تاریخچه‌ای از نظریهٔ احتمالاتی اعداد [۱]

علی رجالی [۲]

چکیده

« نظریه احتمالاتی اعداد، در حقیقت مطالعهٔ مدل احتمالاتی تابعهای حسابی است. بعضی از نویسندگان شروع آن را ارایه حدسیهٔ گاوس در سال ۱۷۹۱ یعنی قضیهٔ عدد اول، می‌دانند. علاوه بر آن دیریکله، در نظر گرفتن میانگین مقادیر تابعهای حسابی را به عنوان تخمینی از این تابعها به گاوس نسبت می‌دهد.

دیریکله، ریمان، آدامار، پاسین و اویلر در این زمینه فعالیتهایی داشته‌اند، ولی همه این کارها جزء نظریهٔ تحلیلی اعداد به حساب می‌آیند. اردوش و عده‌ای دیگر از نویسندگان، مقالهٔ سال ۱۹۱۷ هاردی و رمنوجان دربارهٔ عدد نرمال عاملهای اول عدد n را نقطهٔ آغازین این علم می دانند. اما همان طور که خود اردوش مطرح کرده ، نقطه‌ی اوج این علم، اثبات قضیهٔ معروف اردوش و کک در سال ۱۹۳۷ بوده است.

در این مقاله ضمن معرفی نظریهٔ احتمالاتی اعداد، به بیان تاریخچه مختصری از این رشته از دانش بشری می پردازیم.»

۱ مقدمه

اگرچه نظریهٔ احتمالاتی اعداد می تواند موضوعات متعددی نظیر «مطالعهٔ تجربی توزیع اعداد اول»، «استقلال آماری و کسرهای دنباله‌دار»، «مدلهای مختلف احتمالاتی روی اعداد طبیعی»، «ارتباط بین اعداد اول و فرآیندهای تصادفی»، «توزیع یکنواخت به پیمانه یک[۳]» و «مولدهای اعداد تصادفی[۴]» را شامل شود ولی همان‌طور که دلانژ[۵] می‌گوید بهتر است نام این رشته را نظریه احتمالاتی تابعهای حسابی [۶] نامید، چون عمدتاً دربارهٔ تابعهای حسابی صحبت می کند.[۱]

---

۱ probabilistic Number Theory

۲ علی رجالی، دانشکده علوم ریاضی دانشگاه صنعتی اصفهان
(این مقاله در نخستین سمینار تاریخ ریاضیات در اسفندماه ۱۳۷۶ در بندرعباس ارایه گردید.)

۳ Weyl's distribution

۴ Random Number Generators

۵ Delange

۶ Probabilistic Theory of Arithmetic Functions

و یادآوری می نماید که یک تابع حسابی، دنباله‌ای از اعداد حقیقی یا مختلط است مثل:

$$\begin{aligned} d(n) &= \sum_{d|n} d \\ \varphi(n) &= |\{m \leq n : m \in N, (m,n) = 1\}| \\ &= n\Pi_{p|n}(1 - \frac{1}{p}) \end{aligned}$$

و

$$w(n) = |\{p : p|n\}|$$

(وقتی $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$، آنگاه $w(n) = k$)، و یا

$$\Omega(n) = \sum_{i=1}^{k} \alpha_i$$

۲ توزیع اعداد اول

برخی از نویسندگان اعتقاد دارند که این شاخه از دانش بشری با حدسیهٔ گاوس [۷] در سال ۱۷۹۱ به نام قضیهٔ عدد اول آغاز شد. از زمان اقلیدس[۸]، یعنی حدود ۳۰۰ سال قبل از میلاد، معلوم بود که « بینهایت عدد اول وجود دارد». ولی با تدوین جدولهای اعداد آنها مشخص شد که توزیع اعداد اول در میان اعداد طبیعی غیرعادی و نامنظم است. در ابتدا سعی می‌شد فرمولی برای nاُمین عدد اول (p_n) یافت شود که اعداد اول را توسط آن تولید کنند ولی همه این تلاشها بی‌نتیجه بود[۹]. پس از آن تلاش شد که تابع

