

بخش پذیری

بخش ۱. تعریف

بخش پذیری همان مفهومی را دارد که از دوران راهنمایی به یاد دارید. اگر a و b دو عدد صحیح باشند و $b \neq 0$ ، می‌گوییم a بر b بخش پذیر است، هرگاه اگر a را بر b تقسیم کنیم به باقیمانده صفر برسیم. برای مثال، ۱۸ بر ۹ بخش پذیر است. بر اساس همین مفهوم می‌خواهیم تعریفی معادل از بخش پذیری بیان کنیم.

تعریف. فرض کنید a و b اعدادی صحیح باشند و $b \neq 0$. می‌گوییم a بر b بخش پذیر است هرگاه عددی صحیح مانند q موجود باشد به طوری که $a = bq$. در این صورت q را خارج قسمت تقسیم a بر b می‌نامیم.

بنابراین از این به بعد برای اینکه بخش پذیری a بر b را ثابت کنیم، عددی صحیح مانند q می‌یابیم یا ثابت می‌کنیم وجود دارد به طوری که تساوی $a = bq$ برقرار باشد.

مثال ۱.۲ $10002 - 1$ بر ۹۹۹ بخش پذیر است زیرا $10001 \times 999 = 10002 - 1$ ، در این مثال $10002 - 1$ ، ۹۹۹ و ۱۰۰۰۱ به ترتیب نقش a ، b و q در تعریف بخش پذیری را دارند. ▲

مثال ۲.۲ 751° بر 31° بخش پذیر است زیرا $251^\circ \times 31^\circ = 751^\circ$. ▲

نکته. به تساوی $11 = 2 \times 5/5$ توجه کنید. از این تساوی نمی‌توان نتیجه گرفت که ۱۱ بر ۲ بخش پذیر است، زیرا $5/5$ عددی صحیح نیست.

بخش ۲. اعداد زوج و اعداد فرد

مجموعه $\{2, 4, 6, 8, \dots\}$ را مجموعه اعداد زوج می‌نامند. اعداد زوج اعدادی اند که بر ۲ بخش پذیرند: $1 = 2 \times 0, 2 = 2 \times 1, 4 = 2 \times 2, 6 = 2 \times 3, \dots$ درحقیقت، هر عدد زوج عددی به شکل $2 \times k$ است که k عضوی از مجموعه $\{0, 1, 2, 3, \dots\}$ است. هر عددی را که زوج نباشد، فرد می‌نامیم. مجموعه اعداد فرد برابر است با $\{1, 3, 5, 7, \dots\}$. اعداد فرد در تقسیم بر ۲ باقیمانده صفر ندارند، پس باقیمانده یک دارند. این اعداد به شکل $2k + 1$ اند که k عضوی از مجموعه $\{0, 1, 2, \dots\}$ است. حاصل جمع هر دو عدد زوج، عددی زوج است زیرا اگر این دو عدد $2r$ و $2s$ باشند، $2(r + s) = 2r + 2s$ که عددی زوج است. حاصل جمع هر دو عدد فرد نیز عددی زوج است زیرا اگر این دو عدد $2r + 1$ و $2s + 1$ باشند، $2(r + s + 1) = (2r + 1) + (2s + 1)$ که عددی زوج است. حاصل جمع عددی فرد و عددی زوج، عددی فرد است (به تساوی $2(r + s) + 1 = (2r) + (2s + 1)$ توجه کنید). حاصل ضرب هر تعداد عدد فرد، عددی فرد است، زیرا

$$(2r + 1)(2s + 1) = 4rs + 2r + 2s + 1 = 2(2rs + r + s) + 1$$

حاصل ضرب هر تعداد عدد، مثلاً دو عدد، اگر حداقل یکی از آن‌ها زوج باشد عددی زوج است، زیرا اگر آن عدد زوج را $2r$ و عدد دیگر را t بنامیم آنگاه $(2r)t = 2(rt)$.

مثال ۳.۲ $2^1 + 1$ عددی فرد است زیرا 2^1 عددی زوج و یک، عددی فرد است. ▲

مثال ۴.۲ $(2^1 + 1)^1$ عددی فرد است زیرا حاصل ضرب 1^0 عدد فرد است. ▲

مسئله ۵.۲ ثابت کنید که عددی صحیح مانند a وجود ندارد به طوری که $1 = a^4 + a^3 + a^2 + a$.

