کشف فرمول اعداد اول و نتایج آن*

(حل مسأله‌های لاینحل ۲۳۰۰ ساله)

قسمت ۴

معادله‌های سیال و تعیین یک جواب عمومی با استفاده از اتحادهای حلال معادله‌ها

$p_1, p_2, \ldots, p_k < p \;;\; a_1X_1^{p_1} + a_2X_2^{p_2} + \cdots + a_kX_k^{p_k} = X_{k+1}^{p}$

$p_1, p_2, \ldots, p_k \in \mathbb{N} \;,\; p \in \mathbb{P}$ (مجموعه ی اعداد اول)

$(p, m) = 1 \;;\; a_1X_1^{p} + a_2X_2^{p} + \cdots + a_kX_k^{p} = X_{k+1}^{m}$

$a_1, a_2, \ldots, a_k \in \mathbb{Q}$ (مجموعه‌ی اعداد گویا)

$(m, N) = 1 \;;\; a_1X_1^{m} + a_2X_2^{m} + \cdots + a_kX_k^{m} = X_{k+1}^{N}$

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

اشاره

با توجه به روش حل معادله‌هایی مانند:

$p_1, p_2 \in \mathbb{N} \;,\; p_1, p_2 < p \;;\; X_1^{p_1} + X_2^{p_2} = X_3^{p}$

$(p, m) = 1 \;;\; X_1^{p} + X_2^{p} = X_3^{m}$

$(m, N) = 1 \;;\; X_1^{m} + X_2^{m} + X_3^{N}$

که در شماره‌ی پیش ارایه شد، در این شماره می‌خواهیم تعمیم این گونه معادله‌ها را بررسی و یک سلسله جواب عمومی معادله را تعیین کنیم. نتیجه‌ی جالب و بسیار مهم از حل معادله‌ی اخیر این است که مجموع توان mام دو عدد را می‌توان به هر توان دلخواه با شرط $(m, N) = 1$ نوشت. برای مثال،

معادله‌ی $x^n + y^n = z^{2003}$ به ازای هر n با شرط $(n, 2003) = 1$ دارای جواب است؛ یعنی همه‌ی معادله‌های زیر جواب عمومی دارند:

$$n = 2:\ x^2 + y^2 = z^{2003}$$
$$n = 3:\ x^3 + y^3 = z^{2003}$$
$$n = 4:\ x^4 + y^4 = z^{2003}$$
....

$$n = 1386:\ x^{1386} + y^{1386} = z^{2003}$$
....

$$n = 2002:\ x^{2002} + y^{2002} = z^{2003}$$
$$n = 2004:\ x^{2004} + y^{2004} = z^{2003}$$
$$n = 2005:\ x^{2005} + y^{2005} = z^{2003}$$
....

توجه: اگر n مضربی از عدد ۲۰۰۳ باشد، در واقع مسأله به حل معادله‌ی سیال قوای متشابه تحویل می‌شود که همان قضیه‌ی بزرگ فرما یا در اصل حکم بزرگ‌فرما است؛ یعنی معادله‌ی:

$$(n, 2003) = 2003\ ;\ x^n + y^n = z^{2003}$$

که به حکم بزرگ‌فرما تبدیل می‌شود و جوابی به جز صفر ندارد.

الف) معادله‌ی سیال به صورت عمومی زیر را بررسی و یک سلسله جواب عمومی برای آن تعیین می‌کنیم:

$$a_1X_1^{p_1} + a_2X_2^{p_2} + \cdots + a_kX_k^{p_k} = X_{k+1}^{p} \qquad (1)$$

در معادله‌ی ۱، pعددی اول و a_1، a_2، ...و a_k عددهایی گویا هستند و شرط زیر نیز برقرار است:

$$p_1, p_1, p_3, \dots, p_k < p$$

برای تعیین یک جواب عمومی برای معادله‌ی ۱، کافی است یک سلسله جواب عمومی معادله‌ی زیر را به‌دست آوریم:

$$a_1x_1^n + a_2x_2^n + \cdots + a_kx_k^n = x_{k+1}^{n+1} \qquad (2)$$

برای تعیین یک جواب عمومی معادله‌ی ۲ کافی است آن را با اتحاد زیر مقایسه کنیم:

$$\begin{aligned}&a_1(a_1b_1^{n+1} + a_2b_1b_2^n + \cdots + a_kb_1b_k^n)^n\\&+ a_2(a_1b_2b_1^n + a_2b_2^{n+1} + \cdots + a_kb_2b_k^n) + \cdots\\&\cdots + a_k(a_1b_kb_1^n + a_2b_kb_2^n + \cdots + a_kb_k^{n+1})^n\\&= (a_1b_1^n + a_2b_2^n + \cdots + a_kb_k^n)^{n+1} \qquad (3)\end{aligned}$$

