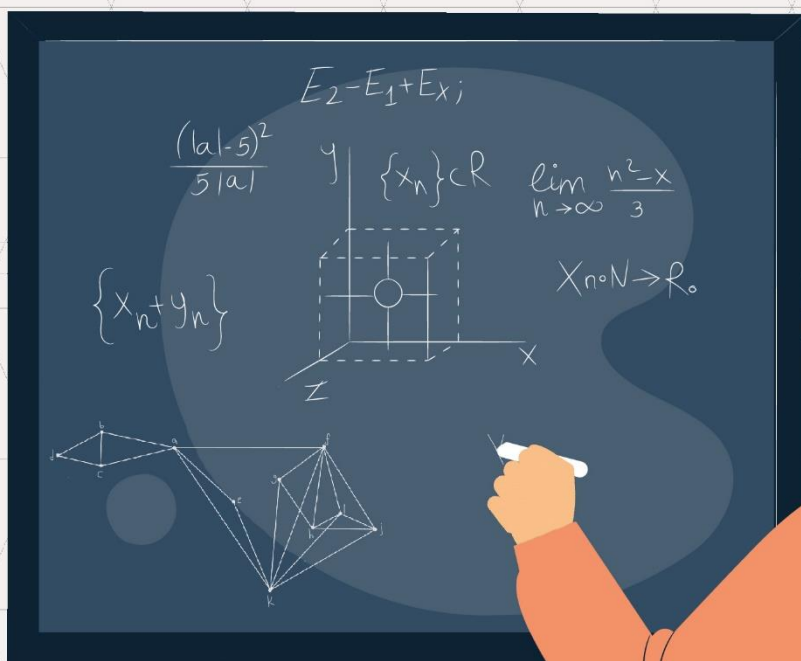


ریاضیات گسسته دوازدهم

مسطه دوم

(نکات و خلاصه درس)





فصل اول: آشنایی با نظریه اعداد

درس اول: استدلال ریاضی

درک و فهم ریاضی بدون استدلال امکان پذیر نمی باشد و آموزش ریاضی را محدود به حفظ کردن خواهد کرد. هدف از این درس آشنایی با برخی از روش های استدلال و اثبات ریاضی است .

روش های اثبات:

۱. مثال نقض : برای رد یک حکم کلی، از مثال نقض استفاده می شود. اگر گزاره ای به صورت کلی بیان شود، ارائه حتی یک مثال که در آن گزاره نادرست باشد، کافی است تا حکم کلی رد شود.

- مثال: اگر گزاره ای بگویید "همه اعداد فرد اول هستند"، عدد ۹ یک مثال نقض است، زیرا فرد است ولی اول نیست.





۲. اثبات با مثال : ارائه مثال برای اثبات درستی یک گزاره کلی کافی نیست. حتی اگر نتوانیم مثال نقضی پیدا کنیم، این به معنای درستی گزاره نیست.

– مثال: گزاره‌ای مانند "هر عدد زوج بزرگ‌تر از ۲ مجموع دو عدد اول است" (حدس گلدباخ) هنوز اثبات نشده، ولی مثال‌های زیادی آن را تأیید می‌کنند.

۳. اثبات مستقیم: برای اثبات درستی یک گزاره، می‌توان از استدلال منطقی استفاده کرد.

– مثال: برای اثبات اینکه مجموع سه عدد متوالی طبیعی مضرب ۳ است، داریم:

$$n + (n + 1) + (n + 2) = 3n + 3 = 3(n + 1)$$

که نشان می‌دهد مجموع این سه عدد همیشه مضرب ۳ است.

نتیجه:

– مثال نقض برای رد حکم کلی.

– اثبات با مثال کافی نیست.

– اثبات مستقیم نیاز به استدلال منطقی دارد.





اثبات با مثال نقض :

به مثالی که کلیت یک حکم را باطل می کند مثال نقض می گویند.

اگر بتوان با یک مثال حکم کلی را رد کرد آن استدلال با کمک مثال نقض است .

– مثال: آیا گزاره "عدد $2^n + 1$ به ازای همه عددهای طبیعی، عددی اول است" صحیح است؟

پاسخ: اگر $n = 5$ را در نظر بگیریم

$$2^{2^5} + 1 = 4294967297 = 641 \times 6700417$$

به وضوح حاصل یک عدد اول نیست چون که به صورت حاصلضرب دو عدد (به غیر از خودش و یک) نوشته شده است.

