زیبایی‌هایی از اعداد اول

مهدی حسنی
دانشیار گروه ریاضی دانشگاه زنجان
mehdi. hassani@znu.ac.ir

اشاره

در این نوشتار مطالبی دربارهٔ عددهای اول ارائه می‌کنیم که با اطلاعات دورهٔ متوسطه قابل فهم و بررسی است. این مطالب عمدتاً پاسخ به پرسش‌هایی هستند که دبیران و دانش‌آموزان دربارهٔ عددهای اول از مؤلف داشته‌اند. طرح مکرر چنین پرسش‌هایی که کاملاً به‌طور طبیعی به ذهن‌ها خطور می‌کند، نشان می‌دهد که جای این مطالب در آموزش‌های مدرسه‌ای چقدر خالی است. برخی از این سؤال‌ها که در نوشتار حاضر طرح و بررسی می‌شوند، عبارت‌اند از اینکه: آیا برای هر عدد اول دلخواه، قاعدهٔ بخش‌پذیری وجود دارد، یا این پرسش که: کدام چندضلعی‌ها را می‌توان با خط‌کش و پرگار رسم کرد؟ جالب آنکه سؤال دوم هر چند ظاهری هندسی دارد، پاسخ آن در حوزهٔ عددهای اول داده می‌شود.

۱. مقدمه

مقاله را با ارائهٔ تعریفی از عددهای اول آغاز می‌کنیم. این تعریف براساس تعداد شمارنده‌های[۱] مثبت عددهای طبیعی انجام می‌شود. عددی طبیعی را که دارای دقیقاً دو شمارندهٔ مثبت باشد، «عدد اول»[۲] نامیم. مجموعهٔ این عددها را با P نشان می‌دهیم[۳] عبارت‌اند از:

$$P=\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,\ldots\}$$

عددهایی را که بیش از دو شمارندهٔ مثبت دارند، «عددهای مرکب»[۴] نامند. عدد ۱ دقیقاً یک شمارندهٔ مثبت دارد که خودش است، و لذا با طبقه‌بندی حاضر، نه اول محسوب می‌شود و نه مرکب.

اجازه دهید خیلی سریع به این پرسش که: «چرا عددهای اول مهم هستند؟» پاسخ دهیم. حکم مهمی در ریاضیات، معروف به «قضیهٔ اساسی حساب»[۵] بیان می‌کند که هر عدد طبیعی را می‌توان به‌صورت حاصل‌ضرب عددهای اول نوشت. این حکم یکی از دو قضیهٔ مهمی است که توسط **اقلیدس اسکندرانی**[۶] دربارهٔ عددهای اول بیان و اثبات شده است و تضمین می‌کند که: «عددهای اول به معنای واقعی سنگ بنای همهٔ عددهای صحیح هستند.»

دومین قضیهٔ مهم اقلیدس در خصوص عددهای اول خاتمه‌ناپذیر بودن مجموعهٔ عددهای اول را بیان و اثبات می‌کند. مسئلهٔ دیگری که در ریاضیات باستان دربارهٔ این عددها بررسی شد، تشخیص اول بودن یک عدد طبیعی (آزمون اول بودن[۷]) و غربال کردن عددهای اول از بین عددهای طبیعی بود. این کار حدود یک قرن پس از اقلیدس و توسط **اِراتُستِن**[۸]، جغرافی‌دان، ریاضی‌دان و مسئول کتابخانهٔ دانشگاه «اسکندریه»[۹] صورت گرفت.

۲. آزمون اول بودن و غربال اراتستن

اساس کارکرد غربال اراتستن و آزمون اول بودن عددها به روش اراتستن حکم زیر است.

لم ۱-۲. فرض کنید $n>1$ عددی مرکب باشد. در این صورت n عامل اولی مانند p دارد که: $p\le\sqrt{n}$.

اثبات: چون n مرکب است، می‌توان نوشت: $n=ab$ که $1<a\le b<n$. اگر داشته باشیم: هم $a>\sqrt{n}$ و هم $b>\sqrt{n}$، آن‌گاه: $n=ab>(\sqrt{n})^2=n$ که تناقض است. پس اقلاً $a\le\sqrt{n}$ یا $b\le\sqrt{n}$ خواهد بود. مثلاً فرض کنیم: $a\le\sqrt{n}$. چون: $a>1$ اختیار شده است، لذا یا اول است و یا مرکب. در هر دو صورت حتماً عامل اولی چون p دارد. عدد اول p عامل n و البته نابیشتر از $\sqrt{n}$ نیز هست. اثبات کامل است.

نتیجهٔ ۱-۲. (آزمون اول بودن اراتستن) اگر عدد $n>1$ بین تمام عددهای اول نابیشتر از $\sqrt{n}$ عامل اولی نداشته باشد، آن‌گاه اول است.

نتیجـــهٔ ۲-۲. (الگوریتم غربال اراتســـتن) می‌خواهیم از بین عددهـــای $1,2,3,...,n$ عددهای اول را غربال کنیم. برای این‌کار مراحل زیر را انجام می‌دهیم:

۱. عدد۱ را چون اول نیست، خط می‌زنیم.

۲. عدد بعدی (یعنی۲) که اول اســـت را نگـــه می‌داریم و تمام مضرب‌های آن را خط می‌زنیم.

۳. عدد بعدی (یعنی۳) که اول اســـت را نگـــه می‌داریم و تمام مضرب‌هایش را خط می‌زنیم.

این کار را تا آخرین عدد اول نابیشتر از $\sqrt{n}$ ادامه می‌دهیم. باقی عددها همگی اول‌اند و دقیقاً عددهای اول بین ۱ تا n خواهند بود.