از مقایسه‌ی معادله‌ی ۲ و اتحاد ۳ خواهیم داشت:

$$\left|\begin{array}{l}x_1 = a_1b_1^{n+1} + a_2b_1b_2^n + \cdots + a_kb_1b_k^n\\x_2 = a_1b_2b_1^n + a_2b_2^{n+1} + \cdots + a_kb_2b_k^n\\x_3 = a_1b_3b_1^n + a_2b_3b_2^n + a_3b_3^{n+1} + \cdots + a_kb_3b_k^n\\\dots\dots\dots\dots\dots\dots\dots\dots\\\dots\dots\dots\dots\dots\dots\dots\dots\\x_k = a_1b_kb_1^n + a_2b_kb_2^n + \cdots + a_kb_k^{n+1}\\x_{k+1} = a_1b_1^n + a_2b_2^n + \cdots + a_kb_k^n\end{array}\right. \qquad (4)$$

در این‌جا، با فرض $n = (p-1)!$، معادله‌ی۲ به معادله‌ی زیر تحویل می‌شود:

$$a_1x_1^{(p-1)!} + a_2x_2^{(p-1)!} + \cdots + a_kx_k^{(p-1)!} = x_{k+1}^{(p-1)!+1} \qquad (5)$$

طبق قضیه‌ی ویلسن، اگر p عددی اول باشد، عبارت $(p-1)!+1$ بر p بخش‌پذیر است. از طرف دیگر ثابت می‌شود، برای هر عبارت تجزیه‌پذیر[1] (p عددی اول و $\lfloor\ \rfloor$ نماد قسمت درست عدد است):

$$(p-1)!+1 = p\left(1 + 2\left\lfloor \frac{(p-1)!+1}{2p} \right\rfloor\right) \qquad (6)$$

از رابطه‌ی ۶ و با توجه به شرط $p_1, p_2, \dots, p_k < p$، معادله‌ی ۵ را به صورت زیر می‌توان نوشت $(p \in \mathbb{P})$:

$$a_1\left(x_1^{\frac{(p-1)!}{p_1}}\right)^{p_1}+a_2\left(x_2^{\frac{(p-1)!}{p_2}}\right)^{p_2}+\cdots$$

$$+a_k\left(x_k^{\frac{(p-1)!}{p_k}}\right)^{p_k}=\left(x_{k+1}^{1+2\left\lfloor\frac{(p-1)!+1}{2p}\right\rfloor}\right)^{p} \qquad (7)$$

از مقایسه‌ی معادله‌ی ۱ با اتحاد ۷، بلافاصله یک سلسله از جواب‌های معادلـه‌ی ۱ حاصل می‌شود. در اتحاد۷، اگر $H(m)$ (فرمول اعداد اول) را جایگزین p کنیم، در این صورت، دامنه‌ی متغیر به مجموعه‌ی اعداد طبیعی گسترش خواهد یافت؛ زیرا به ازای هر $m \in \mathbb{N}$ ، مقدار $H(m)$ عددی اول است:

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

$$,\quad \Delta_m=\left\lfloor\frac{2m+1}{(2m)!+1}\left\lfloor\frac{(2m)!+1}{2m+1}\right\rfloor\right\rfloor$$

