فصل ۵

اعداد اول

در فصل قبل، تقسیم‌پذیری هر دو عدد صحیح به عنوان یک رابطه مطرح شد. برخی از اعداد بر تعداد زیادی از اعداد طبیعی تقسیم‌پذیرند، مثل ۲۴ که بر اعداد طبیعی ۱، ۲، ۳، ۴، ۶، ۸، ۱۲ و ۲۴ تقسیم‌پذیر است. با این حال دسته‌ای دیگر از اعداد طبیعی هیچ مقسوم علیهی به‌جز 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 تقسیم‌پذیر نباشد **عدد اول** گویند. هر عدد طبیعی به‌جز ۱ را 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.

قضیه‌ی 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 مجموعه‌ی 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.

قضیه‌ی ۲ : بی‌نهایت عدد اول وجود دارند.[1]

اثبات: می‌دانیم اعداد ۲، ۳، ۵ و ... اول‌اند، حال اگر این دنباله متناهی باشد، فرض می‌کنیم

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

$p_1, p_2, \cdots, p_n$ تنها عدد اول باشند. $m = p_1 p_2 \cdots p_n + 1$ را درنظر می‌گیریم. چون m یک عدد طبیعی و مخالف p_1 ، p_2 ... و p_n است، m باید مرکب باشد. پس یک مقسوم‌علیه اول دارد که آن را p_j می‌نامیم. داریم :

$$p_j | m \ , p_j | p_1 p_2 \cdots p_n$$

پس $m - (p_1 p_2 \cdots p_n)$ بر p_j تقسیم‌پذیر است. یعنی $p_j | 1$ که غیر ممکن است. لذا تعداد اعداد اول نامتناهی است. □

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

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

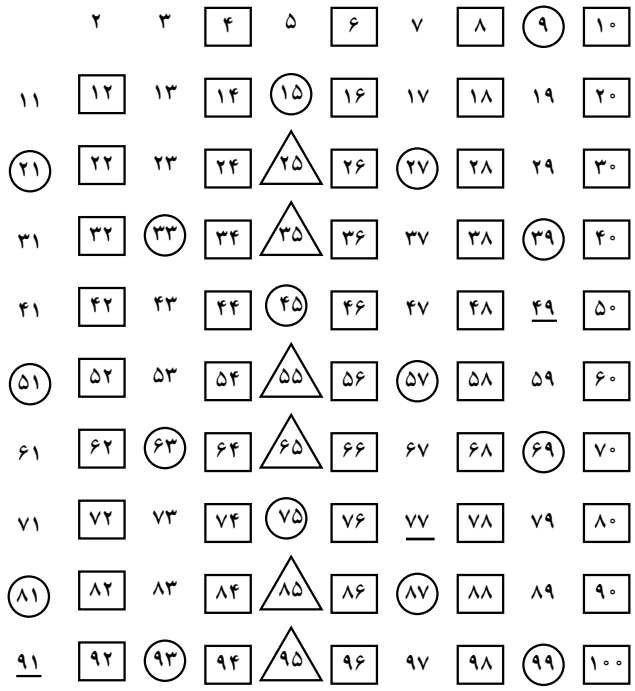
به کمک قضیه‌ی ۳ می‌توان اول بودن هر عددی را بررسی کرد.

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

۲/۴۷ , ۳/۴۷ , ۵/۴۷

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

قضیه‌ی ۳ اساس فرایند **غربال اِراتِسْتِـنْ** است. مثلاً برای تعیین اعداد اول کوچک‌تر از ۱۰۰، تمام مضرب‌های اول اعداد کوچک‌تر از $\sqrt{100} = 10$ یعنی مضرب‌های ۲ ، ۳، ۵ و ۷ را از جدول اعداد از ۱ تا ۱۰۰ حذف می‌کنیم. جدول صفحه‌ی‌بعد نمونه‌ای از غربال اراتستن است.



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

۵ــ۱ــ بزرگ‌ترین مقسوم‌علیه مشترک

می‌دانیم که عدد صحیح c را مقسوم‌علیه یا شمارنده‌ی 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[1].

۱ــ مقسوم‌علیه مشترک a و b را با نماد $a \sqcap b$ هم نمایش می‌دهند.

