(حل مسأله‌های لاینحل ۲۳۰۰ ساله)

کشف فرمول اعداد اول و نتایج آن*

قسمت ۲

● سید محمدرضا هاشمی موسوی**
hashemi – moosavi@yahoo.com

اشاره:

در قسمت اول مقاله با تاریخ جستجو برای کشف فرمول اعداد اول و تلاش‌های فراوان ریاضیدانان در طی ۲۳۰۰ سال گذشته آشنا شدیم و اینک با کشف فرمول اعداد اول و نتایج بسیار ارزنده آن که به قرار ذیل است آشنا می‌شویم :

✓ توابع تشخیص اعداد اول
✓ توابع مولد اعداد اول
✓ توابع مولد اعداد اول بسیار بزرگ ناشناخته
✓ تعیین تعداد اعداد اول به طور دقیق
✓ حل معادله زتای ریمان
✓ تعیین kامین عدد اول
✓ تعریف مجموعه اعداد اول
✓ تعریف مجموعه‌های اعداد اول مرسن و تام
✓ اثبات بی‌نهایت بودن اعداد اول دوقلو و تعریف مجموعه دوقلوهای اول
✓ حل معادله‌های درجه‌ی nام سیال در حالت عمومی

۱. کشف تابع مولد همه‌ی اعداد اول (۱۳۸۲/۵/۱۴)

ابتدا ماتریسی از صفر و یک برای اعداد فرد طبیعی با توجه به بخش‌پذیری آن‌ها بر هریک از اعداد فرد تشکیل می‌دهیم :

÷	۱	۳	۵	۷	۹	۱۱	۱۳	۱۵	۱۷	۱۹	۲۱	۲۳	۲۵	۲۷	۲۹	۳۱	۳۳	۳۵	۳۷	۳۹	۴۱	
۱	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۳	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۵	۱	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۷	۱	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۹	۱	۱	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۱۱	۱	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۱۳	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۱۵	۱	۱	۱	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۱۷	۱	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۱۹	۱	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
۲۱	۱	۱	۰	۱	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	…

جدول (۱)

توضیح: در صورتی که اعداد ستونی بر اعداد سطری بخش‌پذیر باشند، در جدول تقاطع آن‌ها را یک و در غیر این صورت صفر قرار می‌دهیم. توجه داشته باشید:

- ستون اول فقط ۱ است؛ زیرا همه‌ی اعداد، مضرب عدد ۱ هستند.
- ستون دوم مضارب عدد ۳ را نشان می‌دهد.
- ستون سوم مضارب عدد ۵ را نشان می‌دهد.
- به همین ترتیب هر ستون مضارب یک عدد است.

با توجه به سطرهای جدول ملاحظه می‌شود، در حالتی که در مقابل هر عدد ستونی فقط دو عدد ۱ نوشته شده باشد، در واقع آن عدد ستونی عددی اول است؛ زیرا:

«هر عدد اول تنها بر یک و خودش بخش‌پذیر است.»

می‌دانیم: «برای تشخیص عدد مفروض N کافی است که N را بر اعداد اول نابیش‌تر از $\sqrt{N}$ تقسیم کنیم.» برای تشخیص اعداد ستونی کافی است به سطر آن عدد توجه شود. در صورتی که در هر سطر بیش‌تر از دو عدد ۱ وجود داشته باشد، در واقع آن عدد ستونی اول نیست. برای مثال، سطر مربوط به عدد ۱۵ دارای چهار عدد ۱ است؛ زیرا بر ۱، ۳، ۵ و ۱۵ بخش‌پذیر است. بنابراین، عدد ۱۵ مرکب است. ولی سطرهای مربوط به اعداد ۳، ۵، ۷، ...، ۱۷ و ۱۹، و... فقط دارای دو عدد ۱ است، پس این اعداد اول هستند.