در واقع به اتحادهای حلال معادله‌ها دست خواهیم یافت و در نتیجه می‌توان نوشت:

$$(8)\left|\begin{array}{l}
X_1=\left(a_1b_1^{(p-1)!+1}+a_2b_1b_2^{(p-1)!}+\cdots+a_kb_1b_k^{(p-1)!}\right)^{\frac{(p-1)!}{p_1}}\\
X_2=\left(a_1b_2b_1^{(p-1)!}+a_2b_2^{(p-1)!+1}+\cdots+a_kb_2b_k^{(p-1)!}\right)^{\frac{(p-1)!}{p_2}}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
X_k=\left(a_1b_kb_1^{(p-1)!}+a_2b_kb_2^{(p-1)!}+\cdots+a_kb_k^{(p-1)!+1}\right)^{\frac{(p-1)!}{p_k}}\\
X_{k+1}=\left(a_1b_1^{(p-1)!}+a_2b_2^{(p-1)!}+\cdots+a_kb_k^{(p-1)!}\right)^{1+2\left\lfloor\frac{(p-1)!+1}{2p}\right\rfloor}
\end{array}\right.$$

مثال: معادله‌ی زیر را بررسی کنید و یک سلسله از جواب‌های عمومی آن را بیابید.

$$x_1+x_2^2+x_3^3+x_4^4+\cdots+x_{10}^{10}=x_{11}^{11} \qquad (9)$$

حل: کافی است در رابطه‌های ۸، مقادیر زیر را جایگزین کنیم:

$k=10:\ a_1=a_2=\cdots=a_{10}=1$;

$p_1=1, p_2=2,\cdots,p_{10}=10, p=11$

در این صورت، یک مجموعه جواب معادله حاصل می‌شود:

$$(10)\left|\begin{array}{l}
x_1=\left(b_1^{10!+1}+b_1b_2^{10!}+\cdots+b_1b_{10}^{10!}\right)^{10!}\\
x_2=\left(b_2b_1^{10!}+b_2^{10!+1}+\cdots+b_2b_{10}^{10!}\right)^{\frac{10!}{2}}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
x_{10}=\left(b_{10}b_1^{10!}+b_{10}b_2^{10!}+\cdots+b_{10}^{10!+1}\right)^{9!}\\
x_{11}=\left(b_1^{10!}+b_2^{10!}+\cdots+b_{10}^{10!}\right)^{329891}
\end{array}\right.$$

بدیهی است که با در دست داشتن یک سلسله جواب عمومی۱۰، بررسی معادله خاتمه می‌یابد.

ب) بررسی معادله‌ی عمومی $X_1^p+X_2^p=X_3^m$ با شرط $(p,m)=1$ انجام شد. اکنون در این‌جا به بررسی تعمیم این معادله می‌پردازیم:

$$(p,m)=1:\ a_1X_1^p+a_2X_2^p+\cdots+a_kX_k^p=X_{k+1}^m \qquad (1)$$

با توجه به بررسی $X_1^p+X_2^p=X_3^m$ ، تعمیم این معادله را بررسی می‌کنیم.

حل: برای تعیین یک سلسله از جواب‌های عمومی معادله‌ی۱، ابتدا معادله‌ی زیر را بررسی می‌کنیم:

$$a_1x_1^{n-1}+a_2x_2^{n-1}+\cdots+a_kx_k^{n-1}=x_{k+1}^n \qquad (2)$$

برای تعیین یک سلسله از جواب‌های عمومی معادله‌ی۲، کافی است آن را با اتحاد زیر مقایسه کنیم:

$$a_1(a_1b_1^n+a_2b_1b_2^{n-1}+\cdots+a_kb_1b_k^{n-1})^{n-1}+a_2(a_1b_2b_1^{n-1}$$
$$+a_2b_2^n+\cdots+a_kb_2b_k^{n-1})^{n-1}+\cdots+a_k(a_1b_kb_1^{n-1}+a_2b_kb_2^{n-1}$$
$$+\cdots+a_kb_k^n)^{n-1}=(a_1b_1^{n-1}+a_2b_2^{n-1}+\cdots+a_kb_k^{n-1})^n \quad (3)$$

از مقایسه‌ی معادله‌ی ۲ با اتحاد۳، خواهیم داشت:

$$(4)\left|\begin{array}{l}
x_1=a_1b_1^n+a_2b_1b_2^{n-1}+\cdots+a_kb_1b_k^{n-1}\\
x_2=a_1b_2b_1^{n-1}+a_2b_2^n+\cdots+a_kb_2b_k^{n-1}\\
x_3=a_1b_3b_1^{n-1}+a_2b_3b_2^{n-1}+\cdots+a_kb_3b_k^{n-1}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
x_k=a_1b_kb_1^{n-1}+a_2b_kb_2^{n-1}+\cdots+a_kb_k^n\\
x_{k+1}=a_1b_1^{n-1}+a_2b_2^{n-1}+\cdots+a_kb_k^{n-1}
\end{array}\right.$$