$$\pi(x) = |\{p \leq x, \text{اول } p\}|$$

را محاسبه، یا مقدار تقریبی برای آن پیدا کنند. این کار منجر به بیان و اثبات قضیه عدداول[۱۰] شد. لژاندار[۱۱] در سال ۱۸۰۸ حدسیهٔ قبلی خود را

$$\pi(x) = \frac{x}{\ln x + A(x)}$$

که در آن $\lim_{x\to\infty} A(x) = 0$، بیان کرد. گاوس در سال ۱۷۹۲ یا ۱۷۹۳ این حدسیه را در یکی از جدولهای اعداد اول خود بیان داشت ولی ۵۰ سال بعد از آن، تقریب بهتری را برای این تابع حدس زد[۱۲]:

$$\pi(x) \sim lix = lim_{\epsilon\to 0^+}(\int_0^{1-\epsilon} \frac{dt}{\ln t} + \int_{1+\epsilon}^{x} \frac{dt}{\ln t}) \cdot$$

تابع $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ برای $s > 1$ و $s \in \mathcal{R}$ که در قرن هیجدهم توسط اویلر[۱۳] معرفی شد، در تلاش برای اثبات قضیهٔ عدد اول اهمیت فراوان دارد. این تابع که با دامنهٔ اعداد مختلط ($Re\ s > 1$) به نام تابع زتا[۱۴] معروف است، حالت خاصی از سری دیریکله [۱۵]، ($\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$)، است. ریمان در سال ۱۸۵۹ گسترش تحلیلی این تابع را برای اعداد مختلط با قسمت حقیقی کوچکتر یا مساوی ۱ ($Re\ s \leq 1$) هم، به دست آورد و حدسیه [۱۶] معروف او مبنی بر اینکه «تمام صفرهای این تابع روی خط $Re\ s = \frac{1}{2}$ قرار دارد» هنوز حل نشده است[۱۷]. ارتباط قضیهٔ عدد اول با این تابع، توسط اویلر و با استفاده از فرمول

$$\zeta(s) = \Pi_p(1 - \frac{1}{p^s})^{-1}$$

به دست آمده است، که در جریان تلاش برای پیدا کردن برهان دیگری بر **نامتناهی بودن تعداد اعداد اول**، کشف شد. ایدهٔ آن در تجزیه اعداد طبیعی به عاملهای اول $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

---

۷ Gauss
۸ Euclid
۹ (به ۳ جلد کتاب دیکسون مراجعه شود[۲].)
۱۰ Prime Number Theorem (PNT)
۱۱ Legendre
۱۲ به مقالات گلدشتاین و بیتمن و دیاموند مراجعه کنید[۳، ۴].
۱۳ Euler
۱۴ Zeta Function
۱۵ Dirichlet Series
۱۶ Reimann's Hypothesis
۱۷ به کتاب تیچمارش مراجعه کنید[۵].

مشاهده می‌شود.

تلاشهای زیادی برای اثبات قضیهٔ عدد اول انجام شده است. به طور مثال استیل‌یس[۱۸] در سال ۱۸۸۵ ادعا کرد که حدسیهٔ ریمان را ثابت کرده است. با قبول این حدسیه، مقدار تقریبی بهینه‌ای برای قضیه‌ی عدد اول توسط کوچ[۱۹] به صورت زیر به دست آمد:

$$\pi(x) - lix = O(x^{\frac{1}{2}+\epsilon})$$

که در آن ϵ مقدار بسیار کوچکی است. اما بالاخره در سال ۱۸۹۶، آدامار[۲۰] و واله‌پاسین[۲۱] مستقلاً قضیهٔ عدد اول را اثبات کردند. در این برهانها صورتهای معادل قضیه‌ی عدد اول با استفاده از ویژگیهای تابع زتا، یا مشتق آن ثابت شده است.[۲۲] لاندا [۲۳] مطالبی را دربارهٔ قضیهٔ عدد اول جمع‌آوری و سعی کرد آنها را ساده‌تر نموده و نتایج آن را تعمیم دهد. او اولین کسی بود که قضیهٔ عدد اول را بدون استفاده از معادلهٔ تابعی ζ ثابت کرد. او تابع زتا را به ربع اول و چهارم فضای مختلط به صورت زیر بسط داد،

$$\zeta(s) - \frac{s}{s-1} = s\int_1^\infty \frac{\lfloor x\rfloor - x}{x^{s+1}}dx \quad , \quad Re\, s > 0$$