مثال ۳: مقسوم‌علیه‌های مشترک ۲۴ و ۸۴ عبارت‌اند از :

$$\pm ۱, \pm ۲, \pm ۳, \pm ۴, \pm ۶, \pm ۱۲$$

پس :

$$(۲۴, ۸۴) = ۱۲$$

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 قضیه‌ی زیر را داریم :

قضیه‌ی ۴ : بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح a و b که حداقل یکی از آن‌ها صفر نیست، برابر است با کوچک‌ترین عضو مجموعه‌ی

$$S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > ۰\}$$

اثبات: مجموعه‌ی S حداقل یک عضو دارد (چرا؟) پس دارای کوچک‌ترین عضو است. فرض می‌کنیم d کوچک‌ترین عضو S باشد،

$$d = m_۰a + n_۰b > ۰ \ , \ m_۰, n_۰ \in \mathbb{Z}$$

از الگوریتم تقسیم داریم

$$a = dq + r \ , \ ۰ \le r < d$$

اگر $r > ۰$ می‌دانیم $r \notin S$ چون $r < d$ ، ولی

$$r = a - m_۰aq - n_۰bq = (۱ - m_۰q)a - (n_۰q)b$$

ترکیب خطی[۱] a و b است که با کوچک‌ترین بودن d در تناقض است. پس $r = ۰$. یعنی $d \mid a$. به همین ترتیب $d \mid b$. یعنی d مقسوم‌علیه مشترک a و b است. اگر $c > ۰$ ، $c \mid a$ و $c \mid b$ ، آن‌گاه $c \mid (am_۰ + bn_۰)$ یعنی $c \mid d$ پس $c \le d$. در نتیجه d بزرگ‌ترین مقسوم‌علیه 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 مقسوم‌علیه مشترک دو عدد صحیح a و b است.

الگوریتم اقلیدس بدین‌گونه عمل می‌کند که اگر $r_۰ = a > ۰$ و $r_۱ = b > ۰$ ، آن‌گاه

$$r_۰ = r_۱q_۱ + r_۲ \qquad ۰ \le r_۲ < r_۱$$

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

پس :

$$(a,b)=(r_{\circ},r_{۱})=(r_{۱},r_{۲})$$

هم‌چنین

$$r_{۱}=r_{۲}q_{۲}+r_{۳} \qquad \circ\le r_{۳}<r_{۲}$$

$$(a,b)=(r_{۱},r_{۲})=(r_{۱},r_{۳})$$

$$\vdots$$

$$r_{n-۳}=r_{n-۲}q_{n-۲}+r_{n-۱} \qquad \circ\le r_{n-۱}<r_{n-۲}$$

$$(a,b)=(r_{n-۳},r_{n-۲})=(r_{n-۱},r_{n-۲})$$

$$r_{n-۲}=r_{n-۱}q_{n-۱}+r_{n} \qquad \circ\le r_{n}<r_{n-۱}$$

$$(a,b)=(r_{n-۱},r_{n-۲})=(r_{n-۱},r_{n})$$

چون

$$a=r_{\circ}>r_{۱}>r_{۲}\cdots\ge\circ$$

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 $r_{n+۱}=\circ$ و $r_{n-۱}=r_nq_n$. در نتیجه

$$(a,b)=(r_{n-۱},r_{n})=(r_{n},\circ)=r_{n}$$

که r_n آخرین باقیمانده‌ی غیرصفر در این رشته از تقسیم‌های متوالی است.

مثال ۴:

$$(۳\circ,۷۲)=(۳\circ,۷۲-۲\times۳\circ)=(۳\circ,۱۲)$$

$$=(۲\times۱۲+۶,۱۲)=(۶,۱۲)=(۶,۲\times۶+\circ)=(۶,\circ)=۶$$

که معمولاً به صورت خلاصه‌ی نردبانی زیر می‌نویسند :

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

Δ

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

۱) $d|a$ و $d|b$ و

۲) هرگاه $c|a$ و $c|b$، آن‌گاه $c|d$.

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 $c|b$ آن‌گاه $c|d$ یعنی شرط ۲ هم برقرار است.

برعکس اگر d در دو شرط فوق صدق کند و c یک مقسوم‌علیه مشترک مثبت a و b باشد، آن‌گاه $c|d$ یعنی $c \le d$. پس d بزرگ‌ترین مقسوم‌علیه مشترک a و b است. □

تعریف: دو عدد صحیح a و b را **نسبت به هم اول** یا **متباین** گویند، هرگاه $(a,b)=۱$.