در این‌جا، با فرض $n=m^{p-1}$ ، معادله‌ی۲ به معادله‌ی زیر تحویل می‌شود:

$$a_1x_1^{m^{p-1}-1}+a_2x_2^{m^{p-1}-1}+\cdots+a_kx_k^{m^{p-1}-1}=x_k^{m^{p-1}} \qquad (5)$$

طبق قضیه‌ی فرما، اگر p عددی اول باشد، عبارت $(m^{p-1}-1)$ بر p بخش‌پذیر است، در صورتی که m و p نسبت به هم اول باشند: $(m,p)=1$

از طرف دیگر می‌توان نوشت:

$$(m,p)=1:\ m^{p-1}-1=p\left(1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor\right) \qquad (6)$$

(در رابطه‌ی ۶، p عدد اول و $\lfloor\ \rfloor$، نماد قسمت درست عدد است). حال با استفاده از رابطه‌ی۶، می‌توان معادله‌ی ۵ را به صورت زیر نوشت:

$$a_1\left(x_1^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\right)^p+a_2\left(x_2^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\right)^p+\cdots$$

$$+a_k\left(x_k^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\right)^p=\left(x_{k+1}^{m^{p-2}}\right)^m \qquad (7)$$

از مقایسه‌ی معادله‌ی ۱ با اتحاد۷، بلافاصله یک مجموعه جواب عمومی برای معادله‌ی۱ حاصل می‌شود:

$$(8)\left|\begin{array}{l}
X_1=\left(a_1b_1^{m^{p-1}}+a_2b_1b_2^{m^{p-1}-1}+\cdots+a_kb_1b_k^{m^{p-1}-1}\right)^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\\
X_2=\left(a_1b_2b_1^{m^{p-1}-1}+a_2b_2^{m^{p-1}}+\cdots+a_kb_2b_k^{m^{p-1}-1}\right)^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
X_k=\left(a_1b_kb_1^{m^{p-1}-1}+a_2b_kb_2^{m^{p-1}-1}+\cdots+a_kb_k^{m^{p-1}}\right)^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\\
X_{k+1}=\left(a_1b_1^{m^{p-1}-1}+a_2b_2^{m^{p-1}-1}+\cdots+a_kb_k^{m^{p-1}-1}\right)^{m^{p-2}}
\end{array}\right.$$

مثال: یک مجموعه جواب عمومی برای معادله‌ی زیر بیابید، در صورتی که p و m نسبت به هم اول باشند.

$$(p,m)=1:\ X_1^p+X_2^p+\cdots+X_k^p=X_{k+1}^m \qquad (9)$$

حل: کافی است در رابطه‌های ۸، قرار دهیم:

$a_1=a_2=a_3=\cdots=a_k=1$

در این صورت، بلافاصله یک مجموعه جواب عمومی با k پارامتر دلخواه برای معادله‌ی۹ حاصل می‌شود:

$$(10)\left|\begin{array}{l}
X_1=\left(b_1^{m^{p-1}}+b_1b_2^{m^{p-1}-1}+\cdots+b_1b_k^{m^{p-1}-1}\right)^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\\
X_2=\left(b_2b_1^{m^{p-1}-1}+b_2^{m^{p-1}}+\cdots+b_2b_k^{m^{p-1}-1}\right)^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
X_k=\left(b_kb_1^{m^{p-1}-1}+b_kb_2^{m^{p-1}-1}+\cdots+b_k^{m^{p-1}}\right)^{1+2\left\lfloor\frac{m^{p-1}-1}{2p}\right\rfloor}\\
X_{k+1}=\left(b_1^{m^{p-1}-1}+b_2^{m^{p-1}-1}+\cdots+b_k^{m^{p-1}-1}\right)^{m^{p-2}}
\end{array}\right.$$