و کران بالایی را برای مشتق تابع زتا در ناحیه‌ای بدون صفر پیدا کرد. با استفاده از این روش، لاندا مسائل دیگری را نیز حل کرد. از آن جمله، تخمین تعداد ایده‌آلهای اول با نرم حداکثر x در حلقهٔ اعداد صحیح یک میدان جبری عددی را می‌توان نام برد. این مسأله موجب حل بخشی از هشتمین مسأله هیلبرت [۲۴] شد. نظریه‌های تاوبری[۲۵] که در مسائل احتمالاتی هم کاربرد فراوان دارند، نتیجه‌ای از به کارگیری این روشها برای اثبات ساده‌تر و پیدا کردن مقدار تقریبی بهتر برای قضیه عدد اول است[۲۶].

یکی از تلاشهای جالب در این راه، بیان **احتمالاتی نظریهٔ عدد اول** با استفاده از غربال اراتستن[۲۷] و در نظر گرفتن نسبت تعداد اعداد حذف شده در هر مرحله به عنوان احتمال اعداد حذف شده از غربال است[۹].

۳ نظریهٔ احتمالاتی اعداد

دیریکله[۲۸] ادعا می‌کند که گاوس مقدار میانگین $\frac{1}{x}\sum_{n\le x} f(n)$ را برای تخمین مقادیر تابع حسابی f به ازای اعداد طبیعی بزرگ n، در نظر گرفت. دیریکله از این مفهوم برای تابع d استفاده کرد و برای اثباتها، سری دیریکله $\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ را به کار برد. اردوش [۲۹] و بسیاری دیگر از نویسندگان اعتقاد دارند که مقالهٔ سال ۱۹۱۷ هاردی و رمنوجان [۱۰] دربارهٔ عدد نرمال تعداد عاملهای اول عدد n، آغازگر **نظریهٔ احتمالاتی اعداد** است. آنها تابعهای w و Ω را در نظر گرفتند و با استفاده از نابرابری چبیچف [۳۰]:

$$\pi(x) < A\frac{x}{\ln x}$$

نشان دادند که

$$|\{n \le x : w(n) = k\}| \le \frac{c_1 x}{\ln x}\,\frac{(\ln\ln x + c_2)^{k-1}}{(k-1)!}$$

---

۱۸ T. J. Stieltjes
۱۹ Koch
۲۰ Jacques Hadamard
۲۱ Charles-Jean de la Vallee Poussin
۲۲ به کتاب نظریهٔ تحلیلی اعداد نوشته آپوستل مراجعه کنید[۶].
۲۳ E. Landau, Hand Buch der Lehr von der Verteilung der Primzahlen
۲۴ Hilbert
۲۵ Tauberian Theorems
۲۶ به کتاب نظریه تحلیلی اعداد چانداراسرخاران مراجعه کنید[۷]. کتاب ری بن بویم[۸] مرجع مناسبی برای دریافت آخرین اطلاعات در مورد اعداد اول است.
۲۷ Sieve of Eratosthenes
۲۸ Dirichlet
۲۹ Paul Erdos
۳۰ Tchebychev

که در این نابرابری c_1 و c_2 مقادیر ثابت و مستقل از عدد طبیعی k هستند. علاوه بر آن نشان دادند که هرگاه $x \to \infty$، آنگاه

$$\frac{1}{x}|\{n \le x : |w(n) - \ln\ln x| > \varphi(x)\sqrt{\ln\ln x}\}| \to 0$$