مثال ۵: اعداد **۹** و ۱۰ و نیز دو عدد **۲۵** و **۴۲** نسبت به هم اول‌اند. Δ

با استفاده از قضیه‌ی **۴**، می‌توان ثابت کرد که دو عدد صحیح a و b نسبت به هم اول‌اند اگر و تنها اگر اعداد صحیح m و n وجود داشته باشند که

$$۱ = ma + nb$$

قضیه‌ی ۶ : (لم اقلیدس). اگر $a|bc$ و $(a,b)=۱$ آن‌گاه $a|c$.

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

$$۱ = ma + nb$$

پس :

$$c = cma + cnb$$

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

$$c = cma + naq = (cm + nq)a$$

یعنی $a|c$. □

قضیه‌ی ۷ : اگر p یک عدد اول باشد و $p|ab$، آن‌گاه $p|a$ یا $p|b$.

اثبات: اگر $p\nmid a$، آن‌گاه $(p,a)=۱$، زیرا اگر $(p,a)=d$ و $d\neq ۱$ آن‌گاه $d=p$. (چرا؟) پس $p|a$ که یک تناقض است. در نتیجه $(p,a)=۱$، پس طبق قضیه‌ی **۶**، $p|b$.

□

تعریف بزرگ‌ترین مقسوم‌علیه مشترک دو عدد را به چند عدد نیز می‌توان تعمیم داد :

تعریف: بزرگ‌ترین مقسوم‌علیه مشترک n عدد صحیح $a_n, \cdots, a_2, a_1$ که همگی آن‌ها صفر نیستند عبارت است از بزرگ‌ترین عدد صحیحی که تمام این اعداد صحیح را بشمارد. این عدد را با $(a_1, a_2, \cdots, a_n)$ نمایش می‌دهند. می‌توان ثابت کرد که

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

مثال ۶:

$$(24, 30, 72) = (24, (30, 72))$$
$$= (24, 6) = 6$$

Δ

۵ــ۲ــ قضیه‌ی بنیادی حساب

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

قضیه‌ی ۸ : هر عدد طبیعی بزرگ‌تر از ۱ را می‌توان بدون توجه به ترتیب به‌طور یکتا به صورت حاصل‌ضرب اعداد اول نوشت. یعنی n را می‌توان به صورت $n = p_1 p_2 \cdots p_k$ نمایش داد که در آن برای هر i، p_i عددی اول است. این نمایش را تجزیه‌ی عدد n به عامل‌های اول می‌نامند.

نکته‌ی ۱: در تجزیه اعداد طبیعی به عامل‌های اول، می‌توان حاصل‌ضرب چند عدد اول مساوی را به‌صورت توانی از آن نوشت، یعنی

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

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

نکته‌ی ۲: برای $n = 1$ ، می‌توان $1 = p^0$ را درنظر گرفت، درحالی که p هر عدد اولی می‌تواند باشد.

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

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

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

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

یعنی $p^{\alpha_p(n)} | n$ ولی $p^{\alpha_p(n)+1} \nmid n$ (واضح است که اگر $p > n$ ، حتماً $\alpha_p(n) = 0$)

حال قضیه‌ی زیر را بدون اثبات بیان می‌کنیم :

قضیه‌ی ۹ : اگر $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ و $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ ، آن‌گاه

$$d = (a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$$

که در آن برای هر عدد i،

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

(دقت کنید که اگر برای عدد اول p، $p \nmid n$ ، آن‌گاه توان آن را در نمایش n برابر با صفر می‌گیریم.)

مثال ۷:

$$۳۰ = ۲^۱ \times ۳^۱ \times ۵^۱$$

$$۷۲ = ۲^۳ \times ۳^۲ = ۲^۳ \times ۳^۲ \times ۵^۰$$

$$\text{پس } (۳۰, ۷۲) = ۲^۱ \times ۳^۱ \times ۵^۰ = ۶$$

Δ

۵ــ۳ــ 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 $b|c$ آن‌گاه $m \le c$. کوچک‌ترین مضرب مشترک دو عدد a و b را با $[a.b]$[1] نمایش می‌دهند.

