قسمت دوم

نظریه‌ی اعداد

مقدمه

نظریه‌ی اعداد یکی از شاخه‌های زیبا و جالب ریاضی است که ریشه در تاریخ بشر دارد و به دلیل زیبایی و کارایی همواره مورد علاقه بوده است. پیشرفت‌های علوم دیگر مانند کامپیوتر و رمزنگاری که تکیه بر نظریه‌ی مقدماتی اعداد دارند، به شادابی و زنده بودن این شاخه از دانش بشری کمک کرده‌اند.

در این قسمت مباحثی مقدماتی از نظریه‌ی اعداد را ارائه می‌دهیم و انتظار داریم دانش‌آموزان عزیز با توجه به محتوای غنی این رشته و نیز تأثیر مثبت حل مسائل آن در جهت تقویت تفکّر ریاضی، مسائلی جالب از نظریه‌ی اعداد را انتخاب و حل کنند.

فصل ۴

کلیّات و تقسیم‌پذیری

۴ــ۱ــ برخی از اصول نظریه‌ی اعداد

نظریه‌ی اعداد شاخه‌ای از ریاضیات است که بیشتر به خواص اعداد طبیعی

$$۱, ۲, ۳, \cdots$$

می‌پردازد. در مورد چگونگی به‌وجود آمدن اعداد طبیعی اطلاع درستی در دست نیست، اما شواهدی وجود دارند که نشان می‌دهند بشر اوّلیه اعداد طبیعی را برای شمارش مورد استفاده قرار داده است و به تدریج روش‌هایی را برای نمایش اعداد و انجام محاسبات اختراع کرده است.

شمارش گوسفندان قبل از رفتن به چرا و پس از بازگشت آن‌ها با استفاده از مفهوم تناظر یک به یک بین مجموعه‌ی گوسفندها و زیرمجموعه‌ای از اعداد طبیعی، یا به صورت یک انگشت، یا یک علامت روی سنگ و یا کنار گذاشتن یک تکه چوب به جای هر گوسفند، حتی هنوز هم گاهی به‌طور ابتدایی معمول است. این عمل که برای تهیه‌ی آمار و حتی رأی‌گیری‌های ساده هم به‌کار می‌رود از شواهد اوّلیه‌ی شناخت اعداد طبیعی است.

دنباله‌ی اعداد طبیعی از ۱ شروع می‌شود و هر عضو دیگر آن با افزودن یک واحد به عدد قبلی به‌دست می‌آید.

در سال‌های گذشته، با مجموعه‌ی اعداد طبیعی

$$\mathbb{N} = \{۱, ۲, ۳, \cdots\}$$

و عمل‌های جمع و ضرب آن‌ها و با ویژگی‌های این دو عمل اصلی و نیز با عمل تفریق روی مجموعه‌ی **اعداد صحیح**

$$\mathbb{Z} = \{\cdots, -۳, -۲, -۱, ۰, ۱, ۲, ۳, \cdots\}$$

آشنا شده‌ایم.

ما در این‌جا ساختار اعداد صحیح را به روش اصل موضوعی مطرح نکرده بلکه فقط اصل موضوع «**خوش‌ترتیبی**» و یا معادل آن اصل موضوع «**استقرای ریاضی**» را به عنوان زیربنای قضیه‌های نظریه‌ی اعداد بیان می‌کنیم.

اصل خوش‌ترتیبی

هر زیرمجموعه‌ی ناتهی از اعداد طبیعی دارای **کوچک‌ترین عضو** است، یعنی اگر $S \subset \mathbb{N}$ و $S \neq \varnothing$، آن‌گاه عضوی از S مانند $s_\circ$ وجود دارد که به ازای هر s متعلق به S،

$$s_\circ \leq s$$

(کوچک‌ترین عضو مجموعه‌ی A را **عضو ابتدای مجموعه‌ی** A هم می‌نامند)[1].

اصل استقرای ریاضی

هر زیر مجموعه‌ی S از $\mathbb{N}$ که دارای دو خاصیت زیر باشد، با مجموعه‌ی $\mathbb{N}$ برابر است :

الف) $۱ \in S$

ب) هرگاه $n \in S$، آن‌گاه $n+۱ \in S$.

با پذیرفتن هریک از اصل‌های فوق می‌توان اصل دیگر را به‌عنوان یک قضیه اثبات کرد.

