حتی‌المقدور پیشنهاد شما را مراعات خواهیم کرد.

برادر فاضل قربانعلیان دوم ریاضی شهید باهنر دماوند، از اینکه نام شما جزء حل‌کنندگان مسائل شماره ۲۱ درج نشده متأسفیم. آدرس آقای مصحفی تهران خیابان شهید خالد اسلامبولی (پارک) مرکز نشر دانشگاهی است. در مورد منابع سؤالات المپیاد داخلی و خارجی باید گفت اخیراً چندکتاب در تهران منتشرشده است علاوه‌برآن می‌توانید به مجلات رشد مراجعه کنید.

برادر علی‌صرامی فروشانی از اهواز، امیدوارم مجله از نظر انتشار به موقع روال منطقی خود را پیدا کند. در مورد مصاحبه‌ها هم فعلاً به این کار ادامه می‌دهیم.

برادر رامبد حاجی امیری دانش‌آموز چهارم تجربی، برای محاسبه مجموع اعداد متوالی فرمول هست.

برادر کامبیز کاویانی از تهران: برای مجله نه وقت و نه امکان حل مسائل ارسالی شما است مگر اینکه مسائل شما با ذکر منبع و حل فرستاده شود و در صورت تشخیص مناسب بودن‌آنها در مجله به نام خود شما درج شود.

برادرکامبیز کاویانی: سعی می‌کنیم مطالب مجله بیشتر مورد استفاده دانش‌آموزان قرار گیرد.

برادر امیرحسین صبوری سوم ریاضی از مشهد، مسائل مثلثات جالب اگر پیدا شود چاپ می‌کنیم. فعلاً به درج مصاحبه‌ها هم ادامه خواهیم داد.

برادر روشنک (یا هوشنگ) مرحتمی دانش‌آموز سوم تجربی‌سلماز، متأسفانه رشته تجربی‌نمی‌تواند درالمپیاد ریاضی کشور شرکت کند.

برادر مهدی نجفی‌خواه دانشجوی ریاضی دانشگاه علم وصنعت، مقاله‌های خودتان را با ذکرمنابع برای مجله بفرستید تا در صورت تطبیق با شرایط مجله چاپ شود.

برادر پیام ناصرطیوب سوم ریاضی از شیراز، برای چاپ

کتابتان به ناشرین مراجعه‌کنید. فرمولهای خودتان را هم اگر مایل بودید برای مجله بفرستید.

برادر علی شاه‌علی از تهران، از ارسال حل مسأله مثلثات صمیمانه متشکریم.

برادر جمشید فلاحی دانش‌آموز سوم ریاضی از سنندج، مطلب ارسالی شما با کتاب ژرژ گاموف تطبیق داده شد. اگر عدد جفت همان عدد زوج باشد، مطلب کتاب درست نیست.

برادر امیرمعطر ازاندیمشك، از ارسال حل مسائل متشکریم درصورت لزوم ازآنها استفاده خواهیم کرد.

برادر شاهرخ مسعودی‌فر دانش‌آموز سوم ریاضی از اندیمشك، در حل مسائل بیشتر دقت کنید.

بردار علی ربیعی دانش‌آموز دوم ریاضی، حل مسأله (قضیه)ارسالی شما درست است راه حل‌های دیگری هم وجود دارد که بعضی‌ازآنها در مجله رشد چاپ شده است.

برادرکوروش جبارزاده چهارم ریاضی، در حل مسائل بیشتر دقت کنید. در فرمول ارسالی‌تان θ زاویه‌ای است که اینطور تعریف می‌شود: دایره اصلی بیضی را رسم می‌کنیم، اگر از هر نقطه بیضی عمودی بر قطر کانونی واردکنیم دایره اصلی را در نقطه‌ای مثلاً M قطع می‌کند زاویه‌ای که OM با قطر کانونی می‌سازد θ است O مرکز بیضی می‌باشد.

برادر علی دارمی ازاهواز، مقاله شما را دریافت‌کردیم چون نیاز به پاسخ‌کتبی داشت جداگانه این پاسخ را برای شما ارسال داشته‌ایم. توفیق شما را آرزومندیم.

برادر مهرداد ابوالقاسمی از تهران، آنچه درباره هندسه فضایی نوشته‌اید مطالب ساده از متن‌کتاب هندسه است و تازگی ندارد. راجع‌به هندسه غیراقلیدسی باید مطالب زیادی بخوانید تاآنگاه‌متوجه شوید‌که هندسه‌اقلیدسی‌وغیراقلیدسی‌را نمی‌توان درهم ادغام‌کرد. زیرا حکم اصل پنجم در این دو هندسه با هم مغایرت دارند.

برادر ساسان فتح‌پور سوم ریاضی‌ازاصفهان، مسائل‌ارسالی خیلی دیر به دست ما رسید.

برادر عبدالحسین‌کلهر از تهران، رسم مجله براین پایه استوار است‌که به تقاضای حل مسائل ترتیب اثر داده نمی‌شود. مسأله شما را در مجله به نام خودتان درج می‌کنیم وحل آن را از خوانندگان‌که خود نیز جزآنها هستید، می‌خواهیم. و از سایر مسائل شما درصورت لزوم استفاده خواهیم‌کرد.