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

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

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

$$۱۲,۲۴,۳۶,\cdots$$

که کوچک‌ترین آن‌ها ۱۲ است. یعنی $[۴,۶]=۱۲$. Δ

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

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

۱) $a|m$ و $b|m$ و

۲) اگر $a|c$ و $b|c$، آن‌گاه $m|c$.

قضیه‌ی۱۱ : اگر $a=p_۱^{\alpha_۱}p_۲^{\alpha_۲}\cdots p_n^{\alpha_n}$ و $b=p_۱^{\beta_۱}p_۲^{\beta_۲}\cdots p_n^{\beta_n}$ ، آن‌گاه

$$m=[a,b]=p_۱^{\theta_۱}p_۲^{\theta_۲}\cdots p_n^{\theta_n}$$

که در آن برای هر i، $\theta_i=\max\{\alpha_i,\beta_i\}$

قضیه‌ی۱۲ : برای هر دو عدد صحیح غیرصفر a و b داریم :

$$[a,b](a,b)=|ab|$$

مثال ۹:

$$۳۰=۲^۱\times۳^۱\times۵^۱$$

$$۷۲=۲^۳\times۳^۲=۲^۳\times۳^۲\times۵^۰$$

$$[۳۰,۷۲]=۲^۳\times۳^۲\times۵^۱=۳۶۰$$

$$[۳۰,۷۲]\times(۳۰,۷۲)=۳۶۰\times۶=۲۱۶۰$$

$$۳۰\times۷۲=۲۱۶۰$$

Δ

تعریف: کوچک‌ترین مضرب مشترک اعداد صحیح غیرصفر $a_۱,a_۲,\cdots,a_n$ عبارت است از کوچک‌ترین عدد صحیح مثبت که بر همه‌ی آن‌ها تقسیم‌پذیر باشد، و آن را با $[a_۱,a_۲,\cdots,a_n]$ نمایش می‌دهند.

می‌توان ثابت کرد که

$$[a_۱,a_۲,\cdots,a_n]=[a_۱,a_۲,\cdots,a_{n-۲},[a_{n-۱},a_n]]$$

مثال ۱۰ :

راه اول : $[۱۰,۴,۶]=[۱۰,[۴,۶]]=[۱۰,۱۲]=۶۰$

راه دوم : $۱۰=۲^{۱}\times۵^{۱}=۲^{۱}\times۳^{۰}\times۵^{۱}$

$۴=۲^{۲}=۲^{۲}\times۳^{۰}\times۵^{۰}$

$۶=۲\times۳=۲^{۱}\times۳^{۱}\times۵^{۰}$

$[۱۰,۴,۶]=۲^{۲}\times۳^{۱}\times۵^{۱}=۶۰$

Δ

۵ــ۴ــ تمرین‌ها

۱ــ کدام یک از اعداد زیر اول و کدام‌یک مرکب‌اند؟

الف) ۱ ب) ۷۳۷ پ) ۱۸۹۱ ت) ۲۰۷۹۱

۲ــ ثابت کنید بی‌نهایت عدد اول به صورت $۴q+۳$ یافت می‌شوند.

۳ــ اعداد زیر را به عوامل اول تجزیه کنید :

الف) ۹۵۵۵ ب) ۹۹۷۳- پ) ۳۷۴۲۳ ت) ۲۸۰۰۰

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

۵ــ اگر $p_{۱}, p_{۲}, \ldots, p_{n}$ و q اعداد اول باشند و $q \mid p_{۱}p_{۲}\cdots p_{n}$ ثابت کنید به ازای یک i، $۱\le i\le n$، $p_{i}=q$.

۶ــ 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 $b_{۱}, b_{۲}, \ldots, b_{n}$ اول باشد، نسبت به $b_{۱}b_{۲}\cdots b_{n}$ هم اول خواهد بود.

۷ــ نشان دهید اگر a و b نسبت به هم اول باشند و $c \mid a+b$، آن‌گاه c نیز نسبت به a و b اول خواهد بود.

۸ ــالف) اگر a و b نسبت به هم اول باشند، نشان دهید که برای اعداد طبیعی m و n، a^{n} و b^{m} هم نسبت به هم اول‌اند.

ب)اگر برای عدد طبیعی n، $a^{n} \mid b^{n}$ ثابت کنید $a \mid b$.