

اعداد اول

در فصل قبل، تقسیم پذیری هر دو عدد صحیح به عنوان یک رابطه مطرح شد. برخی از اعداد بر تعداد زیادی از اعداد طبیعی تقسیم پذیرند، مثل ۲۴ که بر اعداد طبیعی ۱، ۲، ۳، ۴، ۶، ۸، ۱۲ و ۲۴ تقسیم پذیر است. با این حال دسته‌ای دیگر از اعداد طبیعی هیچ مقسوم‌علیه‌ی به جز ۱ و خود آن عدد ندارند. این اعداد غیر ۱ را اعداد اول می‌نامند.

تعریف: هر عدد طبیعی غیر از ۱ را که جز بر ۱ و خودش بر هیچ عدد طبیعی دیگری تقسیم پذیر نباشد عدد اول گویند. هر عدد طبیعی به جز ۱ که اول نیست، عدد مرکب می‌نامند.

مثال ۱: اعداد ۲، ۳، ۵، ۷ و ۱۱ اول و اعداد ۴، ۶، ۸، ۹ و ۱۰ مرکب‌اند.

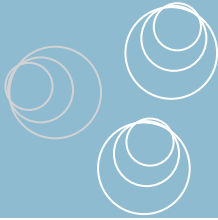
قضیه ۱: هر عدد صحیح به جز ۱ و -۱ حداقل یک مقسوم‌علیه اول دارد.

اثبات: هر عدد صحیح مورد نظر را a می‌نامیم. اگر $a = 0$ ، هر عدد اولی آن را می‌شمارد.

اگر $a \neq 0$ ، فرض می‌کنیم S مجموعه تمام مقسوم‌علیه‌های بزرگ‌تر از ۱ عدد صحیح a باشد. S تهی نیست، چون $a \in S$. کوچک‌ترین عضو S را m می‌نامیم. (چرا S کوچک‌ترین عضو دارد؟) m اول است، زیرا اگر m اول نباشد آن‌گاه عدد طبیعی $m_1 > 1$ ، $m_1 \neq m$ وجود دارد که $m_1 | m$. پس m_1 هم عضو S است (چرا؟) که با کوچک‌تر بودن m در تناقض است. پس a حتماً یک مقسوم‌علیه اول مانند m دارد.

قضیه ۲: بی‌نهایت عدد اول وجود دارند.^۱

۱- این قضیه را اقلیدس در حدود سال ۳۰۰ قبل از میلاد اثبات کرده است.



اثبات : می‌دانیم اعداد ۲، ۳، ۵ و ... اول اند، حال اگر این دنباله متناهی باشد، فرض می‌کنیم p_1, p_2, \dots, p_n تنها عدد اول باشند. $m = p_1 p_2 \dots p_n + 1$ را در نظر می‌گیریم. چون m یک عدد طبیعی و مخالف p_1, p_2, \dots, p_n است، m باید مرکب باشد. پس یک مقسوم علیه اول دارد که آن را p_j می‌نامیم. داریم :

$$p_j | m, \quad p_j | p_1 p_2 \dots p_n$$

پس $m - (p_1 p_2 \dots p_n)$ بر p_j تقسیم پذیر است. یعنی $p_j | 1$ که غیر ممکن است. لذا تعداد اعداد

اول نامتناهی است. ■

قضیه ۳ : اگر n یک عدد مرکب باشد، آن‌گاه n حداقل یک مقسوم علیه اول کوچک‌تر از \sqrt{n} یا مساوی با آن دارد.

اثبات : چون n مرکب است، پس $n = ab$ به طوری که $1 < a \leq b < n$. اگر $a > \sqrt{n}$ ، آن‌گاه $b > \sqrt{n}$ و در نتیجه $n = ab > n$ که یک تناقض است. پس حتماً $a \leq \sqrt{n}$. چون $a \neq 1$ ، پس بنابر قضیه ۱ عدد اول p وجود دارد که $p | a$ و چون $a | n$ پس $p | n$. اما $p \leq a$ ، یعنی عدد اول p وجود دارد که $p \leq \sqrt{n}$ و $p | n$.

به کمک قضیه ۳ می‌توان اول بودن هر عددی را بررسی کرد.

مثال ۲ : می‌خواهیم تحقیق کنیم عدد ۴۷ اول است یا نه. مشاهده می‌کنیم :

$$2/47, \quad 3/47, \quad 5/47$$

و چون $6 < \sqrt{47} < 7$ ، لذا تنها اعداد اول کوچک‌تر از $\sqrt{47}$ یا مساوی با آن اعداد ۲، ۳ و ۵ هستند که هیچ‌کدام ۴۷ را نمی‌شمارند. پس ۴۷ اول است.