مثال ۱-۲. می‌خواهیم تعیین کنیم که آیا ۶۴۱ اول اســـت یا مرکب؟ با مراجعه به جدولی از عددهای مربعی مشاهده می‌کنیم که: $۲۵^۲ = ۶۲۵ < ۶۴۱ < ۶۷۶ = ۲۶^۲$ پس $۲۵ < \sqrt{۶۴۱} < ۲۶$، و در نتیجه:

$$\{p \in P : p \le \sqrt{۶۴۱}\} = \{۲,۳,۵,۷,۱۱,۱۳,۱۷,۱۹,۲۳\}$$

از آنجا که هیچ‌کدام از عددهای مجموعهٔ اخیر ۶۴۱ را نمی‌شمارد، بنابر آزمون اول بودن اراتستن ۶۴۱ عددی اول است.

احتمالاً این پرســـش در ذهن خوانندهٔ کنجکاو پیش آمده است کـــه: «در مثال بالا چگونه متوجه شـــدیم که ۶۴۱ بر هیچ‌کدام از عددهای اول نابیشتر از مجذورش بخش‌پذیر نیست؟» به‌طور کلی در اجرای عملی آزمون اول بودن اراتســـتن و برخی موارد محاســـباتی دیگر، لازم اســـت بخش‌پذیری بر عددهای اول را تشخیص دهیم.

۳. قواعد بخش‌پذیری برای تمام عددهای اول

برای هر $a \in \mathbb{Z}$ قرار می‌دهیم $ud(a)$ نشانگر «رقم یکان» عدد a باشـــد. بخش‌پذیری بر ۲ و ۵ بر اساس رقم یکان قابل تشخیص است. عددی بر ۲ بخش‌پذیر است که رقم یکانش ۰،۲،۴،۶ و یا ۸ باشد. همچنین، عددی بر ۵ بخش‌پذیر است که رقم یکانش ۰ و یا ۵ باشد.۲ و ۵ تنها عددهای اولی هستند که بخش‌پذیری n بر آن‌ها تنها براساس $ud(n)$ قابل تشخیص است.

بـــا وجود آزمون‌های پراکنده برای بخش‌پذیری بر عددهای اول متفاوت، روشی واحد برای تمام آن‌ها مطلوب و مفید است. اخیراً نگارنده در مقالهٔ آموزشی- پژوهشی [۵]، روشی بازگشتی برای بخش‌پذیری بر تمام عددهای اول، به جز ۲ و ۵ ارائه داده و درستی آن را اثبات کرده است. برای تبیین این روش توجه می‌کنیم که برای تمام عددهای اول p، به جز ۲و۵ داریم: $ud(p) \in \{۱,۳,۷,۹\}$

بر همین اساس، قضیهٔ زیر بررسی بخش‌پذیری عدد طبیعی n بر p را، به بررسی بخش‌پذیری عددی کوچک‌تر از n (که غالباً یک رقم کمتر از n دارد) تحویل می‌کند.

قضیهٔ ۱-۳. فرض کنید p عددی اول به جز ۲ و ۵ است.

- اگر $ud(p) = ۱$ باشد، قرار می‌دهیم: $f(p) = \frac{p-۱}{۱۰}$.
- اگر $ud(p) = ۳$ باشد، قرار می‌دهیم: $f(p) = \frac{۷p-۱}{۱۰}$.
- اگر $ud(p) = ۷$ باشد، قرار می‌دهیم: $f(p) = \frac{۳p-۱}{۱۰}$.
- اگر $ud(p) = ۹$ باشد، قرار می‌دهیم: $f(p) = \frac{۹p-۱}{۱۰}$.

در این صورت عدد طبیعی n بر p بخش‌پذیر اســـت، اگر و تنها اگر رقم یکان n را حذف و از بقیه، $f(p)$ برابر رقم یکان n را کم کنیم، حاصل بر p بخش‌پذیر باشد.

توجه می‌کنیم که بر اساس حکم بالا، فرایند بررسی بخش‌پذیری عدد طبیعی n بر عدد اول p معادل بررسی بخش‌پذیری عددی کوچک‌تر از n بر p است. لذا با تکرار این روش بالاخره می‌توان به عددی آن‌قدر کوچک رسید که بخش‌پذیری‌اش بر p به راحتی دیده شود. مثال‌های زیر این پدیده را بیشتر روشن می‌کنند.

مثال ۱ -۳. برای $p=۱۳$ داریم: $f(۱۳)=۹$. در نتیجه «عددی بر ۱۳ بخش‌پذیر اســـت که اگر ۹ برابر رقم یکان آن‌را از باقی عدد کم کنیم، حاصل بر ۱۳ بخش‌پذیر باشد.» مثلاً برای ۸۹۷ داریم:

$۸۹-۹\times۷=۲۶$

چون ۲۶ بر ۱۳ بخش‌پذیر است، لذا ۸۹۷ نیز بر ۱۳ بخش‌پذیر است.

مثال ۲-۳. آزمون بخش‌پذیری بر عـــدد اول ۶۴۱ را بیان و به کمک این آزمون بررســـی می‌کنیم، آیا عدد ۴۲۹۴۹۶۷۲۹۷ بر ۶۴۱ بخش‌پذیر است یا خیر. برای انجام این کار توجه می‌کنیم که:

$$f(۶۴۱) = \frac{۶۴۱-۱}{۱۰} = ۶۴$$

لذا «عددی بر ۶۴۱ بخش‌پذیر است که اگر ۶۴ برابر رقم یکان آن را از باقی عدد کم کنیم، حاصل بر ۶۴۱ بخش‌پذیر باشد.» با اعمال مکرر این قاعده بر عدد ۴۲۹۴۹۶۷۲۹۷ نتیجه می‌شود:

$۴۲۹۴۹۶۷۲۹-۷\times۶۴=۴۲۹۴۹۶۷۲۹-۴۴۸=۴۲۹۴۹۶۲۸۱$

$۴۲۹۴۹۶۲۸-۱\times۶۴=۴۲۹۴۹۶۲۸-۶۴=۴۲۹۴۹۵۶۴$

$۴۲۹۴۹۵۶-۴\times۶۴=۴۲۹۴۹۵۶-۲۵۶=۴۲۹۴۷۰۰$

$۴۲۹۴۷۰-۰\times۶۴=۴۲۹۴۷۰-۰=۴۲۹۴۷۰$

$۴۲۹۴۷-۰\times۶۴=۴۲۹۴۷-۰=۴۲۹۴۷$

$۴۲۹۴-۷\times۶۴=۴۲۹۴-۴۴۸=۳۸۴۶$

$۳۸۴-۶\times۶۴=۳۸۴-۳۸۴=۰$

و چون ۰ بر ۶۴۱ بخش‌پذیر اســـت، لذا ۴۲۹۴۹۶۷۲۹۷ نیز بر ۶۴۱ بخش‌پذیر است (توجه کنید که: $۴۲۹۴۹۶۷۲۹۷ = ۲^{۳۵} + ۱$).