برادر عباس خانمحمدی دانشجو از تهران، به نامه شما جداگانه و بطور مفصل جواب داده خواهد شد.

برادر علی دارمی تکنیسین مخابرات از اهواز، مقاله شما را دریافت‌کردیم. چون نیاز به پاسخ مشروحی داشت، جداگانه این پاسخ را برای شما ارسال داشته‌ایم.

برار محمد علیپوراسکندانی دانشجو از تهران، مقاله ارسالی شما در هیأت تحریره مطرح شد و چون مقاله شما با مقاله‌کامل‌تر دیگری فصل مشترك دارد، از چاپ‌آن معذوریم. موفقیت شما را آرزومندیم.

برادر احد مردیان دانش‌آموز رشته علوم تجربی، طرفین مساوی را نمی‌توان به صفر تقسیم‌کرد.

برادر محمدحسین‌کاظمی، چاپ مقاله شما به صورت حاضر، برای مجله مقدور نیست. از مسائل مندرج درآن در وقت مناسب استفاده خواهیم‌کرد.

برادرآرتا، آریاپاد از رشت، مسأله هندسه قابل طرح در مجله است ولی راه‌حل شما صحیح و طولانی است. هندسه اولین دانش با روش اصل موضوعی است.

برادر خ. شکوری از زنجان، خوشحالیم‌که، بالاخره به قول خودتان، بخودآمده‌اید. بنابراین مشکلات را هم پشت سرخواهیدگذاشت. با نصیحت‌کردن، آن هم در مجله ریاضی کاری درست نمی‌شود بنابراین تنها به نیروی خودتان متکی باشید.

برادر مسعود، دانش‌آموز دوم ریاضی از قم، مسائل شما دیر به دست ما رسید.

برادران سید عادل موسوی دانش‌آموزدوم‌ریاضی و پرویز ساعدی‌نیا از اهواز: نامه تکمیلی شما را هم دریافت‌کردیم.

برادر اکبر شاهین دبیر ریاضی از تبریز، از لطف‌شما متشکریم. سعی می‌کنیم نظرات شما را حدالامکان تأمین کنیم. از مسائل ارسالی شما درصورت لزوم استفاده خواهیم کرد. شماره‌های درخواستی شما تمام شده است. برای شما آرزوی توفیق داریم.

برادر افشین خاشعی دانش‌آموز دوم ریاضی از تهران، از مسائل ارسالی شما متشکریم. در مجله رشد مسائلی را درج می‌کنیم‌که در مطبوعات دیگرکشور قبلاً چاپ نشده باشد. اگر چنین مسائلی در دسترس شما باشد با ذکر منبع برای ما بفرستید.

مسائل مسابقه ریاضی دانشجویی فروردین ۱۳۶۸

فرستنده: دکتر محمدعلی شهابی
عضو هیأت علمی دانشگاه تبریز

الف ـ سؤالات آنالیز (وقت ۲ ساعت)

۱ـ فرض کنیم $f: R \rightarrow R$ انتگرال پذیر و

$$f(x+y)=f(x)+f(y)$$

برای هر x و y در R. نشان دهید برای یك عدد ثابت c، $f(x)=cx$.

۲ـ نشان دهید هرگاه a_n و b_n در R باشند و برای هرعدد طبیعی n، $(a_n+b_n)b_n \neq ۰$ و هر دو سری $\sum \frac{a_n}{b_n}$ و $\sum \left(\frac{a_n}{b_n}\right)^{۲}$ همگرا باشند، آنگاه سری $\sum \frac{a_n}{a_n+b_n}$ نیز همگرا است.

۳ـ اگر $f_n: [۰, ۱] \rightarrow R$ دنباله‌ای از توابع مشتق‌پذیر باشد به قسمتی که $\|f'_n\| \leqslant ۱$، نشان دهید که اگر برای هر تابع پیوسته $g: [۰, ۱] \rightarrow R$ داشته باشیم

$$\int_{۰}^{۱} f_n g \longrightarrow ۰$$

در این صورت دنباله توابع f_n به طور یکنواخت به صفر میل می کند.

ب ـ سؤالات جبر (مدت ۲ ساعت)

۱ـ اگر R حلقه‌ای یکدار، جابه‌جایی و نا شما را باشد، به طوری‌که برای هر ایده‌آل $I \neq ۰$ حلقه خارج قسمتی $\frac{R}{I}$ شما را باشد، آنگاه R یك حوزه صحیح است.

۲ـ R حلقه‌ای متشکل از ماتریس‌های ۲×۲ با درایه‌های گویا تحت جمع و ضرب ماتریس است ثابت کنید اگر

$$(*) \text{ برای هر } \alpha \in D، \quad \begin{pmatrix} \alpha & ۰ \\ ۰ & \alpha \end{pmatrix} \in R$$

آنگاه هر ایده‌آل چپ (یا راست) R دارای مجموعه مولد متناهی است. با یافتن یك ایده‌آل چپ در حلقهٔ

$$T=\left\{\begin{pmatrix} z & q_{۱} \\ ۰ & q_{۲} \end{pmatrix} \mid z \in Z,\ q_{۱}, q_{۲} \in D\right\}$$

که دارای مجموعه مولد متناهی نیست، نشان دهید که شرط (*) را نمی‌توان حذف کرد.