راه حل. a یا فرد یا زوج است. در هر حال، حاصل جمع چهار عدد سمت چپ زوج است اما عدد سمت راست فرد است. ▲

نمادگذاری. وقتی a بر b بخش پذیر است، می‌نویسیم $a \mid b$. عبارت $a \mid b$ را به این شکل‌ها هم می‌توان خواند: « a, b را عادی می‌کند»، « b, a را می‌شمارد» و « b مقسوم‌علیه a است» و « b عاملی از a است». دو عبارت اول متداول‌ترند. اگر a, b را عادی نکند می‌نویسیم $a \nmid b$.

مثال ۶.۲ $300 \mid 5^0$ یا به عبارت دیگر $5^0, 300$ را عادی می‌کند. $1 - 1000^2 \mid 999$ ، یا به عبارت دیگر $999, 1 - 1000^2$ را می‌شمارد. ▲

مثال ۷.۲ هر عدد ناصفر، خودش را عادی می‌کند، زیرا اگر a عددی صحیح و ناصفر باشد، $a = a \times 1$ (چون بخش پذیری بر صفر نامفهوم است، a را ناصفر فرض می‌کنیم). توجه کنید که صفر بر هر عدد غیرصفر بخش پذیر است. ▲

▲ مثال ۸.۲ $a^2 + a = a(a + 1)$ بر a بخش پذیر است زیرا $a^2 + a = a(a + 1)$.

بخش ۳. خواص بخش پذیری

خاصیت اول. اگر $a | b$ و $b | c$ آنگاه $a | c$.

یعنی اگر a بر b و b بر c بخش پذیر باشند، آنگاه a بر c بخش پذیر است. برای اثبات این مطلب می توان به این شکل عمل کرد: چون a بر b بخش پذیر است پس عددی صحیح مانند q موجود است که $a = bq$ و به دلیل بخش پذیری b بر c ، $c = bq'$ که q' نیز عددی صحیح است. از دو تساوی اخیر می توانیم بنویسیم $a = c(qq')$ که اگر qq' را که عددی صحیح است q'' بنامیم، آنگاه $a = cq''$. پس بنابر تعریف بخش پذیری، $a | c$. این خاصیت به تعدّی موسوم است.

خاصیت دوم. اگر $a | b$ و $d | c$ آنگاه $ad | bc$.

یعنی اگر a بر b و d بر c بخش پذیر باشند آنگاه ad بر bc بخش پذیر است. برای اثبات می نویسیم $a = bq$ و $d = cq'$ که q و q' اعدادی صحیح اند. حالا طرفین دو تساوی را در هم ضرب می کنیم و می نویسیم $ad = bc(qq')$. پس از نام گذاری عدد صحیح qq' به q'' ، به دست می آوریم $ad = (bc)q''$ پس ad بر bc بخش پذیر است.

▲ مثال ۹.۲ $۶ | ۳$ و $۱۸ | ۱۸$ پس بنابر خاصیت اول، $۳ | ۱۸$.

▲ مثال ۱۰.۲ $۸ | ۴$ و $۹ | ۳$ پس بنابر خاصیت دوم، $۷۲ | ۱۲$.

خاصیت سوم. اگر $a | b$ و $b | c$ آنگاه $b | a + c$ و $b | a - c$.

یعنی اگر دو عدد مانند a و c بر b بخش پذیر باشند آنگاه حاصل جمع و حاصل تفریق آنها نیز بر b بخش پذیر است. برای اثبات می نویسیم $a = bq$ و $c = bq'$ ، پس

$$a + c = bq + bq' = b(q + q') = bq''$$

که $q'' = q' + q$. پس $a + c$ بر b بخش پذیر است. اثبات $b | a - c$ نیز مشابه اثبات بالاست، ولی با عمل تفریق.

خاصیت چهارم. اگر $a | b$ و k عددی صحیح باشد آنگاه $a | ak$.