۴. روش تجزیهٔ عددهـــای بزرگ و آزمون اول بودن فرما

بخش‌پذیـــری بر عددهای اول، علاوه بر کاربردش در آزمون اول بودن اراتستن، در اجرای عملی قضیهٔ اساسی حساب نیز مفید

است؛ یعنی زمانی که بخواهیم عدد طبیعی داده شده را به حاصل‌ضرب عددهای اول تجزیه کنیم. با این حال، اگر عوامل اول عددی که قرار است تجزیه شود، بزرگ باشند، کار تجزیه دشوار می‌شود.[10] در چنین مواردی اگر بتوان عدد داده شده را به ضرب عوامل کوچک‌تر (نه لزوماً اول) تجزیه کرد، می‌توان اندکی از پیچیدگی کار کاست. «روش فرما»[11] برای تجزیهٔ عددهای بزرگ در این مورد می‌تواند مفید باشد. اساس بررسی درستی روش و کارکرد آن اتحاد مزدوج است.[12]

لم۱-۴. فرض کنید n عددی فرد باشد. در این صورت n را می‌توان به دو عامل (نه لزوماً اول) تجزیه کرد، اگر و تنها اگر بتوان n را به‌صورت تفاضل دو مربع نوشت.

اثبات: اگر n را به دو عامل (نه لزوماً اول) تجزیه کرده باشیم، می‌توان نوشت: $n=ab$. با استفاده از اتحاد مربع جمع و تفاضل دو جمله داریم:

$$n = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$$

و البته حواسمان هست که چون هر دوی a,b فردند، لذا $a \pm b$ هر دو زوج‌اند. برعکس، اگر بتوان n را به صورت تفاضل دو مربع نوشت، آن‌گاه داریم: $n=x^2-y^2$ و در نتیجه: $n=(x-y)(x+y)$، و لذا n را می‌توان به دو عامل (نه لزوماً اول) تجزیه کرد.

نتیجهٔ ۱-۴. (روش فرما برای تجزیهٔ عددهای بزرگ): این روش براساس لم بالا کار می‌کند. به این صورت که طبق لم، اگر بتوانیم n را به صورت $n=x^2-y^2$ بنویسیم، تجزیه انجام شده است. چون: $x^2 - n = y^2 \geq 0$، لذا: $x \geq \sqrt{n}$. اگر: $x > \sqrt{n}$ آن‌گاه n مربع کامل است و $n = \sqrt{n} \times \sqrt{n}$ تجزیه‌ای برای n. اگر: $x > \sqrt{n}$ آن‌گاه x را مقادیر صحیح بزرگ‌تر از $\sqrt{n}$ قرار می‌دهیم و مقدار $x^2 - n$ را محاسبه می‌کنیم. هر زمان که به عددی مربع کامل مانند y^2 رسیدیم، کار تمام شده است.

نکتهٔ مهم در روش بالا این است که نهایتاً به ازای $x = \frac{n+1}{2}$، در $y = \frac{n-1}{2}$ به عدد مربع کامل می‌رسیم؛ چون همواره داریم:

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

در واقع اگر در حالت مرزی بالا به مربع کامل برسیم، آن‌گاه تجزیهٔ مربوط به صورت $n=n\times 1$ خواهد بود که نشان از اول بودن n دارد. این حقیقت را به صورت رسمی‌تر در زیر بیان می‌کنیم.

به نظر می‌رسد، یکی از انگیزه‌های فرما برای ابداع روش تجزیهٔ عددهای بزرگ تجزیهٔ عدد ۴۲۹۴۹۶۷۲۹۷ بوده است.

نتیجهٔ ۲-۴. (آزمون اول بودن فرما): فرض کنید n عددی فرد باشد و برای تمام عددهای طبیعی x، با شرط $\sqrt{n} \leq x < \frac{n+1}{2}$ تفاضل x^2-n مربع کامل نباشد. در این صورت n عددی اول است.

مثال ۱-۴. برای تجزیهٔ $n= ۲۵۷۲۸۰۷$ به روش فرما مشاهده می‌کنیم که:

$۱۶۰۳ < \sqrt{n} \leq ۱۶۰۴$

با قرار $x=۱۶۰۴$ می‌بینیم: $x^2-n=9=3^2$ که مربع کامل است. لذا:

$n=۱۶۰۴^2-۳^2=۱۶۰۱\times ۱۶۰۷$

هر دو عامل به دست آمده اول هستند و همان‌طور که می‌بینید، بسیار به هم نزدیک‌اند. به همین سبب روش به سرعت به انتها رسید. موارد زیر نیز از همین قبیل هستند:

$۲۰۲۱=۴۳\times ۴۷$

$۲۳۱۰۳۷=۴۶۳\times ۴۹۹$

مثال ۲-۴. در مقایسه با نمونه‌های بالا، حال $n=۱۳۹۱$ را در نظر می‌گیریم که عدد نسبتاً کوچک‌تری است. داریم: $۳۷ < \sqrt{n} \leq ۳۸$، و لذا الگوریتم از $x=۳۸$ با محاسبهٔ $x^2-۱۳۹۱$ آغاز می‌شود. پس از محاسبات طولانی (و طی بیش از بیست مرحله) می‌بینیم که بالاخره برای $x=۶۰$ تفاضل مذکور مربع کامل می‌شود. در واقع داریم: $۶۰^2-۱۳۹۱=۴۷^2$. در نتیجه:

$۱۳۹۱=۶۰^2-۴۷^2=۱۳\times ۱۰۷$

هر دو عامل به دست آمده عددهای اول‌اند و البته از هم دورند. به همین علت روش پس از طی مراحل بسیار به انتها رسید. این وضع دربارهٔ عددهای اول بدتر نیز می‌شود. لذا بررسی اول بودن عددها به روش فرما مستلزم محاسبات طولانی است و در عمل کاربردی نیست.

