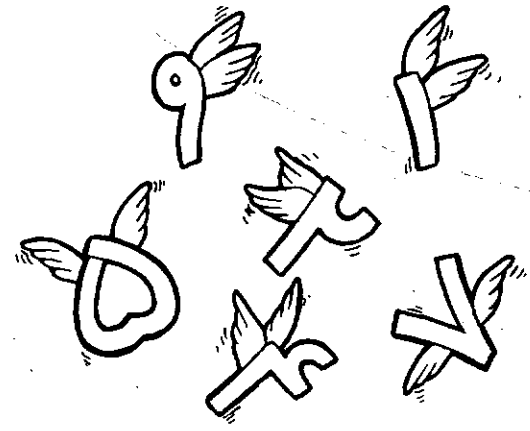
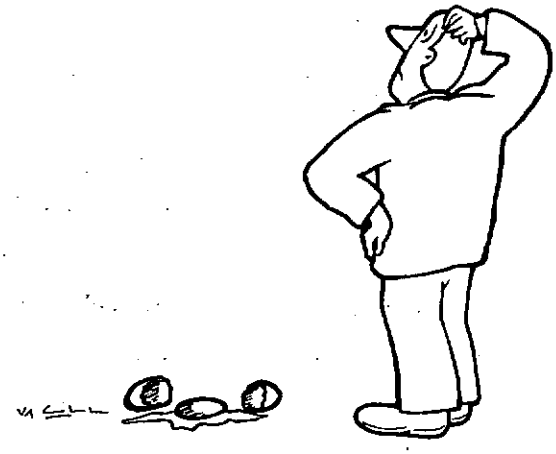
گشت و گذاری در ریاضیات معاصر

نظریهٔ اعداد



● غلامرضا یاسی پور



کار اوّلیهٔ «نظریهٔ اعداد» "number theory" بررسی ویژگیهای اعداد صحیح بوده است. گسترش سیستماتیک این نظریه به عنوان شاخه‌ای از ریاضیات، نسبتاً دیر انجام گرفت. در دوران باستان، نتایج خاصی از این نظریه ـ به عنوان مثال، برای **اقلیدس** "EUCLID" (حدود ۳۰۰ ق.م.) و **دیوفانت** "DIOPHANTOS" (در حدود ۲۵۰ ب.م.) ـ معلوم بود.

در قرن هفدهم کشفیات علمی مهمی و بیشتر از همه، در زمینهٔ تحقیقات **پی‌یر فرما** "PIERRE FERMAT" (۱۶۰۱ـ۱۶۶۶) رخ داد. در آثار بسیار **لئونهارد اویلر** "LEONHARD EULER" (۱۷۰۷ـ۱۷۸۳) قدمهای بزرگی به طرف جلو برداشته شد، که پر از اندیشه‌های وسیع و دامنه‌دار بود.

سرانجام، **کارل فردریش گاوس** "CARL FRIEDRICH GAUSS" (۱۷۷۷ـ۱۸۵۵) نظریه‌ای یکدست تنظیم کرد. وی در سال ۱۸۰۱ حساب تجسسات "*Disquisitiones arithmetic*" خود را منتشر کرد؛ اثری به‌جا ماندنی، که اساس حساب عالی "*higher arithmetic*" در مفهوم دقیق آن شد.

امروزه، نظریهٔ اعداد، نظریه‌ای با شاخه‌های وسیعی است، که هم از جبر مجرّد "*abstract algebra*" (بخصوص در نظریهٔ اعداد جبری "*algebraic number theory*") و هم از روشهای بنیادی آنالیز (در نظریهٔ اعداد تحلیلی "*analytic number theory*") استفادهٔ بسیاری می‌برد. این کار به مسائل و نظریه‌های جدیدی می‌انجامد که تنها ارتباطهایی غیرمستقیم با اعداد صحیح دارد.