۴ــ۲ــ معادل‌های اصل استقرای ریاضی

معادل‌های دیگری برای اصل استقرای ریاضی وجود دارند که برخی را در این‌جا مطرح می‌کنیم :

الف) فرض کنیم $P(n)$ عبارتی درباره‌ی عدد طبیعی n باشد. اگر $P(۱)$ درست باشد و به ازای هر عدد طبیعی n از درستی $P(n)$، درستی $P(n+۱)$ نتیجه شود، آن‌گاه $P(n)$ به ازای هر عدد طبیعی n درست است.

تعمیم این مطلب به صورت زیر است :

ب) فرض کنیم $P(n)$ عبارتی درباره‌ی عدد صحیح n باشد. اگر به ازای یک $m \in \mathbb{Z}$، $P(m)$ درست باشد واگر به ازای هر $n \geq m$، از درستی $P(n)$ درستی $P(n+۱)$ نتیجه شود، آن‌گاه $P(n)$ به

۱ــ نماد $s_\circ = \min S$ برای کوچک‌ترین عضو مجموعه‌ی S به‌کار می‌رود.

ازای هر عدد صحیح $n \geq m$ درست است.

می‌توان ثابت کرد که الف، ب، و اصل استقرای ریاضی دو به دو معادل‌اند.

درکتاب جبر و احتمال، مثال‌های متعددی وجود دارند که ما را با نحوه‌ی استفاده از اصل استقرای ریاضی آشنا می‌کنند. در این‌جا ذکر یک نکته را ضروری می‌دانیم :

در اثبات به روش استقرا باید درستی هر دو شرط بررسی شوند. مثلاً، عبارت زیر را درنظر بگیرید :

$$۱ + ۳ + ۵ + \cdots + (۲n - ۱) = n^۲ + ۳$$

اگر چه گام دوم استقرای ریاضی (یعنی اثبات درستی به ازای $n+۱$، با فرض درست بودن به ازای n) برقرار است ولی هیچ عدد طبیعی n در این عبارت صدق نمی‌کند.

همان‌طور که گفتیم می‌توان ثابت کرد که اصل خوش‌ترتیبی و اصل استقرای ریاضی معادل‌اند. یعنی می‌توان به دلخواه یکی را اصل گرفت و دیگری را به عنوان قضیه ثابت کرد ؛ مثلاً داریم :

قضیه‌ی ۱ : اصل استقرای ریاضی از اصل خوش‌ترتیبی نتیجه می‌شود.

اثبات: فرض کنیم $P \subset \mathbb{N}$، $۱ \in P$ و اگر $n \in P$ آن‌گاه $n+۱ \in P$. می‌خواهیم ثابت کنیم $P = \mathbb{N}$. اگر چنین نباشد پس $T = \mathbb{N} - P \neq \varnothing$. لذا T کوچک‌ترین عضوی دارد که آن را $t_۰$ می‌نامیم. $t_۰ \neq ۱$ (چرا؟)، پس $t_۰ - ۱ \in \mathbb{N}$ و $t_۰ - ۱ < t_۰$، لذا $t_۰ - ۱ \notin T$، یعنی $t_۰ - ۱ \in P$ پس $t_۰ - ۱ + ۱ = t_۰ \in P$، که با $t_۰ \in T$ در تناقض است. در نتیجه $P = \mathbb{N}$. □

اصل استقرای قوی ریاضی

هر زیرمجموعه‌ی S از $\mathbb{N}$ که دارای دو خاصیت زیر باشد، با مجموعه‌ی $\mathbb{N}$ برابر است :

الف) $۱ \in S$

ب) اگر اعداد طبیعی کوچک‌تر از n در S باشند، آن‌گاه $n \in S$.

اصل استقرای قوی ریاضی با اصل استقرای ریاضی و در نتیجه با اصل خوش‌ترتیبی معادل است. برای نشان دادن نحوه‌ی استفاده از اصل استقرای قوی ریاضی، به مثال زیر توجه کنید :