۵. عددهای اول فرما

به نظر می‌رسد، یکی از انگیزه‌های فرما برای ابداع روش تجزیهٔ عددهای بزرگ که در بخش قبل شرح دادیم، تجزیهٔ عدد ۴۲۹۴۹۶۷۲۹۷ بوده است. این عدد متعلق به دستهٔ خاصی از عددهاست که بعدها عددهای فرما نام گرفتند. حکم زیر خاستگاه اولیه این عدد را تشریح می‌کند.

لم۱-۵. فرض کنید $a,m>۱$ و $a^m+۱$ عددی اول باشد. در این‌صورت a عددی زوج است و داریم: $m=۲^n$ که در آن: $n \in \mathbb{N}$.

اثبات: توجه می‌کنیم که: $a^m+۱ \geq ۲^2+۱=۵$. اگر a فرد باشد،

آن‌گاه a^m فرد و لذا a^m+1 زوج است، و این با فرض اول بودنش مغایرت دارد. پس a باید زوج باشد. دربارهٔ m، اگر به شکلی که ادعا شده است نباشد، آن‌گاه لزوماً دارای عامل فردی چون $s \geq 3$ است؛ یعنی: $m=ns$. در نتیجه:

$$a^m+1=a^{ns}+1=(a^n+1)(a^{n(s-1)}+a^{n(s-2)}+\ldots-a^n+1)$$

از آنجا که $s \geq 3$، لذا هر دو عامل در تجزیهٔ بالا بزرگ‌تر از واحدند و این با فرض اول بودن a^m+1 در تناقض است. بنابراین m عامل فردی نداشته و به شکل $m=2^n$ است که در آن: $n \in \mathbb{N}$. اثبات کامل است.

ساده‌ترین انتخاب برای a در لم بالا $a=2$ است. در این صورت ممکن است عددهای به شکل $2^{2^n}+1$ اول باشند. فرما بررسی اول بودن این عددها را که بعدها با F_n نشان داده شدند، آغاز کرد. در جدول ۱ مقادیر آغازین $F_n=2^{2^n}+1$ را محاسبه کرده‌ایم. فرما توانست اول بودن همهٔ F_nهای مذکور در جدول را، به جز F_5، اثبات کند. وی در مکاتباتش با برخی ریاضی‌دانان معاصرش، از جمله **پاسکال**[13]، ادعا کرد که تمامی عددهای تولید شده توسط رابطهٔ F_n برای $n \geq 0$ اول‌اند.

جدول ۱. اعداد فرما که پنج‌تای نخست اول‌اند

n	۰	۱	۲	۳	۴	۵
F_n	۳	۵	۱۷	۲۵۷	۶۵۵۳۷	۴۲۹۴۹۶۷۲۹۷

دیری نپایید که **اویلر**[14] ثابت کرد F_5 اول نیست و حدس فرما را رد کرد. با توسعهٔ تحقیقاتش در این زمینه، اویلر در حالت کلی‌تر ثابت کرد که اگر F_n بر عدد اول p بخش‌پذیر باشد، آن‌گاه داریم: $p=2^{n+2}k+1$ که در آن: $k \in \mathbb{N}$. با استفاده از همین واقعیت، او مرکب بودن عددهای فرمای F_{9448} و F_{23471} را نیز ثابت کرد. توجه کنید که عددهای فرما به سرعت رشد می‌کنند و بزرگ می‌شوند، و لذا بررسی اول بودنشان بسیار دشوار است. با این‌حال آزمون اول بودن ویژه‌ای برای این عددها، موسوم به«آزمون پپین[15]»، ابداع شده است که تا حدی کار را راحت می‌کند. در زیر اثباتی آسان برای مرکب بودن F_5 می‌آوریم. این اثبات تنها از اتحاد مزدوج استفاده می‌کند، و لذا نمونه‌ای جالب از استدلالی است که در آن استفادهٔ معنادار از اتحادهای دبیرستانی صورت گرفته است.

گزارهٔ ۱-۵. عدد $F_5=2^{2^5}+1=4294967297$ بر ۶۴۱ بخش‌پذیر است.

اثبات: قرار می‌دهیم: $a=2^7$ و $b=5$. داریم: $1+ab=641$ و $1+ab-b^4=2^4$. بنابراین، بدون محاسبهٔ مستقیم F_5 می‌توان نوشت:

$$\begin{aligned}
F_5 &= 2^{2^5}+1=2^{32}+1=(2^8)^4+1=(2a)^4+1\\
&=2^4a^4+1=(1+ab-b^4)a^4+1=(1+ab)a^4+(1-a^4b^4)\\
&=(1+ab)a^4+(1-a^2b^2)(1+a^2b^2)\\
&=(1+ab)a^4+(1-ab)(1+ab)(1+a^2b^2)\\
&=(1+ab)(a^4+(1-ab)(1+a^2b^2))\\
&=(1+ab)(a^4-a^3b^3+a^2b^2-ab+1)
\end{aligned}$$

در نتیجه $1+ab=641$ عاملی اول برای F_5 است.