یعنی اگر a بر b بخش پذیر باشد هر مضربی از a هم بر b بخش پذیر است. برای اثبات می نویسیم $a = bq$ ، پس $ak = bdk$. با نام گذاری qk بر q' به دست می آوریم $ak = bq'$ پس ak بر b بخش پذیر است. البته این خاصیت حالتی خاص از خاصیت دوم نیز هست، زیرا $a | a$ و $k | k$ ، اما به دلیل اهمیت این خاصیت، آن را جداگانه آوردیم.

مثال ۱۱.۲ اگر $a \mid b$ و $b \mid c$ و x و y دو عدد صحیح باشند آنگاه $b \mid az + cy$. درستی حکم بالا از خاصیت‌های سوم و چهارم معلوم می‌شود.

▲ مسئله ۱۲.۲ اگر $a \mid b$ آنگاه $a^2 \mid b^2$.

راه‌حل. برای اثبات حکم از خاصیت دوم با در نظر گرفتن دو رابطه $a \mid b$ و $b \mid a$ استفاده می‌کنیم. ▲ با استفاده از دو رابطه $a \mid b$ و $b \mid a^2$ و خاصیت دوم رابطه $a^3 \mid b^3$ به دست می‌آید. به همین اگر n عددی طبیعی باشد با استفاده مکرر از خاصیت دوم، رابطه $a^n \mid b^n$ به دست می‌آید.

مثال ۱۳.۲ بخش‌پذیری $a^2 + a$ بر a را می‌توان با استفاده از هر یک از خواص سوم و چهارم نیز بیان کرد. (چرا؟)

مسئله ۱۴.۲ اگر a عددی طبیعی باشد ثابت کنید که $(5^a + 1)^{\circ} \mid 10^{24}$ بر 10^{24} بخش‌پذیر است. راه‌حل. 5^a فرد است پس $5^a + 1$ زوج است، یعنی $5^a + 1 = 2k$. پس $(5^a + 1)^{\circ} = 2^{\circ} k^{\circ} = 10^{24} k^{\circ}$ و در نتیجه $(5^a + 1)^{\circ} \mid 10^{24}$.

مسئله ۱۵.۲ دو عدد صحیح مانند r و s مفروض‌اند، به طوری که $2r + 3s$ بر 17 بخش‌پذیر است. ثابت کنید $9r + 5s$ نیز بر 17 بخش‌پذیر است.

راه‌حل. بنابر فرض مسئله، $17 \mid 2r + 3s$. بنابر خاصیت چهارم $17 \mid 13(2r + 3s)$ پس $17 \mid 26r + 39s$ چون $17 \mid 17(r + 2s)$ ، پس از تفریق دو رابطه اخیر (خاصیت سوم) به دست می‌آوریم $(26r + 39s) - (17r + 34s) = 9r + 5s$ پس $17 \mid 9r + 5s$.

مسئله ۱۶.۲ ثابت کنید که اگر $2n + 1$ بر 3 بخش‌پذیر باشد آنگاه $8n^2 + 2n - 1$ بر 9 بخش‌پذیر است. راه‌حل. بنابر فرض، $3 \mid 2n + 1$ و چون $3 \mid 3n$ ، با تفریق دو رابطه به دست می‌آوریم $3 \mid 3n - (2n + 1)$ یعنی $3 \mid n - 1$ ، پس $n - 1 = 3k$ یعنی $n = 3k + 1$. بنابراین

$$\begin{aligned} 8n^2 + 2n - 1 &= 8(3k + 1)^2 + 2(3k + 1) - 1 \\ &= 8 \times 9k^2 + 48k + 8 + 6k + 2 - 1 \\ &= 8 \times 9k^2 + 54k + 9 = 9(8k^2 + 6k + 1) \end{aligned}$$

▲ پس $9 \mid 8n^2 + 2n - 1$.

مسئله ۱۷.۲ تمام اعداد صحیح مانند a را پیدا کنید به طوری که $a^2 + 1$ بر $a + 1$ بخش‌پذیر باشد. راه‌حل. فرض کنید $a^2 + 1 \mid a + 1$. با استفاده از خاصیت چهارم نتیجه می‌شود $a + 1 \mid a(a + 1)$.