مثال ۱: چند جمله‌ی اول دنباله‌ی موسوم به **دنباله‌ی اعداد لوکا** عبارت‌اند از :

$$۱, ۳, ۴, ۷, ۱۱, ۱۸, ۲۹, ۴۷, \cdots$$

اگر جمله‌ی nام را با L_n نمایش دهیم این دنباله از به اصطلاح «رابطه‌ی بازگشتی» زیر

$$L_n = L_{n-۱} + L_{n-۲} \qquad n \geq ۳$$

و شرایط اولیه‌ی

$$L_۲ = ۳\ ,\ L_۱ = ۱$$

به‌دست می‌آید. با استفاده از اصل استقرای قوی ریاضی ثابت می‌کنیم که به ازای هر عدد طبیعی n،

$$L_n < (\frac{۷}{۴})^n$$

اگر $S = \{n \in \mathbb{N} : L_n < (\frac{۷}{۴})^n\}$، آن‌گاه $۱ \in S$ و $۲ \in S$. (چرا؟) حال اگر $n \geq ۳$ و به ازای هر k وقتی که $k < n$، $k \in S$، آن‌گاه $L_{n-۱} < (\frac{۷}{۴})^{n-۱}$ و $L_{n-۲} < (\frac{۷}{۴})^{n-۲}$. پس

$$L_n < (\frac{۷}{۴})^{n-۱} + (\frac{۷}{۴})^{n-۲} = (\frac{۷}{۴})^{n-۲}(\frac{۷}{۴}+۱) < (\frac{۷}{۴})^n$$

یعنی $n \in S$. پس $S = \mathbb{N}$. لذا برای هر عدد طبیعی n داریم، $L_n < (\frac{۷}{۴})^n$. Δ

۴ــ۳ــ تقسیم‌پذیری

یکی از چهار عمل اصلی روی اعداد صحیح، تقسیم است. می‌دانیم حاصل تقسیم دو عدد صحیح الزاماً یک عدد صحیح نیست. مثلاً، حاصل تقسیم ۱۲− بر ۵، عدد صحیح نیست. در مواردی حاصل تقسیم عددی بر عددی دیگر یک عدد صحیح می‌شود مثل ۱۲ و ۶. در این حالت می‌گوییم عدد ۶ عدد ۱۲ را می‌شمارد، یا عدد ۱۲ بر ۶ تقسیم‌پذیر است. در واقع ۱۲ یک مضرب ۶ است : $۱۲ = ۶ \times ۲$. در حالت عمومی تعریف زیر را ارائه می‌دهیم :

تعریف: عدد صحیح a را بر عدد صحیح $b \neq ۰$، **تقسیم‌پذیر** یا (بخش‌پذیر) گوییم هرگاه عدد صحیحی مانند q یافت شود به گونه‌ای که $a = bq$. در این صورت می‌نویسیم $b|a$ و چنین می‌خوانیم : a بر b تقسیم‌پذیر است[1] و یا b یک شمارنده یا **مقسوم‌علیه** a است. هرگاه a بر b تقسیم‌پذیر نباشد می‌نویسیم $b \nmid a$. در حالت $b = ۰$، چون به ازای هر $q \in \mathbb{Z}$، $۰ \times q = ۰$، می‌توان تعریف تقسیم‌پذیری

۱ــ هرگاه a بر b تقسیم‌پذیر باشد می‌گوییم b عدد a را می‌شمارد (عاد می‌کند)، یا a مضرب b است، یا b یک سازه‌ی (عامل) a است.

را گسترش داد و عبارت «0 بر 0 تقسیم‌پذیر است» را نیز پذیرفت.

در مثال فوق $b=6$ ، $a=12$ ، $q=2$ و $2\times 6=12$ و می‌نویسیم $6|12$. از تعریف بالا نتایج زیر به‌دست می‌آیند :

الف) صفر بر هر عدد b، تقسیم‌پذیر است.

ب) اعداد ۱ و ۱− ، هر عدد صحیح را می‌شمارند. (چرا؟)

با توجه به مفهوم رابطه که در سال‌های قبل با آن آشنا شده‌ایم، می‌توان تقسیم‌پذیری را به عنوان یک رابطه با ویژگی‌های زیر بر مجموعه‌ی اعداد صحیح درنظر گرفت.

۱ــ این رابطه بازتابی است، زیرا برای هر عدد صحیح a داریم $a=a\times 1$ ، پس $a|a$.

۲ــ این رابطه ترایایی است، یعنی اگر $a|b$ و $b|c$ ، آن‌گاه $a|c$. برای اثبات می‌گوییم : یک عدد صحیح q وجود دارد که $b=aq$ و یک عدد صحیح q' وجود دارد که $c=bq'$. در نتیجه

$$c=(aq)q'=a(qq')$$

یعنی $a|c$.