توجه کنید که در مثال ۲-۳، بخش‌پذیری F_5 بر ۶۴۱ را ثابت کردیم. این زمانی محقق شد که می‌دانستیم ۶۴۱ عامل اولی برای F_5 است، در حالی که در گزارهٔ بالا با تکنیک‌های ساده‌ای این عامل را برای F_5 استخراج کردیم. مضاف بر اینکه در انتهای اثبات، عامل دیگر F_5، یعنی:

$$a^4-a^3b^3+a^2b^2-ab+1=6700417$$

به دست آمد که آن هم عددی اول است. بنابراین:

$$F_5=2^{2^5}+1=641\times 6700417$$

محاسبه‌های رایانه‌ای نشان می‌دهند که:

$$\begin{aligned}
F_6 &= 2^{2^6}+1=2^{64}+1\\
&=18446744073709551617\\
&=274177\times 67280421310721\\
F_7 &= 2^{2^7}+1=2^{128}+1\\
&=340282366920938463463374607431768211457\\
&=59649589127497217\times 5704689200685129054721
\end{aligned}$$

هر چند اویلر حدس فرما مبنی بر اول بودن تمامی جمله‌های دنبالهٔ $(F_n)_{n\geq 0}$ را رد کرد، اما وضعیت این حدس بدتر از آن بود که تصور می‌شد؛ به‌طوری که با وجود توسعهٔ روش‌ها و ابزار محاسبه‌ها، تا به امروز هیچ عدد اول فرمایی به جز همان‌هایی که خود فرما تشخیصشان داد، پیدا نشده است. به موازات پیشرفت ماشین‌های محاسبه، تلاش‌ها در این حوزه با ارائهٔ الگوریتم‌های کارآمدتر کماکان ادامه دارد.

اما چرا؟ اول بودن عددهای فرما چه فایده‌ای دارد؟ برای پاسخ به این سؤال لازم است به یک مبحث هندسی وارد شویم. ارتباط فوق‌العادهٔ بین این بحث شیرین هندسی با حدس فرما و عددهای اولش، نمونه‌ای از ریاضیات توسعه‌یافتهٔ امروزی است که جزئیات آن را در انتهای اغلب کتاب‌های دانشگاهی در حوزهٔ جبر مجرد می‌توان یافت.

۶. چند ضلعی‌های منتظم ترسیم‌پذیر

بخش قابل توجهی از کتاب «اصول» **اقلیدس** به اجرای عملی ترسیم شکل‌های هندسی اختصاص دارد. ابزار مجاز برای این کار، که به ابزارهای اقلیدسی معروف‌اند، عبارت است از پرگار و «سَطّاره» (یا سَتّاره). ستّاره در متن‌های ریاضی قدیمی‌تر فارسی

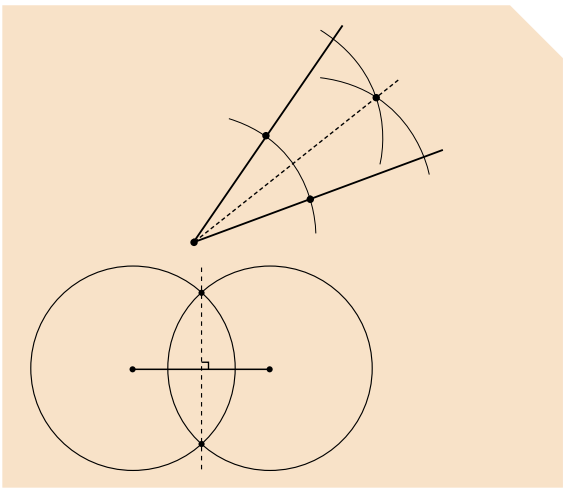
و عربـــی به معنای خط‌کش نامدرج، یعنی ابزاری که تنها با آن می‌توان خط راســـت کشـــید و نه اندازه‌گیری کرد، آمده است. پرگارهای اقلیدسی «فروریزنده» فرض می‌شوند؛ یعنی با برداشتن یک ساق آن از روی کاغذ فرو می‌ریزد. با این‌حال قضیهٔ ۲ از مقالهٔ نخست اصول اقلیدس نتیجه می‌دهد که ستّاره و پرگار اقلیدسی با ستّاره و پرگارهای امروزی که فروریزنده نیستند، معادل‌اند. با اســـتفاده از خط‌کش غیرمدرج و پرگار می‌توان ترسیمات زیر را انجام داد:

۱. ترسیم عمود منصف بر پاره‌خط مفروض (مثلاً به طریق نشان داده شده در نمودار «پایین» شکل ۱).

۲. ترسیم نیم‌ساز زاویهٔ مفروض (مثلاً به طریق نشان داده شده در نمودار «بالا» شکل ۱).

۳. ترسیم خط عمود بر خطی مفروض از نقطه‌ای مشخص خارج از آن.

۴. ترسیم خط موازی با خطی مفروض از نقطه‌ای مشخص خارج از آن.



شکل۱. ترسیم نیم‌ساز زاویه (بالا) و ترسیم عمودمنصف (پایین)

با به کار بســـتن ترسیمات مقدماتی شکل۱، ترسیم سه ضلعی منتظم (مثلث متساوی‌الاضلاع) و چهار ضلعی منتظم (مربع) با استفاده از خط‌کش غیرمدرج و پرگار کار دشواری نیست. سؤالی که به‌طور طبیعی به ذهن می‌رســـد، این است که: آیا می‌توان با خط‌کش غیرمدرج و پرگار، پنج‌ضلعی منتظم نیز رسم کرد؟ پاسخ این پرسش مثبت است، و روش‌های متعددی برای اجرای آن وجود دارد. یکی از این روش‌ها که بیان ساده‌ای دارد، منتسب به **ریچموند**[۱۶] است.