برای تشخیص اعداد، کافی است توابعی را بیابیم که هر یک از ستون‌های جدول را تولید کنند؛ به عبارت دیگر، همه‌ی اعداد صفر یا یک هر ستون را به همان ترتیب ستونی (از بالا به پایین) ارایه کنند. ضابطه‌ی عمومی این گونه توابع به صورت زیر است:

$$F_{2k+1}(x)=\left\lfloor \frac{2k+1}{x}\left\lfloor \frac{x}{2k+1}\right\rfloor\right\rfloor$$

x	$F_3(x)=\left\lfloor \frac{3}{x}\left\lfloor \frac{x}{3}\right\rfloor\right\rfloor$	$F_5(x)=\left\lfloor \frac{5}{x}\left\lfloor \frac{x}{5}\right\rfloor\right\rfloor$	$F_7(x)=\left\lfloor \frac{7}{x}\left\lfloor \frac{x}{7}\right\rfloor\right\rfloor$	$F_9(x)=\left\lfloor \frac{9}{x}\left\lfloor \frac{x}{9}\right\rfloor\right\rfloor$	$F_{11}(x)=\left\lfloor \frac{11}{x}\left\lfloor \frac{x}{11}\right\rfloor\right\rfloor$	…
۱	۰	۰	۰	۰	۰	…
۳	۱	۰	۰	۰	۰	…
۵	۰	۱	۰	۰	۰	…
۷	۰	۰	۱	۰	۰	…
۹	۱	۰	۰	۱	۰	…
۱۱	۰	۰	۰	۰	۱	…
۱۳	۰	۰	۰	۰	۰	…
۱۵	۱	۱	۰	۰	۰	…
۱۷	۰	۰	۰	۰	۰	…
۱۹	۰	۰	۰	۰	۰	…
	⋮	⋮	⋮	⋮	⋮	

جدول (۲)

با توجه به جدول و با توجه به این که برای تشخیص عدد N کافی است، آن را بر اعداد اول نابیش‌تر از $\sqrt{N}$ تقسیم کنیم، N را بر اعداد فرد نابیش‌تر از آن تقسیم می‌کنیم. پس، مجموع توابع اعداد ستونی x کافی است تا عدد فرد نابیش‌تر از $\lfloor \sqrt{N} \rfloor$ محاسبه شود. درنتیجه، اگر N اول باشد، تنها یک عدد ۱ در سطر عدد N خواهیم داشت:

$$S^* = \left\lfloor \frac{\sqrt{2m+1}+1}{2} \right\rfloor \quad \text{و} \quad (1) \quad \sum_{k=0}^{S^*} F_{2k+1}(x) = 1 \quad (\text{N عدد اول})$$

اگر N مرکب باشد:

$$(2) \qquad \sum_{k=0}^{S^*} F_{2k+1}(x) > 1 \quad (\text{N عدد مرکب})$$

$F_1(x) = 1$: ستون اول)

بنابراین، اگر N عددی فرد باشد و $m \in \mathbb{N}$ $(N = 2m+1)$:

$$\Delta_{N(m)} = \left\lfloor \frac{1+\left\lfloor \frac{3}{2m+1} \right\rfloor}{1+\sum_{k=1}^{S^*}\left\lfloor \frac{2k+1}{2m+1}\left\lfloor \frac{2m+1}{2k+1} \right\rfloor \right\rfloor} \right\rfloor$$

$$(3) \qquad = \begin{cases} 1 & N = 2m+1 \ \text{اول باشد} \\ 0 & N = 2m+1 \ \text{مرکب باشد} \end{cases}$$

توجه: عدد $N = 2m+1$، یا **اول** است و یا **مرکب** و این **دو حالت** توسط تابع تشخیص $\Delta_{N(m)}$ معین خواهد شد و همیشه تنها دو حالت (۳)، یعنی ۰ و ۱ پیش خواهد آمد. بنابراین اگر تابعی با استفاده از $\Delta_{N(m)}$ بنویسیم، یک تابع پوشاست (در مجموعه اعداد فرد بزرگ‌تر از ۱):

$$1)\ H(m) = (2m+1-p)\Delta_{N(m)} + p$$

$$2)\ H(m) = p\left(\frac{2m+1}{p}\right)^{\Delta_{N(m)}}$$

* توجه: p عدد اول دلخواه است.

توضیح: عبارت $\left\lfloor \frac{3}{2m+1} \right\rfloor$ فقط برای تشخیص استثنایی عدد ۳ است و اگر $m > 1$ اختیار شود، این عبارت از $\Delta_{N(m)}$ حذف می‌شود:

$$m > 1:\ \Delta_{N(m)} = \left\lfloor \frac{1}{1+\sum_{k=1}^{S^*}\left\lfloor \frac{2k+1}{2m+1}\left\lfloor \frac{2m+1}{2k+1} \right\rfloor \right\rfloor} \right\rfloor$$

این دو تابع هم‌ارز هستند و با فرض این‌که $p = 2$ اختیار شود، دامنه و برد آن‌ها چنین است:

$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$ (مجموعه اعداد اول)

$D_H = \mathbb{N}$ (مجموعه اعداد طبیعی) و $R_H = \mathbb{P}$

توجه: با فرض $p = 2$، برد هر یک از توابع با ضابطه‌های (۱) یا (۲)، مجموعه اعداد اول است.