در برابر سایر بخشهای ریاضیات، بسیاری از مسائل و نتایج نظریهٔ اعداد، برای افراد غیرمتخصص در ریاضیات نیز قابل درک است. اما آشکار است که اثبات قضایا، اغلب به تجهیزات ریاضی وسیعی نیازمند است.

گاوس ریاضیات را ملکهٔ علوم "*queen of the sciences*" نامیده و در سال ۱۸۰۸ (در نامه‌ای به دوستش بولیایی "*BO´LYAI*") چنین گفته است: «جالب توجه است که تمام کسانی که به مطالعهٔ این علم می‌پردازند، به طور جدّی، نوعی دلبستگی به آن پیدا می‌کنند.»

حلقه‌ها و میدانها (هیئتها)

موارد اساسی *نظریهٔ اعداد مقدماتی* "*elementary number theory*" را در فصل اوّل بررسی کرده‌ایم. از نظریهٔ بخشپذیری "*theory of divisibility*" مشخص است که خارج قسمت دوعدد صحیح، ممکن است؛ اما نیاز نیست که عددی صحیح باشد؛ به‌عنوان مثال $\frac{۱۵}{۳}=۵$، اما $\frac{۱۵}{۷}$ عددی صحیح نیست.

در این صورت، می‌گوییم: تقسیم، عمل وارون ضرب، را نمی‌توان همیشه در حوزهٔ اعداد صحیح انجام داد. دستگاه‌هایی عددی که بتوان عملهای جمع، تفریق و ضرب را در آنها، بدون محدودیت انجام داد، حلقه "*ring*" نامیده می‌شوند.

در صورتی که تقسیم (غیراز بر ۰) را نیز بتوان در یک دستگاه عددی انجام داد، از *میدان (هیئت)* "*field*" صحبت می‌کنیم؛ به‌عنوان مثال، اعداد گویا یک میدان تشکیل می‌دهند.

در موارد بعدی، حلقهٔ اعداد صحیح ۰، ۱±، ۲±، ... را با Z و میدان اعداد گویا را با Q نمایش می‌دهیم.

اگر a و b دو عدد در Z باشند و $b\neq ۰$، خارج قسمت a/b در Q، اما نه لزوماً درZ واقع می‌شود. در صورتی که مورد اخیر رخ دهد، آن‌گاه گفته می‌شود a بخشپذیر "*divisible*" بر b یا مضرب "*multiple*" b است.

ایده آلها

بجز Z به حلقه‌های Rای نیاز داریم که عنصرهای آنها می‌توانند اعداد حقیقی یا مختلط باشند. از این دست هستند زیرمجموعه‌های I از حلقهٔ Rای که دارای ویژگیهای زیر می‌باشند:

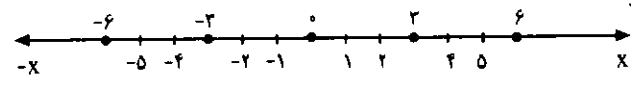
(i) اگر a و b اعدادی در I باشند، آن‌گاه a − b نیز چنین است؛

(ii) به ازای هر عدد r واقع در R و هر عدد a واقع در I، حاصلضرب ra نیز در I قرار دارد. این زیرمجموعه‌های I از R را *ایده‌آلهای* "*ideals*" واقع در R می‌نامیم.

برای مثال، اگر m عددی طبیعی باشد، کل اعداد

$$۰, \pm m, \pm ۲m, \pm ۳m, \ldots$$

ایده‌آلی در Z است (شکل ۳۰ـ۱ ایده‌آل (۳) بر خط عددی).



شکل ۳۰-۱

واضح است که، تفاضل دو مضرب صحیح m بازهم مضربی از m است (ویژگی (i))، و هر مضرب مضربی از m خود مضربی از m است (ویژگی (ii)). در چنین حالتی، ایده‌آل مورد بحث را با $M=(m)$ نمایش می‌دهیم تا مشخص شود که شامل جمیع مضربهای عدد m است.

