فرهنگ و اندیشهٔ ریاضی
شماره ۳۱ (پاییز ۱۳۸۲) صص. ۱ تا ۶

نامساوی برنشتین برای متغیرهای تصادفی وابسته

محمد امینی

چکیده

در این مقاله نامساوی برنشتین را برای متغیرهای تصادفی وابسته تعمیم می‌دهیم، سپس در رابطه با شرایط برقراری همگرایی کامل با استفاده از این نامساوی نتایج جالبی را به‌دست می‌آوریم. مثال‌های متنوعی نیز در ادامه ارائه خواهیم نمود.

۱. مقدمه

نامساوی‌های نمایی در احتمال، به‌ویژه در قضایای حدی قوی نقش کلیدی دارند. به این دلیل، آماردانان بسیاری روی این نامساوی‌ها کار کرده‌اند و نتایج جالبی نیز به دست آورده‌اند. به عنوان مثال، آرکنز (۱۹۹۵)، نامساوی برنشتین را برای $U-$ آماره‌ها و $U-$ فرایندها، و شلگر (۱۹۹۳) نیز نامساوی برنشتین را برای یک کلاس از متغیرهای تصادفی مستقل مطالعه کردند. زاپاریز و زانتن (۲۰۰۱) نیز نامساوی برنشتین را برای مارتینگل‌ها تعمیم دادند. امینی و بزرگ‌نیا نیز در مرجع [۱] با استفاده از نامساوی‌های نمایی رفتار مجانبی چندکها برای متغیرهای تصادفی وابسته را مطالعه نموده‌اند.

علاقه‌مند شدیم تا در این مقاله، نامساوی برنشتین را برای متغیرهای تصادفی وابستهٔ منفی تعمیم دهیم و سپس با استفاده از آن شرایط لازم برای همگرایی سری $\sum_{n=1}^{+\infty}[|S_n| > x]$،

$x > ۰$ را تعیین نماییم که در آن $\{X_n, n \geq ۱\}$ یک دنباله از متغیرهای تصادفی وابستهٔ منفی و $S_n = \sum_{i=۱}^{n} X_i$ است. در ادامه مثال‌ها و نتایج جالبی که در شرایط نامساوی صدق می‌کنند نیز ارائه می‌شود.

تعریف ۱. متغیرهای تصادفی $X_۱$، $\cdots$، X_n را به طور منفی وابسته (ND)[۱] نامند، اگر هر دو نامساوی زیر برای تمام مقادیر حقیقی $x_۱, \ldots, x_n$ برقرار باشند:

$$P[\bigcap_{j=۱}^{n} (X_j \leq x_j)] \leq \prod_{j=۱}^{n} P[X_j \leq X_j]$$

و

$$P[\bigcap_{j=۱}^{n} (X_j > x_j)] \leq \prod_{j=۱}^{n} P[X_j > X_j].$$

دنبالهٔ $\{X_n, n \geq ۱\}$ از متغیرهای تصادفی وابستهٔ منفی هستند، اگر هر زیرمجموعهٔ متناهی از آن به مفهوم تعریف فوق وابستهٔ منفی باشند.

لم‌های ۱ و ۲ دو ویژگی مفید متغیرهای تصادفی وابسته را بیان می‌کنند، که در بخش‌های بعدی مورد استفاده قرار می‌گیرند.

لم ۱. [۲]. فرض کنید $X_۱$، $\ldots$، X_n متغیرهای تصادفی ND و $f_۱$، $\ldots$، f_n توابع بورل همه صعودی (یا همه نزولی) باشند، آنگاه $f_۱(X_۱)$، $\ldots$، $f_n(X_n)$ نیز ND هستند.

لم ۲. [۲]. هرگاه $X_۱$، $\ldots$، X_n متغیرهای تصادفی ND باشند، آنگاه

$$E\left(\prod_{i=۱}^{n} X_i\right) \leq \prod_{i=۱}^{n} EX_i.$$

قضیهٔ ۱. [۴]. برای هر متغیر تصادفی X و هر عدد حقیقی t،

$$P[X \geq t] \leq \inf_{u \geq ۰} \{e^{-tu} E e^{ux}\}, \quad U \geq ۰.$$

لم ۳. [۴]. فرض کنید X یک متغیر تصادفی با میانگین صفر و با احتمال ۱ باشد و $|X| \leq M$، برای ثابت متناهی و مثبت M. داریم:

$$Ee^{uX} \leq \exp\left[\frac{u^۲\sigma^۲}{۲(۱-\frac{Mu}{۳})}\right] \quad \text{و} \quad ۰ < u < ۳/M \quad \text{و} \quad \sigma^۲ = var(X)$$

---

1) Negatively dependent

تعریف ۲. دنباله $\{X_n, n \geq ۱\}$ از متغیرهای تصادفی به‌طور کامل به صفر همگراست $(\lim X_n = ۰, \text{completely})$، اگر برای هر $\varepsilon > ۰$،

$$\sum_{n=۱}^{+\infty} P[|X_n| > \varepsilon] < \infty. \qquad (۱)$$

۲. نامساوی برنشتین

در این بخش نامساوی برنشتین را برای متغیرهای تصادفی وابسته تعمیم می‌دهیم، سپس با استفاده از آن همگرایی کامل مجموعه‌های جزئی را بررسی می‌نماییم.

قضیهٔ ۲. فرض کنید $X_۱$، $X_۲$، ...، X_n متغیرهای تصادفی ND با میانگین صفر وبا احتمال ۱ باشند و $|X_k| < M$، $k = ۱, ۲, \ldots, n$، و برای هر $۰ < M < \infty$، $B_n = \sum_{k=۱}^{n} var(X_k)$، در این صورت برای هر عدد حقیقی مثبت x،

$$P[|S_n| > x] \leq ۲\exp\left[-\frac{x^۲}{۲(B_n + Mx/۳)}\right] \quad \text{و}$$

که در آن $S_n = \sum_{i=۱}^{n} X_i$.

برهان. بنا به لم‌های ۱ و ۲ و ۳ برای هر عدد حقیقی مثبت u به‌طوری که $۳/M > u > ۰$ داریم:

$$\begin{aligned} Ee^{uS_n} &= E\left[\prod_{k=۱}^{n} e^{uX_k}\right] \\ &\leq \prod_{k=۱}^{n} Ee^{uX_k} \\ &\leq \prod_{k=۱}^{n} \exp\left[\frac{u^۲ var(X_k)}{۲(۱ - Mu/۳)}\right] \\ &= \exp\left[\frac{u^۲ B_n}{۲(۱ - Mu/۳)}\right]. \end{aligned}$$

اکنون بنا به لم‌های ۱ و ۲ و قضیهٔ ۱ برای $u = \dfrac{x}{B_n + Mx/۳}$ که در آن $x > ۰$، داریم:

$$\begin{aligned} P[|S_n| > x] &\leq P[S_n > x] + P[-S_n > x] \\ &\leq \exp\left[-\frac{x^۲}{۲(B_n + Mx/۳)}\right] + \exp\left[-\frac{x^۲}{۲(B_n + Mx/۳)}\right] \\ &= ۲\exp\left[-\frac{x^۲}{۲(B_n + Mx/۳)}\right]. \end{aligned}$$

۳. نتایج اصلی

۱) تحت شرایط قضیهٔ ۲ به ازای $x = \varepsilon n^{\beta}$ که $\varepsilon > 0$ و $\beta > 0$ داریم:

$$P[|S_n| > \varepsilon n^{\beta}] \leq 2 \exp\left[-\frac{\varepsilon^{2} n^{2\beta}}{2(B_n + \frac{M\varepsilon n^{\beta}}{3})}\right].$$

۲) اگر سری $\sum_{n=1}^{+\infty} \exp\left[-\frac{\varepsilon^{2} n^{2\beta}}{2(B_n + \frac{M\varepsilon n^{\beta}}{3})}\right]$ برای هر $\beta > 0$ و $\varepsilon > 0$ همگرا باشد آنگاه دنبالهٔ $\left\{\frac{1}{n^{\beta}} \sum_{k=1}^{n} X_k\right\}$ به طور کامل به صفر همگراست.

۳) هرگاه $B_n \leq cn^{\beta}$ که در آن c یک عدد حقیقی مثبت متناهی است و $\beta > 0$، آنگاه سری $\sum_{n=1}^{+\infty} \exp\left[-\frac{\varepsilon^{2} n^{2\beta}}{2(B_n + \frac{M\varepsilon n^{\beta}}{3})}\right]$ همگراست، در نتیجه دنبالهٔ $\left\{\frac{1}{n^{\beta}} \sum_{k=1}^{n} X_k\right\}$ به طور کامل به صفر همگراست.

۴) اگر $var(X_k) = \sigma^{2}$، $k = 1, \ldots, n$ آنگاه کران نمایی در نتیجهٔ ۱، به $\exp\left[-\frac{\varepsilon^{2} n^{2\beta}}{2n\sigma^{2} + \frac{2}{3}M\varepsilon n^{\beta}}\right]$ تبدیل می‌شود. در این حالت برای هر $\frac{1}{2} \leq \beta \leq 1$ سری $\sum_{n=1}^{+\infty} \exp\left[-\frac{\varepsilon^{2} n^{2\beta}}{2n\sigma^{2} + \frac{2}{3}M\varepsilon n^{\beta}}\right]$ همگراست. بنابراین دنبالهٔ $\left\{\frac{1}{n^{\beta}} \sum_{k=1}^{n} X_k\right\}$ برای هر $\frac{1}{2} \leq \beta \leq 1$ و در نتیجه برای هر $\beta > \frac{1}{2}$ به‌طور کامل به صفر همگراست.

۵) اگر $\{X_n, n \geq 1\}$ یک دنباله از متغیرهای تصادفی غیرکراندار باشد، با تعریف $Y_k = \frac{X_k}{\sqrt{B}}$، $k = 1, 2, \ldots, n$ و $c_k = esssup \frac{|X_k|}{\sqrt{B_n}}$ و اینکه بنا به لم ۱ دنبالهٔ $\{Y_k\}$ ND است، با احتمال ۱ و $|Y_k| < c_n$. حال با کاربرد قضیهٔ ۲ برای دنبالهٔ $\{Y_k\}$ به دست می‌آوریم:

$$P[|S_n| > x] = P\left[\frac{|S_n|}{\sqrt{B_n}} > \frac{x}{\sqrt{B_n}}\right] \leq 2 \exp\left[-\frac{x^{2}}{2B_n + \frac{2}{3}c_n\sqrt{B_n}x}\right].$$

۴. مثال‌ها

۱) فرض کنید X_1، ...، X_n دارای توزیع توام دیریکله با تابع چگالی زیر باشند:

$$f(x_1,\ldots,x_n)=\frac{\pi(\sum_{i=0}^{n}\alpha_i)}{\prod_{i=0}^{n}\pi(\alpha_i)}(1-\sum_{i=1}^{n}x_i)^{\alpha_0-1}\prod_{i=1}^{n}x_i^{\alpha_i-1}$$

که در آن $\alpha_i\geq 0$، $x_i\geq 0$، $i=0,1,2,\ldots,n$ و $\sum_{i=1}^{n}x_i\leq 1$.

X_1، ...، X_n متغیرهای تصادفی ND هستند [۲] و [۳]. بنا به لم ۱، $Y_1,\ldots,Y_n$ نیز ND هستند که در آن $Y_i=X_i-EX_i$، $i=1,2,\ldots,n$. متغیرهای $Y_1,\ldots,Y_n$ با $M=2$ و $B_n=\sum_{i=1}^{n}var(X_i)\leq 4n$ در شرایط قضیهٔ ۲ صدق می‌کنند، بنابراین دنبالهٔ $\left\{\frac{1}{n}\sum_{i=1}^{n}(X_i-EX_i)\right\}$ به طور کامل به صفر همگراست.

۲) فرض کنید $X_1,\ldots,X_n\approx MultN(m,p_1,\ldots,p_n)$ متغیرهای تصادفی $X_1,\ldots,X_n$، ND هستند [۲] و [۳]. داریم $EX_i=mp_i$ و $var(X_i)=mp_iq_i$، $i=1,2,\ldots,n$. از اینکه $0\leq X_i\leq m$، اگر $Y_i=X_i-EX_i$ آنگاه $|Y_i|\leq 2m$ و $B_n=\sum_{i=1}^{n}var(X_i)\leq mn$. بنابراین $\left\{\frac{1}{n}\sum_{i=1}^{n}(X_i-EX_i)\right\}$ به طور کامل به صفر همگراست.

مراجع

[1] Amini, D.M. Bozorgnia, A. (2000), “Negatively dependent bounded random variables, probability inequalities, and the strong law of large numbers”, Journal of Applied Mathematics and Stochastic Analysis, 13:3, 261-267.

[2] Block, H. W., Savits, T. H. and Shaked. M. (1982), “Some concepts of negative dependence”, Ann, V.10, No. 3, 765-772.

[3] Bozorgnia, A. Patterson, R. F and Taylor, R. L.(1996), “Limit theorems for dependent random variables”, World Congress Nonlinear Analysis, 92. V. Lakshmikantham, de Gruyter Publ.Berlin-New York. P.1639-1650.

[4] Dudley, R. M. (1999), *Uniform central limit theorems*, Cambridge University Press.

[5] Arcones, M. A. (1995), *A Bernstein-type inequality for U-statistics and U-processes. statistics & probability*, letter 22,239-247.

[6] Schmuckenschlaeger. M.(1993), *Bernsein inequalites for a class of random Variables*, proceedings of the American Mathematical society, V.117, No. 4.1159-1163.

[7] D. Zhaparidze k. and Zanten, J.H.(2001), “On Bernstein-type inequalities for martingales”, Stochastic processes and their applications, 93.109-117

محمد امینی
دانشگاه سیستان و بلوچستان
دانشکده علوم ـگروه ریاضی
پست الکترونیک amini@hamoon.usb.ac.ir

فرهنگ و اندیشهٔ ریاضی
شماره ۳۱ (پاییز ۱۳۸۲) صص. ۷ تا ۲۴

آیا n اول است؟ الگوریتمی «همه» فهم با زمان اجرای چندجمله‌ای*

فولکمار بورنمن

ترجمهٔ: روح‌الله جهانی‌پور

«**روش جدیدی ابداع شده است که یکی از مسایل کلیدی ریاضی را حل می‌کند.**» این، عنوان مطلبی در شمارهٔ ۸، آگوست سال ۲۰۰۲، **مجله نیویورک تایمز** بود که به اثبات گزارهٔ $\text{PRIMES} \in \mathcal{P}$، یعنی یکی ازبزرگترین مسائل حل‌نشده در نظریهٔ الگوریتمی اعداد و علوم نظری کامپیوتری، اشاره داشت. مانیندرا اگروال [۱]، نیراج کایال [۲] و نیتین ساکسنا [۳] از انستیتوی صنعتی هند، این مطلب را به کمک الگوریتمی بسیار عالی و فوق‌العاده ساده، ثابت کردند. تنها چند روز پس از اطمینان از صحت اثبات، متخصصان گفتند:«این الگوریتم بسیار زیباست.»(کارل پومرانس [۴]) یا «این بهترین نتیجه‌ای بوده که در ده سال اخیر شنیده‌ام »(شافی‌گلدواسر[۵]).

درست چهار روز قبل از چاپ این مطلب در نیویورک تایمز، در یک روز یکشنبه، سه نویسندهٔ مذکور، پیش نویس یک مقالهٔ نه صفحه‌ای را با عنوان «اعداد اول متعلق به $\mathcal{P}$ هستند» برای پانزده تن از متخصصان نظریهٔ‌اعداد ارسال کردند. عصر همان روز، جایکومار راداکریشنان [۶] و ویکرامان آرویند [۷] تبریک‌های خود را به مناسبت این اثبات برای آنان فرستادند. صبح روز دوشنبه، کارل پومرانس که از بزرگان این موضوع است، صحت این نتیجه را تأیید کرد و در حالی که غرق در شور و احساس بود، سمیناری فوری برای بعد از ظهر همان روز ترتیب داد و از سارا رابینسون از روزنامهٔ

---

*) این مقاله ترجمه‌ای است که ویراستار *Notices* از مقالهٔ آلمانی که در مجلهٔ

Mitteilungen der Deutschen Mathematiker - Vereinigung

مجلد چهارم سال ۲۰۰۲، صفحات ۱۴ تا ۲۱ چاپ شده، انجام داده است.

1) Manindra Agrawal 2) Neeraj Kayal 3) Nitin Saxena 4) Carl Pomerance

5) Shafi Goldwasser 6) Jaikumar Radhakrishnan 7) Vikraman Arvind

نیویورک تایمز هم دعوت به حضور کرد. روز سه‌شنبه پیش‌نویس اثبات در اینترنت آزادانه در دسترس همه قرار داده شد. روز پنجشنبه هندریک لنسترا پسر[۱] که او نیز از بزرگان نظریهٔ اعداد است، به‌بعضی از خطاهای مختصری که وجود داشت پایان داد و در فهرست آدرس الکترونیکی NMBRTHRY اینگونه‌اظهار نظر کرد:

«تبصره‌های ... بی‌اساس و از نظر منطقی از هم گسیخته‌اند لکن اثبات‌ها مشکل چندان قابل ذکری ندارند. تنهااشتباهی که رخ داده، ... است اما به راحتی می‌توان آن‌را رفع کرد. اشتباه‌های دیگر کوچکتر از آن است که قابل ذکر باشد. مقاله از دید ماهوی کاملاً درست است.»

و بالاخره در روز جمعه، دَن برنشتاین[۲]، اثبات اصلاح شده‌ای را از نتیجهٔ اصلی که به یک صفحه تقلیل یافته بود در شبکهٔ جهانی Web انتشار داد.

کوتاه بودن این دورهٔ زمانی برای بررسی یک مقالهٔ ریاضی، هم مبین ایجاز و ظرافتی است که در استدلال موجود در آن به کار رفته و هم سادگی روش آن است، به‌طوری‌که آن را حتی در سطح کارشناسی نیز قابل درک کرده است. دو تن از نویسندگان این مقاله یعنی کایال و ساکسنا درجهٔ کارشناسی خود را در رشتهٔ علوم کامپیوتر، درست در بهار همان سال گرفته بودند؛ آیاامیدی هست که کار آنها قابلیت درک «همگانی» داشته باشد؟

سال ۱۹۹۸، هانس مگنوس انزنسبرگر[۳] در سخنرانی خود در کنگرهٔ بین‌المللی ریاضیدانان در برلین دیدگاهی را مطرح کرد که بر مبنای آن ریاضیات هم یک «منفور فرهنگی» است و هم در عین حال به واسطهٔ موفقیت‌های ارزشمند آن که او هرگز در هنر تئاتر و در ورزش ندیده است، در میانهٔ دوران طلایی خود قرار دارد. مطمئناً بعضی از این کامیابی‌ها، خود ریاضیدانان را هم وادار ساخته تا دربارهٔ فاصلهٔ بین **علما** و **عوام** در حوزهٔ ریاضی بیندیشند.افراد غیرحرفه‌ای— ممکن است در ذهن بگذرانید که چه تعداد از ما جزٔ این «همگان» نیستیم ــ نه می‌توانند اثبات وایلز برای قضیهٔ آخر فرما را به درستی بفهمند و نه می‌توانند اهمیت آن را کاملاً درک کنند، هرچند تلاش‌هایی همانند کتاب سیمون سینگ[۴] که در جهت همگانی‌سازی آن صورت گرفته، می‌تواند در آگاهی یافتن از ارتباطات، یاریگر خواننده باشد. احتمالاً نمی‌شود هیچ محققی را یافت که بتواند اهمیت و تبعات ارزشمندی را که موفقیت‌های برندگان سال گذشتهٔ مدال فیلدز به بار آورده است، به «همگان» بفهماند. لذا هر کس می‌کوشد آجر دیگری بر حجرهٔ خود در برج بابلی که ریاضی نام دارد بیفزاید و در ضمن ساختمانی را که در آن مکان بنا کرده مستحکم‌تر سازد. به ندرت پیشرفت‌هایی همانند آنچه در ابتدای آگوست رخ داد، سنگ بنایی بر این برج می‌نهد که برای «همگان» قابل درک باشد.

پاول لیلاند[۵] دیدگاهی را بیان می‌کند که از ذهن بسیاری از ما نیز گذشته است: «حالا همه

1) Hendrik Lenstra Jr. 2) Dan Bernshtein 3) Hans-Magnus Enzensberger
4) Simon Singh 5) Paul Leyland

نگرانند که آیا ممکن است چیز دیگری مشابه با این، موجود باشد که از چشم ما مخفی مانده است؟» بیهوده نیست که اگروال با حیرت تمام می‌گوید: «ما هرگز فکر نمی‌کردیم نتیجه‌ای که به‌دست آورده‌ایم تا این اندازه مورد استقبال ریاضیدانان سنتی قرار گیرد»، چرا که در همان ده روز اول بیش از دو میلیون نفر از سایت اینترنتی که اثبات در آن قرار داده شده بود، بازدید کردند و سیصد هزار برداشت و پرینت انجام شد.

اکنون می‌خواهم به عنوان متخصص در آنالیز عددی و نه در نظریهٔ الگوریتمی اعداد، توانایی خود را به‌سان عضوی از جامعهٔ «عوام» و خارج از حیطهٔ کاری خود در فهم این اثبات محک بزنم.

> زمانی که مسألهٔ حل‌نشدهٔ با سابقه‌ای در ریاضیات سرانجام حل می‌شود، هر ریاضیدانی می‌خواهد با دنبال کردن آنچه در این باره انجام شده است، در نزد خود، در لذت این حل مشارکت جوید، اما در غالب موارد در پیچیدگی بیش از حد ریاضیات دوران معاصر گیر می‌افتد. پاسخ منفی که اخیراً به مسألهٔ دهم هیلبرت داده شد، یک مثال نقض لذت‌بخش است. در این مقاله، بیان کاملی از این راه حل ارائه می‌شود که برای دنبال کردن استدلال‌های موجود در آن، تنها چیزی که خواننده باید بداند کمی نظریهٔ اعداد، به‌خصوص مطالب مقدماتی دربارهٔ بخش‌پذیری اعداد صحیح مثبت و همنهشتی‌های خطی است.
>
> — قسمتی از مقدمهٔ مقالهٔ مارتین دیویس با عنوان «مسألهٔ دهم هیلبرت حل‌پذیر نیست»:
>
> Amer. Math. Monthly, **80**(1973), 233-69

صورت مسأله

جالب است بدانید که انگیزهٔ این سه نفر برای انجام کارشان، اهمیت اعداد اول در رمزنگاری و تجارت الکترونیکی نبوده است، بلکه در وهلهٔ اول دنبال کردن تذکارتاریخی است که دان کنوت[۱] به نقل از ریاضیدان بزرگ، کارل‌فریدریش‌گاوس ،از مقالهٔ شمارهٔ ۳۲۹ کتاب**تحقیقات حسابی** او به سال ۱۸۰۱ بازگو می‌کند و ما در اینجا آن را از ترجمهٔ سال ۱۹۶۶ آرتور ای کلارک[۲] بیان می‌کنیم: «مسألهٔ متمایز ساختن اعداد اول از اعداد مرکب و تجزیهٔ اعداد مرکب به عوامل اولشان، یکی از مهمترین و مفیدترین مسائل در حساب است. این مسأله آنقدر هوش و حواس و سعی و توان محاسبان باستان و جدید را به خود مشغول داشته است که بحث طولانی دربارهٔ اهمیت آن، کار لغوی است؛ به علاوه، شأن و منزلت علمی آن ایجاب می‌کند که هر وسیلهٔ ممکنی برای حل مسأله‌ای چنین جالب و مهم به‌کار گرفته شود.»

1) Dan Knuth 2) Aryhur A. Clarke

در دورهٔ آموزش ابتدایی با غربال اراتستن آشنا می‌شویم. متأسفانه، استفاده از این روش برای تعیین اول بودن عدد طبیعی n مستلزم زمان محاسبه‌ای متناسب با خود n است. از طرف دیگر طول عدد[۱] ورودی به غربال با تعداد ارقام دودویی آن و در نتیجه با $\log_2 n$ متناسب است، لذا الگوریتمی در پیش داریم که زمان اجرای نمایی $O(2^{\log_2 n})$ دارد. مجدداً از مقالهٔ شمارهٔ ۳۲۹ تحقیقات حسابی گاوس نقل قول می‌کنیم که: «علیرغم این، باید ابراز کرد که تمام روش‌هایی که تاکنون ارائه شده‌اند یا محدود به حالت‌های خیلی خاص هستند، یا آنقدر دشوار وخسته‌کننده‌اند که اصلاً نمی‌توان آنها را برای اعداد بزرگ به کاربرد.»

به این ترتیب آیا اصلاً می‌توان دربارهٔ اول بودن اعداد خیلی بزرگ تصمیم کارآمدی گرفت؟ تعبیر ریاضی این پرسش درچهارچوب نظریهٔ پیچیدگی محاسبات، ارائهٔ الگوریتمی با زمان اجرای چندجمله‌ای است. آیا الگوریتمی **تعینی**[۲] وجود دارد که به ازای یک توان ثابت k، برای هر عدد طبیعی n، طی $O(\log^k n)$ مرحله معلوم کند که آیا n اول است یا نه؟ کوتاه سخن اینکه پرسشی که تاکنون بی‌پاسخ مانده بود این است که:«آیا $PRIMES \in \mathcal{P}$؟»

وضعیت پیش از آگوست ۲۰۰۲

از زمان گاوس تاکنون، مسألهٔ اول بودن یک عدد، یک چیز بوده و مسألهٔ تجزیهٔ یک عدد مرکب به عوامل اول، چیزی دیگر. گاوس در مقالهٔ شمارهٔ ۳۳۴ کتاب **تحقیقات حسابی** می‌نویسد: «مطلب دوم بر اولی مقدم است از این نظرکه محاسبات را سریع‌تر می‌کند، لکن تجزیهٔ مورد نظر را برای اعداد مرکب تولید نمی‌کند، بلکه فقط آنها را از اعداد اول متمایز می‌سازد». نقطهٔ آغاز بسیاری از روش‌های تعیین اول بودن یک عدد، قضیهٔ کوچک فرما است حاکی از این که برای هر عدد اول n و هرعدد a متباین با n داریم: $a^n \equiv a \pmod n$. متأسفانه، عکس این قضیه درست نیست؛ یعنی اعداد اول را نمی‌توان با این روش پیدا کرد. از طرف دیگر«استفاده از همنهشتی فرما آنقدر ساده است که دست برداشتن از آن به صرف این‌که تعداد کمی مثال نقض دارد، مایهٔ شرمساری است.»(کارل پومرانس) و لذا تعجبی ندارد که صورت‌های اصلاح‌شده‌ای از این محک مبنای الگوریتم‌های مهمی درتعیین اعداد اول بوده است.

در سال ۱۹۷۶ میلر و رابین[۳] الگوریتم احتمالاتی ساده‌ای ارائه دادند که در آن از یک مولد

---

۱) اختلاف بین اندازهٔ یک عدد و طول آن را به روشنی می‌توان در اعدادی چون تعداد اتم‌های موجود در عالم (حدود 10^{79}) و یا تعداد کل اعمال حسابی که تاکنون انسان‌ها و ماشین‌های محاسبه انجام داده‌اند (حدود 10^{24}) دید: (اولی ۸۰ رقم و دومی ۲۵ رقم) رقم دهدهی آنها را می‌توان نسبتاً سریع نوشت.

۲) یعنی الگوریتمی که همانند الگوریتم‌های احتمالاتی به اعداد تصادفی نیازی نداشته باشد.

3) Miller & Rabin

اعداد تصادفی استفاده می‌شود و پس از k مرحله اجرا، معلوم می‌کند که یا آن عدد مرکب است و یا به احتمال زیاد عددی اول است که در این حالت احتمال خطا از ۴^{-k} کمتر است. پیچیدگی زمانی این الگوریتم از مرتبهٔ $O(k\log^۲ n)$ است که در اینجا Oی بزرگ شامل ثابت نسبتاً کوچکی است. این الگوریتم در عمل بسیار سریع است و کاربردهایی نیز در رمزنگاری و تجارت الکترونیکی به‌منظور تولید «اعداد اول صنعتی» یافته است (هنری کوهن[۱]). به زبان نظریهٔ پیچیدگی محاسبات، خیلی کوتاه می‌توان گفت: $PRIMES \in co-\mathcal{RP}$.

الگوریتم تعیّنی ادلمن[۲]، پومرانس، و راملی[۳] در سال ۱۹۸۳ که از مباحث نظری فراوان و تعمیمی از قضیهٔ کوچک فرما به اعداد صحیح در میدان‌های دایره‌بُری سود می‌جوید، اعداد اول را به طور کامل مشخص می‌کند. این، بهترین الگوریتم تعیّنی است که تا پیش از آگوست ۲۰۰۲ ارائه شده و زمان اجرای آن از مرتبهٔ فوق چندجمله‌ای $(\log)^{O(\log\log\log n)}$ است. لگاریتم سه‌گانهٔ موجود در توان این رتبه، به قدری آرام رشد می‌کند که این‌الگوریتم توانسته است موفقیت‌های بسیار خوبی در کاربردهایی نظیر اثبات اول بودن اعداد با بیش از یک هزار رقم دهدهی به روش رمزشکنی به دست آورد.[۴]

الگوریتم‌های دیگری هم وجود دارد که در آنها از خم‌های بیضوی یا واریته‌های آبلی با گونهٔ بزرگ استفاده می‌شود. با این روش، ادلمن و هوانگ[۵] در تک‌نگاشتی بسیار مشکل و تکنیکی به سال ۱۹۹۲، توانستند الگوریتمی احتمالاتی با زمان اجرای چندجمله‌ای ارائه کنند که پس از k بار تکرار یا جواب قطعی (بدون هیچ‌گونه خطا) می‌داد و یا هیچ پاسخی نمی‌داد، که البته احتمال رخ‌دادن این حالت دوم کمتر از ۲^{-k} بود. به زبان نظریهٔ پیچیدگی محاسبات، خیلی کوتاه می‌توان گفت: $PRIMES \in \mathcal{ZPP}$.

با این پیش زمینه و نظر به سطح دشواری مسأله و فقدان موفقیت دیگری طی ده سال گذشته، به سختی می‌شد انتظار داشت که پاسخی کوتاه و عالی به این پرسش داده شود طوری‌که برای «همگان» قابل درک باشد.

ورود مانیندرا اگروال

مانینْدرااگروال که تحصیل کردهٔ علوم کامپیوتر و نظریهٔ محاسبات است، دکترای خود را در سال ۱۹۹۱ از دانشکدهٔ علوم و مهندسی کامپیوتر انستیتوی صنعتی هند در کانپور ($IITK$) دریافت کرد.

---

1) Henri Cohen 2) Adleman 3) Rumely

۴) پردامیخایلسکو ($Paeda\ Mih\check{a}ilescu$)، که قهرمان داستان دیگری است، در رسالهٔ دکتری خود در ETH زوریخ، ظرافت‌های اساسی در این الگوریتم ایجاد کرد و با این کار، مدت‌های طولانی بازیگر بازی **ثبت اعداد اول** بود. او اخیراً حدس کاتالان را ثابت کرده است.

5) Huang

پس از یک دوره استفاده از بورس هامبولت از دانشگاه Ulm در سال‌های ۹۶—۱۹۹۵ به عنوان استاد به کانپور بازگشت (خود او دربارهٔ این دوره می‌گوید: «واقعاً از زندگی در Ulm لذت بردم و این دوره تأثیر شایانی بر زندگی و تحقیقاتم از جنبه‌های گوناگون داشته است») دو سال پیش، زمانی که صورت ضعیفی از حدس ایزومورفیسم در نظریهٔ پیچیدگی را اثبات کرد، مورد توجه واقع شد[۱]. حوالی سال ۱۹۹۹، به همراه استاد راهنمای خود، سومنانت بیسواز[۲]، روی مسألهٔ تعیین اتحادهای چندجمله به کمک یک الگوریتم احتمالاتی کار می‌کرد و بااین کار توانست آزمون‌های احتمالاتی جدیدی برای اول بودن به‌دست آورد که در مقاله‌ای با عنوان «آزمون‌های اول بودن و همانی به‌کمک باقیماندهٔ چینی» منتشر ساخت[۱].