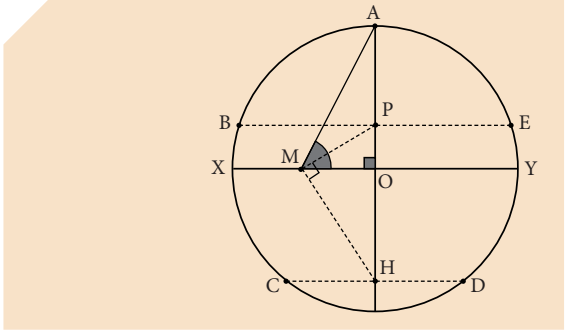
۱-۶. روش ریچموند برای ترسیم پنج‌ضلعی منتظم

این روش را براســـاس شکل۲ توضیح می‌دهیم. نقطهٔ A را روی دایره به مرکز O مشـــخص می‌کنیم. قطر AZ را گذرا از A و

بررسی پراکندگی و توزیع عددهای اول بین عددهـــای طبیعی، موضوع مطالعهٔ بسیاری از ریاضی‌دانان بوده است.

همچنین قطر XY را قائم بر AZ می‌کشیم. M را نقطهٔ وسط شـــعاع OX انتخاب و A را به M وصل می‌کنیم. نیم‌ساز زاویهٔ AMO را رســـم می‌کنیم و امتداد می‌دهیم تا شعاع OA را در نقطهٔ P قطع کند.

همچنین خطی عمود بر MP رسم می‌کنیم تا شعاع OZ را در نقطهٔ H قطع کند. حال خطوط گذرا از نقطه‌های P و H و موازی قطر XY را رســـم می‌کنیم تا دایره را به ترتیب در نقطه‌های B و E، و همچنیـــن C و D قطع کنند. پنج نقطهٔ A، B، C، D و E رأس‌های یک پنج ضلعی منتظم هستند.



شکل۲. روش ریچموند برای ترسیم پنج‌ضلعی منتظم

مسلماً با نیم‌ســـاز کردن زاویه‌های مرکزی هر n ضلعی منتظم رسم شـــده می‌توان به یک ۲n ضلعی منتظم رسید. به همین ترتیب می‌توان به ۴n ضلعی منتظم، ۸n ضلعی منتظم، ۱۶n ضلعی منتظم، و به طور کلی به یک $2^k n$ ضلعی منتظم رسید $(k \geq 0)$.

بنابراین، چون رسم مربع را در اختیار داریم، می‌توانیم هر 2^{k+2} ضلعی منتظم $(k \geq 0)$ را با اســـتفاده از خط‌کـــش غیرمدرج و پرگار ترسیم کنیم. همچنین، چون مثلث متساوی‌الاضلاع را رسم کرده‌ایم، می‌توانیم با نیم‌ســـاز کردن زاویه‌های مرکزی دایرهٔ محاطی‌اش به ۶ ضلعی منتظم، ۱۲ ضلعی منتظم، ۲۴ ضلعی منتظم، و به‌طور کلی به یک 3×2^k ضلعی منتظم رسید $(k \geq 0)$.

وضعیت مشـــابهی دربارهٔ ۵ ضلعی منتظم، ۱۰ضلعی منتظم، ۲۰ ضلعـــی منتظم، و به‌طور کلـــی برای هر 5×2^k ضلعی منتظم $(k \geq 0)$ برقرار اســـت. سؤال اساسی در اینجا این است که: «کدام nضلعی‌های منتظم را با اســـتفاده از خط‌کـــش غیرمدرج و پرگار می‌توان ترسیم کرد؟»

اگر فرایند نیم‌ساز کردن زاویه‌های مرکزی دایرهٔ محاطی و رسیدن به دو برابر اضلاع را بدیهی انگاریم، ســـؤال پایه‌ای‌تر این‌اســـت که: برای nهای فرد کدام nضلعی‌های منتظم را با اســـتفاده از خط‌کش غیرمدرج و پرگار می‌توان ترسیم کرد؟

۲-۶. طبقه‌بندی چندضلعی‌های منتظم ترسیم‌پذیر

همان‌طور که در بالا اشاره کردیم، تاکنون هیچ عدد اول فرمایی به جز همان‌هایی که خود فرما تشخیصشان داده بود، پیدا نشده است. حال می‌توان به این پرسش پرداخت که اول بودن عددهای فرما چه فایده‌ای دارد؟ پاسخ این سؤال را **گاوس**[17] با به دست آوردن شرط کافی برای ترسیم‌پذیری ارائه کرد. کار وی توسط ریاضی‌دان کمتر شناخته شدهٔ فرانسوی به نام **ونزل**[18] با اثبات لازم بودن شرط ارائه شده توسط گاوس برای ترسیم‌پذیری تکمیل شد. در واقع، احکام گاوس و ونزل دربارهٔ چندضلعی‌های منتظم ترسیم‌پذیر با خط‌کش غیرمدرج و پرگار، جانی دوباره به حدس‌فرما بخشید.

قضیهٔ ۱-۲-۶. (گاوس- ونزل) تنها آن دسته از n ضلعی‌های منتظم ترسیم‌پذیر با خط‌کش غیرمدرج و پرگار هستند که $n=2^{k+2}$ و یا $n=2^k q_1 q_2 \dots q_r$ باشد که در آن: $k \geq 0$ و q_j ها عددهای اول فرمای متمایز هستند.