۳ـ مثالی از یك گروه G به دست آورید که حاوی اعضای a و b بوده به قسمی‌که a و b از مرتبه دو ولی ab دارای مرتبه بینهایت باشد.

۴ـ فرض کنیم $G=GL_{۲}(Z_{۳})$ (گروه ماتریس‌های ۲×۲ وارون پذیر بر میدان $Z_{۳}$) و $K=Z(G)$ مرکز گروه G باشد. قرار دهید:

$$H=\left\{\begin{pmatrix} a & b \\ ۰ & c \end{pmatrix} \mid a, b, c \in Z_{۳},\ ac \neq ۰\right\}$$

(آ) نشان دهید که $K \leqslant H \leqslant G$ و H گروهی از مرتبه ۱۲ است.

(ب) ثابت کنید

$$K=\bigcap_{x \in G} x^{-۱}Hx$$

(ج) $\frac{G}{K} \cong S_{۴}$

۵ـ $A=(a_{ij})$ ماتریس $n \times n$ی است که در آن

$$a_{ij}=\begin{cases} \delta_{i,n} & j=۱ \\ \delta_{i,j-۱} & j>۱ \end{cases}$$

فرض کنیم ξ ریشه nام واحد در C (میدان اعداد مختلط) باشد. قرار می‌دهیم

$$\vartheta(\xi)=\begin{pmatrix} ۱ \\ \xi \\ \xi^{۲} \\ \cdot \\ \cdot \\ \cdot \\ \xi^{n-۱} \end{pmatrix}$$

ثابت‌کنید $\vartheta(\xi)$ یك بردار ویژهٔ A است و مقدار ویژه نظیر آن را به دست آورید.

ج ـ معلومات عمومی (وقت ۱ ساعت)

۱ـ در دایره‌ای به شعاع واحد، یك n ضلعی منتظم محاط کرده‌ایم. نقطه‌ای مانند M روی این دایره به دلخواه اختیار کرده و مجموع مجذورات فواصل نقطه M تا رؤس n ضلعی را به دست می‌آوریم. ثابت‌کنید این مجموع مساوی $۲n$ است.

۲ـ تمام چند جمله‌ایهای با ضرایب دو، مانند $f(x)$ را پیدا کنید به قسمی‌که به ازای هر مقدار اصم x، مقدار $f(x)$ اصم باشد.

۳ـ n خط موازی درفضا موجودندکه همگی در یك‌صفحه نیستند. نشان دهیدکه دست‌کم n صفحه متمایز وجود دارد که هرکدام حداقل از دو خط از این خطوط می‌گذرند. $(n > ۲)$.

حل سؤالات آنالیز

۱ـ از طرفین $f(t+y)=f(t)+f(y)$ روی $[۰, x]$ نسبت به t انتگرال می‌گیریم. خواهیم داشت:

$$xf(y)=\int_{۰}^{x+y} f(t)dt$$

$$-\int_{۰}^{x} f(t)dt-\int_{۰}^{y} f(t)dt$$

با تبدیل x به y عبارت سمت راست تغییر نخواهدکرد ولذا $xf(y)=yf(x)$، پس برای $x \neq ۰$، $\frac{f(x)}{x}=ctc$ و ازآنجا $f(x)=cx$ و در نتیجه:

$$f(x)=xf(۱)$$

۲ـ به ازای n به قدرکافی بزرگ، $\left|\frac{a_n}{b_n}\right| < ۱$ و لذا به ازاء چنین n بزرگ،

$$\frac{a_n}{(a_n+b_n)}=a_nb_n^{-۱}\left(۱-\frac{a_n}{b_n}\right)\left(۱-\left(\frac{a_n}{b_n}\right)^{۲}\right)^{-۱}$$

$$=a_nb_n^{-۱}\left(۱-\frac{a_n}{b_n}\right)\left(۱+\sum_{k=۱}^{\infty}\left(\frac{a_n}{b_n}\right)^{۲k}\right)$$

به ازای n بزرگ، $\sum_{k=۱}^{\infty}\left(\frac{a_n}{b_n}\right)^{۲k}$ که با δ_n نشان داده می‌شود یك عددکوچك است. از این‌رو

$$\sum\frac{a_n}{(a_n+b_n)}=\sum\left(\frac{a_n}{b_n}-\left(\frac{a_n}{b_n}\right)^{۲}\right)(۱+\delta_n)$$

بنابر مفروضات و حقیقت اینکه δ_nها همگن غیر منفی‌اند و بالاخره کوچك می‌باشند، نتیجهٔ مطلوب به دست می‌آید.