نقطهٔ آغاز داستان، تعمیمی از قضیهٔ کوچک فرما به چندجمله‌ای‌ها بود که تمرین ساده‌ای برای یک درس مقدماتی در نظریهٔ اعداد یا جبر است. صورت این تعمیم چنین است که اگر اعداد طبیعی a و n نسبت به هم اول باشند، آنگاه n اول است اگر و فقط اگر $(x-a)^n \equiv (x^n - a) \pmod n$ در حلقهٔ چندجمله‌ای‌های $\mathbb{Z}[x]$. هر چند این، روشی بسیار عالی برای تعیین اعداد اول است، استفاده از آن دشوار است. محاسبهٔ $(x-a)^n$ به تنهایی مستلزم زمانی بیش از آن چیزی است که غربال اراتستن نیاز دارد. با این حال، اگروال و بیسواز دقیقاً برای چندجمله‌ای‌ها از همین اندازه، آزمون احتمالاتی برای تعیین اتحادشان ارائه دادند که احتمال خطای آن کراندار بود و به طور کلی از بسط دادن چندجمله‌ای‌ها در آن پرهیز شده‌بود. متأسفانه، این آزمون با اینکه زمان محاسبه‌اش از نوع چندجمله‌ای است، قابل رقابت با آزمون میلر و رابین نیست. به این ترتیب، ایدهٔ جدیدی تولد یافته بود، لکن در بدو امر، تنها می‌توانست به‌سان یک پاورقی بر تاریخ آزمون‌های اول بودن، ثبت شود. دو سال بعد اگروال به همراه دانشجویانش در IITK شروع به بررسی جزئیات توانایی روش جدید در تشخیص اعداد اول کرد و به این توانایی اعتقاد راسخ داشت.

دو پروژهٔ کارشناسی

فرآیند پذیرش دانشجو در انستیتوی صنعتی هند دقیق و انتخابی است. یک آزمون مرسوم دو مرحله‌ای به‌نام آزمون ورودی ناپیوسته (JEE) به‌منظور پذیرش دانشجو در هفت رشتهٔ درسی در ITT و دو انستیتوی دیگر انجام می‌شود. سال گذشته ۱۵۰۰۰۰ هندی درخواست پذیرش داده بودند که پس از یک آزمون اولیه سه ساعتی در ریاضی، فیزیک و شیمی ۱۵۰۰۰ نفر از آنها برای مرحلهٔ دوم دعوت شدند. این مرحله نیز متشکل بود از یک آزمون دو ساعتی در همان سه موضوع

---

۱) حدس ایزومورفیسم برمن ($Berman$) و هارتمنیس ($Hartmanis$)، حاکی است که $\mathcal{P} \neq \mathcal{NP}$. اگر این حدس ثابت شود، اولین مسأله از هفت مسألهٔ جایزه‌دار قرن که بنیاد ریاضی کِلِی برای هر کدام از آنها یک میلیون دلار جایزه وضع کرده است، حل خواهد شد.

2) Somenat Biswas

و در نهایت ۲۹۰۰ نفر توانستند پذیرش بگیرند و از میان آنها ۴۵ نفر در رشتهٔ علوم کامپیوتر قبول شده بودند. تعجبی ندارد که در هند، برای آماده‌سازی داوطلبان شرکت در آزمون JEE، پول خوبی دریافت می‌شود و فارغ‌التحصیلان این دانشگاه در هر کجای دنیا مشتاقانه دعوت به‌کار می‌شوند.

اکنون [پس از دو سال] اگروال با چنین دانشجویان با انگیزه‌ای مشغول کار بر روی آزمون‌های اول بودن، بود. در ضمن کار با راجات باتاشارجی[1] و پارشات پندی [2] این ایده بروز کرد که لازم نیست جستجو را در میان چندجمله‌ای‌های $(x-a)^n$ با توان به این بزرگی انجام داد، بلکه کافی است ماندهٔ آن را پس از تقسیم بر $x^r - 1$ در نظر بگیریم و اگر r رابطه‌ای لگاریتمی با n داشته باشد، آنگاه این ماندهٔ خیلی کوچکتر را می‌توان به طور مستقیم و طی زمانی چندجمله‌ای با یک الگوریتم مناسب محاسبه نمود. اگر n عددی اول باشد، مطمئناً به ازای همهٔ r و nهای متباین با a داریم[3]:

$$(x-a)^n = x^n - a \pmod{x^r - 1, n} \qquad (T_{r,a})$$

سؤال این است که کدام a و r می‌توانند به نتیجهٔ عکس منجر شوند، یعنی اول بودن n؟ دو دانشجوی مزبور در پروژهٔ کارشناسی مشترک خود [5] با فرض $a = 1$، شرط‌های روی r را مورد بررسی قرار دادند. آنها با بررسی آزمون‌هایی که به ازای $r \le 100$ و $n \le 10^{10}$ انجام دادند، به حدس زیر رسیدند: اگر r و n نسبت به هم اول باشند و

$$(x-a)^n \equiv \quad \pmod{x^r - 1, n} \qquad (T_{r,1})$$

آنگاه یا n اول است یا $n^2 \equiv 1 \pmod r$. برای یکی از اولین $\log_2 n$ تا عدد اول r، این حالت دوم رخ نمی‌دهد، لذا اثباتی برای اول بودن n به‌دست آمده بود که زمان اجرای آن چندجمله‌ای از مرتبهٔ $O(\log^{3+\varepsilon} n)$ بود.

در اینجا، دو قهرمان داستان ما که تاکنون در پشت پردهٔ نمایش بودند، وارد می‌شوند. دو دانشجو به نام‌های نیراج کایال و نیتین ساکسناکه هر دو در المپیاد بین‌المللی ریاضی سال ۱۹۹۷ عضو تیم هند بودند. آنها به‌جای ریاضیات، در رشتهٔ علوم کامپیوتر تحصیل می‌کردند زیرا آیندهٔ شغلی بهتری در انتظار آنان است، با این حال توانستند در نظریهٔ پیچیدگی محاسبات، راهی برای ادامهٔ فعالیت در ریاضی در سطوح بالا، بیابند. آن دو، در پروژهٔ کارشناسی مشترکشان، رابطهٔ بین آزمون $(T_{r,1})$ را با آزمون‌های مشابه با آن که در حالت جواب منفی، اثباتی برای مرکب بودن عدد داده شده ارائه می‌دهد و در حالت جواب مثبت، هیچ پاسخ روشنی به‌دست نمی‌دهد، بررسی کردند. مسأله‌ای بسیار پر و پیمان بود. آنها قادر بودند نشان دهند که با فرض صحت

---

1)Rajat Bhatacharjee 2) Parashant Pandey

۳) من به تبعیت از اگروال و دیگران، تساوی باقیمانده‌های $p(x)$ و $q(x)$ را پس از تقسیم بر $x^2 - 1$ و تقسیم ضرایب بر n با نماد $p(x) \equiv q(x) \pmod{x^2 - 1, n}$ نشان داده‌ام.

فرضیهٔ ریمان، آزمون $(T_{r,1})$ برای اثبات اول بودن را می‌توان به حالت‌های $r = 2, \cdots, 4\log_2^2 n$ محدود کرد. به این ترتیب می‌توان یک الگوریتم تعیّنی با پیچیدگی زمانی $O(\log^{6+\varepsilon} n)$ به‌دست آورد. به علاوه، آنها نشان دادند که حدس باتاشارجی و پندی از حدس باسابقهٔ کارل پومرانس نتیجه می‌شود. همچنین در ارتباط با جستجوی ردهٔ «اعداد درون‌نگر» ایده‌ای از اثبات به ذهنشان رسیدکه بعداً معلوم شد ایده‌ای اساسی است. نتیجهٔ کارهای این دو نفر در آوریل ۲۰۰۲ با عنوان «به سوی آزمون‌های اول بودن با زمان اجرای چندجمله‌ای تعیّنی» انتشار یافت[۹]. یار در خانه و ما گرد جهان می‌گردیم!

تغییر دیدگاه

تابستان آن سال، آنها به منزلشان نرفتند، بلکه مستقیماً تحصیل در دورهٔ دکتری را آغاز کردند. در واقع، ساکسنا می‌خواست برای ادامهٔ تحصیل به خارج از کشور برود ولی از قضای روزگار، نتوانست از دانشگاه مورد نظر خود، بورس تحصیلی بگیرد. هنوز یک تغییر دیدگاه خیلی کوچک مانده بود. آن دو در رسالهٔ کارشناسی خود، آزمون $(T_{r,a})$ را برای $a = 1$ ثابت و r متغیر، مطالعه کرده بودند. اما چه می‌شد اگر r را ثابت و a را متغیر می‌گرفتند؟ رخ‌داد طلایی در صبح روز ۱۰ جولای به وقوع پیوست. با انتخاب پارامتر مناسب، توانستند روشی برای تشخیص توان‌های اعداد اول به‌دست آورند. نتیجه‌ای که آنان به‌دست آوردند، آنطور که دَن برنشتاین بیان می کند این گونه است:

قضیه. (اگروال_ ساکسنا_ کایال) فرض کنید $n \in \mathbb{N}$ و $s \le n$. گیریم q و r اعداد اول باشند که $q|r-1$، $n^{\frac{r-1}{q}} \not\equiv 0, 1 \pmod r$ و $\binom{q+s-1}{s} \ge n^{2[\sqrt{r}]}$.
اگر برای هر $1 \le a \le s$ داشته باشیم:

(i) a نسبت به n اول است، و

(ii) در حلقهٔ چندجمله‌ای‌های $\mathbb{Z}[x]$، $(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$،

آنگاه n یک توان اول است.

اثبات ساده، کوتاه و خلاقانهٔ این قضیه آنقدر مرا به‌وجد آورد که نتوانستم از بیان طرحی از آن در پیوست صرف‌نظر کنم. اکنون این قضیه، مستقیماً به الگوریتم AKS منجر می‌شود[۱]:

۱. ببین که آیا n توانی از یک عدد طبیعی است؟ در این صورت به مرحلهٔ ۵ برو.

۲. (q, r, s) را طوری انتخاب کن که در فرض‌های قضیه صدق کند.

---

۱) در سایت اینترنتی

http://www.tum.de/m3/ftp/Bornemann/PARI/aks.txt

دستورهای اجرایی نرم‌افزار $PARI.GP$ که مخصوص نظریهٔ اعداد است، آزادانه در دسترس همه قرار داده شده است.

۳. برای $a = ۱, \cdots, s-۱$ مراحل زیر را انجام بده.

(i) اگر a مقسوم علیه n است به مرحلهٔ ۵ برو.

(ii) اگر $(x-a)^n \not\equiv x^n - a \pmod{(x^r-۱, n)}$ به مرحلهٔ ۵ برو.

۴. n اول است، الگوریتم تمام.

۵. n مرکب است، الگوریتم تمام.

مرحلهٔ اول را می‌توان به کمک صورتی از روش تکرار نیوتن طی زمان چندجمله‌ای انجام داد . زمان اجرای مرحلهٔ ۳ که مرحلهٔ اصلی است، با استفاده از محاسبات مبتنی بر روش FFT (تبدیل فوریهٔ سریع) برابر است با $\widetilde{O}(sr\log^۲ n)$ که در اینجا علامت مد روی O، چند عامل لگاریتمی در s، r و $\log_۲ n$ را با هم یکی می‌کند. به این ترتیب برای رسیدن به مقصود نهایی باید r و s با سرعت حداکثر چندجمله‌ای برحسب $\log n$ رشد کند. این وظیفه بر عهدهٔ مرحلهٔ ۲ است. ابتدا نشان می‌دهیم اصلاً چه چیزی ممکن است رخ دهد. قرار دهید $s = \theta q$ که θ عامل ثابت است. فرمول استرلینگ رابطهٔ مجانبی

$$\log \binom{q+s-۱}{s-۱} \sim c_\theta^{-۱} q$$

را به‌دست می‌دهد. بر این اساس، شرایط قضیه مستلزم تخمین مجانبی

$$q \geq ۲c_\theta \lfloor \sqrt{r} \rfloor \log n$$

هستند. برای nهای بزرگ این وضعیت فقط وقتی رخ می‌دهد که بینهایت عدد اول r موجود باشد که $r-۱$ عامل اول $q \geq r^{\frac{۱}{۲}+\delta}$ دارد. اینجاست که ارتباطی مابین این مسأله و مسألهٔ مشهوری در نظریهٔ تحلیلی اعداد به‌وجود می‌آید.

سوفی ژرمن و قضیهٔ آخر فرما

مقدار بهینهٔ نسبت هزینه—سود $\frac{q}{r}$ به ازای اعداد اولی به‌دست می‌آید که به افتخار سوفی ژرمن، به نام او نام‌گذاری شده است: اینها اعداد اول فرد q و r هستند که $r = ۲q + ۱$ نیز اول است. در سال ۱۸۳۳ سوفی ژرمن نشان داد که برای این دست اعداد اول، به اصطلاح حالت اول قضیهٔ آخر فرما برقرار است: وقتی $q \nmid xyz$، معادلهٔ $x^q + y^q = z^q$ جواب صحیح ندارد. بنابراین، پرسشی که علاقه‌مندی شدیدی را ایجاد کرده بود این بود که آیابینهایت عدد اول از این نوع وجود دارد یا نه ؟ متأسفانه تا به امروز کسی پاسخ این سوال را نمی‌داند. در سال ۱۹۲۲ هاردی و لیتلوود[1] با الهام از

1) Hardy & Littlewood

ملاحظات شهودی، توانستند حدس دقیقی از چگالی واقعی اعداد اول ژرمنی ارائه دهند:

$$\#\{q \leq x;\ \ q \text{ و } 2q+1 \text{ اول هستند}\} \sim \frac{2c_2 x}{ln^2 x}$$

که در آن $c_2 = 0/6601618158000$ ثابت اعداد اول دوقلو است. اگر این حدس درست بود، می‌شد اعداد اول q و $r = 2q+1$ از اندازهٔ $O(\log^2 n)$ پیدا کرد که در فرض‌های قضیه صدق کند و در آن صورت الگوریتم AKS زمان اجرای چندجمله‌ای از مرتبهٔ $\widetilde{O}(\log^6 n)$ می‌داشت. چون صحت حدس فوق تا $x = 10^{10}$ تأیید شده است، الگوریتم AKS مانند الگوریتمی رفتار می‌کند که برای اعداد n با حداکثر ۱۰۰۰/۰۰ رقم، دارای پیچیدگی $\widetilde{O}(\log^6 n)$ است.

در سال ۱۹۸۵، حدود ۱۰ سال قبل از آنکه اندرو وایلز قضیهٔ آخر فرما را ثابت کند، ادلمن، فاوری[1] و هیث براون[2] چیزی را ثابت کردند که اصلاً نمی‌شد به کمک اعداد اول ژرمنی ثابت کرد؛ و آن این بود که حالت اول قضیهٔ آخر فرما، به ازای بی‌نهایت عدد اول برقرار است[۸]. در واقع ادلمن و هیث‌براون در تعمیم اعداداول ژرمنی، دقیقاً آن جفت‌های q و r را بررسی کردند که در الگوریتم AKS نقش کلیدی بازی می‌کنند.

مدال فیلدز

آنچه این سه نفر نیاز داشتند، دقیقاً این بود که تخمین

$$\#\{r \leq x;\ r \text{ و } q \text{ اولند};\ q|r-1\ ;\ q \geq x^{\frac{1}{2}+\delta}\} \geq c_\delta \frac{x}{\ln x}$$

به ازای توان مناسب $\delta > \frac{1}{2}$ برقرار باشد. جستجو برای یافتن بزرگترین δ با این خاصیت از سال ۱۹۶۹ با کار موریس گلدفلد[3] [۷] آغاز شد که نتیجه گرفت $\delta \simeq \frac{1}{12}$ و با کار اتین‌فاوری [۶] در سال ۱۹۸۶ به پایان رسید که مقدار $\delta = 0/1687 > \frac{1}{2}$ را به‌دست آورد. همهٔ این کارها از روش‌های بسیار عمیقی در نظریهٔ تحلیلی اعداد برمبنای غربال بزرگ اِنریکو بومبیری[4] سود می‌جستند. او غربالش را در سال ۱۹۶۵ در سن ۲۵ سالگی منتشر ساخت و در سال ۱۹۷۴ مدال فیلدز را دریافت کرد. بنابراین کسی که می‌خواهد جزئیات اثبات این تخمین را درک کند، وظیفهٔ سخت و سنگینی بردوش دارد. مانیندراااگروال در پاسخ به سؤال من که آیا از شما سه نفر کسی حاضر شد این وظیفه را برعهده گیرد، نوشت:

> «تلاش کردیم! ولی نظریهٔ غربال برای ما خیلی سنگین بود و هیچ پیش زمینه‌ای در نظریهٔ تحلیلی اعداد هم نداشتیم، لذا پس از مدتی آن را رها کردیم.»

البته نیازی هم نبود که آنها این کار را انجام دهند، چون «نتیجه‌ای که لازم داشتند قبلاً با دقت تمام بیان شده بود» و آنها می‌توانستند با اعتماد بر داور و گذشت زمان، بردرستی آن اطمینان داشته باشند

1)Fouvry 2) Heath-Brown 3)Morris Goldfeld 4) Enrico Bombieri

ــ البته همین طور هم بود چون نتیجه‌ای که فاوری دربارهٔ موضوع داغ قضیهٔ آخر فرما به‌دست آورده بود، در مجلهٔ *Inventions* چاپ شده بود. ولی اگر این جور نبود چه؟ فاوری در ارجاع دادن به لمی از بومبیری، فریدلندر[1] و ایوانیک[2] یک شرط اضافی را از قلم انداخته بود و این شرط اضافی، مقدار δ را به $\delta = ۰/۱۶۸۳ < \frac{۱}{۶}$ تقلیل می‌داد. حتی می‌توانست مقدار بحرانی δ کمتر از این باشد، چنانکه، بعداً فاوری به راجربیکر[3] گفت که او و گلین‌هارمن[4] مقدار اصلاح شدهٔ δ را در یک مقاله دوره‌ای در سال ۱۹۹۶ منتشر کرده‌اند[۳]. اتفاقاً، اگروال، کایال، و ساکسنا در ضمن جستجو در سایت اینترنتی *Google* در فهرست مراجع مقاله‌ای از پومرانس و شپارلنسکی[5]، به مقالهٔ فاوری برخورد کردند و زمانی که نیاز خود را به بهترین مقدار δ اعلام کردند، پومرانس آنها را به مقالهٔ بیکر و هارمن ارجاع داد. صرف‌نظر از مقدار بهینهٔ δ، شرط $\delta > ۰$ وجود سه تایی (q, r, s) را برای الگوریتم AKS با اندازهٔ لزوماً چندجمله‌ای از مرتبهٔ $r = O(\log^{\frac{۱}{\delta}} n)$ و $q, s = O(\log^{۱+\frac{۱}{۲\delta}} n)$ تضمین می‌کند، لذا با این اوصاف، می‌توان تضمین کرد که الگوریتم AKS دارای زمان اجرای $\widetilde{O}(\log^{۳+\frac{۳}{۲\delta}} n)$ است و به این ترتیب گزارهٔ $PRIEMS \in \mathcal{P}$ ثابت می‌شود: بسیار خوب! موفقیت حاصل شد. مقدار اصلاح شده‌ای که فاوری برای δ ارائه داد، زمان اجرای الگوریتم را به $\widetilde{O}(\log^{۱۱/۹۱۳} n)$ تبدیل می‌کند که اگر بخواهیم از شرّ علامت مَد خلاص شویم و به یاد سپردنش هم راحت‌تر باشد، $O(\log^{۱۲} n)$ [6]. سانجی داند[7] رئیس $IITK$، پس از مشاهدهٔ عنوان نیویورک تایمز، آنقدر هیجان زده شده بود که اعلام کرد اگروال جزو نامداران تراز اول در ریاضیات خواهد شد. جالب است بدانید که در سال ۲۰۰۶ اگروال تازه چهل ساله خواهد شد[8].

میزان عملی بودن الگوریتم

سؤالی که بلافاصله در مجامع خبری داخل اینترنت و در روزنامه‌ها مطرح شد، این بود که کاربردهای

1) Friedlander 2) Iwaniec 3) Rojer Baker 4) Glyn Harman 5) Shparlineski

۶) در ۲۲ ژانویه ۲۰۰۳، دن‌برنشتاین صورت جدیدی از مقالهٔ اولیهٔ خود را در اینترنت قرار داد که در آن با تغییر مختصری در قضیهٔ اگروال‌ـکایال ـساکسنا، که او آن را از لنسترا آموخته بود، اثبات حکم $PRIEMS \in \mathcal{P}$ را بدون ارجاع به مباحث عمیق در نظریهٔ تحلیلی اعداد، کامل‌تر کرده بود. قضیه‌ای از چبی‌شف وجود دارد حاکی از این‌که حاصل‌ضرب اعداد اول کوچکتر یا مساوی $۲k$ دست‌کم ۲^k است. تنها به کمک همین قضیه می‌توان از وجود دو عدد $r, s = O(\log^۵ n)$ که برای الگوریتم مناسب باشد، اطمینان حاصل کرد. این نشان می‌دهد که دشواری ریاضی مطلب که همانند سدّی جلوی درک کامل و «همگانی» این نتیجه را گرفته بود، فروریختنی است. شاید پاولو ریبنبوم (Paulo Ribenboim) حق داشته باشد که برای من نوشت: «ریاضیدانان باید در باب پیچیدگی استدلال‌هایشان تأمل کنند.»

7) Sanjay Dhande

۸) او قبلاً در ۳۰ اکتبر ۲۰۰۲ از بنیاد تحقیقاتی کلی جایزه گرفته بود. برندگان قبلی عبارت بودند از اندرووایلز، سمیرنف و شرام که احتمال‌دان هستند و برندگان مدال فیلدز یعنی کُن، لافورگ، و ویتن.

عملی این الگوریتم تا چه اندازه است؛ زیرا این روزها اعداد اول بزرگ نقش مهمی در رمزنگاری و تجارت الکترونیکی دارند. در بدو امر، باور داریم که یک مسألهٔ نظری مهم که سالیان سال از چنگ متخصصان فن می‌گریخت، حل شده است. خود اگروال تأکید می‌کند که او به این مسأله صرفاً به چشم یک چالش فکری می‌نگریست و الگوریتم کنونی AKS خیلی کندتر از الگوریتم‌هایی است که رکورد اثبات اول بودن را برای اعداد تا ۵۰۲۰ رقم شکسته‌اند[۱]. و بالاخره نباید فراموش کرد که تعریف رده‌های پیچیدگی نظیر $\mathcal{P}$، نظری محض است و شکل مجانبی با $n \longrightarrow \infty$ دارد. بنابراین در یک مورد خاص، مزیت یک الگوریتم با زمان اجرای چندجمله‌ای، بر یک الگوریتم فوق چندجمله‌ای، به احتمال زیاد فقط برای آن nهایی معلوم می‌شود که آنقدر بزرگ هستند که مدت زمان پاسخ برای هیچ کدام از این دو الگوریتم، به کمک سخت‌افزارهای موجود، به عمر ما قد نمی‌دهد. علاوه بر این، ثابت‌های موجود در Oی بزرگ هم در تخمین‌های عملی نقش بازی می‌کنند. با استفاده از آزمون میلر ـ رابین و به کمک یک رایانهٔ شخصی از ردهٔ $2GHz$ می‌توان اعداد اول صنعتی را که ۵۱۲ رقم دودوئی دارند در کسری از ثانیه تولید کرد، به علاوه در صورت لزوم می‌توان به روش $ECPP$ منسوب به اتکین ـ موراین[۲] که بر مبنای خم‌های بیضوی قرار دارد، در دو ثانیه، اول‌بودن آنها را هم ثابت کرد[۳]. پیچیدگی زمان محاسبهٔ این الگوریتم احتمالاتی در هاله‌ای از ابهام است (کارل‌پومرانس)، لکن ملاحظات شهودی حاکی از این است که یحتمل، مقدار آن حوالی $\widetilde{O}(\log^{6} n)$ است. از طرف دیگر، به علت ارزش زیادی که همنهشتی‌های چندجمله‌ای در مرحلهٔ سوم AKS دارد، ثابت موجود در کران بالای زمان اجرا یعنی $\widetilde{O}(\log^{6} n)$ آنقدر بزرگ است که تخمین زده می‌شود اجرای این الگوریتم برای عدد اول با ۵۱۲ رقم دودوئی، دو روز به طول بینجامد، هرچند دَن برنشتاین، هندریک لنسترا، فیلیپ والش[۴]، بیورن پونن[۵] و جف والِر[۶] قبلاً این ثابت را با ضریبی به اندازهٔ 2×10^{6} برابر ثابت موجود در الگوریتم اصلی، اصلاح کرده بودند. اوضاع و احوال تا ۲۵ ژانویه ۲۰۰۳ بدین منوال بود.[۴]

به این ترتیب، عاملی به اندازهٔ 10^{5} از ثابت‌های موجود در الگوریتم حذف می‌شود تا این الگوریتم به سطح قابل رقابت با بقیه برسد. روش $ECPP$ با ایدهٔ جدیدی منسوب به گلدواسر

---

۱) این مطلب را با ثبت بزرگترین عدد اول شناخته شده که در حال حاضر $2^{13466917} - 1$ عددی اول از نوع مرسن، با ۴۰۵۳۹۴۶ رقم دهدهی است خلط نکنید. ساختار این اعداد آنقدر شناخته شده است که می‌توان الگوریتم‌های مرسوم را در مورد آنها به‌کار برد.

2) Atkin-Morain

۳) به منظور دسترسی آزاد به برنامهٔ $PRIMO$ منسوب به مارسل مارتین($Marcel\ Martin$) که در حال حاضر رکورد را از آن خود دارد، به آدرس اینترنتی **http://www.ellipsa.net/pages/primo.html** رجوع کنید.

4) Felipe Voloch 5) Bjorn Poonen 6) Jeff Vaaler

و کیلیان آغاز شد که کاملاً غیرتجربی و در عین حال بسیار زیربنایی بود. چون روشی که اگروال، کایال، و ساکسنا ابداع کردند به طور غیرمنتظره‌ای جدید و عالی است، یقیناً باید منتظر باشیم که با کاملتر شدن این الگوریتم، توانایی‌های دیگر آن معلوم شود.

پخش رسانه‌ای

به جز گزارش جامع، محققانه، از نظر علمی درست و خواندنی که در هفته‌نامهٔ هندی $Frontline$ به تاریخ ۱۷ آگوست چاپ شده بود، نحوهٔ گزارش این خبر در رسانه‌های عمومی تأسف‌بار بود. اگروال درخواست من دربارهٔ اعلام نقش مهم او در این زمینه را مؤدبانه رد کرد و گفت: «از پوشش همگانی این رویداد صرف‌نظر کن.» مطمئناً مقاله‌ای که قبلاً اشاره کردیم در نیویورک تایمز چاپ شد، این نتیجه را به عنوان یک پیروزی ارج نهاده بود، اما به‌خاطر جایگزینی بعضی از واژه‌های فنی، به طرز مضحکی ساده و مبهم شده بود؛ مثلاً زمان اجرای چندجمله‌ای را تبدیل کرده بودند به «سریع»، یا «تعیّنی» تبدیل شده بود به «یقینی». با این تغییرات، مقاله را این‌طور می‌شد خواند: «سه نفر هندی به موفقیت بزرگی دست یافتند به خاطر این‌که اکنون دیگر رایانه می‌تواند به‌سرعت و به یقین معلوم کند که آیا عددی اول است یا نه. اما از طرف دیگر، الگوریتم جدید، هنوز کاربردی نیست، به خاطر این‌که روش‌های موجود سریعتر هستند و در عمل خطا هم ندارند.» خوب! خوانندهٔ این خبر با خود خواهد گفت: «عجب شانسی!». خبرگزاری آسوشیتدپرس، مقالهٔ نیویورک تایمز را تبدیل به گزارش تلفنی کرده بود که در آن حتی کلمهٔ «به یقین» تبدیل شده بود به «دقیقاً» و مطالب مربوط به زمان اجرا هم از مقدمهٔ مقاله حذف شده بود. فرجام تأسف‌بار این جریان خبری، مربوط است به سایت اینترنتی $Tagesschau$ در ۱۲ آگوست. عنوان این سایت این بود که «بالاخره اعداد اول را می‌توان دقیقاً محاسبه کرد.» و به دنبال آن مهملاتی از این دست آمده بود: «شادمانی دانش‌آموزان آلمانی بی‌حد و حصر است، چونکه بالاخره می‌توان اعداد اول را بی‌دردسر محاسبه کرد.» این خبر در پی اعتراض اعضای گروه خبری $de.sci.mathematik$ در اینترنت، حذف شد.

غیر از مقاله‌ای که در نیویورک تایمز چاپ شد، در رسانه‌های امریکایی به داستان این کشف واقعاً بی‌توجهی شد. در بریتانیا در شمارهٔ ۱۷ اگوست مجلهٔ «نیوساینتیست» مقاله‌ای چاپ شد که لااقل عبارت‌هایی چون «زمان چندجمله‌ای» در آن به کار رفته بود. با این حال، صحبت از الگوریتمی می‌کرد که در زمانی معقول، پاسخ مشخصی به مسأله می‌دهد. یک مقالهٔ مروری در شمارهٔ ۴ نوامبر **وال استریت جورنال** هم چاپ شده بود که عنوانی غلط‌انداز داشت:«یک ذهن زیبای هندی اینترنت را به جنب و جوش واداشته است». در شمارهٔ ۱۵ دسامبر **نیویورک تایمز** هم، کلایو تامپسون در **ستون اخبار آخر سال**، ادعا کرده بود: «از زمان یونانیان باستان، یافتن راهی برای اثبات اول بودن یک عدد طبیعی، جام مقدس ریاضیات شده بود.... اما در سال جاری سرانجام این جام را

یافتند.... این الگوریتم جدید، اول بودن اعداد بسیار بزرگی را معلوم می‌کند که استفاده از آنها، به ظاهر، امنیت تمام عیار خطوط انتقال پیام را فراهم می‌آورد.»

اما مشهورترین روزنامهٔ آلمانی زبان **نویه‌زوریخرزایتونگ**، اولین گزارش خود را در این زمینه در ۳۰ آگوست به چاپ رساند. در این مقاله به غلط، ادعا شده بود که تاکنون هیچ محک کاملاً مطمئنی که بتواند اول بودن را در مدت زمانی قابل قبول مشخص کند، ارائه نشده است. الگوریتمی که به‌خصوص برای اعداد اول مورد استفاده در رمزنگاری مناسب باشد، و امروز سه ریاضیدان هندی دقیقاً به این هدف نائل شده‌اند؛ لکن نتیجه‌ای که آنان به دست آورده‌اند چندان مورد ستایش شبکه‌های خبری و رسانه‌ها واقع نشد، به این دلیل که نمی‌توان آن را در مورد بزرگترین عدد اول شناخته شده به کار برد.

در تاریخ ۹ آگوست، **فرانکفورترالگماینه‌زایتونگ**، در ستون هنری خود متنی نمادین تحت عنوان «خدایان چندجمله‌ای، هندی‌های بااستعداد و اعداد اولشان» چاپ کرده بود، که در آن ابتدا ارتباطی برقرار می‌کرد بین ریاضیات هندی و معابد هندی و سپس چهار تن از این خدایان، دربارهٔ این نتایج جدید با یکدیگر مباحثهٔ کوتاهی می‌کردند: آگنی معترضانه گفت: «خوب این نتیجه به چه دردی می‌خورد؟» لکشمی جواب داد:« برای حمله‌کردن! برای کدگذاری داده‌ها در پیام‌رسانی‌های الکترونیکی، به اعداد اول نیاز داریم. الگوریتم‌های رمزنگاری متعددی وجود دارند مثل RSA و رمزنگاری استاندارد داده‌ها DES.کلید این رمزها اعدادی هستند با عامل‌های اول، و امروز می‌توان این عامل‌ها را به راحتی در مدت زمانی که به صورت یک چندجمله‌ای برحسب داده‌های ورودی است پیدا کرد». رودرا حرف او را قطع کرد و گفت: «اما پیش از این، آزمون‌هایی نظیر آزمون میلر—رابین شناخته شده بودند که اگر به دفعات کافی آنرا تکرار کنیم می‌توان اول بودن یک عدد را تا هر درجه از دقتی که بخواهیم، با احتمال زیاد مشخص کنیم، حتی برای بزرگترین اعداد شناخته شده. و کدگذاری به روش تجزیه به اعداد اول، ربطی به آزمون تعیین اول بودن یک عدد ندارد، که این مسأله‌ای است کاملاً متفاوت. آنچه که این هیولاها کشف کرده‌اند، به درد مقاصد امنیتی نمی‌خورد». بالاخره اوشاس که میزبان بود ترانهٔ آشتی را سرود و گفت: «سخت نگیرید. بیایید از این نتیجه هوشمندانه‌ای که غرب را به تحسین واداشته است و از این نفس مسیحایی ریاضیات مقدسمان لذت ببریم». آیا خوانندهٔ این متن با خود نمی‌اندیشد که دلیل این همه قیل و قال چیست؟!