توضیح اینکه چگونه یک مسئلهٔ ترسیمی، با خانوادهٔ خاصی از عددهای اول مرتبط می‌شود، به مفاهیمی نیاز دارد که خارج از سطح این مقاله است. آنچه که می‌توان اشاره کرد این است که این حکم جالب، در کنار حکم‌های مربوط به سه مسئلهٔ معروف ریاضیات یونان باستان، در پی «مجردسازی» مفاهیم مربوط به ترسیمات هندسی حاصل شده است. مجردسازی مفاهیم ترسیم یعنی آزاد کردن امر ترسیم از اجرای عملی آن و مربوط کردنش به مفاهیمی از ریاضیات که می‌توان بر اساس آن‌ها، برای امکان یا عدم امکان ترسیم برهان ریاضی اقامه کرد. به همین دلیل حکم بالا فقط یک طبقه‌بندی از چندضلعی‌های منتظم ترسیم‌پذیر با خط‌کش غیرمدرج و پرگار ارائه می‌دهد، و مطلقاً هیچ راهکار عملی برای ترسیم آن چند ضلعی‌ها روی صفحهٔ کاغذ ارائه نمی‌کند. به دست آوردن راهکار عملی برای ترسیم چندضلعی‌هایی که امکان رسمشان وجود دارد، کاری است از جنس روش ریچموند برای ترسیم پنج‌ضلعی منتظم که براساس ترفندهای هندسه و مثلثات حاصل می‌شود. این کار برای تعدادی از چندضلعی‌های منتظم ترسیم‌پذیر، از جمله ۱۷، ۲۵۷ و ۶۵۵۳۷ ضلعی‌های منتظم انجام شده است که البته بسیار پیچیده هستند.

همان‌طور که گفتیم تا به امروز تنها عددهای اول فرمای شناخته شده ۳، ۵، ۱۷، ۲۵۷ و ۶۵۵۳۷ هستند و مشخص نیست آیا عدد فرمای اول دیگری وجود دارد یا خیر. هر چند تحقیقات انجام شده در این زمینه مشخص کرده است که به احتمال قوی تنها عددهای اول فرمای شناخته شده همین پنج عدد هستند. لذا در حال حاضر، پاسخ این سؤال پایه‌ای‌تر که برای nهای فرد، کدام n ضلعی‌های منتظم را با استفاده از خط‌کش غیرمدرج و پرگار

عددهای اول سرشار از شگفتی‌ها و اسرار سر به مُهر هستند. صحبت از عددهای اول برای همهٔ سطوح دانش‌آموزان مقدور، و رسیدن به مرزهای حل نشده در آن به سرعت قابل حصول است.

می‌توان ترسیم کرد، عبارت است از اینکه: «عددهای مذکور و حاصل ضرب‌های متفاوت آن‌ها با عوامل متمایز»؛ که جمعاً ۳۱ عدد می‌شوند. تعدادی از عددهای مزبور از این قرارند

$$3(=F_0),5(=F_1),17(=F_2),$$
$$257(=F_3),65537(=F_4),$$
$$15(=F_0F_1),51(=F_0F_2),\dots$$
$$168430090(=F_2F_4),$$
$$255(=F_0F_1F_2),3855(=F_0F_1F_3)\dots,$$
$$2863311153(=F_2F_3F_4),$$
$$65535(=F_0F_1F_2F_3),16711935(=F_0F_1F_2F_4)\dots,$$
$$1431655765(=F_1F_2F_3F_4),$$
$$4294967295(=F_0F_1F_2F_3F_4).$$

دقت کنید که مثلاً نمی‌توان ۳×۳=۹ یا ۵×۵=۲۵ ضلعی‌های منتظم را با استفاده از خط‌کش غیرمدرج و پرگار رسم کرد. متمایز بودن عوامل در حکم گاوس- ونزل الزامی است.

۷. نتیجه‌گیری و جمع‌بندی

بررسی پراکندگی و توزیع عددهای اول بین عددهای طبیعی، موضوع مطالعهٔ بسیاری از ریاضی‌دانان بوده است. شکل۳ توزیع عددهای اول در فاصلهٔ ۱ تا ۲۰۰۰۰ را نشان می‌دهد. در این تصویر، فاصله‌های بین عددهای اول متوالی و رخنه‌های بین آن‌ها دیده می‌شود. زوج‌هایی از عددهای اول را که تنها یک واحد رخنه بینشان وجود دارد، «دوقلوهای اول»[19] می‌نامند. چند دوقلوی اول آغازین عبارت‌اند از:

$$(3,5),(5,7)(11,13),(17,19),(29,31),$$
$$(41,43),(59,61),(71,73),(101,103)$$

یکی از پرسش‌های عمیق این است: آیا نامتناهی دوقلوی اول وجود دارد؟ حدس زده می‌شود که پاسخ این سؤال مثبت باشد. این حدس را «حدس عددهای اول دوقلو» می‌نامند. این حدس دربارهٔ «تکرار تمام نشدنیِ فاصلهٔ حداقلی بین عددهای اول» است. حدس عددهای اول دوقلو می‌گوید که این مقدار حداقلی باید ۲ باشد. یکی از آخرین دستاوردهای بسیار مهم در این زمینه که حاصل کار گروهی جمعی از برجسته‌ترین ریاضی‌دان‌هاست، تأیید مقدار حداقلی ۲۴۶ است.

از این قبیل حقایق در داستان عددهای اول فراوان وجود دارد؛ از

جمله «حدس **گلدباخ**»[20]، «حدس **ریمان**»[21] و موارد بسیاری که سال‌ها فکر ریاضی‌دان‌ها را به خود مشغول کرده است. مسلماً بیـــان این حقایق در شـــنوندهٔ علاقه‌مند هیجان علمی به‌وجود می‌آورد و همین هیجان می‌تواند در وی شوق و علاقه ایجاد کند. عددهای اول سرشـــار از شگفتی‌ها و اسرار سر به مُهر هستند. صحبت از عددهای اول برای همهٔ ســـطوح دانش‌آموزان مقدور، و رســـیدن به مرزهای حل نشده در آن به سرعت قابل حصول است. آنچه در این مقاله ارائه شد، بخشی از سخنرانی‌های نگارنده در جمع معلمان و دانش‌آموزان بود. گاهی بین همین جلســـات بحث‌های مفیدی صورت گرفته‌اند؛ مانند قواعد بخش‌پذیری برای تمام عددهای اول که در بخش ۳مقاله ارائه شد.

پی‌نوشت‌ها

۱. شمارنده یا مقسوم‌علیه هر عدد صحیح n عددهایی هستند که n بر آن‌ها بخش‌پذیر است. مقسوم‌علیه می‌تواند مثبت یا منفی باشد. در این مقاله منظور ما از شمارنده یا مقسوم‌علیه، شمارنده‌های مثبت است.