نتیجه: در حالت خاص، اگر $k=2$، آن‌گاه:

$$X_1^p+X_2^p=X_3^m \qquad (11)$$

معادله‌ی ۱۱ برای هر p اول با شرط $(p,m)=1$، همیشه جواب دارد. بنابراین، معادله‌ی ۱۱ نشان می‌دهد که مجموع قوای متشابه‌ی دو عدد را ممکن است به صورت توانی از یک عدد نوشت، به شرطی که توان‌ها نسبت به هم اول باشند. به بیان دیگر، اگر m مضربی از p نباشد، یعنی $(t\in\mathbb{N})m\neq tp$ و در واقع حکم بزرگ فرما پیش نیاید $\left(p>2:\ x^p+y^p=z^p\right)$، معادله‌ی۱۱ همیشه جواب دارد. هم‌چنین، اگر $m\neq tp$، معادله‌ی۹ نیز همیشه دارای جواب است.

ج) با توجه به بررسی معادله‌ی $X_1^m+X_2^m=X_3^N$، تعمیم این معادله را بررسی می‌کنیم:

$$(m,N)=1:\ a_1X_1^m+a_2X_2^m+\cdots+a_kX_k^m=X_{k+1}^N \quad (1)$$

در حالت خاص، اگر $a_1=a_2=\cdots=a_k=1$، معادله‌ی زیر حاصل می‌شود:

$$X_1^m+X_2^m+\cdots+X_k^m=X_{k+1}^N$$

در معادله‌ی۱، a_1، a_2، ...و a_k اعداد گویای دلخواه و m و Nنسبت به هم اول‌اند.

حل: برای حل معادله ی ۱ و تعیین یک مجموعه جواب برای آن، ابتدا یک سلسله ازجواب‌های معادله‌ی زیر را به دست می‌آوریم:

$$a_1x_1^{n-1}+a_2x_2^{n-1}+\cdots+a_kx_k^{n-1}=x_{k+1}^n \qquad (2)$$

به این منظور کافی است، معادله‌ی ۲ را با اتحاد زیر مقایسه کنیم:

$$a_1\left(a_1b_1^n+a_2b_1b_2^{n-1}+\cdots+a_kb_1b_k^{n-1}\right)^{n-1}$$
$$+a_2\left(a_1b_2b_1^{n-1}+a_2b_2^n+\cdots+a_kb_2b_k^{n-1}\right)^{n-1}+\cdots$$
$$\cdots+a_k\left(a_1b_kb_1^{n-1}+a_2b_kb_2^{n-1}+\cdots+a_kb_k^n\right)^{n-1}$$
$$=\left(a_1b_1^{n-1}+a_2b_2^{n-1}+\cdots+a_kb_k^{n-1}\right)^n \qquad (3)$$

از مقایسه‌ی معادله‌ی ۲ با اتحاد ۳ خواهیم داشت:

$$(4)\left|\begin{array}{l} x_1=a_1b_1^n+a_2b_1b_2^{n-1}+\cdots+a_kb_1b_k^{n-1}\\ x_2=a_1b_2b_1^{n-1}+a_2b_2^n+\cdots+a_kb_2b_k^{n-1}\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ x_k=a_1b_kb_1^{n-1}+a_2b_kb_2^{n-1}+\cdots+a_kb_k^n\\ x_{k+1}=a_1b_1^{n-1}+a_2b_2^{n-1}+\cdots+a_kb_k^{n-1}\end{array}\right.$$

در این جا، با فرض $n=N^{\varphi(m)}$ ، معادله‌ی ۲ به معادله‌ی زیر تحویل می‌شود:

$$a_1x_1^{N^{\varphi(m)}-1}+a_2x_2^{N^{\varphi(m)}-1}+\cdots+a_kx_k^{N^{\varphi(m)}-1}=x_{k+1}^{N^{\varphi(m)}} \qquad (5)$$

در معادله‌ی ۵، φ تابع اویلر است و $\varphi(m)$ برابر با تعداد اعداد طبیعی و کوچک‌تر از m است که نسبت به آن اول هستند. برای مثال، $\varphi(18)$ برابر ۶ است؛ زیرا:

$\{1,5,7,11,13,17\}=$ مجموعه اعدادی که نسبت به ۱۸ اول‌اند ;

$\varphi(18)=6$

نکته: همیشه باید توجه داشت که عدد ۱ نسبت به تمام عددهای بزرگ‌تر از خودش، اول است. طبق قضیه‌ی اویلر، اگر $(m,N)=1$ ، آن‌گاه عبارت $(N^{\varphi(m)}-1)$ بر m بخش‌پذیر است. از طرف دیگر می‌توان نوشت:

$$(m,N)=1\ ;\ \ N^{\varphi(m)}-1=m\left(1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor\right) \qquad (6)$$

(در رابطه‌ی ۶، $\lfloor\ \rfloor$ نماد قسمت درست عدد است).