تدابیر آینده

این سه نفر تصمیم گرفتند نتایج کارشان را برای مجلهٔ Annals of Math ارسال کنند و در این باره در حال گفتگو با پیترسارنک[1] هستند. می‌خواهند مقاله را از این قالب علوم کامپیوتری خارج کرده

1) Peter Sarnak

ریاضی‌وارتر کنند تا برای چاپ در Annals مناسب‌تر باشد. اگروال دربارهٔ وضعیت روحی و آیندهٔ دو دانشجوی دکترای خود، کایال و ساکسنا می‌گوید: «آنها خوشحالند ولی در عین حال نسبت به ادامهٔ کار دلسرد هستند. من به آنها گفتم که پسران باهوشی هستند. در مورد برنامهٔ دکترای آنها هم مطمئنم این کار به عنوان رسالهٔ دکتری آنها قبول خواهد شد. با این حال از آنها خواستم که دو سال دیگر در دانشگاه بمانند، چون این مدت، زمان مناسبی است تا بر آموخته‌های خود بیفزایند. آنها هنوز می‌بایست با چیزهای بیشتری آشنا شوند، ولی در تصمیم‌گیری آزادند، گویا از TIFR (انستیتوی تحقیقات بنیادی تاتا) پیشنهاد پذیرش داشته باشند».

پیوست

آنچه در زیر می‌آید طرحی از اثبات قضیهٔ آگروال، کایال و ساکسنا است به آن صورتی که دَن‌برنشتاین ارائه کرده است.[۴]

طرح اثبات: عامل اول p از n را در نظر می‌گیریم که $p^{\frac{r-1}{q}} \not\equiv 0, 1$ به هنگ r و نشان می‌دهیم که اگر (i) و (ii) برای هر $1 \leq a \leq s$ برقرار باشد، آنگاه عدد n توانی از p است. به این منظور همان کاری را انجام می‌دهیم که اگروال در صبح روز دهم جولای پس از یافتن قضیه انجام داد، یعنی حاصل‌ضربهایی به شکل $t = n^i p^j$ که $0 \leq i, j \leq \lfloor\sqrt{r}\rfloor$ در نظر می‌گیریم. اصل لانه‌کبوتری نتیجه می‌دهد که دو جفت مجزای (i_1, j_1) و (i_2, j_2) از این نوع توان‌ها موجودند که $t_1 = n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} = t_2$ به هنگ ۲ . هدف، این است که ثابت کنیم در واقع $t_1 = t_2$ و از این رو به ازای عددی چون l، $n = p^l$. از (ii) و به کمک قضیهٔ کوچک فرما، نتیجه می‌شود که

$$(x-a)^{t\mu} \equiv x^{t\mu} - a \pmod{x^r - 1, p} \qquad (*)$$

برای هر $1 \leq a \leq p$ و $\mu = 1, 2$. کایال و ساکسنا در پروژهٔ خود این نوع توان‌ها را «خودنگر» نامیدند و نشان دادند که برای این قبیل توان‌ها، همنهشتی $t_1 \equiv t_2$ به هنگ r، به همنهشتی $t_1 \equiv t_2$ به هنگ $\#G \gg r$ تبدیل می‌شود. با انتخاب مناسب پارامترها، # آنقدر بزرگ می‌شود که نتیجه می‌گیریم: $t_1 = t_2$. اگروال معتقد است این تبدیل همنهشتی، «بهترین قسمت مقاله است». اما این تبدیل همنهشتی چگونه صورت می‌گیرد؟ چون $t_1 = t_2 \pmod{r}$ نتیجه می‌گیریم که $x^r - 1$ تفاضل $x^{t_1} - x^{t_2}$ را عاد می‌کند، لذا از $(*)$ به‌دست می آوریم که

$$(x-a)^{t_2} \equiv (x-a)^{t_2} \pmod{x^r - 1, p}$$

بنابراین $g^{t_1} = g^{t_2}$ برای هر $g \in G$ که در اینجا گروه ضربی تولید شده توسط عوامل خطی $(\zeta_r - a)$ در میدان دایره‌بری روی $\mathbb{Z}/p\mathbb{Z}$ است که از الحاق ریشه‌های rام یکه یعنی ζ_r بدست می‌آید. با انتخاب یک عنصر اولیه g، یعنی عنصری از مرتبهٔ $\#G$ نشان می‌دهد که $\#G|(t_1 - t_2)$. از طرف دیگر بنابر (i) و اینکه $p^{\frac{r-1}{p}} \not\equiv 0, 1$ به هنگ n و کمی استفاده از ترکیبیات و نظریهٔ مقدماتی

میدان‌های دایره‌بُری می‌توان نتیجه گرفت که گروه G است که $\binom{q+s-1}{s}$ عنصر دارد . بنابراین فرض‌های مربوط به ضرایب دو جمله‌ای نتیجه می‌دهند که

$$|t_1 - t_2| < n^{\lfloor\sqrt{r}\rfloor} p^{\lfloor\sqrt{r}\rfloor} \leq n^{2\lfloor\sqrt{r}\rfloor} \leq \binom{q+s-1}{s} \leq \#G$$

و از اینجا تساوی مطلوب $t_1 = t_2$ به‌دست می‌آید.

نکتهٔ افزوده شده بر اثبات

در اوایل مارس ۲۰۰۳ ، اگروال، کایال و ساکسنا، اصلاحیه‌ای از صورت اولیهٔ مقاله‌شان را در اینترنت منتشر ساختند:

http://www.cse.iitk.ac.in/news/primality-V3.pdf

این اصلاحیه مشتمل است بر اصلاحات لنسترا به اضافهٔ یک کران جدید $O(\log^{7/5} n)$ برای پیچیدگی زمانی، مذکور در قضیهٔ ۳.۵.

تشکر و قدردانی

از مانیندرا اگروال صمیمانه تشکر می‌کنم که با وجود هزاران پیام تبریک الکترونیکی که برای او رسیده بود، حاضر شد به‌سؤالات من دربارهٔ پیش‌زمینه‌های موضوع، مهربانانه و به طور کامل پاسخ دهد.

مراجع

[1] MANINDRA AGRAWAL and SOMENATH BISWAS, Primality and identity testing via Chinese remaindering, in *40th Annual Symposium on Foundations of Computer Science*, IEEE Computer Soc., Los Alamitos, CA, 1999, pp. 202-8.

[2] MANINDRA AGRAWAL, NEERAJ KAYAL, and NITIN SAXENA, PRIMES is in P, IIT Kanpur, Preprint of August 8, 2002, http://www.cse.iitk.ac.in/news/primality.html.

[3] Roger C. BAKER and GLYN HARMAN, The Brun-Titchmarsh Theorem on average, in *Proceedings of a Conference in Honor of Heini Halberstair*, vol. 1, Birkhäuser Boston, Boston, MA, 1996, pp. 39-103.

[4] DANIEL BERNSTEIN, Proving Primality after Agrawal-Kayal-Saxena, version of January 25, 2003, http://cr.yp.to/papers.html#aks.

[5] RAJAT BHATTACHARJEE and PRASHANT PANDEY, Primality Testing, Bachelor of Technology Project Report, IIT Kanpur, April 2001, http://www.cse.iitk.ac.in/research/btp2001/primality. html.

[6] ÉTIENNE FOUVRY, Théorème de Brun-Titchmarsh; application au théorème de Fermat, Invent. Math. 79(1985) 383-407.

[7] MORRIS GOLDFELD, On the number of primes p for which $p+a$ has a large prime factor. Mathematika **16** (1969) 23-27.

[8] D. ROGER HEATH-BROWN, The first case of Fermat's Last Theorem, *Math. Intelligencer 7*, no. 4(1985), 40-47, 55.

[9] NEERAJ KAYAL and NITIN SAXENA, *Towards a Deterministic Polynomial-Time Primality Test*, Bachelor of Technology Project Report, IIT Kanpur, April 2002, http://www.cse.iitk.ac.in/research/btp2002/primality.htm1.

[10] R. RAMACHANDRAN, A Prime solution, *Frontline*, India's National Magazine, **19** (August 17, 2002), http://www.flonnet.com/fl1917/19171290.htm.

ترجمه: روح‌ا... جهانی‌پور
دانشگاه کاشان، گروه ریاضی
پست الکترونیک: jahanipu@kashanu.ac.ir

فرهنگ و اندیشهٔ ریاضی
شماره ۳۱ (پاییز ۱۳۸۲) صص. ۲۵ تا ۴۰

مسائل‌سکه و تمبرفرابنیوس و مجموعه‌های مطلوب

مهدی جوادی و محمدرضا رجب‌زاده مقدم

چکیده

یکی از مسائل تاریخی در نظریهٔ اعداد، مسألهٔ سکه و تمبر است که به فرابنیوس نسبت داده می‌شود. بدین معنی که اگر در کشوری ارزش سکه و تمبر بر پایهٔ مجموعه‌ای از اعداد ضرب و چاپ شده باشد، و شهروندی مایل باشد مبلغی را از ترکیب سکه‌های خود بپردازد و یا ترکیبی از تمبرها را در ارسال نامه پستی خود استفاده کند، آنگاه تعیین بیشترین مقداری که نتواند از ترکیب سکه‌ها بپردازد، یا کمترین مقدار هزینهٔ پستی که از ترکیب تمبرها نتواند استفاده کند، از مسائل جالب توجه در نظریهٔ اعداد هستند که توجه بسیاری از ریاضیدانان را به خود جلب کرده است.

در این مقاله سعی می‌شود موضوع را مورد بحث و بررسی قرار داده و به مطالعهٔ مجموعه‌های مطلوب بپردازیم. همچنین تا حد امکان اثبات قضایا را با روشی متفاوت و ساده‌تر ارائه می کنیم.

۱. مقدمه

با توجه به ملموس بودن اعداد اول بعضی از کشورها سکه‌ها و تمبرهای خود را برمبنای اعداد اول

واژه‌های کلیدی: مسأله فرابنیوس، عدد فرابنیوس، مجموعه‌های مطلوب

ارزش گذاری، ضرب و چاپ می‌کردند.

به عنوان مثال فرض کنید سکه و تمبرهای کشوری با مقادیر ۱، ۵، ۷ و ۱۳ واحدی ارزش‌گذاری شده‌اند، و شهروندی فاقد سکهٔ یک واحدی بوده ولی از بقیهٔ سکه‌ها به تعداد کافی داراست. بیشترین مقداری را که نمی‌تواند از ترکیب سکه‌های موجودش بپردازد، چقدر است؟ از طرف دیگر چنانچه از هر تمبر به تعداد کافی داشته باشد، ولی پاکت نامه وی حداکثر چهار فضا برای چسباندن تمبر داشته باشد، کمترین هزینه پستی را که نتواند از ترکیب تمبرهای بر روی پاکت خود بچسباند چقدر خواهد بود؟

مسائلی از این قبیل سالها به عنوان سرگرمی در ریاضیات مطرح بوده‌اند و تا سال ۱۹۳۰ به طور جدی مورد مطالعه قرار نگرفته بودند، ولی در نیمهٔ دوم قرن گذشته به طور بسیار گسترده‌ای مورد بررسی و تحقیق قرار گرفته‌اند.

دو مسألهٔ مطروحهٔ فوق ارتباط بسیار نزدیکی با هم دارند، که به طور خیلی خلاصه هر مطلب در بخشی جداگانه معرفی و مورد بحث قرار خواهد گرفت.

بخش چهارم مقاله به مطالعه بر روی مجموعه‌های مطلوب[۱] اختصاص می‌یابد و مسائل مطرح شدهٔ مذکور، به ویژه تمبرهای پستی می‌توانند به کمک مجموعه‌های مطلوب به صورت جامعی مطالعه شوند.

لازم به یاد آوری است که مجموعه‌های مطلوب توسط اولین نویسنده [۴ و ۵] معرفی و مورد مطالعه قرار گرفته‌اند.

۲. مسألهٔ سکه و عدد فرابنیوس

مسأله سکه غالباً به فرابنیوس نسبت داده می‌شود که وی همواره در سخنرانیهای خود آن را یادآوری می‌کرد. اولین نتایج در این خصوص توسط یکی از دانشجویان فرابنیوس در سال ۱۹۴۲ به نام براوِر[۲] [۱] منتشر شد. سپس هوف مایستر[۳] [۱۱] در یک سری از کتابنامه‌های درسی بدان پرداخته است. همچنین مهدی جوادی[۴] [۳] در سال ۱۹۷۲ در پایان‌نامهٔ فوق لیسانس خود این مسأله را مورد بحث و بررسی قرار داده است. فرض کنید b_1، b_2، ...، b_k اعداد صحیح مثبت و نسبت به هم اول باشند، یعنی

$$(b_1, b_2, \ldots, b_k) = 1$$

1) Pleasant sets 2) A. Brauer 3) G. Hofmeister 4) M. Djawadi

عدد صحیح نامنفی N دارای نمایشی[1] بر پایهٔ مجموعهٔ اعداد

$$B_k = \{b_1, b_2, \dots, b_k\}$$

است، هرگاه اعداد صحیح نامنفی x_1، x_2، ...، x_k وجود داشته باشند به قسمی که

$$N = x_1 b_1 + x_2 b_2 + \dots + x_k b_k. \qquad (1)$$

تعیین بزرگترین عدد صحیح

$$g(B_k) = g(b_1, b_2, \dots, b_k)$$

که نتواند نمایشی همانند (۱) داشته باشد، به مسألهٔ فرابنیوس[2] مشهور است. معمولاً عدد صحیح $g(B_k)$ را عدد فرابنیوس[3] با پایهٔ B_k نامند.

به آسانی ملاحظه می‌شود که اگر $1 \in B_k$، تمام اعداد صحیح $N \geq 0$ دارای نمایشی به صورت (۱) می‌باشند. در این حالت عدد فرابنیوس را معمولاً -1 در نظر می‌گیرند، یعنی $g(B_k) = -1$.

حال نشان می‌دهیم که هر مجموعهٔ B_k دارای عدد فرابنیوس است.

لم ۱.۲. فرض کنید $B_k = \{b_1, b_2, \dots, b_k\}$ مجموعه‌ای از اعداد صحیح نامنفی باشند، به قسمی که

$$(b_1, b_2, \dots, b_k) = 1.$$

در این صورت هر عدد صحیح به اندازهٔ کافی بزرگ N دارای نمایش زیر است:

$$N = x_1 b_1 + x_2 b_2 + \dots + x_k b_k,$$

که در آن x_i ها اعداد صحیح نامنفی هستند.

اثبات. چون $(b_1, b_2, \dots, b_k) = 1$، در نتیجه عدد ۱ را می‌توان به صورت ترکیبی خطی از b_i ها نوشت، یعنی

$$1 = -\underbrace{(y_1\beta_1 + \dots + y_s\beta_s)}_{Y} + \underbrace{(z_{s+1}\beta_{s+1} + \dots + z_k\beta_k)}_{Z},$$

که در آن $y_i > 0$، $z_i \geq 0$ و β_1، β_2، ...، β_k جایگشتی از اعداد صحیح b_1، b_2، ...، b_k هستند.

1) Representation 2) Frobenius problem 3) Frobenius number

حال $b_۱$ را به طور متوالی به صورت ترکیبی خطی از B_kها می‌نویسیم:

$$\begin{array}{lcll} N & = & (b_۱-۱) & Y \\ N+۱ & = & (b_۱-۲) & Y+Z \\ N+۲ & = & (b_۱-۳) & Y+۲Z \\ & \vdots & & \\ N+b_۱-۲ & = & & Y+(b_۱-۲)Z \\ N+b_۱-۱ & = & & \quad (b_۱-۱)Z \end{array}$$

که تمام ضرایب نامنفی می‌باشند. بدیهی است که با اضافه کردن مضارب $b_۱$ به ترکیب خطی فوق، تمام اعداد صحیح بزرگتر نیزدارای نمایشهایی به صورت مورد نظر هستند.

فرض کنید $B_k=\{b_۱,b_۲,\dots,b_k\}$ مستقل[1] باشد، یعنی هیچ عنصر b_j ای نمایشی بر حسب سایر عناصر B_k نداشته باشد.

لم ۲.۲. اگر B_k پایه‌ای مستقل باشد، آنگاه

$$k\leq \min\{b_i\ ;\ ۱\leq i\leq k\}$$

اثبات. فرض کنید $\min\{b_i\}=b_۱$. (برهان خلف) فرض کنیم:

$$k\geq b_۱+۱.$$

در این صورت تعداد عناصر $b_۲$، $b_۳$، $\dots$، b_k حداقل $b_۱$ تا است. بنابر این یا $i\geq ۲$ وجود دارد که $b_i\overset{b_۱}{\equiv}۰$، یا $i,j\geq ۲$ موجودند به قسمی که

$$b_i\overset{b_۱}{\equiv}b_j$$

که در هر دو حالت منجر به وابستگی بین عناصر پایهٔ B_k می‌شود و خلاف فرض است.

کارایی همنهشتی عناصر پایهٔ B_k به پیمانهٔ یکی از عناصر پایه مانند $b_۱$ در مطالعهٔ مسألهٔ فرابنیوس بسیار اساسی است.

فرض کنید L دستگاه کامل مانده‌های[2] $l\overset{b_۱}{\not\equiv}۰$ باشد. به ازای هر $l\in L$، کوچکترین عدد صحیح مثبتی مانند $t_l\overset{b_۱}{\equiv}l$ با نمایشی به وسیلهٔ $b_۲$، $b_۳$، $\dots$، b_k وجود دارد. مجموعهٔ $\{t_l\ ;\ l\in L\}$ را دستگاه کمین[3] به پیمانهٔ $b_۱$ می‌نامیم.

فرض کنید N عددی صحیح نامنفی باشد. اگر $N\overset{b_۱}{\equiv}۰$، آنگاه N دارای نمایشی به وسیلهٔ تنها $b_۱$ است. اگر $N\overset{b_۱}{\equiv}l\overset{b_۱}{\not\equiv}۰$، آنگاه N دارای نمایشی به وسیلهٔ B_k است اگر و فقط اگر $N\geq t_l$.

1) Independent 2) Complete system of residues 3) Minimal system

بحث فوق گزاره زیر را ایجاب می‌کند.

گزارهٔ ۳.۲. (براور و شوکلی[1] [۲]). با توجه به بحث فوق، عدد فرابنیوس به صورت زیر است:

$$g(B_k) = \max_{l\in L} t_l - b_۱.$$

تبصره. فرض کنید $B_k = \{b_۱, b_۲, \ldots, b_k\}$ یک پایه باشد. یکی از مسائل دیگر تعیین کوچکترین عددی است که نتواند به صورت ترکیب خطی از پایهٔ B_k نوشته شود، که آن را با $n(B_k)$ نشان می‌دهیم.

مثال. فرض کنید $B_۳ = \{۵, ۷, ۱۳\}$ یک پایه باشد. در این صورت به آسانی ملاحظه می‌شود که هیچ یک از اعداد زیر

$$۱, ۲, ۳, ۴, ۶, ۸, ۹, ۱۱, ۱۶$$

نمایشی بر حسب $B_۳$ ندارد، و عدد فرابنیوس $g(B_۳) = ۱۶$. همچنین $n(B_۳) = ۹$.

نتیجهٔ جالب زیر همانند گزارهٔ ۳.۲ است، که توسط سلمر[2] [۱۲] اثبات شده، ولی در اینجا اثبات بسیار ساده‌ای از آن ارائه شده است.

قضیهٔ ۴.۲. (سلمر [۱۴]). فرض کنید B_k یک پایه و L همانند فوق تعریف شده باشد. در این صورت:

$$n(B_k) = \frac{۱}{b_۱}\sum_{l\in L} t_l - \frac{b_۱ - ۱}{۲}.$$

اثبات. واضح است که تعداد $N \overset{b_۱}{\equiv} l \not\equiv ۰$ با شرط $۰ < N < t_l$، برابر است با $[\frac{t_l}{b_۱}]$ (جزء صحیح $\frac{t_l}{b_۱}$). با فرض $۰ < l < b_۱$، داریم:

$$[\frac{t_l}{b_۱}] = \frac{(t_l - b_۱)}{b_۱}$$

حال اگر روی عناصر $l \in L$ مجموع بگیریم، حکم حاصل می‌شود.

تبصره. کاربرد دو قضیهٔ فوق را در ساده‌ترین حالت زیر مورد مطالعه قرار می‌دهیم. فرض کنید:

$$B_۲ = \{b_۱, b_۲\},$$

---

1) J. E. Shockley 2) E. S. Selmer

که در آن $(b_1, b_2) = 1$. به وضوح دستگاه کمین مانده‌ها به پیمانهٔ b_1 به صورت زیر است :

$$\{t_l\} = \{b_2, 2b_2, \ldots, (b_1 - 1)b_2\}.$$

حال بنا بر گزارهٔ ۳.۲،

$$g(b_1, b_2) = \max_{l\in L} t_l - b_1$$

در نتیجه

$$g(b_1, b_2) = (b_1 - 1)b_2 - b_1 = b_1b_2 - b_2 - b_1. \tag{2}$$

همچنین قضیهٔ ۴.۲ ایجاب می‌کند که

$$\begin{aligned} n(b_1, b_2) &= \frac{1}{b_1}\sum_{l\in L} t_l - \frac{b_1 - 1}{2} \\ &= \frac{1}{b_1}(b_2 + 2b_2 + \ldots + (b_1 - 1)b_2) - \frac{b_1 - 1}{2} \\ &= \frac{1}{2}(b_1 - 1)(b_2 - 1) \end{aligned}$$

یا

$$n(b_1, b_2) = \frac{1}{2}(g(b_1, b_2) + 1). \tag{3}$$

سالهاست که دو فرمول (۲) و (۳) شناخته شده‌اند و به لحاظ تاریخی فرمول (۳) به سیلوستر[1] [۵] در سال ۱۸۸۴ منسوب می‌شود.

۳. مسألهٔ تمبرهای پستی

همان طور که در بخش قبل بیان شد در گذشته‌های دور سکه‌ها و همچنین تمبرهای پستی بر پایهٔ اعداد اول ارزش گذاری می‌شدند. فرض کنید ارزش تمبرهای پستی کشوری به صورت ۱، ۵، ۷ و ۱۳ واحدی باشد، و شخصی به تعداد کافی از هر تمبر دارا ست، ولی پاکت نامهٔ وی حداکثر برای ۴ تمبر مکان مناسب دارد.

این سؤال مطرح است که:

«کمترین هزینه‌ای را که از ترکیب چهار تمبر نمی‌تواند بر روی پاکت تمبر بچسباند چقدراست؟»

1) J. J. Sylvester

با کمی دقت و محاسبه به آسانی ملاحظه می‌شود که این عدد ۲۹ است، زیرا هر عدد کمتر از آن را می‌توان به صورت ترکیب خطی از ۱، ۵، ۷ و ۱۳ نوشت. (البته با رعایت انتخاب حداکثر چهار تمبر!) در نتیجه ۲۹ کوچکترین عددی است که نمی‌تواند به صورت ترکیب خطی از اعداد ۱، ۵، ۷ و ۱۳ نوشته شود. (به عنوان مثال: $۱۴ = ۱ + ۱۳ = ۲ \times ۷ = ۲ \times ۱ + ۵ + ۷$ یا $۲۸ = ۴ \times ۷ = ۲ \times ۱ + ۲ \times ۱۳$)

حال مسأله را به روش کلی مطرح می‌کنیم. فرض کنید

$$A_k = \{a_۱, a_۲, \dots, a_k\} \ , \ \ ۱ = a_۱ < a_۲ < \dots < a_k$$

مجموعه‌ای از اعداد طبیعی باشد، که آن را پایهٔ صحیح[1] نیز نامند (همان مجموعهٔ ارزش تمبرهاست). به ازای عدد صحیح h (تعداد محل‌های ممکن تمبر بر روی پاکت)، مجموعهٔ ترکیبات خطی زیر را تشکیل می‌دهیم

$$\{x_۱a_۱ + x_۲a_۲ + \dots + x_ka_k; x_i \geq ۰ \ , \ x_۱ + \dots + x_k \leq h\} \qquad (۴)$$

حال تعیین کوچکترین عدد صحیح $N_h(A_k)$ که به صورت ترکیب خطی فوق نمایش پذیر نباشد، از اهمیت ویژه‌ای برخوردار است. معمولاً کران زیر مورد بحث قرار می‌گیرد:

$$n_h(A_k) = N_h(A_k) - ۱,$$

که در این صورت تمام اعداد صحیح کمتر یا مساوی $n_h(A_k)$ نمایشی به صورت (۴) دارند، ولی برای $n_h(A_k) + ۱$ چنین نیست.

در نظریهٔ اعداد معمولاً بازه‌ها[2] به صورت زیر تعریف می‌شوند:

$$[a, b] = \{a, a + ۱, a + ۲, \dots, b - ۱, b\},$$

که در آن $a, b \in \mathbb{Z}$ و $a \leq b$.

بنابر این در بحث فوق می‌توان گفت که تمام اعداد صحیح در بازهٔ $[۰, n_h(A_k)]$ دارای نمایشی به صورت (۴) هستند، در حالی که برای $n_h(A_k) + ۱$ چنین نیست. از این رو قرار می‌دهیم $A'_k = A_k \cup \{۰\}$.

همچنین فرض کنیم

$$\begin{aligned} hA_k &= \{a_۱ + a_۲ + \dots a_i \ ; \ a_i \in A_k \ , \ i = ۱, ۲, \dots, h\} \\ &= \{a_۱ \ , \ a_۱ + a_۲ \ , \ a_۱ + a_۲ + a_۳ \ , \ \dots \ , \ a_۱ + \dots + a_{h-۱} \ , \ a_۱ + \dots + a_h\} \end{aligned}$$

1) Integral basis 2) Intervals

حال

$$n_h(A_k) = \max\{n \in \mathbb{N} \ ; \ [0, n] \subseteq hA_k'\}$$

را h–برد[1] $n_h(A_k)$ تعریف می‌کنیم، و مجموع

$$x_1 a_1 + x_2 a_2 + \ldots + x_k a_k$$

را که $\sum x_i \leq h$ به عنوان h–نمایش[2] در نظر می‌گیریم، حتی اگر تعداد جملات کمتر از h مؤلفه باشد.

بدیهی است که عدد نامنفی n دارای چندین نمایش بر حسب پایهٔ A_k است.
کمترین تعداد مؤلفه‌ای که در نمایش n به کار می‌رود با

$$A(n) = \min\{\sum_{i=1}^{r} x_i \ ; \ \sum_{i=1}^{r} x_i a_i = n \ , \ x_i \geq 0\}$$

نشان می‌دهیم. در این صورت نمایش n را با $A(n)$ مؤلفه (که یکتا نیست) کمین[3] نامیم.

مثال ۱.۳. در مثال شروع این بخش، اگر شخص فاقد تمبر ۱۳ واحدی باشد، یعنی $k = 3$،

$$A_3 = \{1, 5, 7\}$$

و $h = 4$. با محاسبات مستقیم می‌توان نشان داد که تمام اعداد صحیح نامنفی $n \leq 22$ دارای ۴–نمایش‌اند، ولی $n = 23$ دارای چنین نمایشی نیست! بنابر این $n_4(A_3) = 22$.

حال چنانچه $h = 3$ در نظر بگیریم و $A_3 = \{a_1 = 1, a_2 = 5, a_3 = 7\}$، به آسانی مشاهده می‌شود که حتی با وجود $a_1 = 1$، بحث از ترکیبات اعضای A_3 (در حالت کلی A_k) معقول نیست، زیرا تمام اعداد کمتر از $a_2 = 5$ را نمی‌توان ترکیب خطی با $h = 3$ مؤلفه نوشت، مثلاً عدد ۴ را نمی‌توان مجموع ۳ مؤلفه از A_3 (در حالت کلی از A_k) نوشت. از این رو به وضوح بایستی شرط $h \geq a_2 - 1$ را قائل شویم.

به آسانی ملاحظه می‌شود که، اگر $A_1 = \{a_1 = 1\}$ آنگاه

$$n_h(A_1) = n_h(\{1\}) = h.$$

حال در زیر می‌توان فرمول جامعی برای A_2 ارائه نمود.

قضیهٔ ۲.۳. فرض کنید $A_2 = \{a_1, a_2\}$ یک پایه باشد که $1 = a_1 < a_2$. در این صورت

$$n_h(A_2) = (h + 2 - a_2)a_2 + a_2 - 2$$

1) h-range 2) h-representation 3) Minimal

اثبات. بدیهی است که باید $a_۲$ را هر چقدر ممکن است انتخاب کرد و سپس در صورت وجود مکانی کافی روی پاکت برای حداقل $a_۲ - ۱$ تمبر از نوع $a_۱ = ۱$، می‌توان از مضرب انتخاب $a_۲$ به انتخاب بعدی رفت. ولی این عملی نیست. هنگامی که $h + ۲ - a_۲$ تمبر از نوع $a_۲$ به کار می‌بریم، می‌توان به آن $a_۲ - ۲$ تمبر از نوع $a_۱ = ۱$ اضافه کرد. بنابر این

$$n_h(A_۲) = (h + ۲ - a_۲)a_۲ + a_۲ - ۲$$

تبصره. تا آنجا که اطلاع در دست است، فرمول جامعی برای $n_h(A_k)$ با $k \geq ۳$، وجود ندارد.

۴. مجموعه‌ها و پایه‌های مطلوب

یک h–نمایش به صورت (۴) را منظم[1] یا اقلیدسی[2] نامند، هرگاه نخست بزرگترین تمبر a_k را هر چقدر ممکن است به کار گیریم، سپس تمبر $a_{k-۱}$ را به هر تعداد ممکن مورد استفاده قرار دهیم و غیره. این بدین معناست که شرط اضافی زیر را همواره مورد نظر داشته باشیم:

$$x_۱a_۱ + x_۲a_۲ + \ldots + x_ja_j \;<\; a_{j+۱} \quad , \quad j = ۱, ۲, \ldots, k - ۱ \qquad (۵)$$

حال اگر تنها چنین نمایشهایی مجاز باشند و حداکثر با h مؤلفه در نظر گرفته شوند، آنگاه طول بزرگترین بازهٔ $[۱, n]$ با h–نمایشهای منظم را h–برد منظم می‌نامیم و با نماد $g_h(A_k)$ نشان می‌دهیم. بدیهی است که به ازای هر h و هر A_k،

$$g_h(A_k) \leq n_h(A_k), \qquad (٦)$$

زیرا نمایش منظم یک عدد ممکن است کمین نباشد ((۵) را ملاحظه کنید).

مثال. فرض کنید $k = ۳$، $A_۳ = \{۱, ۵, ۷\}$، $h = ۴$ و

$$A(n) = \min\{\sum_{i=۱}^{۴} x_i \;\; ; \;\; \sum_{i=۱}^{۴} x_ia_i = n \quad , \quad x_i \geq ۰\}$$

به آسانی ملاحظه می‌شود که نمایشهای منظم $n \leq ۹$ کمین هستند، در حالی که $۱ \times ۳ + ۷ \times ۱ = ۱۰$ منظم و $۵ \times ۲ = ۱۰$ کمین است. با توجه به کران $h \leq ۴$، در مورد عدد ۱۱ چنین نیست، $۱ \times ۴ + ۷ \times ۱ = ۱۱$ در نتیجه $g_۴(A_۳) = ۱۰ < n_۴(A_۳) = ۲۲$.