قضیه ۳ اساس فرایند غربال اراتستن است. مثلاً برای تعیین اعداد اول کوچک‌تر از 1000 ، تمام مضرب‌های اول اعداد کوچک‌تر از $1000 = \sqrt{1000}$ یعنی مضرب‌های ۲، ۳، ۵ و ۷ را از جدول اعداد از ۱ تا 1000 حذف می‌کنیم. جدول صفحه بعد نمونه‌ای از غربال اراتستن است.

	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰
۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰
۳۱	۳۲	۳۳	۳۴	۳۵	۳۶	۳۷	۳۸	۳۹	۴۰
۴۱	۴۲	۴۳	۴۴	۴۵	۴۶	۴۷	۴۸	۴۹	۵۰
۵۱	۵۲	۵۳	۵۴	۵۵	۵۶	۵۷	۵۸	۵۹	۶۰
۶۱	۶۲	۶۳	۶۴	۶۵	۶۶	۶۷	۶۸	۶۹	۷۰
۷۱	۷۲	۷۳	۷۴	۷۵	۷۶	۷۷	۷۸	۷۹	۸۰
۸۱	۸۲	۸۳	۸۴	۸۵	۸۶	۸۷	۸۸	۸۹	۹۰
۹۱	۹۲	۹۳	۹۴	۹۵	۹۶	۹۷	۹۸	۹۹	۱۰۰

و در نتیجه تنها اعداد اول بین ۱ تا ۱۰۰ عبارت‌اند از:

۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹, ۳۱, ۳۷, ۴۱, ۴۳, ۴۷, ۵۳, ۵۹, ۶۱, ۶۷, ۷۱, ۷۳, ۷۹, ۸۳, ۸۹, ۹۷

۵-۱- بزرگ‌ترین مقسوم‌علیه مشترک

می‌دانیم که عدد صحیح c را مقسوم‌علیه یا شمارندهٔ مشترک دو عدد صحیح a و b گویند هرگاه

$c|a$ و $c|b$.

تعریف: عدد طبیعی d را بزرگ‌ترین مقسوم‌علیه مشترک (ب.م.م) دو عدد صحیح a و

b (که حداقل یکی از آنها مخالف صفر است) گویند، اگر d یک مقسوم‌علیه مشترک a و b باشد، و

مقسوم‌علیه‌های مشترک دیگر a و b ، از d کوچک‌تر باشند. بزرگ‌ترین مقسوم‌علیه مشترک دو عدد

a و b را با (a, b) نمایش می‌دهند.^۱

۱- مقسوم‌علیه مشترک a و b را با نماد $a \text{ П } b$ هم نمایش می‌دهند.

مثال ۳: مقسوم علیه‌های مشترک ۲۴ و ۸۴ عبارت‌اند از:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$$

پس:

$$(24, 84) = 12$$

با استفاده از نتایج اصل خوش‌ترتیبی می‌توان ثابت کرد که ب.م.م دو عدد صحیح (که هر دو صفر نیستند) همواره وجود دارد. (چرا؟) علاوه بر آن قضیه زیر را داریم:

قضیه ۴: بزرگ‌ترین مقسوم علیه مشترک دو عدد صحیح a و b که حداقل یکی از آنها صفر نیست، برابر است با کوچک‌ترین عضو مجموعه

$$S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$$

اثبات: مجموعه S حداقل یک عضو دارد (چرا؟) پس دارای کوچک‌ترین عضو است. فرض

می‌کنیم d کوچک‌ترین عضو S باشد،

$$d = m_0 a + n_0 b > 0, \quad m_0, n_0 \in \mathbb{Z}$$

از الگوریتم تقسیم داریم

$$a = dq + r, \quad 0 \leq r < d$$

اگر $r > 0$ می‌دانیم $r \notin S$ چون $r < d$ ولی

$$r = a - m_0 a q - n_0 b q = (1 - m_0 q)a - (n_0 q)b$$

ترکیب خطی a و b است که با کوچک‌ترین بودن d در تناقض است. پس $r = 0$. یعنی $d|a$. به همین

ترتیب $d|b$. یعنی d مقسوم علیه مشترک a و b است. اگر $c > 0$ و $c|a$ ، $c|b$ ، آن‌گاه $c|(am_0 + bn_0)$ یعنی

$c|d$ پس $c \leq d$. در نتیجه d بزرگ‌ترین مقسوم علیه مشترک a و b است. ■

می‌توان ثابت کرد که هرگاه $a = bq + r$ آن‌گاه $(a, b) = (b, r)$. (چرا؟)

این مطلب، زیربنای الگوریتم اقلیدس برای یافتن بزرگ‌ترین مقسوم علیه مشترک دو عدد صحیح

a و b است.