یعنی اینکه مقدار نرمال w، $\ln\ln$ است. شرح زیر را توجیهی بر تقریب فوق می‌توان دانست:

$$\begin{aligned}\sum_{n\le x} w(n) &= \sum_{n\le x}\sum_{p|n} 1 = \sum_{n\le x}\sum_{\{m: pm\le x\}} 1\\ &= \sum_{p\le x}\lfloor \frac{x}{p}\rfloor = x\sum_{p\le x}\frac{1}{p} + O(x)\end{aligned}$$

اما

$$\sum_{p\le x}\frac{1}{p} = \int_{1+}^{x}\frac{d\pi(t)}{t} = \ln\ln x + O(1)$$

بهمن صفاری، دلانژ، دیاکونس[31] و سرانجام نویسنده این مقاله در سالهای بین ۱۹۶۸ تا ۱۹۷۸[۱۴، ۱۳، ۱۲، ۱۱] پیرامون این تابع و تخمین دقیقتر آن کار کرده‌اند. نویسنده[۱۵] در سال ۱۹۸۸، این روش را برای همه تابعهای حسابی جمع‌پذیر به کار برد[32]. توران[33] در سال ۱۹۴۳، برهان ساده‌تری برای قضیهٔ هاردی و رمنوجان با استفاده از نابرابری

$$\sum_{n\le x}(w(m) - \ln\ln x)^2 \le Cx(\ln\ln x)$$

پیدا کرد. روش اثبات او بدون اطلاع، مشابه روشهای چبیچف در مسائل احتمالاتی بود.

در کتاب کوبلیوس[34] بسط این قضیه به نابرابری توران–کوبلیوس برای تمام تابعهای حسابی جمعپذیر بیان شده است[۱۷]. سرانجام اردوش در سال ۱۹۳۸ با استفاده از ایدهٔ توران، شرایط کافی برای داشتن توزیع حسابی را به دست آورد. مدل احتمالاتی بیان شده توسط کوبلیوس، برای $x \in \mathcal{R}$ را به شرح زیر می‌توان بیان داشت:

برای $N = \lfloor x \rfloor$، $S = \{1, 2, 3, \cdots, N\}$ را فضای نمونه‌ای در نظر گرفته، توزیع یکنواخت گسسته را روی آن تعریف می‌کنیم. اگر $A \subseteq S$،

$$P_N(A) = \frac{|A|}{N}$$

۱) گوییم مجموعهٔ A دارای چگالی طبیعی است، هرگاه

$$\lim_{x\to\infty} P_N(A \cap S)$$

موجود باشد.

۲) گوییم تابع حسابی f دارای توزیع حدی یا مجانبی است، اگر برای نقاط پیوستگی یک تابع توزیع F، داشته باشیم:

$$\lim_{x\to\infty} P_N\{n \le x : f(n) \le y\} = F(y)$$

۳) تابع حسابی f دارای چگالی حدی یا مجانبی است، اگر برای یک تابع جرمی مانند g روی مجموعه $\{a_1, a_2, \cdots\}$ داشته باشیم:

$$\lim_{x\to\infty} P_N\{n \le x : f(n) = a_k\} = g(a_k)$$

اما عبارت اردوش در مورد تاریخ نظریهٔ احتمالاتی اعداد [۱۸] به شرح زیر است.

> «در سال ۱۹۳۷، ثابت کردم که چگالی اعداد صحیح n که برای آنها $w(n) > \ln\ln n$، برابر $\frac{1}{2}$ است. من روش بران و قضیهٔ حد مرکزی برای توزیع دوجمله‌ای را به کار بردم. من در آن زمان، قضیه حد مرکزی را نمی‌دانستم، اما مسأله برای حالت توزیع دوجمله‌ای ساده بود. در آن

---
۳۱ Diaconis
۳۲ در مرجع [۱۶] به این نکته اشاره شده است.
۳۳ Turan
۳۴ K. Kubilius
۳۵

زمان حتی حالت خاص آن، یعنی قضیهٔ اردوش و کک را هم به دلیل بی‌خبری از نظریهٔ احتمال نمی‌توانستم فرمولبندی کنم.»[۳۵]