1) Regular 2) Euclidean

تبصرهٔ ۱. برخلاف نمایشهای کمین، نمایشهای منظم یک عدد صحیح یکتاست و به آسانی تعیین می‌شود. همان طور که انتظار می‌رود، این موضوع، مطالعه و بررسی h–بردهای منظم را از h–بردهای معمولی ساده‌تر می‌کند.

تعریف زیر که گویای عنوان بخش حاضر می‌باشد برای اولین بار توسط مهدی جوادی [۴ و ۵] ارائه شده است، و در مطالعات ما نقش بسیار اساسی ایفا می‌کند.

تعریف ۱.۴. (م. جوادی [۴]). فرض کنید $A_k = \{a_1, a_2, \dots, a_k\}$ یک پایه باشد. دراین صورت A_k را یک پایه (یا مجموعهٔ) مطلوب[1] نامیم، هرگاه نمایش منظم تمام اعداد $n \in \mathbb{N}$ بر حسب A_k کمین باشد.

تبصرهٔ ۲. تعریف فوق ایجاب می‌کند که اگر A_k پایه‌ای مطلوب باشد، آنگاه

$$n_h(A_k) = g_h(A_k).$$

به آسانی ملاحظه می‌شود که $A_2 = \{a_1, a_2\}$، $a_1 < a_2$ همواره پایه‌ای مطلوب است، زیرا با به کار بردن a_2 به هر تعداد ممکن بهترین نتیجه حاصل می‌شود.

اینک این سؤال مطرح می‌شود که چه محکی برای مطلوبیت پایه‌های A_k، $(k > 2)$ می‌توان ارائه کرد؟ جواب این سؤال در قضیهٔ ۳.۴ ارائه می‌شود.

بدون تردید می‌توان ادعا کرد که اغلب نتایج اساسی بر روی مجموعه‌های (یا پایه‌های) مطلوب توسط مهدی جوادی، زولنر[2] و سلمر به دست آمده است. برای اطلاعات بیشتر خوانندگان علاقه‌مند را به منابع [۵، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۲، ۱۴ و ۱۶] ارجاع می‌دهیم.

تعریف زیر در اثبات قضیهٔ بعدی مورد نیاز است.

تعریف ۲.۴. h–نمایش زیر را در نظر می‌گیریم:

$$\sum x_i a_i = x_1 a_1 + x_2 a_2 + \dots + x_k a_k \ \ , \ x_i \geq 0$$

که در آن $x_1 + x_2 + \dots + x_k \leq h$. اگر h–نمایش فوق منظم باشد، باید

$$x_1 a_1 + x_2 a_2 + \dots + x_j a_j < a_{j+1} \ \ , \ \ j = 1, 2, \dots, k-1.$$

حال چنانچه در ترکیب

$$\sum e_i a_i = e_1 a_1 + e_2 a_2 + \dots + e_k a_k$$

1) Pleasant basis (or set) 2) J. Zollner

a_i ها را با حاصل

$$a_i = \gamma_{i-۱} a_{i-۱} - \sum_{j=۱}^{i-۲} \beta_j^{(i)} a_j \quad , \quad ۲ \le i \le k \quad , \quad \gamma_i \ge ۲ \quad , \quad \beta_j^{(i)} \ge ۰ \qquad (۷)$$

جایگزین کنیم، آنگاه این عمل را یک a_i–انتقال[۱] نامیم.

به عنوان مثال، در نمایش منظم $n \in \mathbb{N}$، یعنی

$$n = e_k a_k + e_{k-۱} a_{k-۱} + \ldots + e_۲ a_۲ + e_۱ \qquad (۸)$$

می‌توان S_k انتقال همانند (٦) از a_k، سپس $S_{k-۱}$ انتقال از $a_{k-۱}$، و سرانجام $S_۲$ انتقال از $a_۲$ انجام داد، تا به نمایش زیر دست یابیم:

$$n = x_k a_k + x_{k-۱} a_{k-۱} + \ldots + x_۲ a_۲ + x_۱. \qquad (۹)$$

قضیهٔ جالب زیر محکی برای مطلوبیت پایه‌های A_k است، و توسط مهدی جوادی [۴] اثبات شده است. وی در آنجا اثباتی نسبتاً تکنیکی ارائه کرده است، که در اینجا با اثباتی دیگر و ساده‌تر ارائه می‌شود.

قضیه ۳.۴. (م. جوادی [۴]). فرض کنید $A_k = \{a_۱, a_۲, \ldots, a_k\}$ پایه‌ای باشد، که در شرایط (۴) صدق کند. قرار دهید:

$$a_k = \gamma a_{k-۱} - (\beta_{k-۲} a_{k-۲} + \ldots + \beta_۲ a_۲ + \beta_۱), \qquad (۱۰)$$

که در آن $\gamma = [\frac{a_k}{a_{k-۱}}]$ و $\sum_{i=۱}^{k-۲} \beta_i a_i$ به وسیلهٔ $A_{k-۲}$ منظم است. همچنین فرض کنید $A_{k-۱}$ پایه‌ای مطلوب باشد، در این صورت A_k نیز مطلوب است اگر و فقط اگر

$$\gamma > \beta_۱ + \beta_۲ + \ldots + \beta_{k-۲} \qquad (۱۱)$$

اثبات. فرض کنید A_k پایه‌ای مطلوب باشد. بنابر فرض داریم

$$\gamma a_{k-۱} = \beta_۱ + \beta_۲ a_۲ + \ldots + \beta_{k-۲} a_{k-۲} + a_k \qquad (۱۲)$$

ملاحظه می‌شود که طرف راست تساوی، نمایشی منظم است. حال اگر بنابر فرض خلف، حکم نادرست باشد، بایستی

$$\beta_۱ + \beta_۲ + \ldots + \beta_{k-۲} \le \gamma,$$

1) a_i - transfer

آنگاه مجموع ضرایب طرف راست تساوی (۱۲) بزرگتر از ضرایب نامنظم γa_{k-1} است، که بنا بر تعریف ۱.۴، پایهٔ A_k نامطلوب و خلاف فرض است.

به‌عکس، نخست $k = 3$ اختیار می‌کنیم. بنابر رابطهٔ (۱۰) در فرض، داریم:

$$a_3 = \gamma a_2 - \beta_1.$$

حال چون A_2 همواره مطلوب است، در نتیجه بنابر شرط لزوم قضیه، A_3 مطلوب می‌باشد اگر و فقط اگر $\gamma > \beta_1$.

اینک حالت کلی A_k و رابطهٔ (۱۰) را به عنوان یک a_k–انتقال از $n = \sum e_i a_i$ به $n = \sum x_i a_i$ در نظر می‌گیریم (روابط (۸) و (۹) را ملاحظه کنید). از طرفی چون $\sum e_i a_i$ منظم است، $e_k \geq x_k$ و بایستی تعداد $\delta = e_k - x_k$ انتقال از (۱۰) انجام دهیم. در این صورت $\sum e_i a_i = \sum x_i a_i$ را می‌توان به صورت زیر نوشت:

$$\sum_{i=1}^{k-2} e_i a_i + (\delta\gamma + e_{k-1}) a_{k-1} = \sum_{i=1}^{k-2} (x_i + \delta\beta_i) a_i + x_{k-1} a_{k-1} \tag{13}$$

حال کافی است نشان دهیم که رابطهٔ (۱۰) نتیجه می‌دهد که به ازای هر نمایش $\sum x_i a_i$، $\sum e_i \geq \sum x_i$. اینک رابطهٔ (۱۲) را به عنوان دو نمایش متفاوت به وسیلهٔ A_{k-1} در نظر می‌گیریم، و مجموع ضرایب طرف چپ و راست را به ترتیب با $\sum_l$ و $\sum_r$ نشان می‌دهیم. مشاهده می‌شود که

$$\sum_l - \sum_r = \sum_{i=1}^{r-1} (e_i - x_i) + (e_k - x_k)(\gamma - \beta_1 - \beta_2 - \ldots - \beta_{k-2})$$

$$\geq \sum_{i=1}^{k-1} e_i - \sum_{i=1}^{k} x_i > 0.$$

در نتیجه $\sum_l > \sum_r$، که یک تناقض است، زیرا بنابر فرض استقراء A_{k-1} مجموعه‌ای مطلوب می‌باشد و از این رو طرف چپ رابطهٔ (۱۲) به وسیلهٔ A_{k-1} نمایشی منظم خواهد بود. این اثبات قضیه را کامل می‌کند.

قضیهٔ فوق دارای نتیجه جالب زیر است.

نتیجهٔ ۴.۴. اگر A_{k-1} مجموعه‌ای مطلوب باشد و

$$a_k - a_{k-1} = \tau(a_{k-1} - a_{k-2}),$$

آنگاه A_k نیز مطلوب است.

اثبات. بنابر فرض، داریم

$$a_k = (\tau + ۱)a_{k-۱} - \tau a_{k-۲}.$$

فرض کنید

$$\tau a_{k-۲} = \beta_{k-۱}a_{k-۱} + \beta_{k-۲}a_{k-۲} + \ldots + \beta_۲ a_۲ + \beta_۱$$

نمایشی منظم به وسیلهٔ پایهٔ مطلوب $A_{k-۱}$ باشد، و در نتیجه $\sum_{i=۱}^{k-۱} \beta_i \leq \tau$. از این رو

$$a_k = (\tau + ۱ - \beta_{k-۱})a_{k-۱} - (\beta_{k-۲}a_{k-۲} + \ldots + \beta_۲ a_۲ + \beta_۱)$$

در شرط (۱۱) از قضیهٔ ۳.۴ صدق می‌کند، زیرا از $\sum_{i=۱}^{k-۱} \beta_i \leq \tau$ نتیجه می‌شود که $\tau + ۱ > \sum_{i=۱}^{k-۱} \beta_i$ و لذا

$$\tau + ۱ - \beta_{k-۱} > \beta_۱ + \ldots + \beta_{k-۲}.$$

بنابر این A_k مطلوب است.

تعریف ۵.۴. مجموعه (یا پایه) $A_k = \{a_۱ = ۱, a_۲, \ldots, a_k\}$ کاملاً مطلوب[1] نامیده می‌شود، هرگاه هر پایهٔ جزئی[2] آن

$$A_i = \{۱, a_۲, \ldots, a_i\} \quad , \quad i = ۲, ۳, \ldots, k$$

مطلوب باشد.

تبصره ۲. بنابر قضیهٔ جوادی (قضیهٔ ۳.۴)، A_k کاملاً مطلوب است اگر و فقط اگر به ازای هر $i \leq k$، شرط مشابهی همانند (۱۱) برقرار باشد. بنابر این ملاحظه می‌شود که قضیهٔ ۳.۴، محکی است برای تشخیص پایه‌های کاملاً مطلوب.

در [۵] مطلب زیر در خصوص پایه‌های کاملاً مطلوب اثبات شده است، که اثبات ارائه شده در اینجا تا حدی متفاوت و ساده‌تر است.

قضیهٔ ۶.۴. فرض کنید پایهٔ $A_۴$ مطلوب است، در این صورت بایستی پایهٔ جزیی $A_۳$ نیز مطلوب باشد.

اثبات. به روش برهان خلف، فرض کنید $A_۳$ پایه‌ای نا مطلوب باشد. با توجه به رابطهٔ (۱۲) و به ازای $k = ۳$ و ضرایب مناسب q و s، داریم

$$qa_۲ = a_۳ + s$$

1) Completely pleasant 2) Partial basis

حال نمایش نامنظم $qa_۲$ دارای مجموع ضریبی کوچکتر از نمایش منظم $a_۳ + s - ۱$ است. در نتیجه $q < s + ۱$ یا $q \leq s$. اگر اینها را به عنوان نمایشهایی به وسیلهٔ $A_۴$ در نظر بگیریم، که بنابر فرض مطلوب است، ملاحظه می‌شود که باید نمایشی منظم از $qa_۲$ به وسیلهٔ $A_۴$ با حداکثر q عامل وجود داشته باشد. به ویژه این ایجاب می‌کند که

$$a_۴ \leq qa_۲ = a_۳ + s \leq a_۳ + a_۲ - ۱ \leq ۲a_۳ - ۲.$$

بنابر این $۲a_۳ \geq a_۴ + ۲$. در این صورت نمایش نامنظم $۲a_۳$ باید دارای نمایشی منظم در $۲A'_۴ = ۲(A'_۴ \cup \{۰\})$ باشد. به وضوح این تنها وقتی امکان پذیراست که

$$۲a_۳ = a_۴ + a_۲,$$

یا

$$a_۳ + (q - ۱)a_۲ = a_۴ + s$$

با شرط $q \leq s$. ولی طرف چپ رابطهٔ اخیر نامنظم می‌باشد در حالی که طرف راست منظم است و این تناقض، اثبات را کامل می‌کند.

نتیجهٔ ۷.۴. هر پایهٔ مطلوب $A_۴$ کاملاً مطلوب است.

اثبات. بنابر تبصرهٔ ۱، هر پایهٔ $A_۲$ مطلوب است. قضیهٔ فوق بیان می‌کند که $A_۳$ نیز مطلوب می‌باشد. در نتیجه هر پایهٔ جزیی $A_۴$ مطلوب است، و لذا بنابر تعریف ۵.۴، تمام پایه‌های $A_۴$ کاملاً مطلوب هستند.

فصل حاضر را با بیان دو نتیجهٔ جالب از زولنر و جوادی ([۸] را ملاحظه کنید) به پایان می‌بریم.

قضیه ۸.۴. (زولنر [۱۵]) اگر A_k پایه‌ای مطلوب باشد، آنگاه به ازای $۳ \leq i \leq k$، مجموعهٔ $\{۱, a_۲, a_i\}$ نیز مطلوب است.

اثبات. به [۱۵] رجوع شود.

تبصره ۳. در تبصرهٔ ۲ بیان شد که قضیهٔ ۳.۴ محکی برای تمام مجموعه‌ها (یا پایه‌های) کاملاً مطلوب است. حال می‌توان این سؤال را مطرح کرد که چه پایه‌هایی مطلوبند، ولی کاملاً مطلوب نیستند.

مجدداً نخستین نتیجه در این وادی توسط مهدی جوادی در سال ۱۹۷۹ برای حالت $k = ۵$ به صورت زیر ارائه شده است.

قضیهٔ ۹.۴. (م. جوادی [۵]). تمام پایه‌های مطلوب $A_۵$ با پایهٔ جزیی نامطلوب $A_۴$ تنها به

صورت زیر هستند:

$$A_{۵} = \{۱, ۲, b, b + ۱, ۲b\} \quad , \quad b \geq ۴.$$

اثبات. به [۵] رجوع شود.

منابع

[1] Brauer, A., "On a problem of partitions," Amer. J. Math 64 (1942), 299-312.

[2] Brauer, A., and Shockley, J. E. , "On a problem of partitions II", Amer. J. Math 76 (1954), 343-346.

[3] Djawadi, M., "Untersuchung eines speziellen Beispliels Zu einen problem von Frobenius", Diplomarbeit Math. Inst. Joh. Gutenberg - Uni- Mainz, 1972.

[4] Djawadi, M., "Kennzeichnung von Megen mit einer additiven Minimal eigenschaft", Diss. Mainz (1974), 1-69.

[5] Djawadi, M., "Kennzeichnung von Megen mit einer additiven Minimal eigenschaft", J. Rein Angew. Math. 311/312 (1979), 307-314.

[6] Djawadi, M. , "Charakterisierung einer klasse funfelementiger angenehmer Mengen," Mainzer Seminarberichte in additiven Zahlentheorie 1 (1983), 72-74 .

[7] Djawadi, M. , "Neuer Beweis fur die charakterisierung der funfelementigen angenehmen Mengen", Mainzer Seminarberichte in additiven Zahlentheorie 2 (1988), 51-56.

[8] Djawadi, M., and Hofmeister, G. , "Linear diophantine problems", Number Theory, New York Seminar, Springer-Verlag (1996), 91-95.

[9] Djawadi, M., and Hofmeister, G. , "The postage stamp problem", Mainzer Seminarberichte in additiven Zahlentheorie, 3 (1993), 187-195.

[10] Djawadi, M. , and Hofmeister, G. ,"Zahlentheorie," nach den Vorlesungen, im ws 1993/94 und 1994, Dezember 1995.

[11] Djawadi, M. , and Hofmeister, G. ,"Linear diophantine problems", Arch. der Math. Vol. 66 (1996), 19-29.

[12] Hofmeister, G., "Linear diophantine problems," Bull. Iran. Math. Soc. Vol. 8, No. 2 (1981), 121 - 155.

[13] Sylvester, J. J., "Mathematical questions with their solutions", Educational Times 47 (1884), 21.

[14] Selmer, E. S. , "On the postage stamp problem with three stamp denominations", Math. Scand. 47 (1980), 29-71.

[15] Zollner, J. , "Uber angenehmen Mengen," Mainzer Seminarberichte in additiven Zahlentheorie 1 (1983), 53-71.

محمدرضا رجب‌زاده مقدم (نویسنده مسؤول)
Math Stat. Department,
York University, Toronto,
ON. M3J 1P3, Canada
و دانشکده علوم ریاضی، دانشگاه فردوسی مشهد
پست الکترونیک: mrrm5@yahoo.ca
مهدی جوادی
7905 Bayview Ave.
Suite 1013 Thornhill,
ON.L3T 7N3, Canada

فرهنگ و اندیشهٔ ریاضی
شماره ۳۱ (پاییز ۱۳۸۲) صص. ۴۱ تا ۷۵

معرفی و نقد کتاب

ارسلان شادمان

گسترش ریاضیات ۱۹۵۰ تا ۲۰۰۰[1]

به کوشش ژان پل پیه

مقدمه

این کتاب به منزلهٔ جلد دوم از دو مجلّدی است که به گسترش ریاضیات در قرن بیستم اختصاص دارند. جلد نخست آن [P 1994]، مربوط به نیمهٔ اول قرن، در شماره‌های ۲۶ و ۲۷ فرهنگ و اندیشهٔ ریاضی معرفی گردید [ش ۱۳۸۰ آ] و [ش ۱۳۸۰ ب]. پیش‌بینی شده بود که جلد دوم [P 2000] در شماره ۲۸ معرفی شود. با عرض پوزش از تأخیر، اینک به معرفی آن می‌پردازیم. در مقایسهٔ این دو کتاب، باید گفت که از جهات متعددی شبیه‌اند، اما از چند سو با هم اختلاف اساسی دارند. اختلاف ناشی است از تکامل و تکمیل دیدگاه کمیتهٔ علمی، هم‌چنین از تکامل و تکمیل موضوع‌های مورد بحث ریاضی در نیمهٔ دوم قرن، تأسیس نهادهای علمی—اجتماعی و تعدّد مقالات فرهنگی و تاریخی در سال‌های پس از جنگ جهانی دوم و تبلور کاربردهای متنوع‌تر ریاضیات در همهٔ عرصه‌های دانش بشری.

گسترش ۱۹۰۰ [P 1994] زمانی طراحی شده بود که هنوز فکر برگزاری سال جهانی ریاضیات (WMY2000) علنی و مطرح نشده بود. اما گسترش ۱۹۵۰ [P 2000] درست در سال جهانی ریاضیات منتشر گردید. در این کتاب، پیش از فهرست مطالب به این نکته اشاره می‌شود که «برگزاری سال جهانی ریاضیات (WMY2000) را اتحادیهٔ بین‌المللی

1) Development of Mathematics 1950-2000, Edited by Jean-Paul PIER, Birkhäuser Verlag, Basel-Boston-Berlin 2000, ISBN 3-7643-6280-4

ریاضی[1] پیشنهاد کرد و در ۱۹۹۷ مجمع عمومی یونسکو به اتفاق آراء تصمیم گرفت از این فکر حمایت کند. همچنین شورای بین‌المللی علوم[2] موافقت خود را با آن اعلام نمود» سپس اظهار امیدواری شده است که این کتاب «در تدارک پیشامدهای در حال وقوع سهم مفیدی ایفا کند». نهایتاً از حامیان مالی طرح یعنی یونسکو و وزارت تحقیقات علمی لوکزامبورگ، سپاسگزاری شده است.

شاید بتوان گفت که طرح [P 1994] یکی از زمزمه‌های موفقی بود که به شکل‌گیری فکر (WMY2000) کمک کرد و [P 2000] حاصل تلاشی سخت کوشانه است تا نشان دهد کارهای سهل و ممتنع هم با همّتِ بلند و داشتن انگیزهٔ قوی قابل اجرا است و توقع وفای به عهد از کمربستگانِ خدمت به جا که «الکریم اذا وعد وفا».

دربارهٔ معرفی حاضر، باید اقرار کنم که از سویی ناچارم جنبهٔ اجمال را از حد [ش ۱۳۸۰ آ و ب] هم بگذرانم به این معنی که از فهرست جزئیات داخل هر مقاله صرف نظر می‌کنم. وگرنه، با توجه به حجم و محتوای [P 2000] که تعداد مقالات آن سه‌برابر [P 1994] و تعداد صفحاتش تقریباً دوبرابر است و به‌علاوه مقدمه‌ای مبسوط و چندین مصاحبه و فهرست خواندنی دیگر را در بردارد، تقریباً یک شمارهٔ معمول فرهنگ و اندیشهٔ ریاضی تنها به معرفی این کتاب اختصاص خواهد یافت. این هم نه از نظر خوانندگان و نه از نظر هیأت تحریریهٔ مجله قابل قبول است. از سوی دیگر هم، شیوهٔ کارم را تا حدی متفاوت با شیوهٔ [ش ۱۳۸۰ آ و ب] قرار خواهم داد. برای این منظور نکاتی را که از نظر تاریخی و فرهنگی در کتاب مورد بحث جالب‌تر یافته‌ام به عنوان نمونه در این معرفی می‌گنجانم و خوانندگان را به تورق اصل کتاب و خواندن بخش‌های معتنابهی از آن شدیداً توصیه می‌کنم. بخش‌هایی از کتاب عیناً برای ترجمه و درج در فرهنگ و اندیشهٔ ریاضی مناسب است. شاید از آن مهم‌تر این که فهرستی غنی از منابع مورد توجه تاریخ ریاضیات معاصر در این کتاب هست که می‌تواند هم برای فرهنگ و اندیشهٔ ریاضی و هم برای مجلهٔ تاریخ علم و ارائه در سمینارهای مختلف دانشگاهی و یا در جشنواره‌هاو دهه‌های ریاضی ارائه شود. علاوه بر آن، مقالات و منابع ارائه شده در این کتاب و در کتاب قبلی [P 1994] سرمشق‌های خوبی هستند تا با تقلید از آنها به نگارش مقالات مروری—تاریخی— مرجع‌شناسی در زمینه‌های مشابه برای خوانندگان ایرانی پرداخته شود. ریاضیدانان جوان کشور بهتر است بدانند که کار سختِ نوشتنِ مقالات توصیفیِ خوب، می‌تواند و باید در برنامهٔ کاری آنان قرار گیرد. مسلماً یک روز که چندان دیر نخواهد بود، زعمای ستادی کشور متوجه این ضرورت خواهند شد و بهای معنوی و مادی لازم را برای چنین کارهایی بازخواهند شناخت. حتی اگر چنین هم نشود، رشد عمومی بینش علمی جامعه در گروی تهیه و مصرف خوراک

1) International Mathematical Union (IMU) 2) International Council for Sciences (ICSU)

ذهنی در سطحی وسیع برای اقشار مختلف مردم است. بنابراین کسی که این رشد را وجههٔ همت قرار دهد، مزد خویش را پیشاپیش دریافت نموده است: مدعیان علوم باید مبلّغین و داعیان علوم نیز باشند. با این شعار مقدمه را به پایان رسانده به معرفی ظاهر کتاب می‌پردازم.

معرفی مشتمل بر بخش‌های زیر است: الف) ظاهر کتاب، ب) عکس‌ها، ج) دیباچه، سرآغاز، د) دیباچه، بخش یکم: سیری در کتاب، هـ) دیباچه، بخش دوم: جلوه‌هایی از تحول ریاضیات در پنجاه سال اخیر، و) دیباچه، بخش سوم: ریاضیات و جامعه، ز) مصاحبه‌ها، ح) فهرست برندگان جوایز فیلدز و رولف نوانلینا، ط) مقالات مروری، ی) کتابنامهٔ تاریخ ریاضیات معاصر، ک) فهرست نام‌ها، ل) جمعبندی و نتیجه‌گیری. در پایان مراجع مورد استناد معرفی می‌شود.

قسمت یکم تا اواسط بخش «د» را در بر می‌گیرد و ادامهٔ معرفی در قسمت دوم (شمارهٔ آینده) جای داده شده است تا حجم بخش معرفی و نقد کتاب از حد متعارف خارج نشود.

الف) ظاهر کتاب

پشت و روی جلد [P 2000] مانند ظاهر [P 1994] است. چهار عکس جالب سیاه و سفید روی زمینهٔ سبز زینت‌بخش روی جلدند: عکس بزرگی از سمینار بنکه در مونشتر آلمان [1] راجع به آنالیز و هندسهٔ چند متغیرهٔ مختلط، مشتمل بر ۲۶ چهره و نوشته‌هایی روی تخته سیاه راجع به صورت‌های همساز و تمامریخت، عکسی از کنگرهٔ بین‌المللی ریاضیدانان زوریخ (۱۹۹۴) مشتمل بر برندگان مدال فیلدز، آقایان بورگن [2]، ویدگرسن [3]، یوکوز [4]، پ.ل. لیونس [5] همراه خانم روث دریفوس وزیر سویسی، عکسی از پاول اردیش [6] در کنگرهٔ ECM بوداپست (۱۹۹۶) و سرانجام عکسی از آندرووایلز در کنگرهٔ ICM زوریخ (۱۹۹۴) در حال سخنرانی با استفاده از اورهد. پشت جلدِ کتاب، مقابل عکس وایلز، عبارت کوتاهی در معرفی کتاب درج شده است که عظمت تکان‌دهندهٔ رشد ریاضیات را در نیمهٔ دوم قرن بیستم و وضعیت کتاب [P 2000] را نسبت به انعکاس این رشد به تماشا می‌گذارد:

«پنجاه سال گذشته شاهد رشد تماشایی و هیجان‌انگیزی در پژوهش ریاضی، تحول افکار و ظهور شاخه‌های جدید آن بوده‌است. دیگر هیچ ریاضیدانی قادر نیست حتی به صورتی سطحی و مجمل، همهٔ این تحولات را یدک بکشد. این کتاب بی‌مانند، به ارائهٔ تاریخی از ریاضیات معاصر اهتمام ورزیده و به کمک خبرگان ذی‌صلاح، رهنمودهایی جهت طیفی وسیع از نظریه‌های ریاضی فراهم می‌کند. مباحث مطرح‌شده و شیوهٔ ارائهٔ آنها نه جنبهٔ دایرةالمعارفی دارند و نه سطحی‌اند. برعکس، بالغ بر ۴۰ ریاضیدان که اکثراً پژوهشگران فعال و متخصصین نام‌آوری در رشتهٔ تخصصی

1) Behnke seminar in Münster 2) J. Bourgain 3) A. Widgerson 4) J.C. Yoccoz 5) P.L. Lions 6) Paul Erdös

خود هستند، به بحث و ارائهٔ مطلب از دیدگاه شخصی خویش پرداخته‌اند. داده‌های آماری و کتاب شناختی هم‌چنین حدود ۲۰۰ عکس چهرهٔ ریاضیدانان، به تکمیل کتاب کمک کرده‌اند. این کتاب همراه با کتاب گسترش ریاضیات ۱۹۰۰ تا ۱۹۵۰ (به کوشش ژان پل پیه، انتشارات بیرکهاوزر ۱۹۹۴) به شکل یک مرجع جامع با ارزش ماندگار راجع به مفاهیم فراموش‌نشدنی در ریاضیات قرن بیستم درآمده است.»

ب) عکس‌ها

مانند [P 1994]، این کتاب نیز آلبومی از عکس‌های ریاضیدانان را برگزیده و در جای جای کتاب گنجانده است. امّا همهٔ عکس‌های داخل کتاب پُرتْره‌های شخصی‌اند، که از چند آلبوم در بایگانی انستیتوی پژوهش ریاضی پلی‌تکنیک زوریخ انتخاب شده‌اند. اصل آلبوم مربوط به ریاضیدانانی است که برای یک دورهٔ کوتاه‌مدت یا بلندمدت به آنجا رفته‌اند. توضیحاً طبق روال مرسوم بسیاری از انستیتوهای جهان، از ریاضیدانان مقیم و بازدیدکننده عکس یادگاری تهیه می‌کنند و نگه می‌دارند. لذا اکثر عکس‌ها در فاصلهٔ ۱۹۷۸ (سال تأسیس انستیتو) و سال ۲۰۰۰ (سال چاپ کتاب) تحویل انستیتو شده است، اما برخی از آنها مربوط به سال‌های پیش از تأسیس انستیتو است. انتخاب حدود ۲۰۰ عکس از بیش از ۱۵۰۰ عکس از آلبوم عکس‌های انستیتوی پژوهش ریاضی فقط نمونه‌ای از آن را می‌نمایاند بی‌آن‌که انتخاب شدن یا نشدن یک عکس دلیلی بر مهم یا کم‌اهمیت بودن ریاضیدانان بوده باشد. از نظر محل درج عکس‌ها هم سعی شده است مناسبتی با موضوع مقاله داشته باشد یا نام آنان ذکر شده باشد. هرچند این تلاشِ ناشر چندان شفاف نیست، با وجود این، بسیار جالب است که عکس برندگان مدال فیلدز یا ریاضیدانان مشهور معاصر را در میان صفحات کتاب می‌توان دید: آلفورس[۱]، چرن[۲]، ایتو[۳]، سر[۴]، سلبرگ[۵]، عطیه[۶]، بورل[۷]، لیونس (پدر[۸] و پسر[۹])، بومبیری[۱۰]، فالتینگز[۱۱]، ممفرد[۱۲]، گروموف[۱۳]، یوکوز[۱۴]،میلنر[۱۵]، ماندلبروت[۱۶]، لنسترا[۱۷]، کُن[۱۸]، شاپیرا[۱۹]، جونز[۲۰] و عدهٔ کثیری که به اشتهار اینان نیستند اما در رشته‌های تخصصی خود نامدار و مهم هستند: هیمن[۲۱]، دیورن[۲۲]، نارازیمهان[۲۳]، مالگرانژ[۲۴]، مک فرسن[۲۵]، برژه[۲۶]، هفلیگر[۲۷] و غیره. البته از ذکر همهٔ نام‌ها خودداری کرده‌ایم.