الگوریتم اقلیدس بدین‌گونه عمل می‌کند که اگر $r_0 = a > 0$ و $r_1 = b > 0$ ، آن‌گاه

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1$$

پس:

$$(a, b) = (r_0, r_1) = (r_1, r_2)$$

۱- برای هر $ma + nb$ ، $m, n \in \mathbb{Z}$ را یک ترکیب خطی a و b می‌نامند.

$$r_1 = r_2 q_2 + r_2 \quad 0 \leq r_2 < r_1$$

$$(a, b) = (r_1, r_2) = (r_1, r_2)$$

$$\vdots$$

$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1} \quad 0 \leq r_{n-1} < r_{n-2}$$

$$(a, b) = (r_{n-3}, r_{n-2}) = (r_{n-1}, r_{n-2})$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$

$$(a, b) = (r_{n-1}, r_{n-2}) = (r_{n-1}, r_n)$$

چون

$$a = r_n > r_1 > r_2 \dots \geq 0$$

پس از چند مرحله باقیمانده صفر خواهد شد، زیرا بیشتر از a عدد صحیح مختلف بین صفر و a نیست. پس برای یک عدد طبیعی n داریم $r_{n-1} = r_n q_n + r_{n+1} = 0$. در نتیجه

$$(a, b) = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

که r_n آخرین باقیمانده غیر صفر در این رشته از تقسیم‌های متوالی است.

مثال ۴:

$$(30, 72) = (30, 72 - 2 \times 30) = (30, 12)$$

$$= (2 \times 12 + 6, 12) = (6, 12) = (6, 2 \times 6 + 0) = (6, 0) = 6$$

که معمولاً به صورت خلاصه نردبانی زیر می‌نویسند:

خارج قسمت	۲	۲	۲
۷۲	۳۰	۱۲	۶
باقیمانده	۱۲	۶	۰

قضیه ۵: عدد طبیعی d بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح a و b است اگر و تنها اگر

$$d|a \text{ و } d|b$$

(۲) هرگاه $a|c$ و $b|c$ ، آن‌گاه $d|c$.

اثبات: اگر $d = (a, b)$ آن‌گاه $d|a$ و $d|b$ یعنی شرط ۱ برقرار است. علاوه بر آن اعداد صحیح

m و n وجود دارند که

$$d = ma + nb$$

حال اگر $c|a$ و $c|b$ و آن گاه $c|d$ یعنی شرط ۲ هم برقرار است.
 برعکس اگر d در دو شرط فوق صدق کند و c یک مقسوم علیه مشترک مثبت a و b باشد، آن گاه $c|d$ یعنی $c \leq d$. پس d بزرگ ترین مقسوم علیه مشترک a و b است.

تعریف: دو عدد صحیح a و b را نسبت به هم اول یا متباین گویند، هر گاه $(a, b) = 1$.

مثال ۵: اعداد ۹ و ۱۰ و نیز دو عدد ۲۵ و ۴۲ نسبت به هم اول اند.
 با استفاده از قضیه ۴، می توان ثابت کرد که دو عدد صحیح a و b نسبت به هم اول اند اگر و تنها اگر اعداد صحیح m و n وجود داشته باشند که

$$1 = ma + nb$$

قضیه ۶: (لم اقلیدس). اگر $a|bc$ و $(a, b) = 1$ آن گاه $a|c$.

اثبات: اعداد صحیح m و n را می توان پیدا کرد که برای آنها

$$1 = ma + nb$$

پس:

$$c = cma + cnb$$

اما چون $a|bc$ ، پس $bc = aq$. در نتیجه

$$c = cma + naq = (cm + na)q$$

یعنی $a|c$.

قضیه ۷: اگر p یک عدد اول باشد و $p|ab$ ، آن گاه $p|a$ یا $p|b$.

اثبات: اگر p/a ، آن گاه $(p, a) = 1$ ، زیرا اگر $(p, a) = d$ و $d \neq 1$ آن گاه $d = p$. (چرا؟)

پس $p|a$ که یک تناقض است. در نتیجه $(p, a) = 1$ ، پس طبق قضیه ۶، $p|d$.