۳ــ این رابطه متقارن نیست، چون مثلاً $2|6$ ولی $6\nmid 2$

۴ــ این رابطه پاد متقارن نیست، چون مثلاً $2|-2$ و $-2|2$ ولی $2\neq -2$.

۴ــ۴ــ چند ویژگی تقسیم‌پذیری

با قضیه‌های زیر ویژگی‌های عمده‌ی تقسیم‌پذیری را ارائه می‌دهیم :

قضیه‌ی ۲ : به ازای اعداد صحیح a و b، اگر $a|b$ ، آن‌گاه

الف) $-a|b$ ب) $a|-b$ پ) $-a|-b$

ت) به ازای هر عدد صحیح m، $a|mb$. ث) اگر $b\neq 0$ ، آن‌گاه $|a|\leq|b|$.

اثبات: اگر $a|b$ بنا به تعریف $b=aq$. در نتیجه

$$b=aq=(-a)(-q)$$

و نیز

$$-b=a(-q)=(-a)q$$

پس الف، ب و پ برقرارند. علاوه بر آن برای $m\in\mathbb{Z}$

$$mb=m(aq)=a(mq)$$

پس $a|mb$.

برای اثبات قسمت آخر چون $b=aq$ پس $|b|=|a|\ |q|$. ولی $b\neq 0$ در نتیجه $q\neq 0$، پس $|q|\geq 1$ یعنی $|a|\leq|b|$.

□

قضیه‌ی ۳ : به ازای اعداد صحیح a، b و c

الف) اگر $a|1$، آن‌گاه $a=\pm 1$ (تنها مقسوم‌علیه‌های عدد ۱، اعداد ۱و ۱− هستند).

ب) اگر $a|b$ و $b|a$، آن‌گاه $a=\pm b$.

پ) اگر $a|b$ و $a|c$، آن‌گاه به ازای اعداد صحیح و دلخواه m و n، داریم $a|mb+nc$.

اثبات: الف) اگر $a|1$، آن‌گاه $|a|\leq 1$ یعنی $|a|=0$ و یا $|a|=1$. اما اگر $|a|=0$، آن‌گاه $a=0$ ولی $0\nmid 1$ پس $|a|=1$. در نتیجه $a=\pm 1$.

ب) اگر $a|b$ و $b|a$ آن‌گاه عدد صحیح q وجود دارد که $aq=b$ و عدد صحیح q' وجود دارد که $a=bq'$. پس:

$$b=aq=b(qq')$$

اگر $b=0$ الزاماً $a=0$ و در نتیجه $a=b=0$. اگر $b\neq 0$ آن‌گاه $qq'=1$، یعنی $q'|1$ و لذا $q'=\pm 1$. پس $a=\pm b$

پ) اگر $a|b$ و $a|c$ آنگاه عدد صحیح q وجود دارد که $b=aq$ و عدد صحیح q' وجود دارد که $c=aq'$. به ازای اعداد صحیح دلخواه m و n داریم

$$\begin{aligned} mb+nc &= maq+naq' \\ &= (mq+nq')a \end{aligned}$$

پس:

$$a|mb+nc$$

□

۴ــ۵ــ الگوریتم تقسیم

اگر عدد صحیح a بر عدد طبیعی b تقسیم‌پذیر نباشد، در انجام تقسیم باقیمانده‌ای به‌جز صفر پیدا می‌شود. کلیّت مسئله اگرچه یک الگوریتم نیست ولی هنوز اسم سنتی خود «الگوریتم تقسیم» را حفظ کرده و عبارت است از :

قضیه‌ی ۴ : (الگوریتم تقسیم) : اگر a یک عدد صحیح و b یک عدد طبیعی باشد، آن‌گاه اعداد یکتای $q \in \mathbb{Z}$ و r وجود دارند که

$$a = bq + r \ , \ \ 0 \le r < b$$

(**q خارج قسمت**، **r باقیمانده**، **a مقسوم** و **b مقسوم‌علیه** نامیده می‌شوند.)