اثبات مستقیم :

اثبات با در نظر گرفتن تمام حالت ها





– مثال: ثابت کنید برای هر عدد طبیعی n ; $n^2 - 5n + 7$ عددی فرد است.

پاسخ: اگر n زوج باشد به عبارت دیگر $n=2k$ در این حالت داریم:

$$\begin{aligned} n^2 - 5n + 7 &= (2k)^2 - 5(2k) + 7 = 4k^2 - 10k + 6 + 1 \\ &= 2(2k^2 - 5k + 3) + 1 \end{aligned}$$

که حاصل عددی فرد است.

اگر n عددی فرد باشد یعنی $n=2k-1$. در این حالت داریم:

$$\begin{aligned} n^2 - 5n + 7 &= (2k-1)^2 - 5(2k-1) + 7 = 4k^2 - 14k + 13 \\ &= 2(2k^2 - 7k + 6) + 1 \end{aligned}$$

که باز هم عددی فرد است.

اثبات غیر مستقیم: (اثبات به روش برهان خلف)

فرض می‌کنیم حکم نادرست باشد و سپس با استفاده از گزاره‌ها و قوانین به یک نتیجه

غیرممکن یا تضاد می‌رسیم و از آنجا نادرست بودن حکم باطل است و درستی حکم ثابت

می‌شود.





– مثال: ثابت کنید حاصل ضرب هر عدد گویای ناصفر در یک عدد گنگ، عددی گنگ است.

پاسخ: فرض کنیم r یک عدد گویای ناصفر است و x عددی گنگ است ولی rx عددی گویا (برهان خلف) باشد. می‌دانیم حاصل ضرب دو عدد گویا، عددی گویا است. معکوس هر عدد گویای ناصفر هم عددی گویاست.

بنابراین: $(\frac{1}{r})x \in Q$ یا $(\frac{1}{r})(r.x) \in Q$

از آنجا که $x \in Q$ که با فرض در تناقض است. پس فرض خلف باطل و حکم درست است.

اثبات های بازگشتی / گزاره های هم ارز :

اگر ارزش دو گزاره یکسان باشد آن‌ها را گزاره‌های هم ارز می‌نامیم.

$$p \Rightarrow q \text{ و } q \Rightarrow p \Leftrightarrow p \Leftrightarrow q \qquad q \Leftrightarrow p \Leftrightarrow p \Leftrightarrow q$$





- مثال: ثابت کنید اگر $a > 0$ باشد، آنگاه $a + \frac{1}{a} \geq 2$

پاسخ:

$$a + \frac{1}{a} \geq 2 \Leftrightarrow a^2 + 1 \geq 2a \Leftrightarrow a^2 - 2a + 1 \geq 0 \Leftrightarrow (a - 1)^2 \geq 0$$

گزاره همیشه درست است.

- مثال: برای اثبات گزاره "اگر a و b دو عدد مثبت باشند، آنگاه $\frac{a+b}{2} \geq \sqrt{ab}$ است"،

به روش بازگشتی، در نهایت به کدام رابطه بدیهی می‌رسیم.

پاسخ: با توجه به هم ارز بودن دو گزاره در عبارت دو شرطی داریم:

$$\frac{a+b}{2} \geq \sqrt{ab} \Leftrightarrow a+b \geq 2\sqrt{ab} \Leftrightarrow a+b-2\sqrt{ab} \geq 0 \Leftrightarrow (\sqrt{a}-\sqrt{b})^2 \geq 0$$





درس دوم : بخش پذیری در اعداد صحیح

تساوی $15 = 5 \times 3$ را در نظر بگیرید. عدد ۱۵ از سه دسته ۵ تایی تشکیل شده است یعنی در تقسیم عدد ۱۵ بر ۵، خارج قسمت برابر ۳ می شود و باقی مانده صفر است پس می توانیم از یک طرف بگوییم که ۱۵ بر ۵ بخش پذیر است و از طرف دیگر بگوییم که عدد ۵، عدد ۱۵ را می شمارد (عاد می کند)، چون می توان ۱۵ را با دسته های ۵ تایی شمرد. این شمارش یا عاد کردن را در ریاضی با علامت " | " نشان می دهند و می نویسند $5|15$.