● **نتیجه**: مجموعه اعداد اول تعریف‌پذیر است:

$$\mathbb{P} = \left\{ H(m) : m \in \mathbb{N},\ H(m) = 2\left(\frac{2m+1}{2}\right)^{\Delta_{N(m)}} \right\}$$

۲. تابع مولد اعداد اول با استفاده از قضیه‌ی ویلسن

قضیه‌ی ویلسن: اگر p اول باشد، آن‌گاه $(p-1)! \equiv -1$ و برعکس.

نکته: با توجه به قضیه‌ی ویلسن، توابع تشخیص اعداد طبیعی مثل N را به صورت زیر تعریف می‌کنیم:

تذکر: عدد یک نه اول است و نه مرکب.

$$1)\ \Delta_1 = \left\lfloor \cos^2 \pi \frac{(n-1)!+1}{n} \right\rfloor = \begin{cases} 1 & \text{n اول باشد} \\ 0 & \text{n اول نباشد} \end{cases}$$

$$2)\ \Delta_2 = \frac{\sin^2 \pi \frac{(n-1)!^2}{n}}{\sin^2 \frac{\pi}{n}}$$

$$= \begin{cases} 1 & \text{n اول باشد } \left(\frac{(n-1)!^2}{n} = \frac{1}{n} + k \ \text{(عدد صحیح)}\right) \\ 0 & \text{n اول نباشد } \left(n \mid (n-1)!^2\right) \end{cases}$$

$$3)\ \Delta_3^{(*)} = \left\lfloor \frac{n}{(n-1)!+1}\left\lfloor \frac{(n-1)!+1}{n} \right\rfloor \right\rfloor = \begin{cases} 1 & \text{n اول باشد} \\ 0 & \text{n اول نباشد} \end{cases}$$

هریک از این توابع (Δ_i) را می‌توان برای تشخیص عددی

طبیعی مثل N به‌کار برد. ولی چون کار با عدد $(N-۱)!$ حتی برای N نه‌چندان بزرگ غیر عملی است، پس این نوع توابع را فقط به عنوان برهانی تئوریک می‌پذیریم.

با توجه به قضیه‌ی ویلسن، تابع تشخیص اعداد را می‌توان یکی از توابع فوق (Δ_i) در نظر گرفت و با آن، تابع مولد اعداد اول را ساخت. چون هر عدد زوج بزرگ‌تر از ۲ مرکب است، پس بهتر است N را عدد فرد بزرگ‌تر از یک در نظر بگیریم:

$$N = ۲m+۱: \quad \Delta_m = \left\lfloor \frac{N}{(N-۱)!+۱} \left\lfloor \frac{(N-۱)!+۱}{N} \right\rfloor \right\rfloor$$

در صورتی که p عدد اول دلخواهی باشد، با توجه به تابع تشخیص Δ_m توابع مولد اعداد اول پوشا به صورت زیر هستند:

$$۱)H_p(m) = p\left(\frac{۲m+۱}{p}\right)^{\Delta_m}$$

$$۲)H_p(m) = (۲m+۱-p)\Delta_m + p$$

نکته: این دو تابع هم‌ارز هستند و هر یک را می‌توان به‌عنوان تابع مولد اعداد اول به کار برد. واضح است که به تعداد اعداد اول (نامحدود)، تابع مولد اعداد اول می‌توان نوشت:

$$P = ۲: H_۲(m) = ۲\left(\frac{۲m+۱}{۲}\right)^{\Delta_m}; \quad H_۲(m) = (۲m-۱)\Delta_m + ۲$$

$$P = ۳: H_۳(m) = ۳\left(\frac{۲m+۱}{۳}\right)^{\Delta_m}; \quad H_۳(m) = ۲(m-۱)\Delta_m + ۳$$

$$P = ۵: H_۵(m) = ۵\left(\frac{۲m+۱}{۵}\right)^{\Delta_m}; \quad H_۵(m) = ۲(m-۲)\Delta_m + ۵$$

$$P = ۷: H_۷(m) = ۷\left(\frac{۲m+۱}{۷}\right)^{\Delta_m}; \quad H_۷(m) = ۲(m-۳)\Delta_m + ۷$$

....