---

1) Ahlfors 2) Chern 3) Ito 4) Serre 5) Selberg 6) Atiyah 7) A. Borel
8) J.L. Lions 9) P.L. Lions 10) Bombieri 11) Faltings 12) Mumford 13) Gromov
14) Yoccoz 15) Milnor 16) Mandelbrot 17) Lenstra 18) Connes 19) Schapira
20) V. Jones 21) Hayman 22) Duren 23) Narasimhan 24) Malgrange
25) MacPherson 26) M. Berger 27) Häfliger

ج) دیباچه، سرآغاز

یکی از اختلافات بارز بین [P 1994] و [P 2000] در آن است که بر خلاف کتاب قبلی، در کتاب حاضر، مقدمه‌ای مبسوط به امضای کمیتهٔ علمی نوشته شده است. این مقدمه یک دیباچهٔ تمام عیار، خواندنی و بسیار آموزنده است. نویسندگان در آغاز بر این نکته تأکید می‌کنند که تألیف این کتاب پاسخ به یک نیاز و در عین حال کاری دشوار بوده است. مخاطبین کتاب قاطبهٔ ریاضی وسیعی است و هرچند کتاب قصد نداشته است همهٔ موضوع‌ها را بپوشاند، در عین حال نخواسته است خود را به یک برخورد سطحی محدود کند. لذا کمیتهٔ نگارش از ریاضیدانان فعال در زمینه‌های متنوع ریاضی استمداد نموده است. قریب ۳۰ مقاله در این راستا دریافت شده است که بدنهٔ اصلی کتاب را تشکیل می‌دهد. به علاوه با چند ریاضیدان مصاحبه نموده و از ایشان خواسته‌اند که به شرح دیدگاه خود بپردازند. نهایتاً اسنادی را گردآوری نموده‌اند که جنبهٔ آماری یا کتاب شناختی دارند. حاصل کار، کامل و همگن نمی‌توانست باشد. کمیته اقرار می‌کند که نسبت به این نواقص آگاه است. اما اصرار دارد که با وجود این نقص بر ضرورت و اهمیت کتاب تکیه کند و فواید درازمدت آن را گوشزد نماید. موفقیت کتاب قبلی [P 1994]، علی‌رغم نقص و ناهمگنی بیشتر آن از سویی، و از سوی دیگر وفور و تکثّر ایده‌ها، تأسیس رشته‌های مختلف و رشدنمایی محصولات ریاضی در نیمهٔ دوم قرن ، موجب دلگرمی مؤلفین برای تلاش در جهت عمومی‌سازی ریاضی در سطحی والا شد و انگیزهٔ اصلی تألیف جلد دوم را فراهم نمود. در واقع این نیاز در گسترهٔ پهناوری احساس شده و نسبت به آن اقدام‌های مفیدی در سال‌های گذشته صورت گرفته است: از ۱۹۵۰ به این طرف بیش از پیش کنگرهٔ بین‌المللی ریاضیدانان به ایفای این نقش پرداخته است؛ سخنرانی‌های عمومی و نیمه عمومی کنگره، که می‌دانیم هر چهار سال یک بار برگزار می‌شود، خطاب به طیف وسیعی از ریاضیدانان ایراد می‌شوند و یکی از دلایل وجودی کنگره‌اند. موضوع این سخنرانی‌ها مرور وسیع بر یک زمینهٔ ریاضی است. در کشورهای مختلف نیز تلاش برای عمومی‌سازی ریاضی صورت گرفته است. علاوه بر مجموعهٔ کتاب‌های درسی که شاهراه ورود به صحنهٔ دانش‌اند، رشته‌های متنوعی از تک نگاری‌ها و هم‌چنین دائرةالمعارف‌هایی با کیفیت بسیار بالا انتشار یافته‌اند. برخی از مجلات ریاضی که توزیع وسیعی دارند به ویژه در شوروی و ممالک متحدهٔ آمریکا به ارائهٔ مقالات توصیفی مایه‌داری اهتمام نموده‌اند. در فرانسه این نقش را سمینار بورباکی بر عهده داشته است. نویسندگان دیباچه فراموش کرده‌اند مجلهٔ معروف آموزش ریاضی (Ens. Math.) چاپ سویس را که از ۱۸۹۹ عهده‌دار این کار است، نام ببرند.

نویسندگان دیباچه سپس اعلام می‌کنند که «کتاب ما هم قصد دارد سهمی در تاریخ علم معاصر ایفا کند. لذا، از آنجا که به تاریخ می‌پردازیم، لازم شده است که هم به گذشتهٔ این دوره برگردیم، هم از انواع و اقسام سازماندهی‌های مربوط به زندگی ریاضی صحبت کنیم. از این رو، نظر ریاضیدانان فعال در این دوره یا در بخش عمده‌ای از این دوره را خواسته‌ایم». نویسندگان اعلام می‌کنند که نه تنها از غیبت موضوع‌های عدیده و آثار برجسته‌ای در این کتاب آگاهند و از این بابت اظهار تأسف

می‌کنند، اما اقدام به درج فهرست نواقصِ این آثار هم نمی‌نمایند، زیرا معتقدند که هرگونه فهرست نواقص فراهم می‌شد، خود نواقصی در بر داشت و می‌بایست تهیهٔ فهرست نواقص در فهرستِ نواقص همچنان ادامه می‌یافت! لذا کار به انجام نمی‌رسید. در واقع به نوعی عدم تعادل در کتاب هم وقوف دارند. اما به حق می‌گویند: «به نظر ما چنین می‌رسد که مجموعهٔ مقالات با توجه به تنوع آنها قادرند جنبش ریاضیات نیمهٔ دوم قرن را منعکس سازند».

مقالات برحسب ترتیب الفبایی نام نویسندگان در کتاب آمده‌اند، لذا از نظر موضوعی، ترتیب آنها کاملاً تصادفی است. نویسندگان از خواننده دعوت نموده‌اند تا به گردش در کتاب بپردازند و مطالبی جالب کشف کنند. با این وجود، به نوعی معرفی مقالات بر حسب ترتیب منطقی پرداخته‌اند تا **راهنمای گردش در کتاب** باشد. ترجمهٔ انگلیسی این راهنما پس از دیباچه آمده است. پشت سر آن در یک نمودار ارتباط منطقی مقالات درج شده است.

در آخرین سطرهای سرآغازِ دیباچه اشاره شده است به آن که فهرست نام برندگان جایزهٔ فیلدز[1] و برندگان جایزهٔ نِوانلینا[2] در کتاب می‌آید. نهایتاً به فهرستی از اسناد مهم اشاره می‌کند که مشتمل است بر عناوین سخنرانی‌های عمومی یک ساعته در کنگره‌های بین‌المللی ریاضیدانان از ۱۹۵۰ به این سو، مقالات مروری مدعو در مجلهٔ بولتنِ انجمن ریاضی امریکا و مقالات توصیفی مجلهٔ «بررسی‌های مروری ریاضی روسی» که عمدتاً به انگلیسی ترجمه و در امریکا هم منتشر می‌شود. سرانجام به کتابنامه‌ای جهت تدارک منابع در زمینهٔ تاریخ ریاضیات معاصر از ۱۹۵۰ به بعد اشاره می‌شود که آخرین فهرست مفید در این کتاب است.

بدین ترتیب سرآغازِ دیباچه در یک صفحه و نیم همان است که معمولاً مقدمه نامیده می‌شود و کلّ کار را به اختصار معرفی می‌کند. اما اینجا پس از سرآغاز، سه بخش مهم در دیباچه گنجانده شده است که قسمت مهمی از معرفی ما هم ناظر به این سه بخش است.

د) دیباچه، بخش یکم: سیری در کتاب

این بخش زیر عنوان «گردش»[3] به سیری در مقالات کتاب می‌پردازد. ترتیبی که برای معرفی مقالات اتخاذ شده است، تلفیقی است از ترتیب رده‌بندی موضوعی متداول و سلیقهٔ کمیتهٔ علمی. دربارهٔ هر مقاله توضیحی موجز در ۵ تا ۱۰ سطر آمده است و نظر کمیتهٔ علمی را دربارهٔ آن می‌نویسد.

1) Fields Prize Winners 2) Nevanlinna Prize Winners 3) Promenade

چهار مقالهٔ اول، به منطق و مبانی مربوط است:

۱. مقالهٔ ژیرار[1]: از چرا تا چگونه

این مقاله به سیر تحول نظریهٔ برهان[2] در نیمهٔ دوم قرن بیستم می‌پردازد. عنوان آن به خوبی می‌رساند که تحول از مبانی به الگوریتم صورت گرفته و رابطهٔ تنگاتنگ این مباحث را با نظریهٔ آگاهی (یعنی دانش رایانه و انفورماتیک) نشان می‌دهد. پل‌های ارتباطی محکمی را که در آیندهٔ نزدیک با هندسه و فیزیک برقرار خواهد کرد، نوید می‌دهد. مقدمهٔ مقاله در چارچوب تاریخی به کارهای گودل[3]، هربران[4]، گنتسن[5]، شهودگرایی براوِر[6]، حساب لاندای[7] چرچ[8]، کاری[9]، کلین[10] و نهایتاً نقش عمدهٔ کرایزل[11] اشاره می‌کند.

در اینجا چند سطر نخست مقالهٔ ژان ایوْ ژیرار را برای خوانندگان ترجمه می‌کنم شاید خود علاقه‌مند شوند به مطالعهٔ کل مقاله (حدود ۳۰ صفحه) بپردازند. مقاله با این نقل قول تخیّلی شروع می‌شود [البته اشاره نشده است نقل از کی و کجاست]: « در پایان قرن گذشته، ریاضیدانان مورد تهدید شدید تناقضات بودند، اما نظریهٔ برهان توانست مجدداً به سخن این قوم معنا بخشد».

این نقل‌قول تخیلی، ایدئولوژی متوسط نظریه‌پردازان نظریهٔ برهان را در ۱۹۵۰ نشان می‌دهد. بدین ترتیب نظریهٔ برهان را یکجا در چارچوب طرحِ یک نوع مسأله (یعنی رفع تناقضات) قرار می‌دهد و مدعی است که منطق معنای عمیق ریاضیات را ارائه می‌کند. این همان است که من آن را «چرا» می‌نامم. بعدها، حوالی ۱۹۸۵، انفورماتیک نظریهٔ برهان را به رهیافتی عملی‌تر کشاند، این همان است که آن را «چگونه» می‌نامم. البته اصالت و نجابت این **چگونه** کمتر از **چرا** است، اما دم و دستگاه ظریف‌تری را ایجاب می‌کند. اینجا در پانویس توضیح جالبی می‌دهد تا نشان دهد ساز و کار چگونه دست‌کمی از تفرعناتِ **چرا** ندارد: فرانسه (قسمت چسبیده به قارهٔ آن) همبند است، زیرا می‌توان هر شهر آن را به پاریس وصل کرد، اما این سؤال را دست کم نگیرید که فرانسه چگونه همبند است؟ زیرا جواب این سؤال مستلزم آن است که یک شبکهٔ ارتباطی ساخته شود و روشن است که ساختن یک شبکهٔ ارتباطی منحصر به ساختن یک شبکهٔ ستاره شکل با مرکزیت پاریس نیست.

سازماندهی این حیطهٔ فعالیت در اطراف منازعه بین دو جناح است، از سویی یک جناح محافظه‌کار و ایدئولوژیک (طرفدار اصالت فکر) در حال شکست (ولی همچنان صاحب نفوذ) و از سوی دیگر یک جناح نوآور و (گاهی بیش از حد) پراگماتیک (طرفدار اصالت عمل). این نوع دعوا تازگی ندارد و ریشه‌های آن را می‌توان در سال‌های ۱۹۲۰ هم دید. هنگامی که اختلاف دیدگاه‌ها، هیلبرت و براور را در مقابل هم قرار داد و سرانجام براور را از هیأت تحریریهٔ ماتماتیشه آنالن بیرون

1) J. Y. Girard 2) Proof Theory 3) K. Gödel 4) J. Herbrand 5) G. Gentzen
6) Brouwer 7) lambda-calculus 8) Church 9) Curry 10) Kleene 11) G. Kreisel

راند. البته براور به عنوان متخصص منطق و به طریق اولی به عنوان متخصص نظریهٔ برهان شناخته شده نیست اما شهودگرایی براور را باید پدربزرگ چگونه به حساب آورد.

۲. مقالهٔ رسّر[1]: نظریهٔ مدل‌ها و یک مسألهٔ کوچک هاردی.

این مقاله به کاربردی از نظریهٔ مدل‌ها[2] در هندسهٔ حقیقیِ توابع‌نمایی ـ‌جبری و توابع لگاریتمی ـ‌نمایی می‌پردازد. از مدل‌های نااستانده و آنالیز مجانبیِ سری‌های تَرانهایی[3] بهره می‌گیرد و به گونه‌ای غیرمترقبه یک مسألهٔ هاردی[4] را دربارهٔ این توابع حل می‌کند.

۳. مقالهٔ پوازا[5]: پیرامون قضیهٔ مورله

این مقاله حول کارهای بنیادی مورله[6] در دههٔ ۷۰—۱۹۶۰ روی نظریهٔ مدل‌ها دور می‌زند. هم از پیشینهٔ آن سخن به میان می‌آید و هم از سال‌های بعد از آن، دههٔ ۸۰—۱۹۷۰ سال‌های شلاه[7]، دههٔ ۹۰—۱۹۸۰ سال‌های زیلبر[8]. سپس مراجع بر حسب دوره‌های مختلف تنظیم و ارائه گردیده است. آخر سر فهرستی از کتاب‌های جالب راجع‌به نظریهٔ مدل‌ها را معرفی می‌کند، از جمله کتاب خود پوازا با عنوان سنگریزه‌ها[9].

۴. مقالهٔ لاوور[10]: توضیحاتی در باب نظریهٔ توپوز.

این مقاله به گسترش نظریهٔ توپوز می‌پردازد. نظریهٔ توپوزها تلفیق توپولوژی و هندسهٔ جبری با منطق و نظریهٔ مجموعه‌هاست. لاور با این مطلب شروع می‌کند که ابزارهای نظریهٔ رسته‌ها[11] از قبیل تابعگون‌ها[12] و تبدیلات طبیعی[13] در سال‌های ۱۹۳۰ تا ۱۹۴۰ و مفهوم رسته‌های آبلی[14] در دههٔ ۱۹۵۰ و اوایل دههٔ ۶۰ تکمیل شد. کاربردهای عدیدهٔ این نظریه، به ویژه رسته‌های مشتق[15]، در آنالیز ادامه دارد. گروتندیک[16] در یک مقالهٔ ۴ صفحه‌ای به سال ۱۹۵۷ گامی اساسی برداشت و نشان داد که این مفهوم بنیادی در جبر مانستگی [17] روی یک حلقه را می‌توان در مورد بافه‌های روی یک فضا نیز به عنوان اشیاء خطی به‌کار برد. مفهوم دقّت[18] در رسته‌های غیرخطی نیز به تدریج به‌کار رفت. مفهوم تابعگون الحاقی [19] که در اواسط دههٔ ۱۹۵۰ وضع و بررسی شده بود توسط گروتندیک در مبانی هندسهٔ جبری به کار گرفته شد. بدین ترتیب گروتندیک و اطرافیان او در IHES (انستیتوی تحقیقات عالی علمی) حومهٔ پاریس (بور بر روی رودخانهٔ ایوت[20]) در اوایل دههٔ ۱۹۶۰ نظریهٔ توپوز را برای استفاده درهندسه وضع کردند و به گسترش آن پرداختند. نویسندهٔ مقاله آقای لاوور در ۱۹۶۹ مفهوم توپوز را ساده‌تر کرد و کاربردهای متعدد دیگری برای آن را نشان داد.

---

1) J. P. Ressayre 2) Model Theory 3) transfinite 4) Hardy 5) B. Boizat
6) M. Morley 7) S. Shelah 8) B.I. Zilber 9) Les Petits Cailloux 10) F.W. Lawvere
11) Theory of Categories 12) Functors 13) Natural transformations 14) Abelian Categories 15) Derived Categories 16) A. Grothendieck 17) homological algebra
18) exactness 19) adjoint functor 20) Bures sur Yvettr

از کارهای تیرنه[1]، که در جهت نظریهٔ اصل موضوعی بافه‌ها مستقلاً کار کرده بود، نیز بهره گرفت و در کنگرهٔ نیس ۱۹۷۰ به ارائهٔ نظریهٔ ساده شدهٔ توپوزها پرداخت. «با وجود آن که کتاب‌ها و مقالات متعدد در زمینهٔ این نظریهٔ ساده‌شده نوشته شده‌اند، دیده می‌شود که دانشجویان جهان در درک این که واقعاً توپوزها چه هستند، از کجا آمده‌اند، و به کجا می‌روند، با مشکل روبرو هستند». نویسنده اظهار امیدواری می‌کند که این مقاله بتواند در رفع این مشکل مؤثر باشد. بخش‌های مقاله مشتمل است بر: قالبی مشترک برای آنالیز تابعی و توپولوژی جبری، قالبی انعطاف‌پذیر برای منطق و نظریهٔ مجموعه‌ها، فضاهای پارامتر و توپوزهای گروتندیک وابسته به یک توپوز پایه، فضاهای تابعی و مجموعه‌های تابعیِ چسبیده به آنها، رده‌های مثال، کارهای جدید، سرانجام آخرین بخش مقاله از سوی و به سوی فیزیک پیوسته است.

اشاره به کاربردهای جدی نظریه را در منطق می‌توان در بخش آخر ملاحظه نمود: مقالهٔ تیرنه ۱۹۷۲ در صفحات ۱۳ تا ۴۲ کتاب LN274 از سری شپرینگر فرلاک، با عنوان نظریهٔ بافه‌ها و فرضیهٔ پیوستار، مقالهٔ بونگه[2] (در تلفظ آن مشکوکم که آیا بونگه درست است یا بانج) ۱۹۷۴، نظریهٔ توپوز و فرضیهٔ سوسلین، کاربرد نظریهٔ توپوز را در مسائلی از قبیل استقلال فرضیهٔ پیوستار و فرضیهٔ سوسلین نشان دادند. ابزارِ کلیدی، نقش مجموعهٔ توانی است که در نظریهٔ توپوز به عنوان اصل موضوع در نظر گرفته می‌شود که همراه با اصل موضوعِ فضاهای تابعی نشان می‌دهد که مادام که در سطح توپوز کار می‌کنیم «برای صورتبندی تقریباً همهٔ ساختمان‌ها و گزاره‌ها، زبان‌های نامتناهیْ سرشتِ مرتبهٔ بالاتر و دخالت چندی‌گرهای خارجیِ نوعِ فرگه[3] مورد نیاز نیستند.»

سه مقاله در نظریهٔ اعداد، موضوع اشارات بعدی در این گردش است: مقالهٔ فووری و مقالهٔ والداشمیت، نظریهٔ اعداد خالص‌اند و مقالهٔ نیکولا نظریهٔ محاسباتی اعداد است که به رمزنگاری مربوط است.

۵. مقالهٔ فووْری، پنجاه سال در نظریهٔ تحلیلی اعداد: دیدگاهی مابین دیدگاه‌های دیگر: روش‌های غربال.

یکی از خواص نظریهٔ تحلیلی اعداد آن است که پنداره‌هایی را با بیان ساده ولی حل بسیار مشکل دربر می‌گیرد. روش‌های متعددی برای حمله به این مسائل وجود دارد از قبیل روش غربال، روش حاصل‌جمع‌های نمایی، شمارش صفرهای تابع زتای ریمان یا توابع L و غیره. در این میان، اتین فووری[4] روش غربال را برگزیده است. دنباله‌ای متناهی از اعداد طبیعی را در نظر بگیریم و فرض کنیم وضعیت آن نسبت به یک تصاعد حسابی «به طور تقریبی» مشخص باشد. روش غربال آن است که به جدا کردن اعداد اول در بین دنبالهٔ موردنظر بپردازد. معمولاً افراز دنباله به زیرمجموعه‌هایی و اصل رد و قبول برای هر عدد از اعضای افراز، مبنای غربال است. مؤلف نشان می‌دهد که هرچند مسائل اصلی از نظریهٔ اعداد حل نشده باقی مانده و یک خوانندهٔ بدبین ممکن است بگوید کاری انجام نشده است، در عین حال گام‌های بلندی برداشته شده و نتایجی پیشرفته

1) Tierney 2) M. Bunge 3) Fregean quantifiers 4) Etienne Fouvry

به‌دست آمده است . مؤلف دست کم ده قضیه را در مورد غربال بزرگ، سهم ایوانیچ، اعداد اول دوقلو و غیره بیان می‌کند. قضایای مورد بحث تخمین‌های مجانبی برای عبارت‌های پیچیده‌ای هستند که به علت فنی از بیان آنها صرف نظر می‌کنیم. فقط اشاره کنیم که به کار ایوانیچ ــ فوری و پیامدهای آن نیز تکیه می‌شود.

۶. مقالهٔ والداشمیت، نیم قرن اعداد متعالی.

در این مقالهٔ ۶۶ صفحه‌ای بسیار خواندنی، آقای میشل والد اشمیت[1]، انبوهی از مطالب جالب راجع به اعداد متعالی را با شیوه‌ای گیرا و قابل درک ارائه می‌کند. خوانندگان فرهنگ و اندیشه احتمالاً با مقالهٔ آقای والداشمیت در کنفرانس ریاضی شاهرود (۱۳۸۲) آشنا هستند و بیان گویای او را در آن مقاله ستوده‌اند. می‌دانیم نخستین عدد متعالی شناخته شده را لیوویل[2] در ۱۸۴۴ نشان داد. به ازای هر عدد جبری α ثابت‌های C و k وجود دارند به قسمی که هر عدد گویای $\frac{p}{q}$ در نامساوی

$$|\alpha - \frac{p}{q}| \geq \frac{C}{q^k}$$

صدق کند (k را می‌توان درجهٔ عدد جبری α گرفت). پس عددی که تقریب گویای خوبی داشته باشد، عددی است متعالی. سپس در ۱۸۸۴ کانتور[3] نشان داد که تقریباً همهٔ اعداد حقیقی و مختلط اعداد متعالی هستند (زیرا مجموعهٔ اعداد جبری شماراست). با این وجود، در راستای تشخیص اعداد معروفی از حیث گویابودن یا نبودن، جبری بودن یا نبودن هم‌چنان مسألهٔ باز فراوان است. حل هر مسأله‌ای در این زمینه پر ارزش است: در ۱۹۷۸ ثابت شد که $\zeta(۳)$ گویا نیست، اما هنوز نمی‌دانیم آیا $\zeta(۵)$ گویا است یا نه، آیا ثابت اویلر $\gamma = \lim(۱ + \frac{۱}{۲} + \ldots + \frac{۱}{n}) - \log n$ گویا است یا نه؟ یادآوری کنیم که یک تابع تام در $\mathbb{C}$ یا $\mathbb{C}^n$ را که چندجمله‌ای نباشد تابع متعالی نامند. (به شیوهٔ مشابه تابع برخه‌ریخت را نیز که یک کسر گویا نباشد، یک تابع متعالی نامند). یکی از روش‌های مهم (روش مِهلِر) آن است که در بررسی متعالی بودن یا نبودن مقدار یک تابع از معادلهٔ تابعی استفاده شود. مثلاً تابع $f(z) = e^z$ در معادلهٔ $f' = f$ صدق می‌کند و همین معادله در برهان ارمیت[4] راجع به تعالی عدد e و برهان لیندمان[5] راجع به متعالی بودن π به گونه‌ای اساسی به کار می‌رود. جواب منفی مسألهٔ تربیع دایره فرع بر جبری نبودن π است و از اواخر قرن ۱۹ شناخته شده است. قضیهٔ هرمیت — لیندمان که می‌گوید اگر $\beta \neq ۰$ عدد جبری باشد آنگاه e^β متعالی است، و قضیه گلفوند—شنایدر (۱۹۳۴) می‌گوید که اگر α و β دو عدد جبری باشند که α غیر از ۰ و ۱ بوده و β غیرگویا باشد، آنگاه α^β (یعنی $\exp(\beta \log \alpha)$ متعالی است. بدین ترتیب روش پیشنهادی مهلر، به شکلی دیگر در قرن گذشته و نیز در نیمهٔ اول قرن بیستم مورد استفاده بوده است. اما در قرن بیستم این روشِ فراموش شده مجدداً مورد بهره‌برداری قرار گرفت و به‌ویژه در مورد دینامیک مختلط در

1) Michel Waldschmidt 2) J. Liouville 3) G. Cantor 4) Ch. Hermite 5) Lindemann

سال‌های ۱۹۹۳ و ۱۹۹۶ به کار رفت: فرض کنیم $\mathcal{M}$ مجموعهٔ ماندلبروت[1] چندجمله‌ای دهۀ آخر $P = z^۲ + c$ باشد، یعنی $\mathcal{M}$ مجموعهٔ Cهایی در $\mathbb{C}$ است که

$$P(\circ) = c,\ P^{۲}(\circ) = c^{۲} + c,\ P^{۳}(\circ) = (c^{۲} + c)^{۲} + c,\ \ldots$$

به ∞ میل نمی‌کند. اگر φ تابع دوادی—هوبارد[2] باشد که روی $S - \mathcal{M}$، متمم $\mathcal{M}$ در کرهٔ ریمان S، تعریف شده و تحلیلی است، آنگاه به ازای هر عدد جبری $\alpha \in \mathbb{C} - \mathcal{M}$، مقدار $\varphi(\alpha)$ یک عدد متعالی است. این نتیجه را کومیکو نیشیوکا[3] در ۱۹۹۶ ثابت کرد و از متعالی بودن توابع مهلر بهره گرفت. یک مسألهٔ دیگر مهلر راجع به توابع کالبدی[4] در ۱۹۹۵ ثابت شد. بخش‌های دیگر مقاله هم به همین شکل مطالب خواندنی و قابل توجه فراوان دارد. در بخش نتیجه‌گیری و مراجع، آینده‌ای درخشان برای نظریه پیش‌بینی شده و مراجع مروری مبسوطی ارائه شده است، همراه با توضیحاتی که آن را از یک فهرست خشک خارج می‌کند. مطالعهٔ آن به خواننده توصیه می‌شود.

۷. مقالهٔ ژان لویی نیکولا[5]: حساب و رمزنگاری.

در این مقاله، پس از یک مقدمه نقش متقابل الگوریتم‌ها و حساب و کاربرد آنها در رمزنگاری با شیوه‌ای کاملاً قابل درک و مثال‌های ابتدایی و پیشرفته بیان شده است. مقدمه با این جمله شروع می‌شود: نیمهٔ دوم قرن بیستم شاهد رشد سریع رایانه‌ها بوده است. در آغاز تأثیر آن بر نظریهٔ اعداد ناچیز بوده و به چند نفر متخصص نظیر لهمر[6] و شانکس[7] محدود می‌شد. ولی بعداً این تأثیر چنان چشمگیر شد که اکنون می‌توان از «نظریهٔ محاسباتی اعداد[8]» و یا «کاربرد رایانه‌ها در نظریهٔ اعداد» به عنوان یک رشتهٔ تخصصی تمام عیار در ریاضیات سخن راند.

در متن مقاله، از الگوریتم اقلیدس گرفته تا ارقام اعشاری π، تا تجزیهٔ چندجمله‌ای‌های با ضرایب گویا، آزمون‌های اول بودن یک عدد، خم‌های بیضوی و غیره، مطالب خواندنی و قابل درک به قدری فراوان‌اند که ترجمهٔ سریع این مقاله و درج آن را در فرهنگ و اندیشهٔ ریاضی توصیه می‌کنم.

در گردش، پس از آن به یک مقاله دربارهٔ نظریهٔ گراف می‌رسیم.

۸. مقالهٔ کلود برژ[9]: نظریهٔ گراف.

«بررسی گراف‌ها یا نمودارها در همهٔ موضوعات مربوط به آنالیز ترکیبی، احتمالات و انفورماتیک مفید است. حل مسألهٔ چهار رنگ یکی از نتایج برجستهٔ این نظریه بوده است. آقای کلود برژ به بررسی ظرافت روش‌های نظریهٔ گراف و کاربردهایش در تحقیق در عملیات و ترکیبیات می‌پردازد.»

1) Mandelbrot 2) Douady-Hubbard 3) Kumiko Nishioka 4) modular functions
5) Jean Loius Nicolas 6) Lehmer 7) Shanks 8) Computational Number Theory
9) Claude Berge

توضیحات فوق همهٔ مطالبی است که در گردش راجع به این مقاله گفته شده است. خود مقاله هم یکی از کوتاهترین مقالات کتاب است، ۹ صفحه متن به اضافهٔ سه صفحه و نیم مراجع. حدود سه صفحهٔ متن را مقدمهٔ جالبی تشکیل می‌دهد که تاریخچهٔ ضعیف نظریه را پیش از ۱۹۵۰ و تاریخ واقعی آن را در نیمهٔ دوم قرن ترسیم می‌کند و به مباحث مهمی که در مقاله بحث می‌شود می‌پردازد، از جمله ساختارهای ترکیبیاتی فرین در هندسه و نظریهٔ اعداد، نظریهٔ شمارشی، روش‌های احتمالاتی، گراف‌های تصادفی (دههٔ آخر قرن). برعکس، صراحتاً می‌گوید که مسائل مطرح شده در انفورماتیک را به بحث نمی‌گذارد. به گمان بنده این مقاله با توجه به حجم اندک آن و قرابت با مقالهٔ م. بهزاد [۵] مفید است ترجمه و ارائه شود، تا پژوهشگران ما قدر مقالات مروری را به طور کلی و ارزش مقالات فرهنگ و اندیشهٔ ریاضی و همایش‌های ماهانهٔ انجمن ریاضی ایران را به طور خاص‌تر بازشناسند و به ویژه تشویق شوند در جهت نگارش مقالات مروری دست به قلم ببرند.

۹. مقالهٔ چیرو چیلیبرتو[۱]: هندسهٔ واریته‌های جبری. این مقاله به رشد هندسهٔ جبری در نیمهٔ دوم قرن می‌پردازد. به جای مقدمه، بخش یکم مقاله به مروری بر گسترش هندسهٔ جبری اختصاص یافته است. موضوع هندسهٔ جبری مطالعه و رده‌بندی واریته‌های جبری است یعنی زیرمجموعه‌هایی از فضاهای آفین یا تصویری متناهی ـ بعد روی یک میدان که به کمک معادلات چندجمله‌ای مشخص شده باشند. با توجه به اهمیت چندجمله‌ای‌ها در ریاضیات و کاربردهای آن، واضح است که هندسهٔ جبری چه جایگاه مرکزیی در دانش ریاضی دارد. پس از اشاراتی به تاریخ پیش از میلاد و قرون ۱۷ و ۱۸ به دو روش مطرح شده در این تاریخ می‌پردازد: روش جبری و تجزیه‌ـ ترکیب از سویی و روش تحلیلی و توپولوژیک از سوی دیگر. سپس به کارهای مهم قرن ۱۹ می‌پردازد تا آن که نیاز به بازنگری عمیق مبانی هندسهٔ جبری را در قرن بیستم مطرح می‌کند. این کار در نیمهٔ اول قرن بیستم به وسیلهٔ افرادی نظیر وان‌درواردن[۲]، وایل[۳] و زاریسکی[۴] صورت گرفت. اما انقلاب واقعی پس از ابداع نظریهٔ بافه‌ها توسط ژان لُره[۵] و جبر مانستگی[۶] و کاربرد آنها توسط ژان پیر سِر[۷] در ۱۹۵۵ صورت گرفت. اینجاست که مفهوم واریتهٔ جبری شبیه خمینه‌های دیفرانسیل تعریف و بررسی می‌شود. بدین ترتیب بخش دوم مقاله شروع می‌شود که به بافه‌ها[۸]، شِماها[۹](اسکیم‌ها) و همانستگی[۱۰] می‌پردازد. در اینجا توضیحات قابل درکی داده می‌شود که خواننده به خوبی درک می‌کند صحبت دربارهٔ چیست: واریته‌های X و نگاشت‌های منظم یا مورفیسم بین آنها بافهٔ ساختاری $\mathcal{O}_X$ و همانستگی‌های آن $H^i(X,F)$ و کاراکتریستیک اویلر یک بافهٔ F روی X، یعنی $X(F) := \sum_{i=0}^{n}(-1)^i \dim H^i(X,F)$ و گونهٔ[۱۱] $g(X)$ و غیره توضیح داده می‌شود؛ بافه‌های سازگار[۱۲]، تاری‌های برداری رتبه r روی X، یعنی $\mathcal{O}_x^r$ و بافه‌های موضعاً همریخت با آنها. با این

1) Ciro Ciliberto 2) Van der Waerden 3) André Weil 4) Zariski 5) Jean Leray 6) homological algebra 7) Jean Pierre Serre 8) Sheares 9) Schéma(Scheme) 10) Cohomology 11) genous 12) coherent sheaves

مقدمات و توضیحات دیگر در بخش ۲، به بخش ۳ مقاله کار با شِماها در سال‌های ۱۹۵۰ تا ۱۹۷۰ می‌رسد که در آنجا زیربخشهایی مشتمل بر حل تکینگی‌ها، نظریهٔ اشتراک[۱] و هندسهٔ شمارشی[۲]، قضیهٔ گروتندیک — ریمان—رخ[۳]، پندارهای وایل[۴]، نظریهٔ هاج[۵] و همچنین روشن شدن مفهوم فضاهای مدولی که قبلاً به شیوهٔ مبهم در مکاتب ایتالیا و آلمان به کار می‌رفت، می‌پردازد. توضیحات کافی راجع به چندجمله‌ای هیلبرت، تابع هیلبرت و شماریِ هیلبرت و سابقهٔ تاریخی تلاش‌های دیگران در این زمینه دیده می‌شود. بخش چهارم مقاله به نتایج جدید از ۱۹۷۰ تا ۱۹۹۸ اختصاص دارد که بحث مبسوطی است و به زیربخش خمها، رویه‌ها و خمینه‌های ۴—بعدی و واریته‌های با بعد بیشتر می‌پردازد و از هندسهٔ شمارشی و هندسهٔ حسابی سر در می‌آورد.