مفهوم بخش پذیری و علامت " | " :

در ریاضی، وقتی می خواهیم بررسی کنیم که یک عدد، عدد دیگری را "عاد" می کند یا به عبارتی، بدون باقی مانده بر آن تقسیم می شود، از علامت " | " استفاده می کنیم. به این معنی که اگر عدد A بر عدد B بدون باقی مانده تقسیم شود، می نویسیم:

$$A|B \text{ و } B|AB$$

که می خوانیم A عدد B را عاد میکند یا B بر A بخش پذیر است.





گروه‌بندی مهره‌ها :

فرض کنید ۱۵ مهره رنگی داریم و می‌خواهیم آن‌ها را به دسته‌های ۵ تایی تقسیم کنیم. اگر بتوانیم مهره‌ها را طوری دسته‌بندی کنیم که در هر دسته دقیقاً ۵ تا باشد و هیچ مهره‌ای باقی نماند، یعنی ۱۵ کاملاً بر ۵ بخش‌پذیر است.

حالا اگر مهره‌ها را یکی‌یکی داخل گروه‌های ۵ تایی بگذاریم:

- اولین گروه: ۵ مهره
- دومین گروه: ۵ مهره
- سومین گروه: ۵ مهره

همه ۱۵ مهره تمام شدند و هیچ مهره‌ای اضافه نیامد. پس می‌گوییم ۱۵ بر ۵ بخش‌پذیر است و می‌توانیم این را به صورت زیر بنویسیم:

$$5 \mid 15$$

یعنی ۵ عدد ۱۵ را عاد می‌کند.

- قرار دادن تعداد شی در دسته‌های مساوی با دسته‌بندی کردن تعدادی از چیزها را

بدون آنکه باقی مانده‌ای داشته باشیم را **عاد کردن** یا شمارش آن اشیا توسط شمارنده‌ها

می‌گویند.





- در ریاضیات، می‌گوییم عدد صحیح a بر عدد صحیح b **بخش‌پذیر** است، اگر عدد صحیحی مانند q وجود داشته باشد که رابطه‌ی زیر برقرار باشد:

$$b = aq$$

در این حالت، عدد b را "**شمارنده**" یا "**عاد کننده**" عدد a می‌نامیم و به صورت زیر می‌نویسیم:

$b|a$ و می‌خوانیم a, b را عاد میکند یا b بر a بخش‌پذیر است.

اما اگر چنین عددی q وجود نداشته باشد و a بر b بخش‌پذیر نباشد، می‌نویسیم:

$$b \nmid a$$

- **مثال:** می‌توان ۱۸ شی را با شمارنده‌های ۱، ۲، ۳، ۶، ۹، ۱۸ دسته‌بندی یا شمارش کرد.

مثلاً می‌نویسیم $18|9$ و می‌خوانیم عدد ۹ عدد ۱۸ را عاد می‌کند.

نکته: اگر a عددی طبیعی باشد، آنگاه داریم: $1|a$ و $a|a$





ویژگی های رابطه عاد کردن :

ویژگی (۱) $a|b \Rightarrow a|mb$ (اگر عدد a عدد b را عاد کند آن گاه مضرب صحیح b را می-)

(شمارد)

ویژگی (۲) $a|b \wedge b|c \Rightarrow a|c$

ویژگی (۳) $a|b \wedge a|c \Rightarrow a|b \pm c$

ویژگی (۴) اگر $|a| \leq |b| \Rightarrow a|b \wedge b \neq 0$ در نتیجه $a = \pm b$

(اثبات ویژگی ها در کتاب)

تذکر: با توجه به ویژگی های بالا اگر $a|b$ ، آنگاه: $a^n|b^n$

نکته: $a|b$ و $a|c \Rightarrow a|mb \pm nc$





عدد اول:

هر عدد طبیعی و بزرگ‌تر از یک که هیچ شمارنده‌ی مثبتی به جز یک و خودش نداشته- باشد، عدد اول نامیده می‌شود. "در واقع هر عدد طبیعی و بزرگ‌تر از یک که مقسوم‌علیه به غیر از یک و خودش نداشته باشد یا به عبارتی بر هیچ عددی به غیر از خودش و یک بخش‌پذیر نباشد را عدد اول گویند." مجموعه اعداد اول که ثابت شده‌است مجموعه‌ای نامتناهی $\{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$ را نمایش داده می‌شود.