اکنون با استفاده از خاصیت تفاضل و این دو رابطه نتیجه می‌گیریم $1 | a - 1$ یا $1 | a + 1$ از طرفی $1 | a + 1$ پس مجدداً با استفاده از خاصیت سوم به دست می‌آوریم $2 | a + 1$ یعنی $1 | a + 1$ مقسوم‌علیهی از ۲ است پس $1 = \pm 1$ یا $1 = \pm 2$ در نتیجه مقادیر ممکن عبارت‌اند از ۱، ۰، -۲ و -۳. با جاگذاری این مقادیر، رابطه $1 | a^2 + 1$ برقرار می‌شود. پس این رابطه دقیقاً به ازای مقادیر -۳، -۲، ۰ و ۱ برقرار است. ▲

نکته. اگر a و b دو عدد طبیعی باشند و $a | b$ آنگاه $a \leq b$. این مطلب اگر a و b منفی باشند درست نیست، مثلاً $4 | -2$ ولی ۲ از ۴ بزرگ‌تر است. درحقیقت اگر از علامت صرف‌نظر کنیم a کمتر از b یا مساوی b است.

مسئله ۱۸.۲ a و b دو عدد طبیعی‌اند و $a^2 + b^2 | a + b$ ، ثابت کنید که $2a^2 \leq a + b$.

راه‌حل. بنابر خاصیت چهارم، $(a+b)(a-b) | a+b$ ، پس $a^2 - b^2 | a+b$. با جمع این رابطه با رابطه فرض مسئله به دست می‌آوریم $2a^2 | a+b$ پس $2a^2 \leq a+b$. ▲

مسئله ۱۹.۲ اگر a, b, c, d اعدادی طبیعی باشند و هر یک بر $ab - cd$ بخش‌پذیر باشد، ثابت کنید که $ab + cd = \pm 1$.

راه‌حل. بنابر فرض، $a | ab - cd$ و $b | ab - cd$ پس $(ab - cd)^2 | ab$ (بنابر خاصیت دوم)، درضمن به طور مشابه نتیجه می‌شود $(ab - cd)^2 | cd$. اگر این دو رابطه را از هم کم کنیم به دست می‌آوریم $(ab - cd)^2 | ab - cd$. یعنی اگر فرض کنیم $n = ab - cd$ آنگاه $n^2 | n$. یعنی n بر مربع خودش بخش‌پذیر است. تنها حالت ممکن با شرط $n^2 | n$ ، $n = \pm 1$ است، در نتیجه $ab - cd = \pm 1$. ▲

توجه. در اینجا به بعضی اشتباه‌های رایج در مورد بخش‌پذیری اشاره می‌کنیم.

• از دو رابطه $a | b$ و $c | d$ نمی‌توان نتیجه گرفت $a + c | b + d$ به عنوان مثال، $2 | 4$ و $3 | 9$ ولی 5 بر 13 بخش‌پذیر نیست.

• از رابطه $a | b$ نمی‌توان نتیجه گرفت که اگر k عددی صحیح باشد آنگاه $a + k | b + k$ به عنوان مثال $4 | 4$ ولی اگر به طرفین عدد یک را اضافه کنیم نتیجه می‌شود 5 بر 3 بخش‌پذیر است که غلط است.

• از روابط $s | r$ و $t | s$ نمی‌توان نتیجه گرفت $t + r | s$. مثلاً $2 | 4$ و $4 | 4$ ، اما 6 بر 6 بخش‌پذیر نیست.

بخش ۴. چند اتحاد مهم

اتحادهای زیر را احتمالاً در کتاب ریاضی سال اول دبیرستان دیده‌اید.

- $(a + b)^2 = a^2 + 2ab + b^2$
- $(a - b)^2 = a^2 - 2ab + b^2$
- $(a - b)(a + b)$ (اتحاد مزدوج)
- $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
- $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$
- $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$

دو اتحاد آخر به اتحادهای چاق و لاغر معروف‌اند! تعمیم این دو اتحاد به شکل زیر است:

تعمیم اتحاد چاق و لاغر. اگر n عددی طبیعی باشد آنگاه

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + y^{n-1})$$

و اگر n فرد باشد آنگاه

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \dots + y^{n-1})$$

برای اثبات دو اتحاد اخیر کافی است عبارات داخل دو پرانتز را در یکدیگر ضرب و سپس حاصل را ساده کنیم.