m	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰۰۰
$H_۲(m)$	۳	۵	۷	۲	۱۱	۱۳	۲	۱۷	۱۹	۲۰۰۰
$H_۳(m)$	۳	۵	۷	۳	۱۱	۱۳	۳	۱۷	۱۹	۳۰۰۰
$H_۵(m)$	۳	۵	۷	۵	۱۱	۱۳	۵	۱۷	۱۹	۵۰۰۰
$H_۷(m)$	۳	۵	۷	۷	۱۱	۱۳	۷	۱۷	۱۹	۷۰۰۰
...	...	...	...	...	...	...	...	...	...	...
$H_p(m)$	۳	۵	۷	p	۱۱	۱۳	p	۱۷	۱۹	p۰۰۰

نتیجه: دو تابع پوشای مولد اعداد که همه‌ی اعداد اول را به ترتیب تولید می‌کنند و به جای اعداد مرکب، عدد اول ۲ را جایگزین می‌کنند، به صورت زیر هستند:

$$۱)H(m) = ۲\left(\frac{۲m+۱}{۲}\right)^{\left\lfloor \frac{m}{(m-۱)!+۱} \left\lfloor \frac{(m-۱)!+۱}{m} \right\rfloor \right\rfloor}; \quad D_H = \mathbb{N}, \quad R_H = \mathbb{P}$$

$$۲)H(m) = ۲\left(\frac{۲m+۱}{۲}\right)^{\left\lfloor \frac{۱+\left\lfloor \frac{۳}{۲m+۱} \right\rfloor}{۱+\sum_{k=۱}^{S^*} \left\lfloor \frac{۲k+۱}{۲m+۱} \left\lfloor \frac{۲m+۱}{۲k+۱} \right\rfloor \right\rfloor} \right\rfloor}; \quad D_H = \mathbb{N}, \quad R_H = \mathbb{P}$$

توجه: این دو تابع و توابع معادل آن‌ها به نام «**فرمول‌های اعداد اول**» **(H.M)** نام‌گذاری شده‌اند که دامنه‌ی این توابع، مجموعه اعداد طبیعی **($\mathbb{N}$)** و برد آن‌ها، مجموعه اعداد اول **($\mathbb{P}$)** هستند.

۳. تابع مولد اعداد اول با استفاده از تابع حسابی φ اویلر

با استفاده از تابع $\varphi(n)$ (فی اویلر)، تابع با ضابطه زیر را می‌توان برای تشخیص اعداد به‌کار برد ($n \neq ۱$):

$$۴) \quad \Delta_۴^{(*)} = \left\lfloor \frac{\varphi(n)}{n-۱} \right\rfloor = \begin{cases} ۱ & \text{n اول باشد} \\ ۰ & \text{n اول نباشد} \end{cases}$$

$\varphi(n)$ از دترمینان مرتبه‌ی n زیر به دست می‌آید:

$$\varphi(n) = \begin{vmatrix} ۱ & ۰ & ۰ & ۰ & \dots\dots & ۱ \\ ۱ & ۱ & ۰ & ۰ & \dots\dots & ۲ \\ ۱ & ۰ & ۱ & ۰ & \dots\dots & ۳ \\ \dots & \dots & \dots & \dots & \dots & \dots \\ ۱ & \dots & \dots & \dots & \dots & n \end{vmatrix}$$

توجه: با استفاده از ماتریسی نظیر ماتریسی که ابتدای مقاله ارایه شد، ثابت می‌شود که $\varphi(n)$ از دترمینان بالا محاسبه می‌شود و هم‌چنین می‌دانیم:

$$n = p^r.q^s.t^u\cdots, \quad \varphi(n) = n\left(۱-\frac{۱}{p}\right)\left(۱-\frac{۱}{q}\right)\left(۱-\frac{۱}{t}\right)\cdots$$

توضیح: ستون اول این دترمینان همه یک و ستون آخر آن اعداد طبیعی $۱,۲,۳,\dots,n$ است. در ستون kام، هر درایه‌ای که سطرش به k بخش‌پذیر است یک و بقیه جاهای ستون، صفر قرار می‌دهیم ($\varphi(n)$: تعداد اعداد پیش از n که نسبت به n اول هستند).