نتیجه: اگر p عددی اول باشد و a عددی طبیعی و alp ، آنگاه: $a=1$ یا $a=p$

مثال مهم: اگر عدد طبیعی a دو عدد $(9k + 7)$ و $(7k + 6)$ را عاد کند، ثابت کنید:

$$a = 5 \text{ یا } a = 1$$

پاسخ: ابتدا هر عبارت را در ضریب k عبارت دیگر ضرب می‌کنیم:

$$a|(9k + 7) \rightarrow a|63k + 49$$

$$a|(7k + 6) \rightarrow a|63k + 54$$

$$a|63k + 54 - (63k + 49)$$

$$a|5 \rightarrow a = 5 \text{ یا } a = 1$$





بزرگ ترین مقسوم علیه مشترک دو عدد :

d ب م م دو عدد صحیح و ناصفر a و b است $\{d = (a, b)\}$ ، اگر و تنها اگر:

$$d \mid a \wedge d \mid b$$

$$\forall m > 0 : m \mid a \wedge m \mid b \Rightarrow m \leq d$$

نکته: اگر $(a, b) = 1$ باشد، در این صورت می‌گوییم a و b نسبت به هم اول اند.

مثال: ب م م دو عدد ۷۲ و ۶۰ را بیابید.

پاسخ: مجموعه مقسوم علیه‌های ۷۲:

$$72 = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$$

مجموعه مقسوم علیه‌های ۶۰:

$$60 = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

از بین شمارنده‌های طبیعی مشترک دو مجموعه، ۱۲ از همه بزرگ‌تر است.

راه بهتر:

عددها را تجزیه می‌کنیم و عامل مشترک را با توان کوچکتر در هم ضرب می‌کنیم.

$$72 = 2^3 \times 3^2 \text{ و } 60 = 2^2 \times 3 \times 5 \Rightarrow (60, 72) = 2^2 \times 3$$





کوچکترین مضرب مشترک دو عدد:

c کم‌م دو عدد صحیح و ناصفر a و b است $\{c = [a \text{ و } b]\}$ ، اگر و تنها اگر:

$$a|c \wedge b|c$$

$$\forall m > 0 \wedge a|m \text{ و } b|m \Rightarrow c \leq m$$

__مثال: کم‌م دو عدد ۷۲ و ۶۰؟

پاسخ: ضرب عامل‌های مشترک با توان بیشتر در عامل‌های غیر مشترک $= [۷۲ \text{ و } ۶۰]$

$$۲^۳ \times ۳^۲ \times ۵$$

قضیه تقسیم و کاربردها:

وقتی یک عدد را بر عدد دیگری تقسیم می‌کنیم، ممکن است کاملاً بخش‌پذیر باشد (یعنی باقی‌مانده صفر شود) یا ممکن است عددی باقی بماند که دیگر قابل تقسیم بر عدد دوم نباشد. قضیه تقسیم دقیقاً همین موضوع را توضیح می‌دهد و نشان می‌دهد که هر عدد صحیح را می‌توان به شکلی مشخص تقسیم‌بندی کرد.





بیان ساده‌ی قضیه تقسیم:

فرض کنید که یک عدد a را بر عدد b تقسیم می‌کنیم. این تقسیم دو حالت دارد:

۱. اگر a کاملاً بر b بخش‌پذیر باشد، یعنی باقی‌مانده صفر شود، می‌گوییم که b

عدد a را "عاد" می‌کند.

۲. اما اگر تقسیم انجام شود و عددی باقی بماند، یعنی عدد a به‌طور کامل در b جا

نشود، در این صورت، یک مقدار اضافه باقی می‌ماند که از عدد b کوچک‌تر است.

به زبان ساده، هر عدد صحیح را می‌توان به شکل مجموع یک عدد دیگر و یک باقی‌مانده‌ی

کوچک‌تر از آن نوشت.