تعریف ۲.۲. اگر m عددی طبیعی باشد، حاصل ضرب اعداد طبیعی از ۱ تا m را با $m!$ نشان می‌دهیم و آن را « m فاکتوریل» می‌خوانیم و در ضمن تعریف می‌کنیم $0! = 1$.

اگر i و n اعدادی صحیح و نامنفی باشند و $i \leq n$ ، تعریف می‌کنیم $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ (بخوانید « i از n »). اتحاد زیر که به بسط دوجمله‌ای موسوم است، برقرار است.*

اتحاد (بسط دوجمله‌ای). اگر n عددی طبیعی باشد آنگاه

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \dots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

برای خواندن اثبات این اتحاد می‌توانید به کتاب‌های جبر و یا ترکیبیات مراجعه کنید.

*. این ضرایب را ریاضی‌دانان چین و نیز خیام ریاضی‌دان ایرانی دوره اسلامی و پاسکال و نیوتن می‌دانسته‌اند؛ با این حال این بسط به بسط دوجمله‌ای نیوتن معروف شده است.

مثال ۲۱.۲ اگر در اتحاد بالا فرض کنیم $n = 4$ ، به دست می‌آوریم

$$\begin{aligned}(x+y)^4 &= \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4 \\ &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4\end{aligned}$$

▲

اگر فرض کنیم $n = 2, 3$ آنگاه اتحادهای صفحه قبل به دست می‌آیند.

مسئله ۲۲.۲ ثابت کنید که به ازای هر عدد طبیعی مانند n ، $9^n - 1$ بر ۸ بخش پذیر است.

راه حل.

$$9^n - 1 = (9 - 1)(9^{n-1} + 9^{n-2} + \dots + 9 + 1) = 8q$$

▲

که q عبارت داخل پرانتز دوم است. پس $8 \mid 9^n - 1$.

مسئله ۲۳.۲ رابطه $8 \mid 9^n - 1$ را با استفاده از بسط دوجمله‌ای اثبات کنید.

راه حل.

$$9^n = (8 + 1)^n = 8^n + \binom{n}{1}8^{n-1} + \dots + \binom{n}{n-1}8 + 1$$

و در نتیجه

$$9^n - 1 = 8^n + \binom{n}{1}8^{n-1} + \dots + \binom{n}{n-1}8 = 8q$$

▲

مسئله ۲۴.۲ p و q دو عدد فرد متوالی‌اند. ثابت کنید $p^q + q^p \mid p + q$.

راه حل. اگر فرض کنیم $q > p$ آنگاه $q = p + 2$. از طرفی

$$p^q + q^p = p^{p+2} - p^p + p^p + q^p$$

چون p فرد است پس $p^p + q^p$ بنابر تعمیم اتحاد چاق ولاغر بر $p + q$ بخش پذیر است. ضمناً

$$p^{p+2} - p^p = p^p(p^2 - 1) = p^p(p-1)(p+1)$$

چون $p-1$ زوج است پس $p^{p+2} - p^p$ بر $2(p+1)$ بخش پذیر است اما $2(p+1) = p+q$ ، پس

$p^q + q^p \mid p + q$ و قبلاً نتیجه گرفتیم که $p + q \mid p^p + q^p$. پس بنابر خاصیت سوم بخش پذیری

▲

نتیجه می‌شود $p + q \mid p^q + q^p$.

مسئله ۲۵.۲ ثابت کنید اعدادی فرد مانند a ، b و c وجود ندارد به طوری که

$$(a+b)^2 + (a+b)^2 = (b+c)^2$$

راه حل. با ساده کردن تساوی بالا می توانیم بنویسیم $a^2 + ab + ac = bc$. اگر به طرفین bc را اضافه کنیم به دست می آوریم

$$a^2 + ab + ac + bc = 2bc$$

$$a(a+b) + c(a+b) = 2bc$$

$$(a+b)(a+c) = 2bc$$

چون a ، b و c فردند پس $a+b$ و $a+c$ زوج اند. آن ها را به ترتیب $2r$ و $2s$ بنامید. در این صورت $(2r)(2s) = 2bc$ پس $bc = 2rs$ که تناقض است زیرا bc فرد است. پس اعدادی فرد که در شرط ذکر شده در صورت مسئله صدق کنند، وجود ندارند. ▲

مسئله ۲۶.۲ تمام اعداد طبیعی مانند n را بیابید به طوری که $n! + 3 = 3^{n-1}$.