قضیهٔ اردوش و کک عبارت است از اینکه اگر f یک تابع حسابی جمعپذیر، $|f(p)| < c$ و $\sum_p \frac{f^2(p)}{p}$ همگرا باشد (p برای نمایش اعداد اول به کار می‌رود)، آنگاه برای

$$A(N) = \sum_{p \le N} \frac{f(p)}{p} \ , \quad B(N) = \sum_{p \le N} f^2(p)/p \ , \quad N = \lfloor x \rfloor$$

داریم

$$\lim_{x \to \infty} P_N\{m \le x : \frac{f(m) - A(N)}{\sqrt{B(N)}} \le y\} = \int_{-\infty}^{y} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du$$

اردوش اضافه می‌کند:

«کک را نخستین بار در زمستان ۱۹۳۹–۱۹۳۸ در بالتیمور ملاقات کردم. بعداً در ماه مارس، وی دربارهٔ تابعهای حسابی جمعپذیر سخنرانی کرد. او در بین مطالب خود، قضیهٔ اردوش– کک را به عنوان حدسیه‌ای بیان کرد. مدتی طولانی بود که به دنبال قضیه‌ای مانند این حدسیه بودم، اما به دلیل بی‌خبری از نظریهٔ احتمال، حتی نمی‌توانستم فرمول آن را بیان کنم. بعد از این سخنرانی، ما در صدد همکاری برآمدیم و آنجا بود که **نظریهٔ احتمالاتی اعداد** متولد شد.»[۳۶]

همچنین در سال ۱۹۳۹، اردوش و ویتنر[۳۷] قضیهٔ زیر را اثبات کردند[۱۹].

قضیه: تابع حسابی f دارای توزیع مجانبی است اگر و تنها اگر

$$\sum_p \frac{f^+(p)}{p} \quad \text{و} \quad \sum_p \frac{(f^+(p))^2}{p}$$

همگرا باشند، وقتی که

$$f^+(p) = \begin{cases} f(p) & , \ |f(p)| < 1 \\ 1 & , \ |f(p)| \ge 1 \end{cases}$$

و تابع مشخصه[۳۸] توزیع حدی آن عبارت است از

$$\Pi_p(1 - \frac{1}{p})(1 + \sum_{n=1}^{\infty} e^{itf(p^n)}/p^n)$$

و سرانجام کوبلیس در سال ۱۹۶۲، نابرابری توران– کوبلیس را برای هر تابع حسابی به صورت زیر برای هر $x \ge 1$، ثابت کرد:

$$\frac{1}{x} \sum_{n \le x} |f(n) - \sum_{p \le x} \frac{f(p)}{p}|^2 \le C_1 \sum_{p \le x} \frac{|f(p)|^2}{p}$$

و در سال ۱۹۹۲، لی[۳۹] با استفاده از کرانهایی برای گشتاور دوم تابع f مقدار C_1 را برابر $\frac{3}{2}$ به دست آورد[۲۰]. حالت کلی قضیه اردوش– کک هم برای رده‌ای خاص از تابعهای حسابی جمعپذیر توسط کوبلیوس اثبات شده است[۲۱]. محاسبهٔ میانگین و واریانس مجانبی تابعهای حسابی (به عنوان متغیرهای تصادفی) روی مدل طبیعی، چگالی جانبی تابعهای

" In 1937, I proved that the density of integers n for which $w(n) > \ln\ln n$ is $\frac{1}{2}$ .I used Brun's method and the Central Limit Theorem for the binomial distribution. I did not at that time know the C.L.T., but in the binomial case this was easy. At that time I could not have formulated even the special case of Erdos-Kac theorem due to my ignorance of probability."

۳۶ "I, first met Kac in Baltimore in the winter of 1938-1939. Later in March, he lectured on additive number theoretic functions. Among other things he stated the Erdos-Kac theorem, as a conjecture!
I was for a long time looking for a theorem like this conjecture, but due to my lack of knowledge of probability theory, I could not even formulate it. After this lecture, we immediately got together, and then the **Probabilistic number theory** was born."