درک بهتر با یک مثال ساده در صفحه بعد:





مثال: فرض کنیم که ۲۳ شکلات داریم و می‌خواهیم آن‌ها را در بسته‌های ۵ تایی قرار

دهیم:

پاسخ:

- اولین بسته ۵ شکلات
- دومین بسته ۵ شکلات
- سومین بسته ۵ شکلات
- چهارمین بسته ۵ شکلات
- بعد از قرار دادن ۲۰ شکلات در ۴ بسته، هنوز ۳ شکلات باقی می‌ماند.

نتیجه چیست؟ ما توانستیم ۲۳ شکلات را در ۴ بسته‌ی ۵ تایی قرار دهیم و ۳ شکلات باقی ماند. این همان چیزی است که قضیه تقسیم توضیح می‌دهد!

یعنی:

- ۲۳ شکلات را می‌توان به صورت مجموع تعدادی بسته‌ی ۵ تایی به علاوه‌ی ۳ شکلات باقی‌مانده نوشت.
- این باقی‌مانده همیشه باید از اندازه‌ی بسته‌های ما (عدد ۵) کوچک‌تر باشد، در غیر این صورت می‌توانستیم یک بسته‌ی دیگر هم تشکیل دهیم.





قضیه تقسیم :

اگر a عددی صحیح و b عددی طبیعی باشد در اینصورت اعدادی صحیح و منحصر بفرد

مانند q و r یافت می شوند به قسمی که $a = bq + r$ و $0 \leq r < b$.

تذکر: a را مقسوم و b را مقسوم علیه و q را خارج قسمت و r را باقی مانده می نامیم.

مثال: اگر باقی مانده تقسیم اعداد m و n بر ۱۷ به ترتیب ۵ و ۳ باشد در این صورت

باقی مانده تقسیم عدد $(2m - 5n)$ بر ۱۷ را بدست آورید.

پاسخ :

$$m = 17q_1 + 5$$

$$n = 17q_2 + 3$$

$$2m - 5n = (34q_1 + 10) - (85q_2 + 15) = 34q_1 - 85q_2 - 5 = 17(2q_1 - 5q_2) - 5 = 17q_3 - 5$$

چون باقیمانده یک عدد منفی هست پس یک تناقض است. پس به انتهای معادله ضریب

q_3 را اضافه و کم می کنیم. $0 \leq r < b$.

$$\Rightarrow 2m - 5n = 17q_3 - 5 + 17 - 17 = 17q_3 + 17 - 23 = 17(q_3 + 1) - 23 = 17q'_3 - 23$$

$$\Rightarrow r = -23$$





افراز مجموعه Z به کمک قضیه تقسیم:

یکی از روش‌های مهم برای دسته‌بندی اعداد، افراز آن‌ها بر اساس باقی‌مانده‌ی تقسیم بر یک عدد خاص است. این کار به ما کمک می‌کند که همه‌ی اعداد را در چند گروه مشخص قرار دهیم و ویژگی‌های آن‌ها را بهتر بشناسیم.

بیان ساده‌ی مفهوم:

فرض کنید یک عدد صحیح a را بر یک عدد طبیعی b تقسیم کنیم. طبق قضیه تقسیم، می‌دانیم که این تقسیم همیشه یک باقی‌مانده دارد که از عدد b کوچک‌تر است. یعنی باقی‌مانده‌ی تقسیم همیشه یک مقدار مشخص و محدود خواهد بود.

به بیان ساده‌تر:

- اگر عددی را بر ۵ تقسیم کنیم، باقی‌مانده‌ی آن فقط می‌تواند یکی از اعداد ۰، ۱، ۲، ۳ یا ۴ باشد.
- این یعنی همه‌ی اعداد را می‌توان در پنج دسته‌ی مشخص قرار داد که هر دسته اعدادی را شامل می‌شود که باقی‌مانده‌ی تقسیم آن‌ها بر ۵ برابر یکی از این مقادیر باشد.





درک بهتر با مثال:

مثال: فرض کنید می‌خواهیم اعداد صحیح را بر اساس باقی‌مانده‌ی تقسیم بر ۵

دسته‌بندی کنیم. وقتی یک عدد را بر ۵ تقسیم کنیم، ممکن است:

۱. باقی‌مانده صفر باشد: یعنی عدد کاملاً بر ۵ بخش‌پذیر است، مانند:

○ ۵، ۱۰، ۱۵، ۲۰، ۲۵، ...