اثبات: نخست نشان می‌دهیم که $q \in \mathbb{Z}$ ، r وجود دارند و پس از آن یکتا بودن آن‌ها را ثابت می‌کنیم. چون a، b و q اعداد صحیح‌اند، $S = \{a - bq > 0 : q \in \mathbb{Z}\}$ یک زیرمجموعه از اعداد طبیعی است. نشان می‌دهیم که S تهی نیست و اصل خوش‌ترتیبی را به‌کار می‌بریم. به ازای عدد صحیح $q = -|a| - 1$ ، $a - bq > 0$ ؛ زیرا

$$a - bq = a + b|a| + b \ge a + |a| + 1 \ge 1 > 0$$

پس به ازای این مقدار q، $a - bq \in S$. لذا S دارای کوچک‌ترین عضو است. کوچک‌ترین عضو این مجموعه را r می‌نامیم. در این صورت عددی صحیح مانند q وجود دارد که $r = a - bq$. یعنی :

$$a = bq + r$$

اگر $r > b$ ، آن‌گاه

$$r - b = a - b(q + 1) \in S$$

ولی چون $b > 0$ پس $r - b < r$ که متناقض با کوچک‌ترین بودن r است، پس $r \le b$. حال اگر $r = b$ مقدار $q_1 = q + 1$ را درنظر می‌گیریم. در این صورت

$$a = bq_1$$

که به جای r، $r_1 = 0$ را درنظر می‌گیریم. پس همواره $0 \le r < b$. برای اثبات یکتا بودن، فرض کنیم چنین نباشد، یعنی

$$a = bq_1 + r_1 \quad 0 \le r_1 < b \quad , \quad a = bq_2 + r_2 \quad 0 \le r_2 < b$$

پس :

$$0 = b(q_1 - q_2) + r_1 - r_2$$

یا

$$r_2 - r_1 = b(q_1 - q_2)$$

یعنی $b | r_2 - r_1$. اگر $r_2 - r_1 \ne 0$ ، آن‌گاه $b \le |r_2 - r_1|$. از سوی دیگر

$$-b < r_2 - r_1 < b$$

یعنی :

$$|r_2 - r_1| < b$$

که این با $b \le |r_2 - r_1|$ تناقض دارد. پس $r_2 - r_1 = 0$. یعنی $r_2 = r_1$ و چون $b \ne 0$ ، $q_1 - q_2 = 0$ یعنی $q_2 = q_1$. □

توجه کنید که هرگاه $r = 0$ ، آن‌گاه $b|a$.

مثال ۲: برای $a = 1028$ و $b = 34$ ، داریم

$$q = \left\lfloor \frac{1028}{34} \right\rfloor = 30$$

(در این‌جا منظور از نماد $\lfloor x \rfloor$ ، جزء صحیح عدد حقیقی x است.)

و

$$r = 1028 - 30 \times 34 = 8$$

پس :

$$1028 = 34 \times 30 + 8$$

Δ

یکی از کاربردهای قضیه‌ی الگوریتم تقسیم، دسته‌بندی اعداد برحسب باقیمانده‌ی تقسیم آن‌ها بر عدد طبیعی و ثابت b است.

مثال ۳: باقیمانده‌ی هر عدد صحیح بر ۲، عدد ۰ یا ۱ است. این مطلب اعداد صحیح را به دو دسته تقسیم می‌کند. تمام اعدادی را که باقیمانده‌ی آن‌ها بر ۲، ۰ است، یعنی ۲ آن‌ها را می‌شمارد **زوج** و بقیه‌ی اعداد را **فرد** می‌نامند. یعنی می‌توان نوشت :

$$\mathbb{Z} = [0]_2 \cup [1]_2$$

که در آن

$$[0]_2 = \{n \in \mathbb{Z} : n = 2q, q \in \mathbb{Z}\} = \{n \in \mathbb{Z} : 2|n\}$$

مجموعه‌ی اعداد زوج، و

$$[1]_2 = \{n \in \mathbb{Z} : n = 2q+1, q \in \mathbb{Z}\} = \{n \in \mathbb{Z} : 2\nmid n\}$$

مجموعه‌ی اعداد فرد است. Δ

به همین ترتیب هر عدد صحیح را می‌توان تنها به یکی از صورت‌های

$$4q, 4q+1, 4q+2, 4q+3$$

نوشت، که در آن $q \in \mathbb{Z}$. این مطلب اساس مبحث همنهشتی است که در سال گذشته با آن آشنا شده‌ایم.