۳ـ اگر حد f_n وقتی $n \to \infty$ به طور یکنواخت صفر نشود، آنگاه به ازای برخی عدد مثبت δ، برخی $x_۰$ و برخی دنبالهٔ $\{x_n\}_{n=۱}^{\infty}$، می‌توانیم فرض‌کنیم‌که $|f_n(x_n)| \geqslant \delta$ و $x_n \to x_۰$، وقتی $n \to \infty$. همچنین می‌توانیم فرض‌کنیم‌که تمامی $f_n(x_n)$ها مثبت هستند. فرمول

$$f_n(x_n)-f_n(x_۰)=\int_{x_۰}^{x_n} f_n'(x)dx$$

و نامساوی $||f_n'|| \leqslant ۱$ به ازای هر n در N برقرارند. به ازای هر n با استفاده از قضیه مقدار میانگین داریم،

$$f_n(x_n)-f_n(x_۰) \leqslant |x_n-x_۰|$$

بنابراین، اگر به‌ازای n بزرگتر از $n_۰$، $|x_n-x_۰| < \frac{\delta}{۲}$، به ازای برخی n، $f_n(x_۰) \geqslant \frac{\delta}{۲}$. فرمول انتگرال نشان می‌دهدکه به ازای x متعلق به $\left[x_۰-\frac{\delta}{۴} و x_۰+\frac{\delta}{۴}\right]$ و n متعلق به $(n_۰, \infty)$ داریم، $f_n(x) \geqslant \frac{\delta}{۴}$. در $\left(۰, \frac{\delta}{۸}\right)$، ηای هست به طوریکه:

مسائل مسابقه ریاضی دانشجویی فروردین ۱۳۶۸

$$\int_{x_{۰}-\frac{\delta}{۴}}^{x_{۰}-\frac{\delta}{۴}+\frac{\eta}{۲}} f_n(x)dx$$

$$+\int_{x_{۰}+\frac{\delta}{۴}-\frac{\eta}{۲}}^{x_{۰}+\frac{\delta}{۴}} f_n(x)dx < \delta(\delta-\eta)/۸$$

اگر g یك تابع پیوسته وخطی قطعه‌ای (Piecewise linear) باشد که توسط

$$g(x)=\begin{cases} ۱ & ،x \in \left[x_{۰}-\frac{\delta}{۴}+\frac{\eta}{۴} \text{ و } x_{۰}+\frac{\delta}{۴}-\frac{\eta}{۴}\right] \\ ۰ & ،x \notin \left[x_{۰}-\frac{\delta}{۴} \text{ و } x_{۰}+\frac{\delta}{۴}\right] \end{cases}$$

آنگاه

$$\int_{۰}^{۱} f_n(x)g(x)dx \geqslant \delta(\delta-\eta)/۸$$

به ازای n متعلق به (n, ∞) و این یك تناقض است. لذا نتیجه مطلوب حاصل می‌شود.

حل سؤالات جبر

۱ــ اول توجه می‌کنیم که هر ایده‌آل I ناشما را است. زیرا اگر

$$\frac{R}{I}=\{a_n+I\}_{n=۱}^{\infty}$$

آنگاه

$$R=\bigcup_{n=۱}^{\infty}(a_n+I)$$

حال اگر $a(\neq ۰)\in R$ و

$$I=\{r\in R : ar=۰\}\neq ۰$$

به تناقض می‌رسیم. توجه می‌کنیم که تابع

$$f: aR \longrightarrow \frac{R}{I}$$

با ضابطهٔ

$$f(ax)=x+I$$

دوسویی است. پس تناقض مورد نظر به دست می‌آید.

۲ــ گیریم S حلقهٔ کلیه ماتریسهای دو در دو برمیدان اعداد گویا باشد و زیر حلقه S متشکل از ماتریس‌های اسکالر را که با هیأت D یکریخت است با D یکی می‌گیریم. در این صورت توسیع‌های زیر را داریم:

$$D \subseteq R \subseteq S$$

امـــا S یك فضای برداری از بعد چهار بر D است، لذا $\dim_D R \leqslant ۴$. حال اگر I یك ایده‌آل چپ در R باشد آنگاه I یك زیر فضای R است و در نتیجه می‌توان اعضای $x_۱$ ، ... ، $x_۴$ در I یافت که

$$I=Dx_۱+\cdots+Dx_۴$$

واضح است که

$$I=Rx_۱+\cdots+Rx_۴$$

لذا I دارای مجموعه مولد متناهی است.

نظیر این استدلال را می‌توان در مورد ایده‌آل‌های راست در R انجام داد. اگر G زیرگروهی از D باشدآنگاه $J=\begin{pmatrix} ۰ & G \\ ۰ & ۰ \end{pmatrix}$ یك ایده‌آل چپ در T است. چنانچه G به طور متناهی تولید نشود، مثلاً G زیرگروه تولید شده توسط مجموعهٔ $\left\{\left(\frac{۱}{۲}\right)^i : i \geqslant ۰\right\}$ درنظرگرفته شود، آنگاه J نیز متناهیاً تولید نمی‌شود.