ایده‌آلهای شامل جمیع مضربهای عنصر منفردی از حلقهٔ R، در حالت مورد بحث m، به *ایده‌آلهای اصلی* "*principal ideals*" موسوم هستند.

بسادگی می‌توان به اثبات رساند که در Z هر ایده‌آل اصلی است، بنابراین جمیع ایده‌آلهای (m) واقع در Z را با به‌نوبت قراردادن $m=۰,۱,۲,\ldots$، به‌دست می‌آوریم.

مفهوم بخشپذیری را نیز می‌توان برای ایده‌آلها تعریف کرد. دراین مورد می‌گوییم ایده‌آل A بر ایده‌آل B بخشپذیر است. اگر هر عنصر A عنصری از B نیز باشد، به عبارت دیگر، $A\subseteq B$.

در ظاهر، مفهوم اصلی کلمهٔ بخشپذیر در این مورد، به مفهوم مقابل آن تبدیل می‌شود؛ اما ارتباط با نظریهٔ بخشپذیری، بلافاصله دلیل این نام‌گذاری را روشن می‌کند.

کاربردی ازاین تعریف در مورد دو ایده‌آل $A=(a)$ و $B=(b)$ در Z، نشان می‌دهد که A بر B بخشپذیر است؛ اگر و تنها اگر a بر b بخشپذیر باشد.

برای مثال، ایده‌آل (۲) شامل اعداد

$$۰, \pm ۲, \pm ۴, \pm ۶, \pm ۸, \ldots$$

و ایده‌آل (۴) شامل اعداد

$$۰, \pm ۴, \pm ۸, \pm ۱۲, \ldots$$

است. درنتیجه، از لحاظ مجموعه ـ نظریه‌ای $(۴)\subseteq(۲)$؛ اما این بدان معناست که ایده‌آل (۴) بر ایده‌آل (۲) بخشپذیر است؛ زیرا ۴ بر ۲ بخشپذیر است.

سپس، AB، حاصلضرب دو ایده‌آل A و B را تعریف می‌کنیم؛ یعنی، به صورت ایده‌آل شامل جمیع مجموعهای حاصلضربهای به تعداد متناهی ab، که a و b‌ی آن، بترتیب، عنصرهای *دلخواه* A و Bاند. در Z نتیجه می‌گیریم که به ازای $A=(a)$ و $B=(b)$، حاصلضرب $AB=(ab)$، به عنوان مثال، $(۸)=(۴)\cdot(۲)$.

مفهوم ایده‌آل در توسعهٔ نظریهٔ اعداد جبری به‌وجود آمد. نظریهٔ *ایده‌آلها* "*ideal theory*" ساختار حلقه‌ها و ایده‌آلهای آنها را بررسی می‌کند. به خاطر ساده کردن گزارهٔ نتایج، بهتر است که از سبک گفتار زیر استفاده کنیم: فرض می‌کنیم a و b اعدادی از حلقهٔ R و I ایده‌آلی در R باشند؛ دراین صورت می‌گوییم:

$$a\equiv b(\bmod I)$$

(و می‌خوانیم : a هم‌نهشت با b به پیمانهٔ I است) اگر a − b عددی در I باشند.

رابطهٔ هم‌نهشتی "*congruence*" فوق با توجه به ترایا، متقارن و بازتابی بودن، رابطه‌ای هم‌ارزی است.

بر مبنای ویژگیهای فوق، جمیع اعداد R را می‌توان به رده‌های مانده‌های مجزّایی "*disjoint resedue classes*" به پیمانهٔ I، چنان تقسیم کرد که جمیع اعداد هم‌نهشت به پیمانهٔ I متعلق به یک رده باشند.

اهمیت طریق نوشتن صوری مزبور، دراین واقعیت قرار دارد که اغلب قاعدهٔ محاسبهٔ معادله‌ها، درمورد هم‌نهشتیهای به پیمانه‌ای ثابت نیز برقرارند.