پاراگراف‌های این بخش پر از اشارات عالمانه و قابل درک راجع به ایده‌های جدید و حل مسائل مشهور است، ایده‌ها گاهی از فیزیک سرچشمه می‌گیرند، مانند تقارن آینه[۶] و همانستگی کوانتمی[۷] که انگیزهٔ آنها از نظریهٔ ریسمان[۸] و نظریهٔ میدان‌های کوانتومی[۹] گرفته شده است. همچنین به کارهای مانین[۱۰]، فالتینگز[۱۱] و وایلز[۱۲] اشاره و در چند سطر ایدهٔ برهان آخرین قضیهٔ فرما را بیان می‌کند. قریب ۱۵۰ مرجع پایان بخش این مقالهٔ ۴۴ صفحه‌ای است. ترجمهٔ مقاله برای عموم ریاضیدانان و مطالعهٔ اصل مقاله برای همهٔ دانشجویان تحصیلات تکمیلی که مایل به شناخت در زمینهٔ هندسهٔ جبری، هندسهٔ مختلط و هندسهٔ دیفرانسیل هستند، توصیه می‌شود.

۱۰. مقالهٔ خانم ماری فرانسواز روا: هندسهٔ جبری حقیقی.

هندسهٔ جبری حقیقی مدتها مورد غفلت قرار گرفته بود اما در سال‌های اخیر بیشتر به آن توجه می‌شود. رنه توم[۱۳] در کتاب معروف پایداری ساختاری و تحول اشکال[۱۴] به قدری از این موضوع نگران است که با لحن گله‌آمیزی بیان می‌کند: «آیا توجه بیش از حد آنالیز در قرن نوزدهم به میدان مختلط و توابع تحلیلی نقشی شوم در رشد ریاضیات نداشته است؟». در قرن بیستم از جهات متعدّدی، هندسهٔ جبری و حقیقی و هندسهٔ تحلیلی حقیقی، مورد توجه قرار گرفته است. نامساوی های جبری که از دبیرستان با آن آشنا هستیم، تعیین علامت چندجمله‌ای‌ها و نقش مُبیّن در وجود جواب معادلات درجه دوم و جز آن به ریاضیدانی مانند تارسکی[۱۵] اجازه می‌دهند تا به قضیهٔ حذف سور وجودی در نظریه‌های مرتبهٔ اول برای میدان‌های حقیقی بسته دست یابد. مجموعه‌های نیمه جبری و تصمیم‌پذیری به هم مربوط می‌شوند. این مجموعه‌ها هم ویژگی‌های کیفی و هم ویژگی‌های کمی دارند. افرادی مانند هانری کارتان[۱۶] به بررسی واریته‌های تحلیلی حقیقی و مختلط و مقایسهٔ آنها می‌پردازند. قضایای اصلی نظیر صفرهای هیلبرت و غیره در این زمینه نیز به اثبات

1) intersection theory 2) enumerative geometry 3) theorem of Grothendieck-Riemann-Roch 4) Weil's conjectures 5) Hodge theory 6) mirror symmetry 7) quantum cohomology 8) string theory 9) quantum field theory 10) Manin 11) Faltings 12) Wiles 13) René Thom 14) Structural Stability and Morphogenesis 15) Tarski 16) Henri Cartan

می‌رسند. توابع منظم، توابع ناش[1] یعنی توابع حقیقی تحلیلی که روی چندجمله‌ای‌ها جبری هستند مانند $\sqrt{1 + x^2}$، خمینه‌های ناش و مجموعه‌های ناش، $\cdots$ بررسی می‌شوند. ارتباط با مسائل ۱٦ و ۱۷ هیلبرت، توپولوژی و ترکیبیات واریته‌های جبری حقیقی و نهایتاً مدل‌های جبری خمینه‌های C^∞ و مانستگی جبری مجموعه‌های جبری حقیقی مطرح می‌شوند و یک بحث پایانی مختصر (۲ صفحه) دربارهٔ ملاحظاتی در باب هندسهٔ جبری حقیقی، پیش از فهرست مراجع آمده است. آثاری از نویسنده (همراه با دیگران و به تنهایی) در فهرست است که سه عنوان آن مربوط به سال ۱۹۹٦ بیشتر جلب توجه می‌کند: یکی [۵۴] در باب الگوریتم پایه در هندسهٔ جبری حقیقی، که مروری است ٦۷ صفحه‌ای و دیگری [۵۵] به اجسام دوار و الگوریتم‌های هندسهٔ جبری حقیقی مربوط است. سومی [۱۲] راجع به بافه‌هایی روی خمینه‌های ناش است.

۱۱. مقالهٔ ماکس کروبی: گزارشی از K–تئوری (۱۹۵٦ تا ۱۹۹۷).

همهٔ ریاضیدانان به K–تئوری می‌پردازند، بی آن که اکثراً خود بدانند. وقتی مقالهٔ کروبی را خواندم دیدم این ادعای او در مورد من کاملاً صدق می‌کند. در واقع مقاله‌ای نوشته و آن را برای دانشجویان و دبیران در سال‌هایی که به مطالب ابتدایی می‌پرداختم شرح داده بودم. موضوع قرینه‌سازی جبری بود [ش ۱۳٦٦ و ۱۳٦۷]: از یک نیمگروه آبلی S یک گروه آبلی $K(S)$ می‌سازیم. به شکل مشابه در موارد عدیده از یک شیء M یک شیء منظم‌تر $K(M)$ می‌سازیم و این اساس K–تئوری است. آقای کروبی[2] طی مثال‌هایی که در مقدمهٔ مقاله عنوان می‌کند و در طی بخش‌های مقاله آن را بیشتر باز می‌کند به شرح این ماجراها می‌پردازد: تعاریف اولیهٔ K–تئوری، از هم آغاز شرح می‌دهد که گروتندیک[3] قضیهٔ ریمان–رخ را برای واریته‌های تصویری ناتکین[4] و با بعد دلخواه حل کرد و در این راستا نظریهٔ K–تئوری را بنیان نهاد: اگر X یک چنین واریته‌ای باشد، از روی بافه‌های جبری سازگار[5] روی X یک گروه به وسیلهٔ گروتندیک ساخته می‌شود که آن را K–تئوری جبری می‌نامد و با $K^{alg}(X)$ نمایش می‌دهد. حرف K یادآور واژهٔ آلمانی کلاس است و از آن پس نماد بهتری نیافته‌اند که به جای K–تئوری به کار برند. سپس عطیه[6] و هیرتسبروخ[7] به شکل مشابه در مورد فضاهای فشردهٔ X، یک K–تئوری با نماد $K^{top}(X)$ می‌سازند. در اینجا قرینه‌سازی روی مجموعهٔ رده‌های همریختی تاری‌های برداری حقیقی یا مختلط است و قانون ترکیب نیمگروه آن حاصل جمع ویتنی تاری‌های برداری است، که به ترتیب $K_{\mathbb{R}}^{top}$ یا $K_{\mathbb{C}}^{top}$ را نتیجه می‌دهد. شیوهٔ جبری ساخت آن بر مبنای A (که A جبر توابع پیوسته $C(X_i\mathbb{R})$ یا $C(X_i\mathbb{C})$ است) نیز تشریح می‌شود. این روش سِرّ و سوان[8] است، حاصل جمع $A-$ مدول‌ها به جای حاصل جمع ویتنی ظاهر خواهد شد. مشابه این برای خمینه‌های دیفرانسیل‌پذیر نیز با اتخاذ $A = C^\infty(X)$ منجر به K–تئوری دیفرانسیل می‌شود.

خلاصه K ـ تئوری حلقه‌ها و K ـ تئوری فضاها تشکیل می‌شود. در ادامهٔ مقالهٔ نظریه‌های

1) Nash function 2) Max Karoubi 3) Grothendieck 4) non singular
5) Coherent algebraic sheaves 6) Michael Atiyah 7) Hirzebruch 8) Swan

(عطیه—هیرتسبروخ) قضایای مربوط به رده‌های چرن[1] و قضیهٔ عطیه—سینگر[2] به عنوان نتایجی از K—تئوری تشریح می‌شوند. سپس K—تئوری جبرهای باناخ و KK—تئوری کاسپاروف[3]، به دنبال آن K—تئوری جبری باس[4]، میلنر[5] و کویلن[6] مطرح می‌شوند. به تعبیری K—تئوری گروتندیک مفهوم بُعد را تعمیم می‌دهد، حال آنکه K—تئوری باس مفهوم دترمینان را. برای K_0، گروه گروتندیک، K_1 گروه باس و K_2 گروه میلنر تعبیرهای ساده‌ای ارائه می‌شود و برای گروه‌های کویلن K_n نیز تعبیر هوموتوپی مرتبهٔ n ارائه می‌شود، ولی فضای موردنظر یعنی $BGL(A)^+$ فضایی است که کویلن می‌سازد: $K_n(A) = \pi_n(BGL(A)^+)$.

مقاله به K—تئوری فضاها و حلقه‌ها ختم نمی‌شود، بلکه در مورد شِماها نیز صحبت و کاربردهایی از آن را بیان می‌کند. در دو بخش پایانی مقاله، دیدگاه‌های دیگری از K—تئوری جبری، سپس مانستگی دوره‌ای[7] و مقایسهٔ K—تئوری‌های جبری و توپولوژیک بیان می‌شود.

مقاله‌ای نظیر این مقاله برای جامعهٔ ریاضی ما این فایده را دارد که مباحثات خواص را میان عوام خواهد آورد و همهٔ ما را به بینشی روشن‌تر مجهز خواهد ساخت.

۱۲. مقالهٔ مارسل برژه[8]: هندسهٔ ریمانی.

این مقاله که عنوان کامل آن: «ریاضیات در نیمهٔ دوم قرن: هندسهٔ ریمانی» است، به مباحثی می‌پردازد که برای جامعهٔ ریاضی ما قاعدتاً آشناتر است. نویسنده (از IHES) چهرهٔ شناخته شده‌ای است و کتاب درسی موفقی هم در زمینهٔ هندسهٔ دیفرانسیل و آثار متعدد دیگری نیز دارد. مقاله‌ای با عنوان مشابه اما به زبان انگلیسی نیز به سال ۱۹۹۸ منتشر نموده است که در بخش پایانی مقاله به آن ارجاع می‌دهد (چرا که در زمینهٔ تعمیم خمینه‌های ریمانی، به اختصار این بخش نیست و مراجع بیشتری را دربر دارد).
در مقدمهٔ مبسوط مقاله (۵ صفحهٔ کامل) از تعریف خمینهٔ ریمانی (Mg) گرفته تا تانسورهای مختلف و مشتقات d و D و طیف لاپلاسین $\Delta f = -trace_g Ddf$ با سابقهٔ تاریخی آنها گفته می‌شود و سپس تأکید می‌شود که مباحث مقاله بر طبق سلیقهٔ شخصی صورت گرفته و مباحث متعدد فراوانی را نام می‌برد که هیچ یک مورد بحث قرار نخواهند گرفت. مباحث اصلی موردبحث عبارت‌اند از رفتار ژئودزیک‌ها به ویژه تعداد و توزیع ژئودزیک‌های متناوب، سپس خمیدگی و توپولوژی و طیفِ لاپلاسین. در داخل بخش‌ها نیز تاریخچهٔ مفصل‌تری از سر گرفته می‌شود و به مراجعی اشاره می‌کند که متأسفانه در فهرست مراجع نیامده‌اند. از جمله کارهای خود برژه در زمینهٔ خمیدگی که به سال‌های ۱۹۶۰ مربوطند در متن دیده می‌شود ولی در فهرست مراجع نیست. در یک بخش پایانی، علاوه بر سه مبحث نام برده، به مسائل و نتایج دیگری اشاره می‌کند که عبارتند از فضاهای کلیفورد—کلاین[9]، ساختارهای ریمانی ممتاز روی یک خمینهٔ فشردهٔ مفروض، حجم،

1) Chern Classes 2) Atiyah-Singer 3) Kasparov 4) Bass 5) Milnor 6) Quillen
7) cyclic homology 8) Marcel Berger 9) Clifford Klein

خطوط انشعاب، گروه‌های هولونومی، خمینه‌های کِهلری، صورت‌های دیفرانسیل و تاری‌ها، زیرخمینه‌ها، نگاشت‌های همساز و نهایتاً تعمیم خمینه‌های ریمانی. در اینجا پیش‌گویی می‌شود که در آینده فضاهای (mm) یعنی فضاهایی که دارای متر d و اندازهٔ μ با هم هستند و فقط شرایط ضعیفی بین آنها برقرار است مثلاً $(x,y) \mapsto d(x,y)$ اندازه‌پذیر و خود اندازهٔ μ بدون اتم در نظر گرفته می‌شود، مورد مطالعهٔ وسیع قرار خواهند گرفت.

با وجود اهمیت فوق‌العادهٔ این مقاله هم از حیث موضوع و هم از حیث شیوهٔ نگارشِ بسیار روشن و آموزندهٔ آن، از شرح بیشتر آن در اینجا خودداری می‌کنم. امیدوارم به‌زودی این مقاله از زبان فرانسه، یا بهتر از آن مقالهٔ ۱۹۹۸ برژه از انگلیسی، به فارسی برگردانده و در فرهنگ و اندیشهٔ ریاضی درج شود.

۱۳ و ۱۴. مقالات آرنولد: نظریهٔ تکینگی و نظام‌های پویا (سیستم‌های دینامیک)

در این کتاب دو مقالهٔ نخست از آرنولد[1] است، استاد مشترک انستیتو استکلوف مسکو و دانشگاه پاریس ۹. آرنولد تنها فردی است که بیش از یک مقاله در کتاب دارد. در گردش، نخست مقالهٔ دوم کتاب یعنی نظریهٔ تکینگی[2] و سپس به مقالهٔ اول یعنی نظام‌های پویا (سیستم‌های دینامیک)[3] پرداخته شده است.

در **تکینگی‌ها** تکیه روی نظریهٔ موضعی نقاط بحرانی است. در فهرست مراجع، سه کتاب از آرنولد دیده می‌شود، یکی نظریهٔ فاجعه، چاپ ۱۹۹۰ مسکو، برگردان انگلیسی ۱۹۹۳ اشپرینگرفرلاک، دیگری نظریهٔ تکینگی و کاربردهای آن به زبان انگلیسی چاپ ایتالیا ۱۹۹۰، سومی تکینگی‌های صوتی و جبههٔ امواج، انگلیسی چاپ ۱۹۹۰. علاوه بر آن، کتابِ چهارم به قلم آرنولد و دیگران با عنوان تکینگی‌های نگاشت‌های دیفرانسیل‌پذیر در دو جلد چاپ مسکو ۱۹۸۲ و ۱۹۸۴ برگردان فرانسه ۱۹۸۸ و انگلیسی ۱۹۹۰ و نهایتاً جلدهای ۴ و ۵ و ٦ و ۳۹ از دایرهالمعارف EMS چاپ مسکو ۱۹۸۵ تا ۱۹۹۳ (برگردان انگلیسی ۱۹۹۳ تا ۱۹۹۵) دیده می‌شود.

پس از چکیده بخش‌های مقاله با عناوین نقاط بحرانی توابع هموار یا نظریهٔ مورس[4]، نگاشت‌های از رویه‌ها به صفحه یا نظریهٔ ویتنی[5]، نگاشت‌های فضاهای با بعد بیشتر، ابعاد جالب، تکینگی‌های ساده، تکینگی‌های صوتی[6]، شاخه‌های انتگرال نوسانی[7]، نظریهٔ سراسری تکینگی. مقاله پر است از اشکال زیبا، پندارهها و قضایای روشن که در عین حال روشن می‌کند که نظریه به چه علت پیچیده بوده و پدیده‌های طبیعی چگونه بررسیِ پیوسته را به تشخیص‌های گسسته کشانده‌اند (آنچه آرنولد در چکیده به آن تکیه می‌کند همین است که توصیف جهان مستلزم بررسی‌های پیوسته و گسسته است، در نظریهٔ تکینگی دیده می‌شود که پدیده‌های گسسته‌ای از رده‌های پیوسته

1) Vladimir Arnold 2) Singularity theory 3) Dynamical systems 4) Morse theory
5) Withney theory 6) Caustic singularities 7) oscilating integral

سربرآورده‌اند و به علت پیچیدگی و همچنین تحمیلات ریاضیاتِ استنتاجی ـ‌اصل موضوعی و سبک نگارش نظریهٔ مجموعه‌ای نیمهٔ اول قرن، این نظریه تا نیمهٔ دوم قرن به تعویق افتاده است. مقاله حالتی زیبا، سهل و ممتنع دارد که فقط با خواندن آن می‌توانید بفهمید چیزی دریافته‌اید یا نه. به عبارت دیگر از قدرت من خارج است کمکی به خواننده بکنم. او را به خود مقاله ارجاع می‌دهم.

در مقالهٔ نظام‌های پویا نیز چکیده‌ای با این مضمون دیده می‌شود:

نظریهٔ نظام‌های پویا یکی از زمینه‌هایی است که در قرن بیستم انقلابی‌ترین پیشرفت را داشته و موجب پدیدآمدن نمونه‌های بارز جدیدی بوده است. این نظریه در میدان تلاقی شاهراه‌های ریاضیات کاربردی و محض است، از جمله فیزیک آماری، محیط زیست[۱]، مکانیک سماوی[۲] و نظریهٔ نوسان[۳] از سویی و از سوی دیگر توپولوژی، هندسهٔ دیفرانسیل گروه‌های لی و نظریهٔ اعداد را می‌توان نام برد. مقاله پس از چکیده با بخش ۱ شروع می‌شود که به معادلات تحول[۴] اختصاص دارد. پس از این جملهٔ ساده که «فکر اصلی در این نظریه آن است که مسائل دینامیک را به مسائل هندسی تبدیل کند»، به ذکر مثال‌های متعدد می‌پردازد. بخش دوم نظریهٔ انشعاب[۵]، بخش سوم پایداری ساختاری[۶]، بخش چهارم آشوب[۷]، بخش پنجم مسائل باز که دست کم پنج دسته مسأله را مطرح می‌کند و نهایتاً مراجع. نظیر مقالهٔ تکینگی، به چهار جلد کتاب دایرةالمعارف EMS مخصوص سیستم‌های دینامیک چاپ روسی ۱۹۸۵ تا ۱۹۹۰ و چاپ انگلیسی ۱۹۸۸ تا ۱۹۹۳ همراه با کتاب روش‌های هندسی در نظریهٔ معادلات دیفرانسیل معمولی، تألیف آرنولد (چاپ روسی ۱۹۷۸ و چاپ انگلیسی ۱۹۸۳ و ۱۹۸۸) به عنوان مدخلی به موضوع و شرح مبسوطی از مطالب این رشته و کتابنامهٔ مفصل راجع به آن، معرفی شده‌اند. به نظرم این مقاله جزء مقالاتی است که باید با اولویت در دست ترجمه و نشر فارسی قرار گیرد (نشر ریاضی یا فرهنگ و اندیشهٔ ریاضی جایگاه مناسبی برای درج مقالهٔ ترجمه شده هستند). بگذارید این جملات را هم از گردش برایتان نقل کنم: «... خاصیت جهانیِ ساده‌ترین انشعابها، در رسالهٔ پوانکاره نیز موجود بود، اما این خاصیت، توسط گروتندیک در زمینهٔ هندسهٔ جبری و توسط توم در زمینهٔ نظریهٔ تکنیگی دوباره کشف گردید.»

۱۵. مقالهٔ ویویان بالادی[۸]: آهن ربا و پروانه[۹]: صورتبندی ترمودینامیک[۱۰] و نظریهٔ ارگودیک[۱۱] در دینامیک‌های آشوبناک.[۱۲] قسمت عمدهٔ این مقاله ناظر به دینامیک زمان گسسته است، بدین معنی که پدیدهٔ تکرار را برای یک نگاشت $f : M \to M$ در نظر می‌گیرند:

$$f, f^{۲} = f \circ f, \dots, f^{n} = f^{n-۱} \circ f, \dots$$

---

1) ecology   2) celestical mechanics   3) oscilation theory   4) evolutionary equations
5) bifurcation theory   6) structural stability   7) chaos   8) Viviane Baladi
9) The Magnet and the Butterfly   10) Thermodynamic Formalism   11) Ergodic Theory
12) Chaotic Dynamics

و اگر f وارونپذیر باشد، f^{-1} و f^{-2} و $\cdots$ را نیز در نظر گرفته، روی رفتار یک نقطه یا یک پارامتر که f به آن وابسته است، هنگامی که $n \to \infty$ بحث می‌شود. آشوبناکیِ سیستم هنگامی است که تغییر اندکی در نقطه یا در مقدار پارامتر ممکن است در نهایت به اوضاع فاجعه‌آمیزی بینجامد، به‌اصطلاح اگر یک بال پروانه در گوشه‌ای از جو زمین تکان بخورد، ممکن است در آینده موجب گردباد خانمان براندازی در تگزاس شود. بررسی این نوع پدیده موجب انتشار آثار تحقیقی جالب و متعددی در طول نیمهٔ دوم قرن و مخصوصاً در سالهای اخیر گردیده است. بالادی با زیبایی تمام پدیده را تشریح می‌کند، از مقدمات متناهی و آغاز تئوری در دههٔ ۱۹۶۰ گرفته تا کارهای جدید راجع به تابع زتای سیستم دینامیک (با تابع زتای ریمان اشتباه نشود ــ اما زتای دینامیک روی زتای ریمان بی‌تأثیر نیست)، و دترمینانِ حاد[1] که خود از صاحبان اثر در آن است. با توجه به غنای مطلب و این منبع الهام بی‌پایان، یعنی تأثیرات فیزیک و ایده‌های اصلی در تولید و ابداع شاخه‌های ریاضی و خصوصاً با توجه به آن که از نزدیک می‌دانم عده‌ای از پژوهشگران جوان ما مشغول کار پایان‌نامه و رساله در زمینه‌های مشابه هستند امّا از جریانهای همسایگی خود بی‌خبرند، شدیداً توصیه می‌کنم که مقالهٔ بالادی مورد مطالعه قرار گیرد. ترجمهٔ آن نیز توصیه می‌شود. مخصوصاً بخش آخر مقاله، که به مباحث اخیر، با ذکر مرجع، اشاره می‌کند، می‌تواند سرنخ کارهای پژوهشی برای جوانان سرگردان ما باشد. در اینجا فیزیک، احتمالات، آنالیز و هندسه به هم کمک می‌کنند و در طول مقاله آنچه گفته شده است قابل درک است و آنچه ناگفته مانده به اشاره و فهرست‌وار عنوان گردیده است، مانند دینامیک مختلط.

۱۶. مقالهٔ بنوا ب. ماندلبروت: مباحث ریاضی برخاسته از هندسهٔ فراکتال.

هر چند در گردش، نوبت مقالهٔ ماندلبروت به آخر موکول شده است، من به علت قرابت بخش کوچکی از آن با مقاله‌های مربوط به سیستم دینامیک، ترجیح می‌دهم همین جا از این مقاله صحبت کنم. البته کمیتهٔ علمی هم کار موجهی انجام داده زیرا معتقد است که مقالهٔ ماندلبروت خود به‌تنهایی یک گردش در ریاضیات (با انتخاب نویسنده) است.

ماندلبروت در مقدمه این سؤال را مطرح می‌کند که آیا ریاضیات محض (یا محضیده!) به عنوان یک نظام مستقل و با انزوای کامل از جهان محسوسات وجود دارد و به رشد خود ادامه می‌دهد (آن‌گونه که مثلاً به دیدگاه افلاطون منسوب است)؟ یا این که، برعکس، وجود ریاضیات کاملاً محض افسانه‌ای بیش نیست. سپس تکیه می‌کند که کار خود من با محسوسات و شروع از شکل‌هایی بوده است که در آغاز هدف محقرانه‌ای داشتند و می‌خواستند پشتیبان افکاری باشند که بدون شکل هم به کندی صورت می‌گرفتند. اما همین شکل‌ها به من و عده‌ای دیگر کمک کردند تا به افکاری نو و نظریه‌های جدیدی راه یابیم.

1) sharp determinant

صحبت‌هایی از این دست ادامه می‌یابد تا در پایان مقدمه می‌گوید در سال ۱۹۷۵ واژهٔ فراکتال‌را در ضرابخانهٔ خود ضرب کردم، ریشهٔ واژه را از لاتین گرفتم، یعنی از fractus به معنی زمخت و شکسته. در اینجا نکته‌ای به نظر می‌رسد: برگردان فارسی برخال به جای فراکتال احتمالاً ناشی از آن بوده که گمان می‌رفته است فراکتال از fraction یعنی کسر یا برخه آمده است. اما متصدی ضرابخانه نظر دیگری دارد پس باید در بکارگیری واژهٔ برخال احتیاط کرد. هرچند کلمهٔ کسر هم به معنی شکستن است، واژهٔ برخه و برخال به زحمت می‌تواند با شکستن مربوط شود.

ماندلبروت به کتاب هندسهٔ فراکتال طبیعت ۱۹۸۲ به زبان انگلیسی اشاره می‌کند که ویرایش جدیدی از کتاب قبلی ۱۹۷۵ او به زبان فرانسه است با عنوان: «اشیاء فراکتال، شکل، بخت و بُعد» که در ۱۹۹۵ به چاپ چهارم رسیده و در ۱۹۷۷ ترجمهٔ انگلیسی آن چاپ شده بود. هم‌چنین به کتاب «فراکتالها و درجه‌بندی در بازرگانی: گسستگی، تمرکز و خطر ۱۹۹۷»، هم‌چنین دو کتاب جدیدتر ۱۹۹۸ و ۱۹۹۹ ارجاع می‌دهد. در متن به شکل‌ها و عکس‌هایی در این کتابها اشاره می‌کند و هر چند مقاله به زبان ساده‌ای نوشته شده است، اما اکثر اشارات آن برای خوانندگانی مفید خواهد بود که با مراجع فهرست (کتابهای خود ماندلبروت) یا این که مراجع داخل متن آشنا باشند. برخی از کارهای مربوط به دینامیک مختلط را دانشجویان ما بهتر می‌شناسند، اما بسیاری هم برای ما ناشناخته است. مقاله شبیه یک لایحهٔ دفاعیه است که به استناد پوشه‌های متعددی که فقط نام پوشه‌ها ذکر شده باشد، تحویل متخصصین امر می‌شود. در کل، نکات آموزندهٔ بسیار دارد اما به این شکل برای ترجمه توصیه نمی‌شود. روح مقاله که از گرافیک‌های کامپیوتری می‌توان و در واقع باید برای بسیاری از نظریه‌ها الهام گرفت، به تنهایی کفایت می‌کند که این موج جدید مطالعه و پژوهش مورد تشویق قرار گیرد. امروز دانشجوی ریاضی محض که از پردازش کامپیوتری سرباز می‌زند و حتی حاضر نیست مقالهٔ خود را تِک پردازی کند، به جنگ زمانهٔ حاضر می‌رود و چندان موفق نخواهد بود.

۱۷. مقالهٔ سمورودینسکی: آگاهی، انتروپی و سامانه‌های برنویی.

ابزارهای ارتباطی، تلگراف، تلفن، رادیو، تلویزیون که در قرن ۱۹ و اوایل قرن بیستم گسترش یافتند، به انتقال اطلاعات می‌پردازند. در نظریهٔ آگاهی این موضوع بررسی می‌شود که ماهیت این اطلاعات چیست و چگونه اندازه‌گیری می‌شوند؟ این پرسش را نوربرت وینر[1] در کتاب سایبرنتیک[2] خود مطرح کرد. کلودشانُن[3] به بررسی منظم مسأله پرداخت و سپس مطالب در نیمهٔ دوم قرن رشد کرد. هدف میر سمورودینسکی[4] در این مقاله آن است که رشد دانش آگاهی را در نظریهٔ ارگودیک[5] بیان کند. مقالهٔ او کوتاه (۱۵ صفحه) به علاوه چهار صفحه و نیم فهرست مراجع، خواندنی، بسیار آموزنده و شایستهٔ ترجمه است. بخش‌های مقاله عبارت‌اند از بخش ۱ (به جای مقدمه)

1) N. Weiner 2) Cibernetics 3) C. Shannon 4) Meir Smorodinsky 5) ergodic theory

با عنوان اندازهٔ آگاهی[۱]. اینجا طبق نظر وینر و شانن تعریفی از اندازهٔ آگاهی به شرح زیر ارائه می‌شود:

فرض کنید $(\Omega, \mathcal{F}, \mathcal{P})$ یک فضای احتمال، $E \in \mathcal{F}$ یک پیشامد و $t = P(E)$ احتمال وقوع E باشد. یگانه تابع پیوسته و نامنفی I از متغیر t که در شرط $I(ts) = I(t) + I(s)$ صدق کند، به شکل

$$I(t) = -\log_a t$$

است، که $a > 1$. در کار اولیهٔ وینر $a = 2$ گرفته شده ولی در این مقاله $a = e$ گرفته می‌شود (e پایهٔ لگاریتم طبیعی است). در بخش دوم، انتروپی[۲]، به یک متغیر تصادفی X در فضای احتمال $(\Omega, \mathcal{F}, \mathcal{P})$ با مقادیر در مجموعهٔ متناهیِ S، یک افراز اندازه‌پذیر Ω به مجموعه‌های A_s را وابسته می‌کند، $A_s = [X = s] = X^{-1}(s)$، و انتروپی شانن را برای X، یا برای $\alpha = \{A_s | s \in S\}$، به شکل $H(X)$ یا $H(\alpha)$ نشان می‌دهد، که چنین تعریف می‌شود:

$$H(X) = -\sum_{s \in S} P(A_s) \log P(A_s).$$

برای آن که ابهام نباشد قرارداد می‌شود $0 \log 0 = 0$. در ادامهٔ بخش، انتروپی مشروط $H(X|Y)$ و به طور کلی‌تر $H(X|\mathcal{F}_0)$ را هنگامی که Y یک متغیر تصادفی دیگر و $\mathcal{F}_0$ یک زیر σ−میدان $\mathcal{F}$ باشد، در نظر می‌گیرد. بعد از بحث مختصری، فرایند تصادفی ایستا[۳] و ویژگی همتوزیعی مجانبی[۴] (AEP) را روشن می‌کند، و به نخستین کارهای دهۀ ۱۹۵۰، راجع به برهان AEP در فرایندهای مارکوف[۵] و فرآیندهای کلی، اما در هر دو حال مربوط به حالت متناهی[۶] و ارگودیک، که توسط خینچین[۷] و مک میلان[۸] یافته شده‌اند، اشاره می‌کند. در بخش سوم، تبدیلات حافظ اندازه[۹] و تغییر جاهای برنولی[۱۰] یا شیفت‌های برنولی و در بخش چهارم انتروپیِ کولموگوروف و سینایی[۱۱] را برای یک تبدیل به اختصار بیان می‌کند. اما در همین بحث کوتاه که به یک صفحه نمی‌رسد، هم صورت قضیهٔ کولموگوروف ــ سینایی را بیان می‌کند و هم می‌گوید خود او برهان سادهٔ قضیه را از دیوید بلاکْوِل آموخت و ایدهٔ اساسی برهان چه بود. در بخش پنجم یکریختی تغییر جاهای برنولی، در بخش ششم K−خودریختی‌ها و انتروپی، در بخش هفتم قضیهٔ یکریختی اورنشتاین[۱۲] بیان می‌شود تا آنکه در بخش ۸ به نظریهٔ عمومی تبدیلات برنولی می‌رسد. در بخش ۹ به نتایج مثبت و کاربردهایی از آنها اشاره می‌کند، ردهٔ وسیعتر فرایندهای برنولی و فرایندهای برنولی ضعیف را تعریف می‌کند و در پی آن، در بخش ۱۰، یک مسألهٔ ساختاری و نظریهٔ نسبی توونو[۱۳] و چند قضیه را بیان می‌کند و با این یادداشت بخش ۱۰ را پایان می‌دهد که: هر فرایند ایستای ارگودیک

---

1) measure of informatio 2) entropy 3) stationary stochastic process 4) Asymptotic Equirepartition Property 5) Markov Process 6) finite state 7) Khinchin 8) McMillan 9) measure preserving transformation 10) Bernoulli shifts 11) Kolmogorov-Sinai entropy 12) Ornstein 13) Touvenot

با انتروپی مثبت، یکریخت است با یک فرایند $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ جایی که $\mathcal{B}_i$ها فرایندهای برنولی‌اند. (این نتیجه در ۱۹۷۹ توسط توونو و سمورودینسکی ثابت شد.) در بخش ۱۱، نتایج منفی به ویژه مثال‌های نقضی که اورنشتاین و بعد از او کالیکو[1] ساخته‌اند، اشاره می‌کند. در بخش‌های ۱۲ تا ۱۶ به ترتیب مباحث مربوط به ساخت نگاشت‌های یکریخت، شارهای برنولی[2]، تعمیم نظریهٔ رابطهٔ هم‌ارزی کاکوتانی[3]، تعمیم نظریهٔ انتروپی به سامانه‌های پویای توپولوژیک[4] و سمبولیک[5] و سرانجام عملهای گروهی برنولی[6] می‌پردازد. به‌ویژه در بخش‌های نیم صفحه‌ای ۱۵ و ۱۶ ایده‌های ساده و جالبی راجع‌به زنجیرهای مارکوفِ توپولوژیک و گروه‌های میانگین‌پذیر و پیوسته دیده می‌شود که ممکن است تعقیب جدی آنها برای دانشجویان علاقه‌مند به گروه‌های تبدیل و آنالیز همساز جالب باشد. یکی از مراجع (که به ۱۹۸۷ برمی‌گردد) مقالهٔ ۱۴۱ صفحه‌ای در مجلهٔ آنالیز ریاضی نوشتهٔ اورنشتاین و بنیامین وَیس با عنوان «انتروپی و قضایای یکریختی در مورد عمل‌های گروه‌های میانگین‌پذیر» اصولاً باید راهنمای خوبی برای این گونه دانشجویان باشد. به هر حال تاریخ سایر مراجع قبل از ۱۹۸۷ است و در چند مورد هم تاریخ اعلام نشده است، مانند کتاب اورنشتاین از انتشارات دانشگاه ییل با عنوان «نظریهٔ ارگودیک، تصادفی‌بودن و سامانه‌های پویا». خودِ سمورودینسکی هم کتابی در سری LNM به‌شمارهٔ ۲۱۴ با عنوان «نظریهٔ ارگودیک، انتروپی» دارد. خوانندگان عین فهرست مراجع مقاله را ملاحظه فرمایند. اکنون که گشت و گذار سطحی خودم را در این مقاله گزارش کردم به راهنمای کتاب مراجعه می‌کنم و می‌بینم که با کلماتی موجز، مقالهٔ سمورودینسکی را وصف کرده است: «مقالهٔ سمورودینسکی در چهارراه نظریهٔ آگاهی، سامانه‌های پویا و احتمالات قرار دارد. نویسنده به تلخیص نظریهٔ آگاهی شانن می‌پردازد. انتروپی کولموگوروف ـ سینایی را برای یک تبدیل حافظ اندازهٔ احتمال تعریف می‌کند. به این ترتیب قادر است قضیهٔ اورنشتاین را ارائه کند، قضیه‌ای که می‌گوید دو سامانهٔ برنولی به معنی اندازه هم‌ارزند اگر و تنها اگر انتروپی کولموگوروف ـسینایی آنها برابر باشد.»