تعریف بزرگ ترین مقسوم علیه مشترک دو عدد را به چند عدد نیز می توان تعمیم داد:
 تعریف: بزرگ ترین مقسوم علیه مشترک n عدد صحیح a_1, a_2, \dots, a_n که همگی آنها صفر نیستند عبارت است از بزرگ ترین عدد صحیحی که تمام این اعداد صحیح را بشمارد. این عدد را با (a_1, a_2, \dots, a_n) نمایش می دهند. می توان ثابت کرد که

$$(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{n-2}, (a_{n-1}, a_n))$$

مثال ۶:

$$\begin{aligned} (24, 30, 72) &= (24, (30, 72)) \\ &= (24, 6) = 6 \end{aligned}$$



۲-۵- قضیه بنیادی حساب

نقش اصلی اعداد اول به عنوان عناصر سازنده تمام اعداد صحیح بسیار اهمیت دارد. در قضیه زیر این مطلب را بدون اثبات بیان می‌کنیم:

قضیه ۸: هر عدد طبیعی بزرگ‌تر از ۱ را می‌توان بدون توجه به ترتیب به طور یکتا به صورت حاصل ضرب اعداد اول نوشت. یعنی n را می‌توان به صورت $n = p_1 p_2 \dots p_k$ نمایش داد که در آن برای هر i ، p_i عددی اول است. این نمایش را تجزیه عدد n به عامل‌های اول می‌نامند.

نکته ۱: در تجزیه اعداد طبیعی به عامل‌های اول، می‌توان حاصل ضرب چند عدد اول مساوی را به صورت توانی از آن نوشت، یعنی

$$n = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}$$

که در آن p_i اعداد اول متمایز و α_i ‌ها اعدادی طبیعی‌اند. این نمایش را نمایش متعارف عدد n می‌نامند.

نکته ۲: برای $n=1$ ، می‌توان $1 = p^0$ را در نظر گرفت، درحالی‌که هر عدد اولی می‌تواند باشد.

نکته ۳: به طور کلی هر عدد طبیعی را می‌توان به صورت زیر نمایش داد:

$$n = \prod_p p^{\alpha_p(n)} = 2^{\alpha_2(n)} 3^{\alpha_3(n)} 5^{\alpha_5(n)} \dots$$

که در آن \prod_p به مفهوم ضرب روی تمام اعداد اول است و برای هر عدد اول p ، $\alpha_p(n)$ بزرگ‌ترین توان است که عدد n را می‌شمارد و به این صورت می‌نویسند:

$$p^{\alpha_p(n)} \parallel n$$

یعنی $p^{\alpha_p(n)} \mid n$ ولی $p^{\alpha_p(n)+1} \nmid n$ (واضح است که اگر $P > n$ ، حتماً $(\alpha_p(n) = 0)$ حال قضیه زیر را بدون اثبات بیان می‌کنیم:

قضیه ۹: اگر $a = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ و $b = P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n}$ ، آن‌گاه

$$d = (a, b) = P_1^{\gamma_1} P_2^{\gamma_2} \dots P_n^{\gamma_n}$$

که در آن برای هر عدد i ,

$$\gamma_i = \min\{\alpha_i, \beta_i\}$$

(دقت کنید که اگر برای عدد اول p ، p/n ، آن گاه توان آن را در نمایش n برابر با صفر می‌گیریم.)

مثال ۷:

$$30 = 2^1 \times 3^1 \times 5^1$$

$$72 = 2^3 \times 3^2 = 2^2 \times 3^2 \times 5^0$$

$$\text{پس } (30, 72) = 2^1 \times 3^1 \times 5^0 = 6$$



۵-۳- کوچک‌ترین مضرب مشترک

می‌دانیم عدد صحیح c را مضرب مشترک دو عدد صحیح a و b نامند، هرگاه $a|c$ و $b|c$.
تعریف: عدد m را کوچک‌ترین مضرب مشترک (ک.م.م) دو عدد صحیح a و b نامند،
هرگاه m مضرب مشترک مثبت دو عدد a و b باشد و اگر $a|c$ و $b|c$ آن گاه $m \leq c$. کوچک‌ترین مضرب
مشترک دو عدد a و b را با $[a, b]$ نمایش می‌دهند.

وجود کوچک‌ترین مضرب مشترک دو عدد غیرصفر a و b را با استفاده از اصل خوش‌ترتیبی

می‌توان ثابت کرد.