۳ــ قرار می‌دهیم

$$a=\begin{pmatrix} ۱ & ۱ \\ ۰ & -۱ \end{pmatrix} \quad \text{و} \quad b=\begin{pmatrix} ۱ & ۱ \\ ۰ & -۱ \end{pmatrix}$$

(درایه‌های حقیقی). این ماتریسها وارون پذیرند و نیز $a^۲=b^۲=e$ که e ماتریس همانی است. اینك G را گروه (ضربی) تولید شده توسط a و b می‌گیریم و تحقیق می‌کنیم (به استقرا) که به ازای هر n، $(ab)^n=\begin{pmatrix} ۱ & n \\ ۰ & ۱ \end{pmatrix}\neq e$ ، $ab=\begin{pmatrix} ۱ & ۱ \\ ۰ & ۱ \end{pmatrix}\neq e$. در نتیجه ab دارای مرتبه بینهایت

است.

۴ـ (الف) توجه می‌کنیم که

$$|G| = (۳^۲ - ۱)\,(۳^۲ - ۳) = ۸ \times ۶ = ۴۸$$

چـون $K = Z(G)$ شامل مـاتریسهای ۲ × ۲ اسکالد است. پس K فقط شامل $\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}$ و $\begin{pmatrix} ۲ & ۰ \\ ۰ & ۲ \end{pmatrix}$ بوده و لـذا، $|K| = ۲$. بنابراین واضح است که $K \leqslant H \leqslant G$. حال چون c و a فقط مـــــی‌توانند ۱ و ۲ باشند. پس به ازاء $b = ۰, ۱, ۲$ آشکارا خواهیم داشت: $|H| = ۲$.

(ب) چون $|H| = ۱۲$. پس $|G: H| = ۴$. فرض کنید،

$$X = \{g_۱H,\ g_۲H,\ g_۳H,\ g_۴H\}$$

(کــه در آن $g_۱ = e$، $g_۲$، $g_۳$ و $g_۴$ اعضـای G هستند). مجموعهٔ کـوست‌های چپ H در G باشند. G روی X بـا ضرب از چپ عمل می‌کند. یعنی به ازاء $g \in G$،

$$g(g_iH) = gg_iH \in X$$

لذا، هر $g \in G$، متناظر با نگاشت $\rho_g: X \to X$ است کـه توسط:

$$\rho_g(g_iH) = gg_iH$$

تعریف مـی‌شود، ρ_g یـك تـابع ۱ ــ ۱ است، پس ρ_g یك جایگشت روی X تعریف می‌کند، بنابراین تابع

$$\rho: G \longrightarrow S_{|X|} \cong S_۴$$

که توسط

$$\rho: g \in G \longrightarrow \rho_g$$

تعریف مـی‌شود، یك هومومورنیسم است. زیرا بـه ازاء هـر $xH \in X$، داریم:

$$P_{gg'}(xH) = (gg')xH = g(g'xH) = \rho_g\rho_{g'}(xH)$$

(ج) بنابه قضیهٔ اول ایزومورنیسم:

$$\frac{G}{\mathrm{Ker}\rho} \cong I_n\rho \leqslant S_۴$$

$$\frac{G}{K} \cong I_m\rho \leqslant S_۴$$

چون

$$|G: K| = ۲۴ = |S_۴|$$

پس

$$\frac{G}{K} \cong S_۴$$

۵ـ فرض کنید $A\vartheta(\xi)$ بردار ستونی

$$W = \begin{pmatrix} \alpha_{۱۱} \\ \alpha_{۱۲} \\ \cdot \\ \cdot \\ \cdot \\ \alpha_{i۱} \\ \cdot \\ \cdot \\ \cdot \\ \alpha_{i۱} \end{pmatrix}$$

باشد. در این صورت داریم:

$$\alpha_{i۱} = \sum_{k=۱}^{n} a_{ik}\xi^{k-۱} = a_{i۱} + \sum_{k=۲}^{n} a_{jk}\xi^{k-۱}$$

$$= \delta_{in} + \sum_{k=۲}^{n} \delta_{ik-۱}\xi^{k-۱}$$

$$= \begin{cases} ۱ & ، \quad i = n \\ \xi^i & ، \quad i < n \end{cases}$$

یعنی

$$A\vartheta(\xi) = \begin{pmatrix} \xi \\ \xi^۲ \\ \cdot \\ \cdot \\ \cdot \\ \xi^i \\ \cdot \\ \cdot \end{pmatrix} = \begin{pmatrix} \xi \\ \xi^۲ \\ \cdot \\ \cdot \\ \cdot \\ \xi^n \end{pmatrix} = \begin{pmatrix} \vdots \\ \xi \\ \cdot \\ \xi\ \cdot \\ \cdot \\ \xi^{n-۱} \end{pmatrix} = \xi\vartheta(\xi)$$

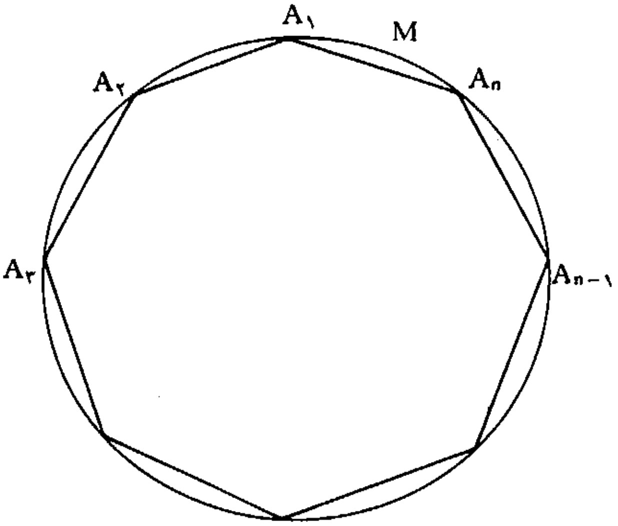
پس $\vartheta(\xi)$ بردار ویژه A با مقدار ویژهٔ ξ است.