حال با استفاده از رابطه‌ی ۶، معادله‌ی ۵ را به صورت زیر می‌نویسیم:

$$a_1\left(x_1^{1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor}\right)^m+a_2\left(x_2^{1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor}\right)^m+\cdots$$
$$+a_k\left(x_k^{1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor}\right)^m=\left(x_{k+1}^{N^{\varphi(m)-1}}\right)^N \qquad (7)$$

از مقایسه‌ی معادله‌ی ۱ با اتحاد ۷، بلافاصله یک سلسله از جواب‌های عمومی معادله‌ی ۱ حاصل می‌شود:

$$(8)\left|\begin{array}{l} X_1=\left(a_1b_1^{N^{\varphi(m)}}+a_2b_1b_2^{N^{\varphi(m)}-1}+\cdots+a_kb_1b_k^{N^{\varphi(m)}-1}\right)^{1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor}\\ X_2=\left(a_1b_2b_1^{N^{\varphi(m)}-1}+a_2b_2^{N^{\varphi(m)}}+\cdots+a_kb_2b_k^{N^{\varphi(m)}}\right)^{1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor}\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ X_k=\left(a_1b_kb_1^{N^{\varphi(m)}-1}+a_2b_kb_2^{N^{\varphi(m)}-1}+\cdots+a_kb_k^{N^{\varphi(m)}}\right)^{1+2\left\lfloor\frac{N^{\varphi(m)}-1}{2m}\right\rfloor}\\ X_{k+1}=\left(a_1b_1^{N^{\varphi(m)}-1}+a_2b_2^{N^{\varphi(m)}-1}+\cdots+a_kb_k^{N^{\varphi(m)}-1}\right)^{N^{\varphi(m)-1}}\end{array}\right.$$

توجه: اگر m عددی اول مانند p باشد:

$$\varphi(p)=\varphi(m)=p-1$$

و در صورتی که m عددی مرکب و به صورت $m=p^r.q^s.t^n.\cdots$ (p، q و t... عامل‌های اول هستند) نوشته شود، همیشه می‌توان نوشت:

$$\varphi(m)=m(1-\frac{1}{p})(1-\frac{1}{q})(1-\frac{1}{r})\cdots=\begin{vmatrix}1&0&0&\cdots&1\\1&1&0&\cdots&2\\1&0&1&\cdots&3\\1&1&0&\cdots&4\\\vdots&\vdots&\vdots&\cdots&\vdots\\1&\vdots&\vdots&\cdots&m\end{vmatrix} \qquad (9)$$

مثال: در این جا $\varphi(m)$ را برای $m=1024$ ، $m=1025$

و ۱۰۲۶ = m ، از رابطه‌ی۹ محاسبه می‌کنیم:

$$m = 1024 = 2^{10} : \varphi(1024) = 1024\left(1-\frac{1}{2}\right) = 512$$

$$m = 1025 = 5^2 \times 41 : \varphi(1025) = 1025\left(1-\frac{1}{5}\right)\left(1-\frac{1}{41}\right) = 800$$

$$m = 1026 = 2 \times 3^3 \times 19 :$$

$$\varphi(1026) = 1026\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{19}\right) = 324$$

مثال: اگر $m = p$ و p عددی اول باشد، معادله‌ی۱ به معادله‌ی زیر تحویل می‌شود:

$$a_1X_1^p + a_2X_2^p + \cdots + a_kX_k^p = X_{k+1}^N \qquad (10)$$

با استفاده از سلسله‌جواب‌های ۸، یک مجموعه جواب عمومی معادله‌ی ۱۰ را نتیجه بگیرید.

حل: کافی است که در رابطه‌های ۸، به جای $\varphi(m)$ عبارت $(p-1)$ را جایگزین کنیم:

$$m = p : \varphi(m) = \varphi(p) = p - 1$$

بنابراین، یک سلسله‌جواب عمومی معادله که پیش از این هم به صورت مستقل به آن رسیده بودیم، نتیجه خواهد شد.