مثال ۸: مضرب‌های مشترک مثبت اعداد ۴ و ۶ عبارتند از:

$$12, 24, 36, \dots$$



که کوچک‌ترین آنها ۱۲ است. یعنی $[4, 6] = 12$.

قضیه‌های زیر را که در رابطه با کوچک‌ترین مضرب مشترک دو عدد بدون اثبات بیان می‌کنیم.

قضیه ۱۰: برای هر دو عدد صحیح غیرصفر a و b ، $m = [a, b]$ اگر و تنها اگر

$$(1) \quad a|m \text{ و } b|m$$

$$(2) \quad \text{اگر } a|c \text{ و } b|c, \text{ آن گاه } m|c.$$

قضیه ۱۱: اگر $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ و $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ ، آن گاه

$$m = [a, b] = p_1^{\theta_1} p_2^{\theta_2} \dots p_n^{\theta_n}$$

$$\theta_i = \max\{\alpha_i, \beta_i\}$$

که در آن برای هر i ,

۱- کوچک‌ترین مضرب مشترک a و b را با نماد $a \cup b$ هم نمایش می‌دهند.

قضیه ۱۲: برای هر دو عدد صحیح غیر صفر a و b داریم:

$$a, b = |ab|$$

مثال ۹:

$$30 = 2^1 \times 3^1 \times 5^1$$

$$72 = 2^3 \times 3^2 = 2^2 \times 3^2 \times 5^0$$

$$[30, 72] = 2^2 \times 3^2 \times 5^1 = 360$$

$$[30, 72] \times (30, 72) = 360 \times 6 = 2160$$

$$30 \times 72 = 2160$$



تعریف: کوچک‌ترین مضرب مشترک اعداد صحیح غیر صفر a_1, a_2, \dots, a_n عبارت است از کوچک‌ترین عدد صحیح مثبت که بر همه آنها تقسیم پذیر باشد، و آن را با $[a_1, a_2, \dots, a_n]$ نمایش می‌دهند. می‌توان ثابت کرد که

$$[a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_{n-2}, [a_{n-1}, a_n]]$$

مثال ۱۰:

$$[10, 4, 6] = [10, [4, 6]] = [10, 12] = 60$$

راه اول:

$$10 = 2^1 \times 5^1 = 2^1 \times 3^0 \times 5^1$$

راه دوم:

$$4 = 2^2 = 2^2 \times 3^0 \times 5^0$$

$$6 = 2 \times 3 = 2^1 \times 3^1 \times 5^0$$

$$[10, 4, 6] = 2^2 \times 3^1 \times 5^1 = 60$$



۵-۴- تمرین‌ها

۱- کدام یک از اعداد زیر اول و کدام یک مرکب‌اند؟

۷۳۷ (ب)

۱ (الف)

۲۰۷۹۱ (ت)

۱۸۹۱ (پ)

۲- ثابت کنید بی‌نهایت عدد اول به صورت $4q + 3$ یافت می‌شوند.

۳- اعداد زیر را به عوامل اول تجزیه کنید :

الف) ۹۵۵۵ (ب) ۹۹۷۳-

پ) ۳۷۴۲۳ (ت) ۲۸۰۰۰

۴- نشان دهید که هر عدد طبیعی بزرگ‌تر از ۱ را می‌توان به صورت حاصل ضرب یک مربع کامل و یک عدد صحیح بدون عامل مربع به جز ۱ (یعنی عددی که بر هیچ عدد مربعی جز ۱ قابل قسمت نباشد) نوشت.

۵- اگر p_1, p_2, \dots, p_n, q اعداد اول باشند و $q | p_1 p_2 \dots p_n$ ثابت کنید به ازای یک i ، $1 \leq i \leq n$ ، $p_i = q$.

۶- الف) نشان دهید اگر a نسبت به b و c اول باشد، نسبت به bc هم اول خواهد بود.

ب) نشان دهید اگر a نسبت به b_1, b_2, \dots, b_n اول باشد، نسبت به $b_1 b_2 \dots b_n$ هم اول خواهد

بود.

۷- نشان دهید اگر a و b نسبت به هم اول باشند و $c | a + b$ ، آن‌گاه c نیز نسبت به a و b اول

خواهد بود.

۸- الف) اگر a و b نسبت به هم اول باشند، نشان دهید که برای اعداد طبیعی n و m ، a^n و b^m

هم نسبت به هم اول اند.

ب) اگر برای عدد طبیعی n ، $a^n | b^n$ ثابت کنید $a | b$.