۱۸. مقالهٔ شالاندار و اِستِرْل: مسألهٔ زیرفضای ناوردا

خانم ایزابل شالاندار[7] و آقای ژان استرل[8] از دانشگاه بُردو، مقالهٔ فوق‌العاده زیبا و رسایی در این مسألهٔ معروف آنالیز تابعی نوشته‌اند. خوشبختانه این مقاله مقدمهٔ مبسوطی دارد که در آن ماجرا به شکل قابل فهم برای هر خوانندهٔ ارشد شرح داده شده است. فرض کنید X یک فضای باناخ مختلط و 1_x نگاشت همانی X باشد. جبر عملگرهای خطی پیوستهٔ $T : X \to X$ را با $\mathcal{L}(\mathcal{X})$ و گروه وارونپذیرهای این جبر را با $GL(X)$ نمایش می‌دهیم. طیف و طیف ویژهٔ T، $\sigma(T)$ و $\sigma_p(T)$، عبارت‌اند از:

$$\sigma(T) = \{\lambda | T - \lambda 1_X \notin GL(X)\} \subset \{\lambda|\, |\lambda| \leq ||T||\} \quad \text{و}$$
$$\sigma_p(T) = \{\lambda | \ker(T - \lambda 1_X) \neq \{o\}\} \subset \sigma(T)$$

---

1) Kalikow 2) Bernoulli flows 3) Kakutani equivalence relation 4) topological dynamics
5) symbolic dynamics 6) Bernolli group actions 7) I. Chalendar 8) J. Esterle

شعاع طیفی $\rho(T)$ عبارت است از

$$\rho(T)=\sup_{\lambda\in\sigma(T)}|\lambda|=\lim_{n\to\infty}||T^n||^{\frac{1}{n}}.$$

یک زیرفضای بستهٔ $F\subset X$ را ناوردا[1] برای T می‌نامیم هرگاه $TF\subset F$. زیرفضای بستهٔ $F\subset X$ را اَبَرناوردا برای T می‌نامیم اگر برای T ناوردا باشد و به ازای هر $S\in\mathcal{L}(\mathcal{X})$ که در شرط $ST=TS$ صدق کند نیز ناوردا باشد. واضح است که $F=X$ و $F=\{o\}$ برای هر $T\in\mathcal{L}$ ناوردا هستند. اگر F ناوردا و متمایز از X و $\{0\}$ باشد آن را ناوردای غیربدیهی می‌نامیم. مسألهٔ اصلی زیرفضای ناوردا این است که: برای دسته‌های مفروض $\mathcal{C}$ و $\mathcal{D}$ از فضاهای باناخ و عملگرهای خطی و به ازای هر $X\in\mathcal{C}$ و هر $T\in\mathcal{D}(\mathcal{X})$، آیا یک زیرفضای ناوردای غیربدیهی موجود است؟ از جبر خطی مقدماتی می‌دانیم که در مورد دستهٔ فضاهای متناهی ـ بعد $\mathcal{C}$ و $\mathcal{D}=\mathcal{L}$ جواب مسأله مثبت است. اینجا نکته‌ای حائز اهمیت است و آن این که در مورد فضاهای حقیقی مسأله صحت ندارد، همان‌گونه که مثال سادهٔ دوران در صفحهٔ $\mathbb{R}^۲$ نشان می‌دهد: جز برای نگاشت همانی و نگاشت تقارن مرکزی، هیچ دوران صفحهٔ $\mathbb{R}^۲$ زیرفضای ناوردای غیربدیهی ندارد. بنابراین کاملاً موجه است که فقط فضاهای باناخ مختلط در نظر گرفته شود.

مسألهٔ زیرفضاهای ناوردا برای فضاهای باناخ، برای فضاهای هیلبرت، برای فضاهای باناخ تفکیک‌پذیر[2] و فضاهای هیلبرت تفکیک‌پذیر و مسائل دیگری در ارتباط با این مسأله یکی از مشغولیت‌های جدی آنالیز تابعی در طول قرن بیستم بوده است. در ربع آخر قرن جواب‌های ظریفی به این مسائل داده شده است و برخی از مسائل هنوز مسألهٔ باز هستند. نکتهٔ جالب آن که آنالیز تابعی و آنالیز مختلط یک متغیره در این زمینه با ریزه‌کاری‌های ویژه‌ای به هم تلفیق یافته و در دههٔ آخر قرن در قالب فضاهای برگمن[3]، این همکاری بیشتر تبلور یافته است.

بخش دوم مقاله، یعنی بی‌درنگ پس از مقدمه، به عملگرهای فشرده[4] اختصاص دارد. عملگر خطی $T:X\to X$ را فشرده گویند هرگاه گوی یکهٔ X را به مجموعه‌ای با بستار فشرده تبدیل کند. این عملگرها قرابت فراوانی با عملگرهای با رتبهٔ متناهی[5] دارند. اگر T فشرده باشد، آنگاه $\sigma(T)\subset\{\circ\}\cup\sigma_p(T)$، یعنی مقادیر طیفی غیر صفر مقادیر ویژه‌اند. پس هر عملگر فشرده‌ای که طیف آن منحصر به $\{\circ\}$ نباشد، دارای مقادیر ویژه و درنتیجه دارای زیرفضای ناوردای غیربدیهی است. اما وقتی $\sigma(T)=\{\circ\}$ مسأله به دقت بیشتری نیازمند است. در مورد فضاهای هیلبرت، این مطلب را فون نویمان[6] در دههٔ ۱۹۳۰ حل کرد اما قضیهٔ خود را منتشر ننمود؛ در سال ۱۹۵۳ مسأله برای حالت کلی فضاهای باناخ توسط آرونساین[7] و اسمیت[8] حل شد. در مقاله، ایدهٔ این برهان آمده است. اگر عملگر T فشردهٔ چندجمله‌ای[9] باشد یعنی به ازای یک چندجمله‌ای p، عملگر

1) invariant 2) separable 3) Bergman spaces 4) compact operators 5) finite rank
6) Von Neumann 7) Aronszajn 8) Smith 9) polynomially compact

$p(T)$ فشرده باشد، مسألهٔ زیرفضای ناوردا چگونه است؟ برنشتاین [1] و رابینسن [2] مسأله را در مورد فضاهای هیلبرت حل کردند و از آنالیز نااستانده [3] در حل مسأله استفاده کردند. در همین سال ۱۹۶۶ هالموس [4] راه حل مسأله را با آنالیز کلاسیک ارائه داد. طی پنج سال بعد، مسأله برای فضاهای باناخ هم حل شد و قضیه تعمیم یافت.

در اینجا می‌خواهم اندکی بیشتر تأمل کنم زیرا مفهوم زیربنایی برهان در کار برنشتاین و رابینسن، مفهوم شبه مثلثی بودن [5] است که نقش عمده‌ای در نظریهٔ عملگرها ایفا می‌کند و در مقاله به کتاب رجوی [6] ــ روزنتال [7] برای اثبات قضیهٔ مهمی ارجاع می‌دهد، قضیهٔ لومونوزوف: اگر T یک تجانس نباشد ولی با یک عملگر فشردهٔ ناصفر S تعویض‌پذیر باشد، $TS = ST$، آنگاه T زیرفضای ابرناوردای غیربدیهی دارد. در همین سال ۱۹۷۳ یعنی سال انتشار کتاب رجوی ــ روزنتال، نتایج متعددی به دست آمده است. از جمله برهان ساده‌ای برای حالت خاصی از قضیهٔ فوق که در مقاله قضیه و برهان آن به اقتباس از هیلدن [8] آمده است. در سال‌های اخیر، ۱۹۹۲، ۱۹۹۶ و بعد از ۲۰۰۰، روش لومونوزوف مورد توجه قرار گرفته است.

در بخش سوم مقاله، چند شیوهٔ حساب تابعی [9] مطرح شده است که می‌دانیم در قلب نظریهٔ طیفی جای دارد. اگر یک تابع تام، یا بهتر بگویم یک تابع تحلیلی در یک مجموعهٔ باز U شامل $\sigma(T)$، مانند $f : U \to \mathbb{C}$ داشته باشیم، می‌توانیم عملگر $f(T)$ را در قالب حساب تابعی دانفورد [10] با ضابطهٔ

$$-۲\pi i f(T) := \int_\Gamma f(\zeta)(\zeta ۱_X - T)^{-۱} d\zeta$$

تعریف کنیم، جایی که Γ خم بسته‌ای است که $\sigma(T)$ را در داخل خود جای داده و کلاً در U قرار دارد. اگر $\sigma(T)$ همبند نباشد، می‌توان به کمک این شیوه زیرفضای ابرناوردا برای T یافت. حتی اگر $\sigma(T)$ همبند هم نباشد ولی از هندسهٔ مناسبی برخوردار باشد، می‌توان با همین رهیافت زیرفضای ابرناوردای غیربدیهی برای T یافت. به‌ویژه حیدر رجوی و روزنتال هنگامی که $\sigma(T)$ شامل یک کمان ژردان باشد مسأله را بررسی کرده‌اند. یکی دیگر از حساب‌های تابعی هنگامی است که $\sigma(T)$ بخشی از دایرهٔ یکه $\mathbb{T} = \{\lambda \mid |\lambda| = ۱\}$ در این مورد $f(T)$ با ضابطهٔ

$$f(T) = \sum_{n=-\infty}^{\infty} \hat{f}(n) T^n$$

تعریف می‌شود، مشروط برآن که $f \in L^۱(\mathbb{T})$ و $\sum_{-\infty}^{\infty} |\hat{f}(n)| \, ||T^n|| < \infty$. این حساب تابعی وِرمِر [11] است و به کمک آن در ۱۹۸۷ قضیهٔ زیر ثابت شده است: اگر $\sum \frac{\log ||T^n||}{۱+n^۲} < \infty$ و $\sigma(T)$

---

1) A.R. Bernstein 2) A. Robinson 3) nonstandard analysis 4) P. Halmos
5) quasitriangularity 6) H. Radjavi 7) Rosenthal 8) H.M. Hilden
9) functional calculus 10) Dunford 11) Wermer

بیش از یک نقطه داشته باشد، آنگاه زیرفضای ابرناوردای غیربدیهی برای T وجود دارد. در ادامهٔ این بخش به شرایط هندسی دیگری روی $\sigma(T)$ توجه شده است: وقتی $\sigma(T) = \{0\}$، شرایط تخمینی روی نرم حلال، $\|(\zeta 1_X - T)^{-1}\|$، و شرایط ظریف دیگری اجازه می‌دهند وجود زیرفضاهای ابرناوردا اثبات شود. وقتی $\sigma(T)$ شامل یک کمان باز $L \subset \mathbb{T}$ باشد، مجموعهٔ xهای عضو X به قسمی که تابع $\zeta \mapsto (\zeta 1_X - T)^{-1}x$ دارای ادامهٔ تحلیلی از خلال L باشد، یک زیرفضای ابرناوردای غیربدیهی برای T است. اغتشاش فشرده[1] در این بخش مطرح می‌شود. یکی از کارهای ارائه شده در این زمینه قضیه‌ای است از رجبعلی‌پور و رجوی در ۱۹۷۶. اشتباهاً در متن Radjabali به جای Radjabalipour نوشته شده ولی در مراجع نشانی صحیح است. هم‌چنین حساب تابعی دینکین[2] آخرین قسمت از این بخش است که در آن از فضاهای هاردی[3] H^2 و عملگرهای توپلیتس[4] استفاده می‌شود. مهمترین قسمت مقاله بخش‌های ۴ و ۵ و ٦ است. در ۴ به روش اسکات براون[5] پرداخته می‌شود. اجمالاً روش براون ناظر به $\mathcal{L}(\mathcal{H})$ برای فضای هیلبرت H است و فضای هاردی H^∞، توابع تحلیلی کراندار در قرص یکه، را به کار می‌گیرد و جبرهای دوگان و جبرهای یکنواخت موضوع اصلی و در واقع عنوان این نظریه‌اند. در بخش ۵ مثال‌های نقض، مدیون انفلو[6]، بوزامی[7]، رید[8] هستند. در مثال انفلو، بردار سیکلیک[9] یا بردار چرخه‌ای در مثال بوزامی بردار سوپرسیکلیک[10] یا ابرچرخه‌ای و در مثال رید فضای l^1 مطرح است، که در مقاله توضیحاتی راجع به آنها داده می‌شود. اکنون مثال‌هایی که $\sigma(T)$ قرص یکه باشد و یا $\sigma(T) = \{0\}$ و T زیرفضای ناوردای غیربدیهی نداشته باشد در دسترس است.

اگر به‌جای فضاهای باناخ، فضاهای برداری توپولوژیک موضعاً محدب کامل را در نظر بگیریم، یافتن مثال نقض برای زیرفضاهای ناورداساده است. مثال‌هایی از آتزمون[11] در آخرین قسمت ۵ ناظر به این مسأله است. در آخرین سطرهای آن این مثال جالب به چشم می‌خورد: عدد $\alpha \in (0, \frac{1}{2})$ و مجموعهٔ توابع تام f با شرط

$$p_n(f) = \sup_{z \in \mathbb{C}} |f(z)| \exp(\frac{-1}{n}(|z| + R(z)) + n|z|^\alpha) < \infty$$

را F بنامیم.

حال اگر فضای فرشهٔ[12] $(F, (p_n) \geq 1)$ و عملگر خطی پیوستهٔ $T : f \mapsto f'$ را در نظر بگیریم، می‌بینیم که عملگر T، مشتق معمولی، زیرفضای ناوردای غیربدیهی ندارد. برای تعاریف و قضایای ساده‌ای راجع به نگاشت‌های خطی پیوسته در فضاهای باناخ خواننده را به ترجمهٔ فارسی کتاب کارتان [ک ۱۳۷٦] و برای فضاهای موضعاً محدب و فضاهای فرشه او را به ترجمهٔ فارسی کتاب بورباکی [ب ۱۳۸۰] ارجاع می‌دهیم.

---

1) compact perturbation 2) Dynkin 3) Hardy spaces 4) Toeplitz 5) Scott Brown
6) P. Enflo 7) B. Beauzamy 8) C. Read 9) cyclic vector 10) supercyclic
11) A. Atzmon 12) Fréchet space

نهایتاً آخرین و فنی‌ترین بخش مقاله، بخش ۶ در بطن آنالیز مختلط یک متغیره قرار دارد، البته اینجا نه از دید نظریهٔ توابع بلکه از دید آنالیز تابعی. نخست به نظریهٔ نوانلینا می‌پردازد، یعنی ردهٔ نوانلینا $\mathcal{N}(\mathbb{D})$ را در نظر می‌گیرد، ردهٔ توابع به شکل $\frac{f}{g}$ که f و g در $H^\infty(\mathbb{D})$ قرار دارند، یعنی f و g توابع تحلیلی کراندار در قرص یکه‌اند، و یا توابعی مانند f که در قرص یکهٔ $\mathbb{D}$ تحلیلی‌اند و تابع زیرهمساز[1] وابسته به آن $V = \sup(\circ, \log|f|)$ در شرط

$$\sup_{\circ \leq r < 1} \int_\circ^{2\pi} v(re^{it})dt < \infty$$

صدق می‌کند. می‌دانیم که $\mathcal{N}(\mathbb{D})$ همهٔ فضاهای هاردی $H^p(\mathbb{D})$ را در بر می‌گیرد و $\mathcal{N}(\mathbb{D})$ در ویژگی حد شعاعی[2] فاتو[3] صدق می‌کند: اگر $f \in \mathcal{N}(\mathbb{D})$ آنگاه تقریباً همه جای روی $\mathbb{T}$، به‌ازای $\zeta = e^{i\theta} \in \mathbb{T}$، حد شعاعی

$$f^*(\zeta) = \lim_{\substack{r \to 1 \\ r < 1}} f(r\zeta)$$

موجود است و $\log|f^*| \in L^1(\mathbb{T})$ البته به شرط $f \neq \circ$. سپس به ازای اعضای غیرصفر ردهٔ نوانلینا، حاصلضرب بلاشکه[4] وابسته به صفرهای تابع، تابع خارجی[5]، تابع داخلی[6] و تابع داخلی تکین[7] را مطرح می‌کند که مفاهیمی کلاسیک در نظریهٔ فضاهای هاردی و فضاهای نوانلینا هستند. (خواننده می‌تواند اکنون اندکی از نظریهٔ فضاهای هاردی را در کتاب رودین [ر ۱۳۸۰] به فارسی مطالعه کند. سپس به کارهای جدیدتر در جهت تعمیم نظریهٔ نوانلینا می‌پردازد، به ویژه مطالعات هیمن[8] و کورنبلوم[9]، نیکولسکی[10] و ماسائف[11] ــ موگولسکی[12] در رابطه با تخمین مجانبی توابع تحلیلی در قرص یکه و بیشینه و کمینهٔ قدر مطلق آنها را که در سال‌های ۱۹۷۷ تا ۱۹۹۰ ارائه شده‌اند با اشاراتی کوتاه مرور می‌کند. پس از آن $B^2(\mathbb{D})$، فضای برگمن[13]، متشکل از توابع تحلیلی f در $\mathbb{D}$ را که انتگرال $|f|^2$ برحسب اندازهٔ دوبعدی لبگ، کراندار است در نظر می‌گیرد. عملگر ضرب توابع در z را با S می‌نمایاند و آن را عملگر شیفتِ برگمن[14] می‌نامد. چند صفحهٔ فنی بقیهٔ مقاله راجع به زیرفضاهای ناوردا برای این عملگر یا عملگرهای شیفت وزندار[15] روی دنباله‌های توابع است، که اینجا بحث راجع به آنها را نمی‌آورم و خواننده را به اصل مقاله ارجاع می‌دهم، زیرا گزارشم راجع به این مقاله خیلی طولانی شد. بگذارید در پایان نظر موجز کمیتهٔ علمی کتاب دربارهٔ این مقاله را نیز نقل کنم: «مسأله وجود یک زیرفضای ناوردا برای یک عملگر پیوسته روی یک فضای باناخ تفکیک‌پذیر، یک نمونهٔ کلاسیک است. در ۱۹۷۵ انفلو یک عملگر پیوسته بدون زیرفضای ناوردا می‌سازد.

1) subharmonic 2) radial limit 3) Fatou 4) Blaschke product 5) outer function 6) inner function 7) singular inner function 8) Hayman 9) Korenblum 10) Nikolski 11) Macaev 12) Mogulski 13) Bergman 14) Bergman shift operator 15) wighted shift

در مورد فضاهای هیلبرت مسأله هنوز حل نشده است. مقالهٔ ا. شاندلار و ژ. استرل نتایج متعددی در رابطه با آنالیز مختلط و آنالیز همساز تشریح می‌کند.»

این مقاله برای ترجمه شدیداً توصیه می‌شود. اندک اشتباه چاپی در آن قابل تصحیح است از جمله در بیان قضیهٔ بویرلینگ ـ مالیاون[1] صفحهٔ ۲۵۷ سطر سوم از آخر، به جای f باید در یک مورد حرف k جایگزین شود.

۱۹. مقالهٔ بوتزر[2]، هیگینز[3] و ستنس[4]: نظریهٔ نمونه‌گیری در آنالیز سیگنال‌ها.

به یک معنی، نمونه‌گیری مبحثی قدیمی است، مانند درونیابی لاگرانژ در چندجمله‌ای‌ها یا درونیابی‌های گوناگون در فضاهای هاردی یا در جبر قرص یکه و جبر گوی یکه[5]. کار درونیابی این است که با داشتن اطلاعاتی از یک تابع در تعداد محدودی نقطه، به وضعیت کل تابع دست یابیم. اگر این موضوع راجع به سری‌های فوریه باشد، به وجه قابل درکی به تجزیه و تحلیل سیگنال‌ها مربوط می‌شود. در این مقاله آقای پل بوتزر و همکارانش از دانشگاه‌های آخن[6] هلند و کیمبریج[7] انگلستان، به ما می‌گویند اگر سیگنال f چنان باشد که تبدیل فوریهٔ آن خارج از بازهٔ فشردهٔ $[-\pi W, \pi W]$ صفر شود، به علاوه خود f پیوسته و دارای انرژی متناهی باشد (یعنی $|f|^{۲}$ انتگرال‌پذیر باشد) آنگاه بنا بر قضیه‌ای که امروز بیشتر به قضیهٔ نمونه‌گیری ویتاکر[8] ـ کوتِلْنیکوف[9] ـ شانن[10] معروف است، مقادیر $f(\frac{k}{W})$ در نقاط گره[11] $\frac{k}{W}$ که به فاصله‌های مساوی در طول خط حقیقی $\mathbb{R}$ قرار دارند، برای شناخت f در هر $t \in \mathbb{R}$ طبق ضابطهٔ زیر کفایت می‌کند:

$$\begin{aligned} f(t) &= \sum_{k=-\infty}^{\infty} f(\tfrac{k}{W}) \frac{\sin[\pi W(t-\frac{k}{W})]}{\pi W(t-\frac{k}{W})} \\ &= \frac{\sin(\pi W t)}{\pi} \sum f(\tfrac{k}{W}) \frac{(-۱)^k}{(Wt-k)}. \end{aligned} \tag{۱}$$

این قضیه مربوط به نیمهٔ اول قرن است. در پانوشت صفحهٔ اول مقاله، نکات تاریخی جالبی راجع به اسناد قضیه در امریکا به شانن و در روسیه به ولادیمیر آلکساندروویچ کوتلنیکوف و توضیحاتی راجع به مشخصات فردی و شغلی این افراد و حتی چگونگی تهیهٔ میکروفیش از مقالهٔ کوتلنیکوف توسط هیگینس و مستقلاً توسط همکار دیگری از آخن به‌نام لوکه[12] داده می‌شود. به کتاب سال‌های طلایی ریاضیات مسکو که جلد ٦ از تاریخ ریاضیات و در ۱۹۹۳ به کوشش پل دیورن[13] با همکاری انجمن ریاضی آمریکا و انجمن ریاضی لندن انتشار یافته، همچنین به دایرةالمعارف بزرگ شوروی ارجاع می‌دهد.

از نظر قدمت کار ویتاکر (۱۹۱۵) مقدم بر کار بقیه است و کار شانن (۱۹۴۹) آخر سر قرار می‌گیرد.

---

1) Beurling-Malliavin 2) P.L. Butzer 3) J. R. Higgins 4) R.L. Stens 5) ball algebra
6) Aacheng 7) Cambridge 8) Wittaker 9) Koteĺnikov 10) Shannon 11) node
12) Lüke 13) P. Duren

به این ترتیب مقدمهٔ مبسوط مقاله با بیش از ۴ صفحه شروع می‌شود؛ در همین مقدمه، ارزیابی کار دیگران و مقایسه با کار شانن از دید فرهنگ و اندیشهٔ حاکم بر کار هر یک تشریح می‌شود. دیده می‌شود که سری فوق در واقع به نحوی حد درونیابی لاگرانژ است هنگامی که تعداد گره‌ها به بینهایت میل می‌کند. خودِ سری، به شکل انتگرال فوریهٔ وارون در حالت گسسته است. هم‌چنین تعبیر با انتگرال‌های پیچشی[1] و حاصل‌جمع‌های پیچشی[2] و انتگرال دیریشله[3] در همین مقدمه ارائه می‌شود. سرانجام دستگاه متعامد $\{W\mathrm{sinc}(Wt-k)\}_{k\in\mathbb{Z}}$ را در فضای هیلبرت توابع نوار محدود[4] که زیرفضای $L^2(\mathbb{R})$ است، به عنوان تعبیر دیگری از نظریهٔ نمونه‌گیری مطرح می‌کند (جایی که سینک و یا سینوس کاردینال با $\mathrm{sinc}t = \frac{sin(\pi t)}{\pi t}$ برای $t \neq 0$ و $\mathrm{sinc}\, 0 = 1$ برای $t = 0$ تعریف می‌شود). این هم ناشی از یک نوع دوگانگی فوریه[5] است. بهترین تقریب f با «چندجمله‌ای‌های» سینک یعنی

$$\sum_{k=-N}^{N} \gamma_k sinc(Wt-k)$$

در نُرم فضای $L^2(\mathbb{R})$، همان سریِ (۱) است. مسألهٔ نمونه‌گیری به مسألهٔ بهینه‌سازی ضرایبِ γ_k در این تقریب منجر می‌شود. مقالهٔ ۱۱ صفحه‌ای شانن که در ۱۹۴۰ واگذار اما فقط پس از ۹ سال در ۱۹۴۹ چاپ شد، منشأ مطالعات وسیعی در نظریهٔ نمونه‌گیری گردید (دست کم در ممالک غربی). زیرا بنا بر نخستین مقالهٔ مروری در این زمینه (به سال ۱۹۷۷) دست کم ۲۵۰ مقاله در مجلات مهندسی راجع به مباحث مختلف نظریهٔ نمونه‌گیری در فاصلهٔ سال‌های ۱۹۵۰ تا ۱۹۷۷ منتشر شده است. دو کتاب مارکس دوم[6] در سال‌های ۱۹۹۱ و ۱۹۹۳ راجع به مدخل نظریهٔ نمونه‌گیری و درونیابی شانن و مباحث پیشرفته در این نظریه است که بالغ بر ۱۰۰۰ مورد و ۸۵۰ نویسنده را در بر می‌گیرد. هدف من از نقل بخش‌های متعددی از این مقدمه آن بود که نشان دهم تحلیل نویسندگان در این متن واقعاً در خور یک مقالهٔ مروری در زمینهٔ تاریخ، فرهنگ و اندیشهٔ ریاضی است. در بقیهٔ بخش‌ها که از تفصیل آنها می گذرم، مباحث گوناگونی با روشنی مطرح شده است. هر کس که علاقه‌مند به آنالیز عددی و ریاضی مهندسی برق باشد و هر که در این عقیده با من شریک شود که بین ریاضیات محض و کاربردی چنان سایه‌ـروشن تدریجی گسترده است که هیچ کس قادر به تعیین یک مرز (غیرفازی) برای آنها نیست، با مطالعهٔ بخش‌های زیر از این مقاله خواهد دید که این عقیده می‌تواند در سرنوشت برنامه‌های آیندهٔ رشته‌های ریاضی به‌ویژه در ارتباط با مهندسی و صنایع عمیقاً مؤثر باشد. بخش‌های مقاله عبارت‌اند از شرح‌های نسبتاً مبسوطی با عناوین زیر:

---

1) convolution integral 2) convolution sums 3) Dirichlet integral 4) band-limited
5) Fourier duality 6) R. J. Marks II

- نمونه‌گیری توابع نوار محدود: دستور جمعبندی پواسون[۱]؛
- نمایش مشتقات در نظریهٔ نمونه‌گیری[۲] و تبدیلات هیلبرت[۳]، نمونه‌گیری در کانال‌های چندگانه[۴]؛
- تخمین‌های خطا[۵]: خطای برش[۶]، خطای دامنهٔ نوسان[۷]، خطای زمان لرزه[۸]؛
- نمونه‌گیری توابعی که الزاماً با نوار محدود نیستند؛ خطای هم‌اثرسازی[۹]؛
- ارتباط با دستور کلی جمعبندی پواسون[۱۰]، با دستورهای جمعبندی اویلر—ماک لورن[۱۱] و آبل—پلانا[۱۲] و هم‌چنین با تابع زتای ریمان[۱۳]؛
- قضیهٔ نمونه‌گیری کرامر[۱۴]؛
- نمونه‌گیری توابع مخصوص[۱۵] و تابع زتای ریمان؛
- سری‌های نمونه‌گیر[۱۶] تعمیم یافته؛
- رفتار سری‌های نمونه‌گیر در نقاط ناپیوستگی پرشی[۱۷]؛
- نمونه‌گیری در قالب‌های مجرد: روش‌های فضای هیلبرت، نمونه‌گیری در گروه‌های آبلی موضعاً فشرده.

البته فقط این عناوین، محتوای غنی مقاله ۴۰ صفحه‌ای را که حدود ۱۰ صفحهٔ آن فهرست مراجع است، منعکس نمی‌کند.

ارتباط تنگاتنگ مطلب با نظریهٔ توابع مختلط، معادلات دیفرانسیل معمولی، مسائل مقدار مرزی، آنالیز تابعی و آنالیز همساز ره‌آوردی است که در این گشت و گذار به دست آوردم و توصیه می‌کنم دانشجویانی که هاله‌ای از محدودیت دور خود تنیده‌اند تا فقط خود را به «محض» یا فقط به «کاربردی» مشغول کنند، هاله را کنار بزنند و با خواندن مقالاتی این چنین و مراجع معرفی شده در آن، به ویژه کتاب‌های مربوط به نمونه‌گیری و درونیابی، به گنج‌های ارزشمندی از منابع الهام در دو جهت (محض$\longleftrightarrow$ کاربردی) دست یابند.