حل سؤالات معلومات عمومی:

۱ـ رئوس را طوری بـا $A_۱$ تا A_n نامگذاری مـی کنیم

کــه نقطهٔ M روی قوس $\widehat{A_۱A_n}$ قرارگیرد قوس $\widehat{MA_۱}$ را α می‌نامیم در این صورت اندازهٔ قوس‌های

$$\widehat{MA_n} ، \dots ، \widehat{MA_۳} ، \widehat{MA_۲}$$



به ترتیب با $\alpha + \frac{۲\pi}{n}$:

$$\pi + \frac{۲(n-۱)\pi}{n} ، \dots ، \alpha + \frac{۴\pi}{n}$$

برابرند. طول هرکدام از وترهای $\overline{MA_i}$ برابر است با:

$$۲\sin \frac{\widehat{MA_i}}{۲} = ۲\sin\left(\frac{\alpha}{۲} + \frac{(i-۱)\pi}{n}\right)$$

پس مجموع مجذورات طول‌های وترهای $\overline{MA_i}$ ، $(i = ۱, ۲, \dots, n)$ عبارت است از:

$$۴\left[\sin^۲\frac{\alpha}{۲} + \sin^۲\left(\frac{\alpha}{۲} + \frac{\pi}{n}\right) + \cdots \right.$$
$$\left. + \sin^۲\left(\frac{\alpha}{۲} + \frac{(n-۱)\pi}{n}\right)\right]$$

طبق قانون تبدیل کوسینوس دو برابر قوس؛

$$= ۴\left[\frac{n}{۲} - \left\{\cos\alpha + \cos\left(\alpha + \frac{۲\pi}{n}\right) + \cdots \right.\right.$$
$$\left.\left. + \cos\left(\alpha + \frac{۲(n-۱)\pi}{n}\right)\right\}\right]$$

$$= ۲n - ۴\sin\pi\cos\left(\alpha + \frac{(n-۱)\pi}{n}\right)$$

$$\sin\frac{\pi}{n} = ۲n - ۰ = ۲n.$$

۲ــ فرض کنیم

$$f(x) = a_n x^n + a_{n-۱} x^{n-۱} + \cdots + a_۱ x + a_۰$$

چند جمله‌ای خواسته شده باشد، بدون اینکه ازکلیت مسأله کم شود می‌توان $a_n = ۱$ فرض کرد. حال اگر p یك عدد اول باشد چند جمله

$$G(x) = f(x) - a_۰ - p$$

را درنظر می گیریم. چون

$$G(۰) = -P < ۰$$

پس $G(x)$ یك ریشهٔ مثبت دارد. این ریشه باید گویا باشد پس یا ± ۱ است یا $\pm p$، اما آشکارا اگر $n > ۱$ باشد می‌توان p را آنقدر بزرگ اختیارکرد که ± ۱ و $\pm p$ ریشه‌های $G(x) = ۰$ نباشد، پس $n = ۱$ و

$$f(x) = ax + b$$

۳ــ اول نشان می‌دهیم که یك صفحه وجود داردکه فقط ازدو خط ازخطوط فوق می گذرد. برای این منظور اول این خطوط را با صفحه‌ای قطع می کنیم تا n نقطهٔ متمایز به دست آید طبق مسأله سیلوستو که درمجله رشد حل آن ارائه شد، در این صفحهٔ جدید یك خط وجود داردکه فقط از دو نقطه از این نقاط می گذرد حال این خط و دو خط موازی که آن را قطع می کنند تشکیل صفحه‌ای می‌دهدکه فقط از همان دو خط موازی می گذرد. حال برای حل مسأله از استقراء استفاده می کنیم. برای $n = ۳$ آشکار است، فرض می‌کنیم برای $(n - ۱)$ درست باشد. حال اگر n خط موازی داشته باشیم. طبق قسمت اول حل یك صفحه وجود داردکه فقط از دو خط ازاین خطوط می گذرد، حال یکی از این دوخط با $n - ۲$ خط دیگر دریك صفحه نیستند، پس طبق فرض استقراء $n - ۱$ صفحهٔ متمایز مربوط به این $n - ۱$ خط داریم که با صفحه‌ای که فقط از دو خط گذشته تشکیل n صفحه می‌دهند.