نتیجه‌ی نهایی

در صورتی که در همه‌ی معادله‌ها و مجموعه‌ی جواب‌های به‌دست آمده، به جای p (عدد اول) فرمول اعداد اول $H(m)$ را جایگزین کنیم، بدیهی است به جواب‌هایی خواهیم رسید که دامنه‌ی متغیر آن اعداد طبیعی است، یعنی $p = H(m)$ و $m \in \mathbb{N}$. و هم‌چنین، اگر در اتحادهای عمومی حلال معادله‌های سیال درجه‌ی n، به جای p (عدد اول) فرمول اعداد اول را جایگزین کنیم، واضح است که به اتحادهای حلال با دامنه‌ی متغیر $m \in \mathbb{N}$ خواهیم رسید. پس در این‌جا نتایج را در قالب سه قضیه‌ی عمومی در رابطه با وجود یا عدم جواب برای معادله‌های سیال عمومی سه‌گانه، با نام قضیه‌های اساسی H.M می‌آوریم.

۱. **قضیه‌ی اول H.M**: اگر p عددی اول و a_1 ، a_2 ، ... و a_k عددهایی گویا باشند و داشته باشیم $p_1, p_2, \ldots, p_k < p$ ، آن‌گاه معادله‌ی زیر در مجموعه‌ی اعداد گویا دارای جواب است:

$$a_1X_1^{p_1} + a_2X_2^{p_2} + \cdots + a_kX_k^{p_k} = X_{k+1}^p$$

۲. **قضیه‌ی دوم H.M**: اگر p عددی اول و m عددی طبیعی باشد و داشته باشیم $(p,m) = 1$ ، آن‌گاه معادله‌ی زیر در مجموعه‌ی اعداد گویا دارای جواب است (با در نظر گرفتن این‌که a_1 ، a_2 ، ... و a_k گویا باشند):

$$a_1X_1^p + a_2X_2^p + \cdots + a_kX_k^p = X_{k+1}^m$$

$$(p,m) = 1;\ \ a_1, a_2, \cdots, a_k \in Q \text{ (مجموعه‌ی اعداد گویا)}$$

۳. **قضیه‌ی سوم H.M**: اگر m و N اعدادی طبیعی و a_1 ، a_2 ، ... و a_k اعدادی گویا باشند و هم‌چنین m و N نسبت به هم اول باشند، معادله‌ی زیر در مجموعه‌ی اعداد گویا دارای جواب است:

$$(m,N) = 1 :\ \ a_1X_1^m + a_2X_2^m + \cdots + a_kX_k^m = X_{k+1}^N$$

● **از کشف فرمول اعداد اول و نتایج آن، احکام زیر نیز حاصل می‌شود:**

۴. **حکم اساسی H.M در رابطه با مولد اعداد اول**: تابع H با ضابطه‌ی زیر:

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

به ازای هر $m \in \mathbb{N}$ ، **همه‌ی اعداد اول** را تولید می‌کند.

توضیح: مولد $H(m)$ همه‌ی اعداد اول را تولید می‌کند و به جای اعداد مرکب عدد ثابت۲ که عددی اول است را جایگزین می‌کند. بنابراین، تابع H یک تابع پوشا با دامنه‌ی متغیر $m \in \mathbb{N}$ است:

$$R_H = \mathbb{P} \text{ (برد تابع) و } D_H = \mathbb{N} \text{ (دامنه تابع)}$$

$$H = \mathbb{P} = \{3, 5, 7, 2, 11, 13, 2, 17, 19, \cdots\} = \{2, 3, 5, 7, \cdots\}$$

۵. **حکم اساسی H.M در رابطه با توزیع اعداد اول**: تابع π با ضابطه‌ی زیر، به ازای هر N طبیعی، تعداد اعداد اول نابزرگ‌تر از N را به‌طور دقیق تعیین می‌کند:

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

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

$$S^* = \left\lfloor \frac{\sqrt{2m+1}+1}{2} \right\rfloor$$

توجه: این حکم در واقع معادل حل معادله‌ی زتای ریمان است:

$$\zeta(s) = 0$$

این مسأله، یکی از مسأله‌های لاینحل جهانی هزاره‌ی هفت‌میلیون دلاری است که در سال ۲۰۰۱ به مسابقه گذاشته شده است و انستیتوی ریاضیات «Clay» آمریکا پس از دو سال جایزه را پرداخت خواهد کرد (جواب معادله‌ی زتای ریمان را در شماره‌ی ۵۳، قسمت دوم مقاله ببینید).