مانند چند مورد پیش، نظر موجز کمیتهٔ علمی راجع به این مقاله را نیز نقل می‌کنم: «آنالیز فوریه نقشی بنیادی بر عهده دارد. مقالهٔ بوتزر_ هیگینس و ستنس ناظر به پایهٔ شانن مرکب از انتقال‌های صحیح سینوس کاردینال است و سینوس کاردینال تبدیل‌یافتهٔ فوریهٔ یک تابع سرشتنمای یک بازه است). این پایه به کمک نمونه‌گیری به تشریح سیگنال‌هایی می‌پردازد که طیف فرکانس‌های آنها

1) Poisson's summation formula 2) sampling representation of derivatives 3) Hilbert transform 4) multichannel sampling 5) error estimates 6) truncation 7) amplitude 8) time-gitter 9) aliasing error 10) general Poisson's summation formula 11) Euler-Maclaurin 12) Abel-Plana 13) Riemann zeta function 14) H. Kramer 15) special functions 16) sampling series 17) jump discountinuity

کراندار است. زمان این سیگنال‌ها کراندار نیست. در واقع، بنا بر اصل عدم قطعیت، تعیین زمان و فرکانس به طور توأم ناچار با محدودیت روبرو می‌شود.»

۲۰. **مقالهٔ ژافار:تجزیه به موجک‌ها:**

آقای استفان ژافار[1] با سلیقهٔ خاصی به نگارش این مقاله پرداخته است: تعداد فرمول‌های آن اندک، به طور میانگین ۲ فرمول در صفحه است؛ فهرست مراجع به ۴ بخش تقسیم شده است. تک‌نگاری‌ها(۱۶ مورد) مقالات مدخل (۷ مورد)، گزارش‌ها و مجلدات ویژهٔ موجک‌ها و آخرسر مقالات پژوهشی (۲۰ مورد)، که جمعاً ۵۵ عنوان را در بر می‌گیرد. در بین مراجع یک تک‌نگاری جزء Memoirs AMS نوشتهٔ استفان ژافار و ایو میر[2] در ۱۹۹۶ و دو مقالهٔ پژوهشی از ژافار است. بالغ بر ۵۰ مرجع از سال ۱۹۹۰ به بعد نوشته شده‌اند و ۵ مرجع دیگر یک استثنا به سال ۱۹۵۲ و بقیه بعد از ۱۹۸۷ منتشر شده‌اند. البته این انتخاب محدود آگاهانه انجام شده است، همان‌گونه که نویسنده در آغاز مقاله (مقدمهٔ بدون عنوان) شرح می‌دهد. کل این مقدمه به شرح زیر است:

«منظور از عبارت «تجزیه‌های موجکی» چیست؟ به معنای کاملاً محدود منظور بررسی تجزیهٔ توابع بر حسب پایه‌های یکامتعامد فضای $L^2(\mathbb{R})$ خواهد بود که به شکل الگوریتمیِ قابل ملاحظهٔ

$$\psi_{j,k}(x) = 2^{j/2}\ \ \psi(2^j x - k), j, k \in \mathbb{Z}$$

هستند، یعنی اعضای این پایه با انتقال و انبساط از روی یک تابع ψ به‌دست می‌آیند. علی‌رغم انحصاری بودن، پذیرش همین دیدگاهِ محدود، یکی از سرنخ‌های اصلی است که مارا به زمینه‌های علمی موردبحث راهنمایی می‌کند. درواقع، تحقیق حول و حوش موجک‌ها، امروزه شامل مجموعه‌ای بس متنوع از تجزیه‌هاست. تقریباً می‌توان ادعا کرد که تنها وجه مشترک این تجزیه‌ها آن است که آنها ابتدا در آغاز دههٔ ۱۹۸۰ توسط گروه علمی کوچکی که دور آلکس گروسمان[3]، ژان مورله[4] و ایو مِیر حلقه زده بودند انجام گرفت، اما اکنون به شدت مورد تهاجم انبوهی از افراد و گروه‌های دیگر است. [در این مقاله] آن دسته از مسائل علمی که انگیزهٔ این فنون متنوع را تشکیل می‌دهند، رابطهٔ بین این فنون، اختلافهایشان و به‌ویژه باروری و بهره‌وری چند منظورهٔ ناشی از این بررسی‌ها را که قادر بوده‌اند اهل دانش رشته‌های مختلف را دور هم جمع کنند و همکاری آنان را موجب گردند، تشریح خواهیم کرد. البته به وقایع‌نگاری بر حسب تاریخ و زمان وقوع آنها نخواهیم پرداخت، زیرا افکار مشابه تحت لوای ظاهراً متفاوت در گوشه‌هایی جدا از هم توسط گروه‌ها و جمعیت‌های گوناگونی به طور مستقل آشکار شده‌اند. برعکس سعی خواهیم کرد چند زمینهٔ مرکزی را انتخاب کنیم و به سیر تحول هر یک و تعامل آنها با هم بپردازیم. هم‌چنین یکی از هدف‌های ما آن است که مدخلی برای مقالات و کتاب‌های این موضوع فراهم کنیم. البته منابع مربوط به این موضوع به شکل غول‌آسایی وسیع است، لذا بیشتر به تک‌نگاری‌ها و مقالات مدخلی

---

1) Stéphane Jaffard   2) Yves Meyer   3) Alex Grossmann   4) Jean Morlet

خواهیم پرداخت، که آنها به نوبهٔ خود کتابنامهٔ تخصصی در حوزه‌های فرعی را در بر دارند.»

پیش از شروع بخش ۱، سپاسگزاری از ایومیر، به خاطر آن که متن حاصل از مذاکرات سودمند با او است، دیده می‌شود. مقاله اساساً ۲ بخش دارد: ۱. چرا به پایه‌های نامشروط توجه می‌شود؟ ۲. کدگذاری اطلاعات، که هر کدام زیربخش‌هایی دارند. مقاله برای ترجمه از دو نظر موکداً توصیه می‌شود: اول آن که موضوع مورد بحث تازه، داغ و مورد علاقهٔ جمع کثیری است. دوم و مهمتر آن که شیوهٔ نگارش فرهنگ و اندیشه آن قوی و سرمشق والایی در این زمینه است. به امید آن که ترجمه دیر نپاید و به ابدیت نپیوندد، از ذکر جزئیات بخش‌ها صرف نظر می‌کنم. نظر کمیتهٔ علمی در معرفی مقاله را نیز می‌آورم: «پایه‌های موجکی که مرکب‌اند از انتقال‌های صحیح و انبساط‌های ۲تایی یک موجک، اجازه می‌دهند که سیگنال‌ها از حیث زمان و از حیث فرکانس به‌خوبی تشریح شوند. درحالی‌که موجک کلاسیک هار[1] ناپیوسته بود، در سال ۱۹۸۶ ایو میر موجکی ساخت که به ردهٔ شوارتس[2] متعلق بود. مقالهٔ اِس. ژافار کاربردهای متعددی از موجک‌ها، از نظریهٔ سیگنال و آمار را در نظریهٔ عملگرها، در فراکتال‌ها و در پایه‌های نامشروط فضاهای تابعی ارائه می‌کند».

۲۱. مقالهٔ یوهان سوشتراند: آنالیز میکرولوکال

این مقاله راجع‌به عملگرهای شبه‌دیفرانسیل[3] و عملگرهای انتگرالی فوریه[4] است که ظرف ۴۰ سال گذشته رشد کرده و امروز به‌نام آنالیز میکرولوکال[5] یا مایکرولوکال و یا با ترجمه تحت‌الفظی «تحلیل موضعیِ ریز» نامیده می‌شود. در مقالهٔ سوشتراند[6](اگر املای فارسی آن را درست نوشته باشم) مروری بر این مبحث مهم در نظریهٔ معادلات با مشتقات پاره‌ای (PDE) می‌شود. در سال ۱۹۶۵ کوهن[7] و نایرنبرگ[8] و بی‌درنگ پس از آنها لارش هرماندر[9] به بررسی عملگرهای شبه دیفرانسیل پرداختند. در جامعهٔ ریاضی ایران، دست کم پس از سخنرانی و اهداء مقالات سخنران مدعو در پنجمین کنفرانس ریاضی کشور(شیراز ۱۳۵۳) با مبحث عملگرهای شبه دیفرانسیل آشنایی حاصل شده است اما (تا آنجا که من اطلاع دارم) هیچگاه مشارکتی جدی در این زمینه به عمل نیامده است. این مقاله می‌تواند به طور قابل درکی مطالب را برای دانشجویان و استادان ما در دسترس قرار دهد. توزیعات شوارتس به‌ویژه فضای $S(\mathbb{R}^n)$، یعنی فضای توابع بینهایت بار دیفرانسیل پذیر $u(x)$ که خود و هر یک از مشتقات جزئی آن در بینهایت سریعتر از هر توان منفی $||x||$ به صفر میل می‌کنند، دانسته فرض می‌شود. در مقدمهٔ روشن و قابل درکِ مقاله، به این نکته اشاره می‌شود که به ازای $u \in S(\mathbb{R})$، بین u و تبدیل یافتهٔ فوریهٔ آن $\hat{u}$ داریم:

$$||u||^{۲} \leq ۲||(x-x_{۰})u||\frac{۱}{\sqrt{۲\pi}}||(\xi-\xi_{۰})\hat{u}||$$

که در آن نرم‌ها همان نرم‌های متداول $L^{۲}$ اند و $\hat{u}(\xi) = \int_e^{-ix\xi} u(x)dx$. اصل عدم قطعیت

---

1) Haar 2) Schwartz 3) pseudodifferential operators 4) Fourier integral operators
5) microlocal analysis 6) Johannes Sjöstrand 7) Kohn 8) Nirenberg 9) L. Hörmander

به شکل زیر از آن نتیجه می‌شود که اگر انرژی u عمدتاً در بازهٔ I به مرکز $x_\circ$ متمرکز شده باشد و انرژی $\hat{u}$ عمدتاً در بازهٔ I، آنگاه حاصلضرب طول بازه‌ها نمی‌تواند خیلی از $\frac{1}{2}$ کمتر شود. این نظر نویسنده است که «هرچند نظریهٔ آنالیز میکرولوکال از نظریهٔ معادلات با مشتقات جزئی سرچشمه گرفته و هنوز هم بیشترین کاربردش در آن است، اما شاید بهترین شیوهٔ درشتنمایی آنالیز میکرولوکال در آن باشد که رهیافتی منظم برای اصل عدم قطعیت هایزنبرگ فراهم می‌کند که می‌گوید نمی‌توانیم توأماً موضع زمان و فرکانس را با دقت کافی مشخص کنیم.» گسترش و کاربرد وسیع آنالیز میکرولوکال در زمینه‌های گوناگون رخ داده است، نویسنده خود را محدود می‌کند به بحث در زمینه‌هایی که به شکل بخش‌های زیر در مقاله جای گرفته‌اند: ۱. عملگرهای شبه‌دیفرانسیل؛ ۲. مجموعه‌های جبههٔ امواج (WF)[1] و انتشار تکینگی‌ها؛ ۳. عملگرهای انتگرالی فوریه؛ ۴. بسط بیشتر در C^∞؛ ۵. چارچوب تحلیلی حقیقی؛ ٦. مسائل غیرخطی؛ ۷. نظریهٔ طیفی و مباحث مربوط به آن.

یکی از ویژگی‌های جالب جبههٔ امواج WF که در مقاله روشن شده این است که اگر $\pi : T^*X\backslash\circ \to X$ تصویر متعارف از فضای فاز $X \times (\mathbb{R}^n\backslash\{\circ\})$ روی مجموعهٔ باز $X \subset \mathbb{R}^n$ باشد، آنگاه $\pi(WF(u) = \text{sing supp}u$. باید گفت که یکی از نحوه‌های نگاه به آنالیز میکرولوکال از دید رفتار مرزی توابع تحلیلی در یک دامنهٔ مختلط در مرز حقیقی آن است که با عنوان ابرتابع[2] شناخته شده است. این دیدگاه را در مقاله ملاحظه نکردم. از سوی دیگر ارائهٔ مفاهیم مقاله در این گزارش سطحی (از هر دیدگاهی که مطرح شود) مستلزم مطالب فنی خواهد بود که از حوصلهٔ گزارش خارج است. پس به همین بسنده کنیم. فکر نمی‌کنم ترجمهٔ آن برای فرهنگ و اندیشه ریاضی در اولویت باشد، زیرا مفاهیم و مباحث مطرح شده در آن نیازمند توضیحات فراوانی خواهد بود تا خوانندهٔ فرهنگ و اندیشه آنها را درک کند.

۲۲. مقالهٔ فرانسیس هـ. کلارک: حساب تغییرات، آنالیز ناهموار و کنترل بهین.

به عبارتی حساب تغییرات جزء قدیمی‌ترین مباحث در کنار حساب دیفرانسیل و انتگرال است. اگر به برخی تاریخچه‌های ریاضیات اعتماد کنیم، باید گفت که از دید آنها واژهٔ انگلیسی calculus به معنی دو حساب دیفرانسیل و انتگرال نیست تا به شکل تثنیه «حسابان ۲» ترجمه شود، بلکه به معنی «حساب» مستطاب[3] است، یا اگر دوست دارید که شخصیت‌های مفهومی ریاضی را دست بیندازید گاهی به جای حسابان بگویید «عالیجناب حساب» . راستی فکرش را بکنید در سفرنامهٔ «از ذره تا بینهایت مهر» [م ۱۳۸۰] یک وقت گردشگر خیالی ما که از رنج گرفتن ویزا و روزهای اول سفر آسوده می‌شد اگر سری هم به تئاتر می‌زد آنجا که نمایشنامهٔ «عالیجناب حساب» روی صحنه بود و او را به جرم سوء استفاده از القاب و مخصوصاً لقب «مستطاب»، یک عالیجناب سرخ پوش (یکی دیگر از مباحث جنجال برانگیز ریاضی) یا سیاهپوش محاکمه می‌کرد. من فکر می‌کنم هیجان

1) Wavefront set 2) hyperfunction 3) calcul par excellencc

دانشجویان درس حسابان و ریاضیات عمومی پس از خواندن چنین نمایشنامه‌ای دو چندان شود. البته روزگار استاد درس خراب می‌شود و برای جوابگویی مجبور است مطالعات خود را بیشتر کند، مثلاً به کتاب گسترش ریاضیات قرن بیستم ۱۹۰۰ تا ۱۹۵۰ و یا ۱۹۵۰ تا ۲۰۰۰ که مورد معرفی و نقد ماست، مراجعه نماید. بهتر بگویم مقالهٔ کلارک را بخواند. باری پس از این چند سطر شوخی، موضوع مقاله را به اختصار گزارش می‌کنم. یافتن یک خم یا یک رویه که با داشتن قیودی کمترین طول یا کمترین سطح را داشته باشد، و مسائل نظیر آن، موضوع حساب تغییرات است. مجموعهٔ خم‌های مورد بحث مجموعه‌ای بینهایت بعدی است و مسائل ماکسیمم ـ مینیمم (بیشینه و کمینهٔ) معمولی توابع یک متغیر یا چند متغیر حقیقی در مورد آنها کارآمد نیست. برعکس، فضاهای باناخِ این توابع، معمولاً چارچوب خوبی برای طرح مسأله است و حساب دیفرانسیل در فضاهای باناخ معمولاً شرایط لازم و حتی شرایط لازم و کافی در برخی موارد برای نقاط فرین[1] یعنی بهترین خم یا رویهٔ مورد نظر فراهم می‌کند. مسألهٔ کمینه و بیشینهٔ نسبی در فضاهای باناخ هم عملاً مانند حالت متناهی‌ـبعد، جزء مواد درسی دورهٔ کارشناسی ریاضی محض و کاربردی است (وقتی مثلاً مرجع درس کتاب [ک ۱۳۷۶] باشد). در واقع مقدمات حساب تغییرات هم فصلی دیگر از کتاب اصلی کارتان [C ۱۹۹۷] است، که ترجمهٔ فارسی آن در سال‌های تعطیلی دانشگاه‌ها پایان یافت اما هنوز چاپ نشده است [ک ؟۱۳۸]. از دید کلارک، این قسمت حساب تغییرات، نظریهٔ سطحی[2] یا کم مایه یا ساده‌لوحانهٔ حساب تغییرات است، به دلیل آن که «وجود» جواب را از پیش فرض می‌کند. نظریهٔ عمیق زمانی است که شرایط وجود جواب هم بررسی شود. یادآوری کنیم، در حساب تغییرات اساساً به کمینه‌سازی[3] عبارتی به شکل

$$J(x) = \int_a^b L(t, x(t), x'(t))dt$$

می‌پردازند (یا عبارت مشابه آن وقتی تابع مجهول به جای تابع یک متغیر $x(t)$ یک تابع چندمتغیره $x(t_1, \ldots, t_N)$ است). تابع عددی L یا تابع لاگرانژ[4] مسأله در $[a, b] \times \mathbb{R}^n \times \mathbb{R}^n$ و یا در $[a, b] \times E \times E$ (که E یک فضای باناخ است) تعریف شده و در حالت سطحی از ردهٔ C^1 فرض می‌شود و روی آن نرم معقولی مثلاً $||x||_\infty + ||x'||_\infty$ را در نظر می‌گیرند. اندک اندک از گذشتهٔ دور متوجه شدند که باید شرط هموار بودن کنار رود مثلاً ردهٔ PWS یعنی توابع پاره‌ـ پاره هموار[5] جایگزین C^1 شود. البته در گوشه‌های خم $t \mapsto x(t)$ مشکلات کوچکی پیش می‌آید که توسط اردمان[6] و وایرشتراس رفع شده است. کار مهم را دوبواـ رَیمون[7] انجام داد که روش‌های بکار گرفته شده توسط او را پیش درآمدی به نظریهٔ توزیع شوارتس[8] می‌شناسند. شرط معروف اویلر، به شکل

$$\frac{\partial L(t, x, x')}{\partial x'} = \int_a^t \frac{\partial L}{\partial x}(s, x, x')ds + \text{ثابت}$$

1) extreme points 2) naive theory 3) minimization 4) Lagrangian function
5) piecewise-smooth 6) Erdmann 7) Dubois-Raymond 8) Schwartz distribution theory

در می‌آید که شکل انتگرالی معادلهٔ اویلر است. نویسنده پس از مقدمه و نظریهٔ سطحی به مسائل جدی که همگی مربوط به قرن بیستم است می‌پردازد، مسألهٔ وجودی با کار تونلّی[۱] در ۱۹۱۱ به نتیجه رسید، جایی که ردهٔ AC از توابع مطلقاً پیوسته[۲] تضمینی برای وجود جواب است: تابع $x(t)$ مطلقاً پیوسته است اگر یک تابع انتگرال‌پذیرِ لبگ[۳] v موجود باشد به قسمی که

$$x(t) = x(a) + \int_a^t v(s)ds$$

و در نتیجه برابری $\frac{dx}{dt} = v(t)$، (لبگ ـتقریباً همه جا) در $[a,b]$ معتبر است. دو شرطِ اساسی که تونلّی یافت: یکی تحدب[۴] L بر حسب v و دیگری کوئرسیوبودن[۵] $||L(t,x,v)|| \geq \beta||v||^۲ + \alpha$ برای $\beta > ۰$ و α ثابت بود. اینجا هم با آن که وجود جواب در AC تضمین شد مسائلی مطرح می‌شود که عمدتاً می‌خواهد موقعیت جواب در AC را با رده‌های $C^۱$ و PWS و غیره بسنجد. در اینجا ردهٔ لیپشیتز هم نقشی ایفا می‌کند. قضایای متعددی در زمینهٔ وجود[۶] و نظم[۷] بیان می‌شود. آنالیز محدب نقش خود را با زیبایی تمام نشان می‌دهد. بخش‌های دیگر مقاله یکی آنالیز ناهموار[۸] است که اساساً توابع نیم‌پیوسته و مفهوم زیردیفرانسیل تقریبی[۹] و گرادیان تعمیم یافته[۱۰] و اهمیت هندسی آنها را مورد بررسی یا اشاره قرار می‌دهد. در بخش پنجم که به شرایط لازم تعمیم یافته و کنترل بهینه[۱۱] اختصاص دارد، مشمولیت اویلر و تابع همیلتونیِ $H(x,p)$ و ارتباط آن با مکانیک تحلیلی بیان می‌شود. پس از مقدماتی، به مفهوم کنترل به عنوان یک تابع اندازه‌پذیر مناسب و بخش‌هایی راجع‌به مکتب روس و به‌ویژه قاعدهٔ ماکسیمم پونتریاگین اشاره می‌کند و پس از بیان یک قضیه ارتباط روش‌های تغییراتی و ارتباط با نظریهٔ کنترل را بیان می‌کند و به کتاب هایی از خود کلارک یا از یانگ[۱۲] ارجاع می‌دهد. در بخش های ٦ و ۷ مبحث معادلهٔ همیلتن ـیاکوبی و نظریهٔ کنترل راجع به یک معادلهٔ دیفرانسیل

$$\frac{dx}{dt} = f(x(t), \mu(t))$$

را مطرح می‌کند و نهایتاً به آنالیز ناهموار و کنترل که عنوان کتابی دیگر از خود کلارک است، ارجاع می‌دهد. از دید من این مقاله برای هر دانشجوی ارشد ریاضی و مهندسی که به معادلات دیفرانسیل معمولی علاقه‌مند است، یا به تحقیق در عملیات می‌پردازد ضروری است. در جمع برای سایر ریاضیدانان نیز بسیار سودمند است. ترجمهٔ آن طیف وسیعی از خوانندگان فرهنگ و اندیشه را ارضاء خواهد کرد. اینجاست که محض و کاربردی دست در دست هم دارند.
اجازه می‌خواهم با نقل جمله‌های کمیتهٔ علمی در وصف این مقاله خاتمه دهم:

---

1) Leonida Tonelli 2) absolutely continuous 3) Lebesgue integrable 4) convexity 5) coercivity 6) existence 7) regularity 8) nonsmooth analysis 9) Proximal subdifferential 10) generalized gradient 11) optimal control 12) Young

«قواعد حساب تغییرات تسهیلات فراوانی برای مسائل غیرخطی فراهم می‌کنند. مقالهٔ ف. کلارک راجع به کمینه‌سازی تابعک کلاسیک حساب تغییرات است. آنالیز ناهموار که نویسنده ابداع کرده است به یک شرط لازم و کافی برای بهینگی در قالب صورت‌بندی همیلتون ـ یاکوبی می‌انجامد. نویسنده هم‌چنین وجود و نظم جواب را بررسی می‌کند، به‌ویژه وجود نظم کمینه‌سازی‌های تکین [1] را با فرض‌های قضیهٔ تونلّی ارائه می‌کند.»

مراجع

[C 1997] Cartan, H., Cours de calcul différentiel, 5ième éd., Hermann, Paris, 1997

[P 1994] **Pier**, J.P. (edited by), *Development of mathematics* 1900-1950, Birkhäuser, Basel 1994.

[P 2000] **Pier**, J.P. (edited by), *Development of mathematics* 1950-2000, Birkhäuser, Basel 2000.

[ب ۱۳۸۰] بورباکی، ن. فضاهای برداری توپولوژیک (کتابچهٔ خلاصه با یادداشت‌های تاریخی)انتشارات دانشگاه تهران، شماره۲۵۱۱، تهران، ۱۳۸۰ (ترجمهٔ ارسلان شادمان).

[ب ۱۳۸۱] بورباکی، ن.، خمینه‌های دیفرانسیل و تحلیلی، جلد یکم بندهای یک تا هفت انتشارات دانشگاه تهران، شماره ۲۵۸۲ ، تهران ۱۳۸۱ (ترجمهٔ ارسلان شادمان).

[ب ۱۳۸۱] بهزاد، م. مروری بر نظریهٔ گراف‌ها، گزارش همایش ماهانه انجمن ریاضی ایران، جلد ۱ (۱۳۸۱)، صص ۱ تا ۲۱.

[ر ۱۳۸۰] رودین، و.، آنالیز حقیقی و مختلط، نشر مبتکران، تهران، ۱۳۸۰ (ترجمهٔ علی اکبر عالم‌زاده).

[ر ۱۳۷۴] رید، م.، هندسهٔ جبری مقدماتی، مرکز نشر دانشگاهی، تهران ۱۳۷٦ (ترجمهٔ رحیم زارع نهندی).

1) singular minimizers

[ش ۱۳٦٦] شادمان، ا. قرینه‌سازی جبری به عنوان یک مسألهٔ جهانی قسمت اول رشد آموزش ریاضی، جلد ۱۱، صص ۳۸ تا ۴۳.

[ش ۱۳٦۷] شادمان، ا. قرینه‌سازی جبری به عنوان یک مسألهٔ جهانی قسمت دوم، رشد آموزش ریاضی، جلد ۱۲، صص ۴۹ تا ۵۳.

[ش ۱۳۸۰ آ] شادمان، ا.، معرفی و نقد کتاب گسترش ریاضیات ۱۹۰۰ تا ۱۹۵۰، فرهنگ و اندیشه ریاضی، شماره ٢٦ (بهار ۱۳۸۰)، صص ۵۳ تا ٦٦.

[ش ۱۳۸۰ ب] شادمان، ا.، معرفی و نقد کتاب گسترش ریاضیات ۱۹۰۰ تا ۱۹۵۰، (قسمت دوم)، فرهنگ و اندیشه ریاضی، شماره ۲۷ (پاییز ۱۳۸۰)، صص ۷۱ تا ۸۳.

[ک ۱۳۷٦] کارتان، هـ. حساب دیفرانسیل، انتشارات دانشگاه تهران شماره ۱۹۷٦ چاپ دوم شماره مسلسل ۳۹۱۱ ،تهران ۱۳۷٦ (ترجمهٔ ارسلان شادمان).

[ک ?۱۳۸] کارتان، هـ.، صورت دیفرانسیل، (ترجمهٔ ارسلان شادمان)، در دست انتشار.

[و ۱۳۸۱] وحیدی اصل م. ق. مروری بر فرایندهای زیرجمعی ارگودیک و چند کاربرد، گزارش همایش ماهانه انجمن ریاضی ایران جلد ۱(۱۳۸۱)، صص ۱۰۷ تا ۱۲۷.

ارسلان شادمان
دانشگاه تهران، دانشکده علوم ریاضی و کامپیوتر
پست الکترونیک: chademan@khayam.ut.ac.ir

.

فرهنگ و اندیشهٔ ریاضی
شماره ۳۱ (پاییز ۱۳۸۲) صص. ۷۷ تا ۷۹

مسأله

این قسمت از فرهنگ و اندیشهٔ ریاضی به طرح و سپس حلِ مسائلی در حدِ دروسِ دوره‌های کارشناسی و کارشناسی ارشدِ ریاضیات اختصاص دارد. از کسانی که مایل به ارسال مسائل یا حل مسائلِ مطرح شده می‌باشند، تقاضا می‌شود مسائل خود را به نشانی تهران، مرکز تحقیقات فیزیک نظری و ریاضی، پژوهشکدهٔ ریاضیات، صندوق پستی ۵۷۴۶ـ۱۹۳۹۵، محمدرضا پورنکی ارسال فرمایند. مسائلِ ارسال‌شده باید همراه با حل کامل مسأله باشد و در مجله به نامِ شخصِ فرستنده درج خواهد شد.

حل مسألهٔ ۵۶:

چون $(a,b)=1$، پس $(a+b,ab)=1$ و لذا $ord_b a$، $ord_a b$ و $ord_{ab}(a+b)$ همگی تعریف شده‌اند. گیریم $ord_b a = l$، $ord_a b = k$ و $ord_{ab}(a+b)=t$.

$$ord_{ab}(a+b)=t \Rightarrow (a+b)^t \overset{ab}{\equiv} 1 \left\{ \begin{array}{l} (a+b)^t \overset{a}{\equiv} 1 \Rightarrow b^t \overset{a}{\equiv} 1 \Rightarrow k|t \\ (a+b)^t \overset{b}{\equiv} 1 \Rightarrow a^t \overset{b}{\equiv} 1 \Rightarrow l|t \end{array} \right.$$

در نتیجه خواهیم داشت $[l,k]|t$. حال داریم:

$$\begin{array}{l} ord_b a = l \Rightarrow a^l \overset{b}{\equiv} 1 \Rightarrow (a+b)^l \overset{b}{\equiv} 1 \Rightarrow (a+b)^{[l,k]} \overset{b}{\equiv} 1 \\ ord_a b = k \Rightarrow b^k \overset{a}{\equiv} 1 \Rightarrow (a+b)^k \overset{a}{\equiv} 1 \Rightarrow (a+b)^{[l,k]} \overset{a}{\equiv} 1 \end{array}$$

در نتیجه با توجه به این که $(a,b)=1$ خواهیم داشت:

$$(a+b) \overset{ab}{\equiv} 1 \Rightarrow t|[l,k].$$

بنابراین $t=[l,k]$. $\square$

حل مسألهٔ ۵۷: واضح است که R و R' جابه‌جایی و از مشخصهٔ ۲ هستند. چون $0 \in R'$، پس پوشا بودن f نتیجه می‌دهد که $y \in R$ موجود است که $f(y)=0$. در نتیجه

$$f(0)=f(0y)=f(0)f(y)=f(0)0=0.$$

حال $a,b \in R$ را دلخواه بگیرید و آنها را تثبیت کنید. چون $f(a+b)-f(a)-f(b) \in R'$، پس $x \in R$ موجود است که $f(a+b)-f(a)-f(b)=f(x)$. می‌توانیم بنویسیم:

$$\begin{aligned}
&f(ax)(f(a+b)-f(a)-f(b)) = f(ax)f(x)\\
&\Rightarrow f(ax+abx)-f(ax)-f(abx) = f(ax)\\
&\Rightarrow f(ax+abx) = f(abx)\\
&\overset{f \text{ یک به یک}}{\Longrightarrow} ax+abx = abx \Rightarrow ax = \circ \quad (\text{به همین ترتیب } bx=\circ)
\end{aligned}$$

اکنون داریم

$$\begin{aligned}
&f(x)(f(a+b)-f(a)-f(b)) = f(x)f(x)\\
&\Rightarrow f(ax+bx)-f(ax)-f(bx) = f(x)\\
&\Rightarrow f(x) = \circ \quad (\text{با توجه به این که } f(\circ)=\circ,\ ax=bx=\circ)
\end{aligned}$$

در نتیجه $f(a+b)=f(a)+f(b)$ و لذا $R \cong R'$. $\square$

حل مسألهٔ ۵۸:

$$(AB)^{۲} = \begin{pmatrix} ۷۲ & ۱۸ & -۱۸ \\ ۱۸ & ۴۵ & ۳۶ \\ -۱۸ & ۳۶ & ۴۵ \end{pmatrix} = ۹\begin{pmatrix} ۸ & ۲ & -۲ \\ ۲ & ۵ & ۴ \\ -۲ & ۴ & ۵ \end{pmatrix} = ۹AB.$$

$$\Rightarrow B(AB)^{۲}A = B(۹AB)A \Rightarrow BABABA = ۹BABA$$

$$\Rightarrow (BA)^{۳} = ۹(BA)^{۳}.$$

از طرفی

$$\begin{aligned}
rank(BA) &\geq rank(ABAB)\\
&= rank((AB)^{۲})\\
&= rank(۹AB)\\
&= rank(AB)\\
&= ۲
\end{aligned}$$

پس $rank(BA)=۲$ و لذا BA وارونپذیر است. در نتیجه $BA=۹I$، یا

$$BA = \begin{pmatrix} ۹ & \circ \\ \circ & ۹ \end{pmatrix}. \square$$

حل مسألهٔ ۵۹: فرض کنید $g \in G$ و $h \in H$ دلخواه باشند.
اگر $ghg^{-۱} \in G\backslash H$، آنگاه بنا بر فرض $u \in H$ موجود است که $g^{-۱}(ghg^{-۱})g = u^{-۱}(ghg^{-۱})u$، $h = u^{-۱}(ghg^{-۱})u$، یا $uhu^{-۱} = ghg^{-۱}$. در نتیجه $uhu^{-۱} \in G\backslash H$ که تناقض است. پس لزوماً $ghg^{-۱} \in H$ که نتیجه می‌دهد $H \trianglelefteq G$.
حال فرض کنید $x,y \in G$ دلخواه باشند.

اگر $x \in H$ آنگاه با توجه به نرمال بودن H در G داریم:

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in H.$$

اگر $x \in G\backslash H$، آنگاه $u \in H$ موجود است که $y^{-1}xy = u^{-1}xu$ و لذا با توجه به نرمال بودن H در G،

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}u^{-1}xu = (x^{-1}u^{-1}x)u \in H.$$

پس در هر صورت $[x, y] \in H$ و لذا $G' \leq H$، که نتیجه می‌دهد G/H آبلی است. □