۳۷ Erdos & Witner
۳۸ Characteristic function
۳۹ J. Lee

مختلف حسابی و کاربرد این قضیه‌ها در محاسبهٔ سرعت الگوریتمهای مختلف و به طور خاص تولید اعداد تصادفی از مباحث دیگر این شاخه از دانش بشری است. (برای اطلاعات بیشتر به کتابهای کوبلیوس [۱۷]، بیو[۲۱]، الیوت ۲۲، ۲۳، ۲۴] [۲۲، پوستانیکوف[۲۵] و تەننبام[۲۶] مراجعه کنید.)

مراجع

[1] H. Delange, *Probabilistic number theory*, Ramanujan Revisited. Proceedings of the centenary conference, Univ. of Ill. at Urbana Champaign (1987), Academic Press (1988) ,pp.153-166.

[2] L.E. Dickson, *History of the theory of numbers*, volume I,II and III, Chelsea (1971).

[3] L.J. Goldstein, *A History of the prime number theorem*, Amer. Math. Monthly 80 (1973) ,pp.599-615.

[4] Paul T. Bateman and H.G. Diamond, *A hundred years of prime numbers*, Amer. Math. Monthly 103 (1996) ,pp. 729-741.

[5] E.C. Titchmarsh and D.R.Heath-Brown, *The theory of Riemann zeta function*, 2nd ed., Oxford (1986).

[6] T.M. Apostol, *Introduction to analytic aumber theory*, Springer (1976).

[7] K. Chandrasekharan, *Introduction to analytic number theory*, Springer (1968).

[8] P. Ribenboim, *The new book of prime number records*, 3rd ed., Springer (1996).

[9] M.C. Wunderlich, *A probabilistic setting for prime number theory*, Acta Arith. (1974), pp.59-81.

[10] G.H. Hardy and S.Ramanujan, *The normal number of prime factors of a number* n , Quart. J. Math 48, (1917),pp. 76-92.

[11] B. Saffari, *Sur quelques application de la methode de l'hyperbole, de Dirichlet ala theorie des nombers premiers*, Enseignement Math. 14 (1988), pp.205-224.

[12] H. Delange, *Sur des formules de atle selberg, Acta Arithmetica* XIX (1971) ,pp.105-146.

[13] P. Diaconis, *Asymptotic expansions for the mean and variance of ...*, Technical Report # 96, Stanford University (1976).

[14] A. Rejali, *On the asymptotic expansions for the moments and limiting distributions of some additive arithmetic functions*, Technical Report no. 116, Department of Statistics, Stanford University (1978).

[15] A. Rejali, *Asymptotic expansions for the moments of additive arithmetic functions*, Bull. Iranian Math. Soc. 15 (1988), pp. 32-48.

[16] P. Diaconis, & E. Lehmann, *Contribution to mathematical statistics: A statistical model, F. Mosteller's contribution to statistics*, Science and Public Policy, Springer (1990).

[17] J.Kubilius, *Probabilistic methods in the theory of numbers*. Translations of Math. Monographs. vol 11, A.M.S. (1964).

[18] P. Erdos, Ramanujan and I, *Number Theory*, Madras 1987, Lecture Notes in Math., 1395, Springer (1989), pp. 1-20.

[19] P. Erdos and A. Witner, *Additive arithmetical functions and statistical independence*. Amer.J. Math. 61, (1939), pp. 713-721.

[20] J.Lee, *On the constant in the Turan-Kubilius inequality*, Proceedings of the Amer. Math.Soc. 114 (1992) no. 4. pp.887-895.

[21] G.J. Babu, *Probabilistic methods in the theory of arithmetic functions*. Macmillan lectures in Math. 2 (1978).

[22] P.D.T.A. Elliott, *Probabilistic number theory* I,II. Springer (1979, 1980).

[23] P.D.T.A. Elliott, *Arithmetic functions and integer products*, Springer (1985).

[24] P.D.T.A. Elliott, Book Review (*Integration et theorie des nombers*, by Jean-Loup Mauclaire) Bull. (New series) of the A.M.S. 18 no.2 (1988) pp. 193-209.

[25] A.G. Postanikov, *Introduction to analytic number theory*. Translations of Mathematical Monographs. vol. 68 A.M.S. (1988).

[26] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Societe Mathematique de France, Paris. (1995).