اخبار ریاضی

همانگونه که قبلاً به اطلاع رسیده است شورای برنامه‌ریزی و تالیف کتب ریاضی دبیرستانی از بهمن ماه ۱۳۶۷ تشکیل و کار تعین اهداف کلی و ریز مواد دروس (اهداف خاص) را شروع کرده است. اکنون پس از تعین و تعریف اهداف کلی آموزش ریاضی دبیرستانی ریز مواد شاخه‌های اصلی در شرف تکمیل شدن است. شورا در نظر دارد که همزمان با بیست‌ویکمین کنفراس ریاضی کشور که امسال در آخر اسفندماه در دانشگاه اصفهان تشکیل خواهد شد یک نشست و میزگرد کلی و احتمالاً کمیته‌های فرعی به منظور بحث و تبادل نظر پیرامون ریز مواد تالیف شده درحاشیه کنفراس گشایش نمایند. لذا ازعموم دبیران محترم ریاضی انتظار دارد که با شرکت در این کنفراس و نشست مذکور شورا را از نقطه نظرهای خود مطلع نمایند.

انشاءالله قبل از اجرای این پروژه (تدریس کتب جدید)، بتوانیم دوره‌ای بازآموزی با شرکت کلیه مؤلفین کتب مربوطه تشکیل بدهیم تا دبیران محترم ریاضی بتوانند با آمادگی کامل به تدریس کتب جدید بپردازند.

دبیر شورای برنامه‌ریزی
و تألیف کتب ریاضی

کتابهای جدید

مجله رشد آموزش ریاضی درنظر دارد تا درهرشماره کتب جدید الانتشار ریاضی راکه ترجمه یا تالیف شده به خوانندگان معرفی نماید. لذا ازکلیه همکاران وناشرین محترم که کتابهایی درزمینه ریاضی ترجمه (تالیف) و منتشر کرده‌اند تقاضا دارد تا جهت معرفی یك نسخه ازکتب خود را به دفتر مجله رشد ریاضی ارسال نمایند. این تصمیم بنا بر درخواست مکرر خوانندگان جهت معرفی منابع آموزشی اتخاذ شده است و هدفمان این است که خوانندگان درجریان نشر کتب ریاضی بخصوص کتب پیش دانشگاهی قرار گیرند.

۱. مسائل مسابقه‌های ریاضی مجارستان (۱)، گردآوری: یوژف کورشاك، ترجمهٔ سعید فاریابی، از سری کتابهای ریاضیات پیش دانشگاهی، ناشر: مرکز نشر دانشگاهی، ۲۵۰ ریال.

۲. مسائل مسابقه‌های ریاضی مجارستان (۲)، گردآوری: یوژف کورشاك، ترجمهٔ محمدمهدی ابراهیمی، از سری کتابهای ریاضیات پیش دانشگاهی، ناشر: مرکز نشر دانشگاهی، ۵۰۰ ریال.

۳. اعداد: گویا و گنگ، ایوان نیرن، ترجمهٔ غلامحسین اخلاقی‌نیا، از سری کتابهای پیش دانشگاهی، ناشر: مرکزنشر دانشگاهی، ۵۰۰ ریال.

(فروشگاه مرکزنشر دانشگاهی: تهران خیابان شهید اسلامبولی (پارك سابق))

افتتاح نمایشگاه و فروشگاه مدرسه

اولین نمایشگاه و فروشگاه دائمی کتابهای کمك آموزشی طی مراسمی باحضور برادران دکتر محمدعلی نجفی وزیر محترم آموزش و پرورش، دکتر اژه‌ای مشاور فرهنگی رئیس‌جمهور دکتر حداد عادل ریاست سازمان پژوهشی وجمعی از مسئولین فرهنگی کشور در تاریخ ۶۸/۷/۱۵ افتتاح شد.

افتتاح فروشگاه انتشارات مدرسه درحقیقت ادامه فعالیتهایی است که دفتر انتشارات کمك آموزشی پس از پیروزی انقلاب اسلامی از سال ۱۳۵۹ شروع کرده است.

هدف از برپایی این نمایشگاه ایجاد مرکزی برای عرضه کتابهای آموزشی، کمك آموزشی وتربیتی به جامعه فرهنگیان و مدارس کشور می‌باشد.

کتابهای ارائه شده در فروشگاه انتشارات مدرسه اولاً از نظر آموزشی و تربیتی بررسی و انتخاب شده است ثانیاً به تفکیك مقاطع تحصیلی برای دوره‌های قبل از دبستان. دبستان، راهنمایی، دبیرستان کارشناسی و تربیت‌معلم ارائه شده است.