۶. حکم اساسی H.M در رابطه با تعیین k امین عدد اول:
تابع P_k با ضابطه‌ی زیر، با فرض $N = 2n+1$ و $\pi(N) = k$ به‌طور دقیق kامین عدد اول را تعیین می‌کند:

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

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

توجه: می‌دانیم بزرگ‌ترین عدد اول شناخته شده در سال ۲۰۰۶، عددی است با حدود ۹/۸ میلیون رقم که چهل‌وچهارمین عدد مرسن اول شناخته شده محسوب می‌شود:

$$M_{44} = 2^{32582657} - 1$$

این اعداد توسط جست‌وجوی اینترنتی تحت برنامه‌ی «GIMPS» به صورت عمومی و با استفاده از سیستم‌های شخصی در جهان انجام می‌گیرد. ارایه و تست هر عدد مرسن به صورت $M = 2^p - 1$ در صورتی که تایید شود، مبلغ یک‌صد میلیون دلار (جایزه) به همراه دارد. در این‌جا می‌توان با استفاده از فرمول اعداد اول، مجموعه‌ی اعداد اول مرسن را تعریف کرد.

۷. حکم اساسی H.M در رابطه با تعریف مجموعه‌ی اعداد اول مرسن: مجموعه‌ی اعداد اول مرسن IM تعریف‌پذیر است:

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

$$= \left\{3, 7, 31, 127, \cdots, 2^{32582657} - 1, \cdots\right\}$$

توجه: با استفاده از فرمول اعداد اول، مجموعه‌های اعداد تام زوج، اعداد اول سامان‌پذیر و سامان‌ناپذیر[2] (در اثبات حکم بزرگ فرما نقش اساسی دارند) قابل تعریف هستند. برای اطلاع بیش‌تر، به کتاب مرجع (*) رجوع شود.

۸. حکم اساسی H.M در رابطه با بی‌نهایت بودن اعداد اول دوقلو (Twin): اعداد اول دوقلو بی‌نهایت‌اند و مجموعه‌ی دوقلوهای اول تعریف‌پذیر است:

$$T = \left\{n \in \mathbb{N} - \mathbb{H} : (6n-1, 6n+1)\right\} \cup \left\{(3,5)\right\}$$
$$= \left\{(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), \cdots\right\}$$

$$\mathbb{H} = \left\{5m \mp 1, 7m \pm 1, 11m \mp 2, \cdots, pm \pm \frac{p \pm 1}{6}\right\},$$
$$m \in \mathbb{N}, \quad p \in \mathbb{P}$$

توجه: لازم به ذکر است که کشف فرمول اعداد اول و نتایج آن، توسط داور بین‌المللی، پروفسور سایمون پورپل[3] داوری شد و بالاترین امتیاز (G) را در سال ۲۰۰۷ که معادل A^{++} است[4]، از آکادمی علوم آمریکا (NAAS) کسب کرد و بار دیگر، جمهوری اسلامی ایران در عرصه‌ی تولید علم درخشید. این کشف نتایج ارزنده و مهم دیگری نیز به دنبال داشت که شرح آن را در کتاب مرجع (*) و فهرست عناوین مطالب را در سایت کاشف (**) می‌توانید مشاهده کنید. ادامه‌ی نتایج را در شماره‌های آتی ملاحظه نمایید.

زیرنویس

۱. اثبات این مطلب در قالب یک قضیه‌ی کاربردی و بسیار مهم (از مؤلف) در کتاب مرجع (*) موجود است.

2. Prime numbers of regular and irregular

3. Simon purple

4. Excellent

منابع

* هاشمی موسوی، سیدمحمدرضا. انتشارات بین‌المللی 2006:Brill/VSP
The discovery of prime numbers formula and its results & other top researches (Author: S.M.R.Hashemi Moosavi)

** سایت کاشف فرمول:
www.primenumbersformula.com