از لحاظ تاریخی، مفهوم هم‌نهشتی ابتدا توسط گاوس برای حلقهٔ Z ایجاد شد. دراین مورد $a \equiv b(\mathrm{mod}\ m)$، بدین معناست که تفاضل دو عدد صحیح a و b در ایده‌آل $M = (m)$ قرار دارد ؛ بنابراین، a − b بر m بخشپذیر است، یا a و b در تقسیم بر m باقیمانده‌های یکسان دارند.

مثالها: $۸۸ \equiv -۱۰(\mathrm{mod}۱۴)$ ؛ زیرا $۸۸-(-۱۰)=۹۸$ بر ۱۴ بخشپذیر است ؛

$۲^{۳۲} \equiv -۱(\mathrm{mod}۶۴۱)$ $\qquad$ $۳^{۷} \equiv ۱(\mathrm{mod}۱۰۹۳)$

اعداد صحیح

ویژگیهای معینی از رده‌های مانده‌های واقع در حلقهٔ اعداد صحیح Z را می‌توان در رابطه با بخشپذیری اعداد بررسی کرد. دراین مورد فرض می‌کنیم (a,b) بزرگترین مقسوم‌علیه مشترک (ب.م.م) دو عدد a، b و p عددی اوّل را نمایش دهد.

حلقهٔ ردهٔ مانده‌ها

رده‌های مانده‌های به پیمانهٔ m را می‌توان با تعریف جمع و ضرب رده‌های مانده‌ها در حلقه به‌کار برد. این مطلب را با مثالی توضیح می‌دهیم.

فرض می‌کنیم $r_۱$ ردهٔ مانده‌های $\bar{۲}$ به پیمانهٔ ۶ شامل اعداد

$$\ldots,-۱۰,-۴,۲,۸,۱۴,\ldots$$

و $r_۲$ ردهٔ مانده‌های $\bar{۵}$ به پیمانهٔ ۶ شامل اعداد

$$\ldots,-۷,-۱,۵,۱۱,\ldots$$

باشد. در این صورت، $r_۱ + r_۲$ را به عنوان ردهٔ مانده‌هایی تعریف می‌کنیم که شامل ۷ = ۵ + ۲ باشد، و در واقع شامل جمیع اعدادی که در تقسیم بر ۶ باقیماندهٔ «۱» را به‌جا می‌گذارند.

در این مورد می‌نویسیم $\bar{۲} + \bar{۵} = \bar{۱}$ ؛ مثالهای دیگر عبارتند از $\bar{۵} + \bar{۰} = \bar{۵}$ ، $\bar{۳} + \bar{۳} = \bar{۰}$ ، حاصلضرب مورد بحث توسط $\bar{۲} \cdot \bar{۵} = \overline{۱۰} = \bar{۴}$ تعریف می‌شود ؛ مثالهای دیگر به پیمانهٔ ۶ عبارت است از : $\bar{۲} \cdot \bar{۳} = \bar{۰}$, $\bar{۳} \cdot \bar{۳} = \bar{۳}$, $\bar{۵} \cdot \bar{۰} = \bar{۰}$

تحت جمع و ضرب تعریف شدهٔ پیشین، رده‌های مانده‌های به پیمانهٔ m، حلقهٔ ردهٔ مانده‌های *"residue class ring"* به پیمانهٔ m را تشکیل می‌دهند. ساختار این حلقه را می‌توان در گزاره‌هایی دقیق توصیف کرد. این حلقه، اگر و تنها اگر m عددی اوّل باشد، میدان است.