آدرس: تهران ـ ایرانشهر شمالی جنب ساختمان شماره ۴
وزارت آموزش و پرورش

اطلاعیه

در بارهٔ نشریات رشد آموزش تخصصی

مجلات رشد آموزش مواد درسی مدارس کشور که بمنظور ارتقاء سطح دانش معلمان و ایجاد ارتباط متقابل میان صاحبنظران، معلمان و دانشجویان با برنامه‌ریزان امور درسی از سوی دفتر تحقیقات و برنامه‌ریزی و تألیف سازمان پژوهش و برنامه‌ریزی آموزشی وزارت آموزش و پرورش هر سه ماه یکبار ـــ چهار شماره در سال ـــ منتشر می‌شود در حال حاضر عبارتند از:

۱ ـــ آموزش ریاضی ۲۳
۲ ـــ آموزش شیمی ۲۱
۳ ـــ آموزش جغرافیا ۱۷
۴ ـــ آموزش ادب فارسی ۱۷
۵ ـــ آموزش زیست‌شناسی ۱۷
۶ ـــ آموزش زبان ۱۸
۷ ـــ آموزش زمین‌شناسی ۱۶
۸ ـــ آموزش فیزیک ۱۶
۹ ـــ آموزش معارف اسلامی ۵
۱۰ ـــ آموزش علوم اجتماعی ۱

دبیران، دانشجویان دانشگاهها و مراکز تربیت معلم و سایر علاقمندان به اشتراک این مجلاّت می‌توانند جهت دریافت چهار مجلّه در سال مبلغ ۴۰۰ ریال به حساب ۹۲۹ خزانه بانک مرکزی ـــ قابل پرداخت در کلیه شعب بانک ملّی ـــ واریز و فیش آن را همراه با فرم تکمیل شده زیر به نشانی تهران، جادّه آبعلی، خیابان سازمان آب بیست متری خورشید مرکز توزیع انتشارات کمک آموزشی کد پستی ۱۶۵۹۸ ـــ تلفن ۷۸۵۱۱۰ ـــ ارسال دارند. ضمناً: معلمان، کارشناسان، مدیران، پژوهشگران و سایر علاقمندان به امور تعلیم و تربیت جهت آگاهی بیشتر از یافته‌های صاحبنظران می‌توانند با پرداخت مبلغ ۸۰۰ ریال در هر سال ۴ جلد **فصلنامه تعلیم و تربیت** *دریافت نمایند.*

قابل توجه:

** شماره آخرین مجلّه منتشر شده در سمت چپ عنوان مجلّه مشخص گردیده است در صورت نیاز به مجلاّت شماره‌های پیشین درخواست خود را به آدرس مرکز توزیع ارسال تا چنانچه موجود باشد با پرداخت وجه مربوطه مجلاّت درخواستی را دریافت نمائید.*

مجلات رشدتخصصی در مراکزاستان درکتابفروشیهای زیر و سایرشهرستانها درفروشگاههای معتبرمطبوعات بصورت فروش آزاد عرضه می‌شود

تهران: کتابفروشی شهید سیدکاظم موسوی ـ اوّل خیابان ایرانشهر شمالی
اهواز: کتابفروشی ایرانپور زیتون کارمندی خیابان کمیل بین زاویه وزهره پلاک ۲۰
اصفهان: کتابفروشی مهرگان چهارباغ ابتدای سیدعلی‌خان
ارومیه: کتابفروشی زینالپورنمایندگی و خبرنگاری روزنامه
اراک: کتابفروشی گنج‌دانش بازارچه امیرکبیر
بندرعباس: کتابفروشی مالوک خیابان سیدجمال‌الدین اسدآبادی
باختران: کتابفروشی دانشمند خیابان مدرس مقابل پارکینگ شهرداری
خرم‌آباد: کتابفروشی آسیا خیابان شهدا شرقی
رشت: کتابفروشی فرهنگستان خیابان نامجوجنب دانشگاه
زنجان: کتابفروشی شهید بهشتی خیابان آیت‌ا... طالقانی
سنندج: کتابفروشی شهریار خیابان فردوسی
ساری: شرکت ملزومات و معارف خیابان انقلاب روبروی اداره برق داخل کوچه
شیراز: پیام قرآن میدان شهدا جنب اداره آموزش‌وپرورش مرکز فرهنگی
کرمان: فرهنگ‌سرای زمین پارک مطهری
مشهد: انتشارات استان قدس رضوی خیابان امام خمینی روبروی باغ ملی
یاسوج: کتابفروشی فرهنگ جنب سینما دنا خیابان شهید هرمزپور.

**** دانشجویان مرکز تربیت معلم می‌توانند با ارسال فتوکپی کارت تحصیلی خود از ۵۰٪ تخفیف برخوردار شوند.***

فرم اشتراک مجلات رشد تخصصی

اینجانب با ارسال فیش واریز مبلغ ۴۰۰ ریال، متقاضی اشتراک یکسالهٔ مجلهٔ رشد آموزش هستم.
نشانی دقیق متقاضی: استان شهرستان خیابان
کوچهٔ پلاک کُد پستی تلفن

Contents

Roshd, Magazine of Mathematical Education, Vol VI No.23, Autumn 1989 Mathematics Section, 274 BLDG - No. 4 Ministry of Education Iranshahr Shomali Ave., Tehran - Iran.

A. Publication of Ministry of Education; Islamic Republic of Iran.

قابل توجه
دبیران و
دانشجویان

آیا شما
مجلات رشد تخصصی
مخصوص دبیران و دانشجویان که
هر سه ماه یکبار در زمینه آموزش
دروس دبیرستانی منتشر می شود
را می خوانید؟