نتایج کشف فرمول اعداد اول:

۱ . تابع تعیین تعداد اعداد اول یعنی $\pi(N)$ ، تا عدد فردی مثل N به طور دقیق :

$$\pi(N)=\frac{N+1}{2}-\sum_{m=1}^{\frac{N-1}{2}}\left\lfloor 2^{-\Delta_{N(m)}}\right\rfloor$$

توجه: توسط این تابع (π) ، حل یکی از مسأله‌های هفت‌گانه‌ی انستیتوی clay (مسأله‌های لاینحل جهانی هزاره‌ی هفت میلیون دلاری) ارایه شده است که دو سال به داوری گذاشته می‌شود (معادله‌ی زتای ریمان $\zeta(s)=0$) .

● جواب معادله‌ی زتای ریمان :

$$\lfloor s\rfloor>1:\quad \pi(p)=\frac{p+1}{2}-\sum_{m=1}^{\frac{p-1}{2}}\left\lfloor s^{-\Delta_{N(m)}}\right\rfloor$$

۲ . تعیین k امین عدد اول :

$\pi(N)=k:$ ($k:N=2m+1$ امین عدد اول)

$$P_k(m)=\left\lfloor\frac{1}{\left|k-\frac{N+1}{2}+\sum_{m=1}^{\frac{N-1}{2}}\left\lfloor 2^{-\Delta_{N(m)}}\right\rfloor\right|+1}\right\rfloor .N$$

$$P_k(m)=\begin{cases}N & \text{اگر N، k امین عدد اول باشد}\\ 0 & \text{اگر N، k امین عدد اول نباشد}\end{cases}$$

بنابراین، اگر k امین عدد اول را به P_k نمایش دهیم، می‌توان نوشت (با استفاده از قضیه‌ی چبیچف داریم: $P_k<2^k$):

$$P_k=\sum_{m=1}^{2^k}P_k(m)$$

۳. تعریف مجموعه‌های اعداد اول مرسن و تام:

($\mathbb{M}$: مجموعه اعداد اول مرسن)

$$\mathbb{M}=\left\{M(n):n\in\mathbb{N},M(n)=3\left(\frac{2^{n+1}-1}{3}\right)^{\Delta_{N(2^n-1)}}\right\}$$

$$=\left\{3,7,31,127,\cdots,2^{30402457}-1,\cdots\right\}$$

($\mathbb{F}$: مجموعه اعداد تام)

$$\mathbb{F}=\left\{F(n):n\in\mathbb{N},M(n)\in\mathbb{M},F(n)=2^{n-1}M(n)\right\}$$

$$=\{6,28,496,\cdots\}$$

توضیح: عدد تام عددی است که مجموع همه‌ی مقسوم‌علیه‌های کوچک‌تر از آن برابر خود عدد است .

۴. تابع مولد اعداد اول بسیار بزرگ ناشناخته

تابع مولد اعداد بزرگ‌تر از بزرگ‌ترین عدد اول $M_{43}=2^{30402457}-1$ (عدد مرسن سال ۲۰۰۶) به صورت زیر تعریف می‌شود :

$$M_{43}=2^{30402457}-1=2n+1;\quad n=\frac{M_{43}-1}{2}=2^{30402456}-1$$

$$H(m)=\left[2(m+n)+1-M_{43}\right]\Delta_{N(m+n)}+M_{43}\qquad \text{یا :}$$

$$H(m)=M_{43}\left[\frac{2(m+n)+1}{M_{43}}\right]^{\Delta_{N(m+n)}}$$

با توجه به عبارت زیر :

$$\Delta_{N(m+n)}=\left\lfloor\frac{1}{1+\sum_{k=1}^{S^*}\left\lfloor\frac{2k+1}{2(m+n)+1}\left\lfloor\frac{2(m+n)+1}{2k+1}\right\rfloor\right\rfloor}\right\rfloor$$

$$=\begin{cases}1 & N=2(m+n)+1\ \text{اول باشد}\\ 0 & N=2(m+n)+1\ \text{مرکب باشد}\end{cases}$$

تابع با ضابطه‌های زیر ، همیشه یا عدد اول M (بزرگ‌ترین عدد شناخته شده‌ی اول مرسن) را و یا عددهای اول بعد از این عدد را تولید می‌کنند :

$$1)\quad m\in\mathbb{N}:H(m)=\left[2(m+n)+1-M_{43}\right]^{\Delta_{N(m+n)}}+M_{43}$$

$$=\begin{cases}N & N=2(m+n)+1\ \text{اول باشد}\\ M_{43} & N=2(m+n)+1\ \text{مرکب باشد}\end{cases}$$

$$2)\quad m\in\mathbb{N}:H(m)=M_{43}\left[\frac{2(m+n)+1}{M_{43}}\right]^{\Delta_{N(m+n)}}$$