گروه رده‌های مانده‌های اوّل

با انتخاب جمیع آنهایی که اعدادشان با m اوّلند، از میان m ردهٔ مانده‌های متمایز

$$\bar{۰}, \bar{۱}, \bar{۲}, \ldots, \overline{m-۱} \mod m$$

رده‌های مانده‌های اوّل به پیمانهٔ m را به‌دست می‌آوریم. به‌ازای m = ۶ دو ردهٔ مانده‌های اوّل $\bar{۱}$ و $\bar{۵}$ موجود است ؛ به ازای m = p همواره P − ۱ حالت وجود دارد ؛ یعنی :

$$\bar{۱}, \bar{۲}, \ldots, \overline{p-۱}$$

تعداد رده‌های مانده‌های اوّل به پیمانهٔ m را با φ(m) (تابع اویلر *"Euler's function"*) نمایش می‌دهیم. برای مثال :

$$\varphi(۶) = ۲ \ , \ \varphi(p) = p-۱$$

φ(m) یک تابع عدد ـ نظریه‌ای "number-theoretical function" است ؛ یعنی، تابعی تعریف شده به ازای آرگومانهای صحیح. تابع مزبور، تابعی ضربی است ؛ یعنی $\varphi(a,b) = \varphi(a)\varphi(b)$ ؛ البته به شرطی که $(a,b) = ۱$. بسادگی می‌توان محاسبه کرد که :

$$\varphi(p^k) = p^k - p^{k-۱} = p^{k-۱}(p-۱)$$

قاعده‌ای که هم‌اکنون به آن اشاره کردیم، محاسبهٔ φ(m) را به‌ازای هر m ممکن می‌کند ؛ به عنوان مثال :

$$\varphi(۳۲۴۰) = \varphi(۲^۳)\varphi(۳^۴)\varphi(۵) = ۴ \cdot ۵۴ \cdot ۴ = ۸۶۴$$

رده‌های مانده‌های اوّل به پیمانهٔ m، تحت عمل ضرب، گروه G_m ای از مرتبهٔ φ(m) می‌سازند. ساختار G_m در مورد جمیع mها دارای اهمیت است ؛ اما در این‌جا تنها به بررسی حالت m = p پرداخته می‌شود.

G_p دوری است، که بدین معناست که هر ردهٔ مانده‌های اوّل به پیمانهٔ p را می‌توان به عنوان توانی از ردهٔ مانده‌های ثابت $\bar{g}$ ای نوشت؛ چنین g‌ای را ریشهٔ اوّلیهٔ *"primitive root"* به پیمانهٔ p می‌نامیم.

برای مثال، به ازای $p=11$، گروه ردهٔ مانده‌های G_{11} که می‌تواند با $\bar{g}=\bar{2}$ (یا $\bar{6}$، $\bar{7}$، $\bar{8}$) برای توانهای:

$$2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5, 2^5 \equiv 10, 2^6 \equiv 9,$$

$$2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6 \pmod{11}$$

تولید شود. جمیع $p-1=10$ ردهٔ مانده‌های اوّل $\bar{1}$، $\bar{2}$، ...، $\overline{10}$ را به‌دست می‌دهد.

از آن‌جا که هر عنصر a از G، گروه متناهی‌ای از مرتبهٔ n، در برابری $a^n = e$ (e عنصر واحد) صدق می‌کند، به ازای $G = G_m$، *قضیهٔ اویلر "Euler's theorem"* را داریم:

> **قضیهٔ اویلر:** $a^{\varphi(m)} \equiv 1 \pmod{m}$ هنگامی که $(a,m)=1$.
> *این قضیه در حالت خاص می‌شود.*
> **قضیهٔ فرما:** $a^{p-1} \equiv 1 \pmod{p}$ هنگامی که بر p بخشپذیر نیست.

هم‌نهشتیها با مجهولات

در حلقهٔ ردهٔ مانده‌ها و گروه ردهٔ مانده‌ها مسائل جبری خاصی را می‌توان حل کرد. برای مثال، می‌توان این پرسش را مطرح کرد که کدام یک از رده‌های مانده‌های $\bar{x}$ پیمانهٔ m و درمعادله‌های مفروضی، مثلاً $\overline{ax} = \overline{b}$، صدق می‌کنند. معادله‌هایی چنین به هم‌نهشتیهای به پیمانهٔ m‌ی با مجهولات می‌انجامند.