۴ــ۶ــ نمایش اعداد صحیح

استفاده از دستگاه دهدهی (اعشاری) متداول‌ترین صورت نمایش اعداد است. اعداد طبیعی را می‌توان به صورت ضرایب توان‌های ۱۰ نمایش داد. مثلاً عدد ۳۴۷۶۵ عبارت است از :

$$۳\times۱۰^{۴}+۴\times۱۰^{۳}+۷\times۱۰^{۲}+۶\times۱۰^{۱}+۵\times۱۰^{۰}$$

شاید یکی از دلایل نمایش اعداد در دستگاه دهدهی یا به اصطلاح در «**مبنای یا پایه‌ی ۱۰**» وجود ۱۰ انگشت دست بوده که در شمارش طبیعی به‌کار می‌رفته است. این نحوه‌ی نمایش را ابتدا هندی‌ها قبل از سال ۸۰۰ میلادی اختراع کرده‌اند. این مطلب را محمدبن موسی خوارزمی در کتاب «جمع و تفریق، بر طبق حساب هندی» شرح داده و نمایش رقم صفر با نماد ۰ هم برای اولین بار در این کتاب آمده است. اروپایی‌ها این دستگاه را هندی ــ عربی می‌نامند. دستگاه دیگری هم که در ریاضیات اسلامی وجود داشته، دستگاه شصت شصتی بوده که مسلمان‌ها فکر آن را از بابلی‌ها گرفتند و آن را تکمیل کردند. مبنای این نمایش عدد شصت بوده است، که در ارتباط با محاسبات نجومی و تقسیم ساعت به ۶۰ دقیقه و دقیقه به ۶۰ ثانیه است. با نمایش اعداد در مبنای ۲ هم که در نمایش داخلی کامپیوتر به‌کار می‌رود آشنا هستیم.

به‌طور کلی هر عدد طبیعی بزرگ‌تر از ۱ می‌تواند مبنا باشد.

قضیه‌ی ۵ : اگر b یک عدد طبیعی بزرگ‌تر از ۱ باشد، هر عدد طبیعی n را می‌توان به طریقی یکتا به صورت

$$n = a_k b^k + a_{k-۱} b^{k-۱} + \cdots + a_۱ b + a_۰$$

نمایش داد، که در آن k یک عدد حسابی[۱] است و برای هر $j = ۰, ۱, ۲, \cdots, k$ ، $۰ \le a_j \le b-۱$ و $a_k \neq ۰$.

اثبات: اگر الگوریتم تقسیم را متوالیاً به صورت زیر به کار گیریم، قضیه ثابت می‌شود. ابتدا n را بر b تقسیم می‌کنیم.

$$n = bq_۰ + a_۰ \qquad ۰ \le a_۰ \le b-۱$$

حال $q_۰$ را بر b تقسیم می‌کنیم

$$q_۰ = bq_۱ + a_۱ \qquad ۰ \le a_۱ \le b-۱$$

۱ــ هر عدد صحیح نامنفی را حسابی گویند.

این عمل را ادامه می‌دهیم

$$q_1 = bq_2 + a_2 \qquad 0 \le a_2 \le b-1$$

$$q_j = bq_{j+1} + a_{j+1} \qquad 0 \le a_{j+1} \le b-1$$

$$\vdots$$

در دنباله‌ی $q_0, q_1, q_2, \dots$ داریم :

$$\vdots$$

$$n > q_0 > q_1 > q_2 > \cdots \ge 0$$

(دقت کنید : $q_j > q_{j+1}$ مگر وقتی که $q_{j+1} = 0$، چون در غیر این حالت، $b > 1$ ، $a_{j+1} \ge 0$ و $q_{j+1} \ge 1$، پس

$$(q_j = bq_{j+1} + a_{j+1} > q_{j+1}$$

لذا این کار را حداکثر تا n مرحله می‌توان ادامه داد. چون دقیقاً $n-1$ عدد صحیح مختلف بین صفر و n وجود دارند. پس در مرحله‌ای $q_k = 0$ و داریم :

$$q_{k-1} = b \times 0 + a_k \ , \ 0 \le a_k \le b-1$$

اگر به ترتیب به جای هر q_{k-1} ، $q_{k-2}, \dots q_2$ ، q_1 ، q_0 حاصل تقسیم آن را بنویسیم، فرمول موردنظر به‌دست می‌آید و بدیهی است که $a_k \ne 0$، زیرا اگر $a_k = 0$ آن‌گاه $q_{k-1} = 0$، و یک مرحله‌ی قبل از آن توقف می‌کردیم. اثبات یکتایی این نمایش را در مقاطع تحصیلی بالاتر خواهید دید. □

(در این حالت n را به صورت زیر نمایش می‌دهند :

$$n = (a_k a_{k-1} a_{k-2} \cdots a_1 a_0)_b$$

این نمایش را[1]، **نمایش عدد n در مبنای b** می‌نامند. هریک از a_i ها را یک **رقم** در مبنای b گویند و $k+1$ ، تعداد ارقام عدد n در مبنای b است و می‌گویند n در مبنای b، $k+1$ رقم دارد.)