راه حل. فرض کنید $n! + 3 = 3^{n-1}$ اگر $n \geq 6$ آنگاه $9 \mid n!$ و $9 \mid 3^{n-1}$ پس $9 \mid n! + 3 - 3^{n-1}$. در نتیجه $3 \mid 9$ که ممکن نیست. بنابراین $n < 6$. یعنی n عضو مجموعه $\{1, 2, 3, 4, 5\}$ است. با آزمایش این اعداد دیده می شود که فقط $n = 3$ و $n = 4$ جواب اند. ▲

مسئله ۲۷.۲ اگر a و b دو عدد فرد باشند آنگاه $a^8 - b^8$ بر ۱۶ بخش پذیر است.

راه حل. بنابر اتحاد مزدج

$$a^8 - b^8 = (a^4 + b^4)(a^2 + b^2)(a+b)(a-b)$$

و چون a و b فردند عبارت داخل هر یک از پرانتزها زوج است. بنابراین $a-b = 2r$ ، $a+b = 2s$ و چون $a^2 + b^2 = 2t$ و $a^4 + b^4 = 2u$ در نتیجه $a^8 - b^8 = 16rstu$ پس $a^8 - b^8$ بر ۱۶ بخش پذیر است. ▲

مسئله ۲۸.۲ ثابت کنید که اگر $2^n + 3^n$ بر ۲۵ بخش پذیر باشد آنگاه n بر ۵ بخش پذیر است.

راه حل. فرض کنید $2^n + 3^n \mid 25$. واضح است که $2 \geq n$. ابتدا ثابت می کنیم که n فرد است.

می‌توانیم بنویسیم

$$2^n + 3^n = 2^n + (5 - 2)^n = 2^n + 5^n - \binom{n}{1} 5^{n-1} \times 2 + \dots + (-1)^{n-1} \binom{n}{n-1} 5 \times 2^{n-1} + (-2)^n$$

چون بنا بر فرض، $2^n + 3^n \mid 25$ پس $5 \mid 2^n + 3^n$ و در نتیجه با توجه به تساوی بالا، $2^n + (-2)^n$ بر ۵ بخش پذیر است که زمانی درست است که n فرد باشد.

اکنون با توجه به تساوی بالا، $5 \times 2^{n-1} \binom{n}{n-1} (-1)^{n-1}$ باید بر ۲۵ بخش پذیر باشد که چون $\binom{n}{n-1} = n$ پس n باید مضرب ۵ باشد. ▲

مسئله ۲۹.۲ تمام اعدادی را بیابید که می‌توان آن‌ها را به شکل حاصل تفاضل دو مربع کامل نوشت.

راه حل. $n^2 - (n+1)^2 = 2n+1$ ، پس هر عدد فرد به شکل تفاضل دو مربع کامل هست. از طرفی $(n-1)^2 - (n+1)^2 = 4n$ پس مضارب ۴ نیز تفاضل دو مربع کامل اند. تنها اعدادی باقی می‌مانند که به شکل $4k+2$ اند که در اینجا k عددی صحیح است. ثابت می‌کنیم که این اعداد به شکل تفاضل دو مربع کامل نیستند. فرض کنید این‌طور نباشد و $n = 4k+2$ یعنی فرض کنید اعدادی صحیح مانند a و b وجود داشته باشند به طوری که $4k+2 = a^2 - b^2$ پس $(a-b)(a+b) = 4k+2$. توجه کنید که $a-b$ و $a+b$ یا هر دو زوج اند یا هر دو فردند و چون حاصل ضرب آن‌ها زوج است پس هر دو زوج اند، مثلاً $a-b = 2r$ و $a+b = 2s$ ، پس $4k+2 = 4rs$ که تناقض است، زیرا از این تساوی نتیجه می‌شود $2k+1 = 2rs$ پس به جز اعدادی که به شکل $4k+2$ اند، بقیه اعداد طبیعی تفاضل دو مربع کامل اند. ▲