2. Prime Number

۳. نماد P برگرفته از کلمهٔ «prime» است.

4. Composite Number

5. Fundamental Theorem of Arithmetic

6. Euclid of Alexandria (325 BC-265 BC)

7. Primality Test

8. Eratosthenes of Cyrene (276 BC-194 BC)

۹. اسکندریه شهر بندری مهم مصر واقع در شمال غرب دلتای رود نیل است. نام شـــهر از نام **اسکندر مقدونی** گرفته شـــده است که پس از فتوحاتش دستور ساخت این شهر را داده بود. پس از مرگ اسکندر و تجزیهٔ امپراتوری او، در حدود سال ۳۰۶ق.م **بطلمیوس** حاکم مصر شد و اسکندریه را به عنوان پایتخت انتخاب کرد و برای جلب دانشـــمندان به شهر خود، دستور ساخت دانشگاه اسکندریه را صادر کرد. دانشگاه در حدود سال ۳۰۰ ق.م افتتاح شد و شـــروع به جذب استاد و پذیرش دانشجو کرد. اغلب استادان از آتن جذب شـــدند. **اقلیدس** به‌عنوان رئیس بخش ریاضی انتخاب شـــد و شروع به کار کرد. مهم‌ترین قسمت دانشـــگاه کتابخانهٔ آن بود که در حدود ۴۰ سال پس از تأسیســـش، بیش از ۶۰۰ هزار طومار پاپیروس در خود داشته است! امروزه تعداد انگشت‌شـــماری از این پاپیروس‌ها باقی مانده‌اند که مهم ترین آن‌ها با محتوای ریاضی،«پاپیروس رایند» و «پاپیروس مسکو» نام دارند.

۱۰. هرچند همین دشواری هم در ریاضیات مفید شناخته می‌شود، زیرا مبنای ســـاخت و طراحی برخی از سیستم‌های امنیتی رمزنگاری است. در واقع، هر قدر تجزیه دشوارتر باشد، کلیدرمز ساخته شده بر پایهٔ آن امن‌تر خواهد بود، و این یعنی تبادل پیام‌ها و اطلاعات در امنیت انجام می‌شود.

11. Pierre de Fermat (1601-1665)

۱۲. اتحاد مزدوج بیان می‌کند که برای تمامی عددهای حقیقی a و b داریم:

$$a^۲ - b^۲ = (a-b)(a+b)$$

. این البته حالت خاصـــی از اتحاد مزدوج اصلی است که بیان می‌کند: برای هر $n \in \mathbb{N}$ داریم:

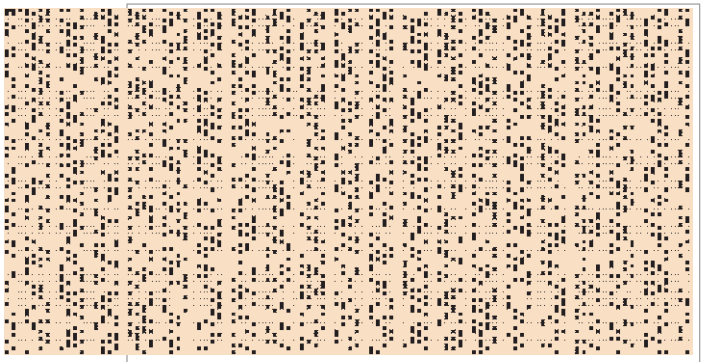
$$a^n - b^n = (a-b)(a^{n-۱} + a^{n-۲}b + a^{n-۳}b^۲ + \ldots + a^۲b^{n-۳} + ab^{n-۲} + b^{n-۱})$$

13.Blaise Pascal (1623-1662).

14.Leonhard Euler (1707-1783)

15.Pépin's Primality Test

16.Herbert William Richmond (1863-1948)



شـــکل ۳. توزیع عددهای اول در فاصلهٔ ۱ تا ۲۰۰۰۰. در این تصویر برای عددهای طبیعی خانه‌هایی مربعی در یکصد سطر دویست‌تایی با شروع از گوشـــهٔ بالا چپ و به سمت راست چیده شده‌اند. در مواضع عددهای اول خانهٔ سیاه و در مواضع عددهای مرکب سفید رنگ‌آمیزی شده است. عدد ۱ که نه اول است و نه مرکب با رنگ قرمز نشان داده شده است.

17.Johann Carl Friedrich Gauss (1777-1855)

18. Pierre Laurent Wantzel (1814-1848)

19.Twin Primes

20.Goldbach Conjecture

21.The Riemann Hypothesis

منابع

[1]D. M. Burton, *Elementary number theory* (Sixth Edition), McGraw-Hill, 2007.

[2] L. E. Dickson,*History of the theory of numbers*Vol. I: Divisibility and primality.Chelsea Publishing Co., 1966.۱۵

[3]H. *Eves,An introduction to the history of mathematics* (Sixth edition. With cultural connections by Jamie H. Eves), Saunders Series. Saunders College Publishing, 1990.

[4]G. H. Hardy, E. M. Wright,An *introduction to the theory of numbers* (Sixth Edition,Edited by D. R. Heath-Brown and J. H. Silverman), Oxford University Press, 2008.

[5]M. Hassani, Tests for divisibility by prime numbers,*The Mathematical Gazette*, Vol.103 (2019), 494–495

[6]E. W. Weisstein,*CRC concise encyclopedia of mathematics*, CRC Press, 2003.

[7]J. J. O'Connor and E. F. Robertson,*The MacTutor History of Mathematics archive*.
http://www-history.mcs.st-andrews.ac.uk/index.html

[8]Wikipedia,the *free encyclopedia*.
http://www.wikipedia.org/

[9]Wolfram MathWorld,*The Web's Most Extensive Mathematics Resource*.
http://mathworld.wolfram.com/