نمایش اعداد در دستگاه **دودویی**، یا در مبنای ۲، به دلیل کاربرد آن در کامپیوتر و نیز تناظری که در رابطه با پرتاب سکه در احتمال دارد بسیار جالب است. علاوه بر آن، قضیه‌ی ۵ در رابطه با پیدا کردن باقیمانده‌ی تقسیم بر برخی از اعداد به‌کار می‌رود. به مثال زیر توجه کنید.

مثال ۴ : قاعده‌ی پیدا کردن باقیمانده‌ی تقسیم بر ۳ یا ۹

اگر $A = (a_n \cdots a_1 a_0)_{10}$ می‌دانیم این عدد برابر است با

$$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0$$

۱ـ در برخی از کتاب‌ها نمایش این عدد به صورت $\overline{a_k a_{k-1} \cdots a_1 a_0}$ است.

$$=(\overbrace{۹۹\cdots۹}^{n}+۱)a_n+(\overbrace{۹۹\cdots۹}^{n-۱}+۱)a_{n-۱}+\cdots+(۹+۱)a_۱+a_۰$$

$$=۹(\overbrace{۱۱۱\cdots۱}^{n}a_n+\overbrace{۱۱\cdots۱}^{n-۱}a_{n-۱}+\cdots+a_۱)+a_n+a_{n-۱}+\cdots+a_۱+a_۰$$

پس باقیمانده‌ی تقسیم A بر ۹ (یا ۳) برابر است با باقیمانده‌ی مجموع

$$a_n+a_{n-۱}+\cdots+a_۱+a_۰$$

بر ۹ (یا ۳). به روش مشابه، قاعده‌ی پیدا کردن باقیمانده‌ی تقسیم یک عدد بر ۱۱ را نیز می‌توان پیدا کرد. (چگونه؟) Δ

۴ــ۷ــ تمرین‌ها

۱ــ کوچک‌ترین و بزرگ‌ترین عضو مجموعه‌های زیر را در صورت وجود پیدا کنید :

الف) $A=\{x\in\mathbb{Z}:۰\leq x<۵\}$

ب) $C=\{x\in\mathbb{Z}:۰<x\leq۱\}$

پ) $E=\{x\in\mathbb{Z}:۰\leq x<۱\}$

(بزرگ‌ترین عضو مجموعه‌ی S عبارت است از $s_۱\in S$، که برای هر $s\in S$ داشته باشیم $s\leq S_۱$)[۱].

۲ــ زیرمجموعه‌ای از اعداد صحیح مثال بزنید که کوچک‌ترین عضو نداشته باشد.

۳ــ ثابت کنید که هر مجموعه‌ی ناتهی از اعداد صحیح و از پایین کراندار، دارای کوچک‌ترین عضو و هر مجموعه‌ی ناتهی از اعداد صحیح و از بالا کراندار دارای بزرگ‌ترین عضو است.

(یادآوری می‌کنیم که $A\subset\mathbb{Z}$ از بالا کراندار است اگر عددی مانند $n\in\mathbb{Z}$ یافت شود که به ازای هر $a\in A$، $a\leq n$ و هم‌چنین $A\subset\mathbb{Z}$ از پایین کراندار است اگر عددی مانند $n\in\mathbb{Z}$ یافت شود که برای هر $a\in A$، $n\leq a$.)

۴ــ خاصیت ارشمیدسی :

ثابت کنید اگر a و b دو عدد طبیعی باشند، آن‌گاه یک عدد طبیعی n وجود دارد به طوری که $na\geq b$.

۱ــ نماد $s_۱=\max S$ برای بزرگ‌ترین عضو مجموعه‌ی S به‌کار می‌رود.

۵ ــ ثابت کنید $\binom{n}{k}$ برای اعداد طبیعی n و $0 \le k \le n$ همیشه عدد طبیعی است.