هم‌نهشتی خطی "Linear Congruence"

$ax \equiv b \pmod{m}$ را نمی‌توان همواره حل کرد، برای مثال، $3x \equiv 2 \pmod{12}$ حل‌ناپذیر است؛ زیرا هیچ مضرب صحیح ۳‌ای در تقسیم بر ۱۲، باقیماندهٔ ۲ به‌جا نمی‌گذارد.

درواقع، $ax \equiv b \pmod{m}$ حل‌پذیر است؛ اگر و تنها اگر، b بر بزرگترین مقسوم‌علیه مشترک (a,m) بخش‌پذیر باشد.

هم‌نهشتی از درجهٔ n

$$x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod{m}$$

می‌تواند جوابهای ناهم‌نهشتی "incongruent solutions" بیش از آنچه درجهٔ nاش مقرّر می‌کند، داشته باشد. برای مثال، $x^2 \equiv 1 \pmod{8}$ دارای جوابهای $x \equiv 1, 3, 5, 7$ است.

این معادله، در صورتی که پیمانهٔ m عدد اوّل p باشد، اصلاً نیاز به داشتن جواب ندارد و نمی‌تواند بیش از n ردهٔ مانده‌ها به عنوان جواب داشته باشد.

مانده‌های توانی

در هم‌نهشتی دوجمله‌ای *"binomial congruence"*

$$x^n \equiv a \pmod{p}$$

a بر p بخش‌پذیر نیست. رده‌های مانده‌های $a \pmod{p}$ی که در مورد آنها این هم‌نهشتی حل‌پذیر است، به مانده‌های توانی "power residues" به پیمانهٔ p موسوم است. در این مورد، دو پرسش اساسی مطرح می‌شود:

۱. مانده‌های توانی nام مربوط به اوّلی، مفروض کدام اعدادند؟

۲. به ازای کدام یک از اوّلهای p عدد مفروض a ماندهٔ توانی nام است؟

به پرسش اوّل توسط معیار اویلر *"euler's criterion"*، یعنی، $a^{(p-1)/d} \equiv 1 \pmod{p}$ که در آن $d=(p-1,n)$، پاسخ داده شد. رده‌های مانده‌های a‌ای که در این شرط صدق می‌کنند و فقط همین رده‌ها مانده‌های توانی nام‌اند.

پاسخ پرسش دوم به *قوانین تقابل "reciprocity laws"* منجر می‌شود، که از جمله دستاوردهای زیبا و بنیادی نظریهٔ اعداد می‌باشند.

به ازای $n=2$، رده‌های مانده‌های $a \pmod{p}$ با $(a,p)=1$، که به ازای آنها هم‌نهشتی $x^2 \equiv a \pmod{p}$ حل‌پذیر است، به *مانده‌ها(ی درجهٔ دوم) "(quadratic)residues"* موسومند و مواردی که به ازای آنها هم‌نهشتی مزبور حل‌ناپذیر است، *نامانده‌ها(ی درجهٔ دوم) "(quadratic) non-residues"* نامیده می‌شوند.

به ازای pهای فرد، تعداد مانده‌ها با تعداد نامانده‌های به پیمانهٔ p برابر است و به عبارت دیگر تعداد هریک $(p-1)/2$ است.

برای مثال، به پیمانهٔ ۱۷ داریم:

$$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 16, 5^2 \equiv 8, 6^2 \equiv 2, 7^2 \equiv 15,$$

$$8^2 \equiv 13$$

در نتیجه، ۱۶، ۱۵، ۱۳، ۹، ۸، ۴، ۲، ۱ هشت مانده و ۱۴، ۱۲، ۱۱، ۱۰، ۷، ۶، ۵، ۳ هشت نامانده‌اند.