۶ــ الف) برای $n \ge 2$ ، ثابت کنید :

$$\binom{2}{2}+\binom{3}{2}+\cdots+\binom{n}{2}=\binom{n+1}{3}$$

ب) با استفاده از قسمت الف و این‌که برای هر عدد طبیعی $m \ge 2$ ،

$$2\binom{m}{2}+m=m^2$$

ثابت کنید که

$$1^2+2^2+\cdots+n^2=\frac{n(2n+1)(n+1)}{6}$$

۷ــ کدام‌یک از اعداد زیر بر ۲۲ تقسیم‌پذیرند؟

الف) ۰ ب) ۴۴۴

پ) ۱۷۱۶ ت) ۳۲۵۱۶-

۸ ــ الف) اگر a، b، c و d اعداد صحیح باشند و $a \ne 0$، $c \ne 0$، $a|b$ و $c|d$ ثابت کنید $ac|bd$.

ب) نشان دهید اگر a، b و $c \ne 0$ اعداد صحیح باشند، آن‌گاه $a|b$ اگر و تنها اگر $ac|bc$.

پ) ثابت کنید اگر برای هر $i=1,2,\dots,n$ ، $a|b_i$ آن‌گاه برای اعداد صحیح دلخواه m_1 ، m_2 ، ... و m_n داریم

$$a|m_1b_1+m_2b_2+\cdots+m_nb_n$$

۹ــ خارج قسمت و باقیمانده را در الگوریتم تقسیم هریک از اعداد زیر، وقتی که بر ۱۷ تقسیم شوند به‌دست آورید.

الف) ۱۰۰ ب) ۴۴-

۱۰ــ الف) ثابت کنید حاصل جمع دو عدد صحیح زوج و هم‌چنین حاصل جمع دو عدد صحیح فرد، زوج است.

ب) ثابت کنید حاصل ضرب دو عدد فرد، فرد است.

۱۱ــ الف) ثابت کنید حاصل‌ضرب هر دو عدد به صورت $4q+1$ و هم‌چنین حاصل‌ضرب هر

دو عدد به صورت $4q+3$ ، به صورت $4q+1$ است. $(q \in \mathbb{Z})$

ب) ثابت کنید منبع هر عدد فرد به صورت $8q+1$ است.

۱۲ـ نشان دهید حاصل‌ضرب دو عدد به صورت $6q+5$ به صورت $6q+1$ است.

۱۳ـ ثابت کنید حاصل‌ضرب ۳ عدد طبیعی متوالی بر ۶ تقسیم‌پذیر است.

۱۴ـ الف) عدد ۲۳۶ را در مبنای ۷ بنویسید.

ب) عدد $(1001011)_2$ برابر چه عددی در مبنای ۱۰ است؟

پ) عدد ۱۸۶۴ را در مبنای ۲ بنویسید.

ت) عدد $(a35b06)_{16}$ را در مبنای ۱۰ بنویسید.

(دقت کنید که اگر مبنا بیشتر از ۱۰ باشد، ارقام بیشتر از ۹ را به ترتیب با a، b، c، d و ... نمایش می‌دهند، یعنی مثلاً در مبنای ۱۶، $a=10$ ، $b=11$ ، $c=12$ ، $d=13$ ، $e=14$ و $f=15$.

البته گاهی هم عدد بالا را با $(10\ 3\ 5\ 11\ 0\ 6)_{16}$ هم نمایش می‌دهند.)

مجله‌ی ریاضی

دستگاه اعداد رمزی را ابتدا یونانی‌ها به‌کار گرفتند. در این دستگاه، اعداد را با حروف نمایش می‌دادند. در دوره‌ی بعد از ظهور اسلام نیز به وفور از حروف ابجد استفاده می‌شد و محاسباتی با آن‌ها صورت می‌گرفت. این طریقه محاسبه را حساب جُمّل می‌گویند و جدول آن به شرح زیر است :

ا	ب	ج	د	هـ	و	ز	ح	ط	ی
۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
	ک	ل	م	ن	س	ع	ف	ص	
	۲۰	۳۰	۴۰	۵۰	۶۰	۷۰	۸۰	۹۰	
ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
۱۰۰	۲۰۰	۳۰۰	۴۰۰	۵۰۰	۶۰۰	۷۰۰	۸۰۰	۹۰۰	۱۰۰۰

حساب جُمّل (حساب ابجدی) در ضبط تاریخ حوادث به عنوان ماده‌ی تاریخ به‌کار می‌رود.