○ این اعداد را می‌توان به صورت $a = 5k$ نوشت.

۲. باقی‌مانده ۱ باشد: یعنی عدد دقیقاً یک واحد از مضرب ۵ بیشتر است، مانند:

○ ۱، ۶، ۱۱، ۱۶، ۲۱، ...

○ این اعداد را می‌توان به صورت $a = 5k + 1$ نوشت.

۳. باقی‌مانده ۲ باشد: یعنی عدد دقیقاً دو واحد از مضرب ۵ بیشتر است، مانند:

○ ۲، ۷، ۱۲، ۱۷، ۲۲، ...

○ این اعداد را می‌توان به صورت $a = 5k + 2$ نوشت.

۴. باقی‌مانده ۳ باشد: یعنی عدد دقیقاً سه واحد از مضرب ۵ بیشتر است، مانند:

○ ۳، ۸، ۱۳، ۱۸، ۲۳، ...

○ این اعداد را می‌توان به صورت $a = 5k + 3$ نوشت.





۵. باقی مانده ۴ باشد: یعنی عدد دقیقاً چهار واحد از مضرب ۵ بیشتر است، مانند:

$$\circ \quad ۴, ۹, ۱۴, ۱۹, ۲۴, \dots$$

○ این اعداد را می توان به صورت $a = ۵k + ۴$ نوشت.

با توجه به قضیه تقسیم می دانیم که اگر a عددی صحیح و دلخواه باشد با تقسیم آن به عدد طبیعی b و با توجه به اینکه باقی مانده تقسیم یعنی r در رابطه $۰ \leq r < b$ صدق می کند، برای باقی مانده دقیقاً b حالت وجود دارد.

در واقع با تقسیم عدد a بر b مجموعه $\mathbb{Z}$ به دسته افراز می شود.

عددهای مضرب b bk

عددهایی که در تقسیم بر b باقی مانده ای برابر ۱ دارند $bk+۱$

⋮

عددهایی که در تقسیم بر b باقی مانده ای برابر $b-۱$ دارند $bk + (b-۱)$





مثال: اگر a بر عدد ۵ تقسیم شود در این صورت عدد a را به ۵ صورت می توان نوشت:

$$a = 5k \text{ و } a = 5k + 1 \text{ و } a = 5k + 2 \text{ و } a = 5k + 3 \text{ و } a = 5k + 4$$

$$\text{و } a = 5k + 4$$

درس سوم : هم نهشتی در اعداد صحیح و کاربردها

زمانی که دو عدد را بر یک عدد مشخص تقسیم می کنیم، ممکن است باقی مانده ی آنها برابر باشد. در این صورت، می گوییم این دو عدد "با هم **هم نهشت**" هستند.

مثال: فرض کنید عددی مانند ۲۳ و عددی مانند ۸ را بر ۵ تقسیم کنیم:

• وقتی ۲۳ را بر ۵ تقسیم می کنیم، باقی مانده ۳ است $23 = 5 \times 4 + 3$

• وقتی ۸ را بر ۵ تقسیم می کنیم، باقی مانده ۳ است $8 = 5 \times 1 + 3$

چون هر دو عدد پس از تقسیم بر ۵ همان باقی مانده را دارند، می گوییم که ۲۳ و ۸ نسبت به ۵ **هم نهشت** هستند.





مثال: اگر ۱۲ و ۲ را بر ۵ تقسیم کنیم:

- ۱۲ بر ۵ تقسیم شود، باقی مانده ۲ است.
- ۲ بر ۵ تقسیم شود، باقی مانده ۲ است.
- پس می‌گوییم ۱۲ و ۲ نسبت به ۵ همنهشت هستند.

مثال: اگر ۱۹ و ۴ را بر ۵ تقسیم کنیم:

- ۱۹ بر ۵ تقسیم شود، باقی مانده ۴ است.
- ۴ بر ۵ تقسیم شود، باقی مانده ۴ است. پس می‌گوییم ۱۹ و ۴ نسبت به ۵ همنهشت هستند.

تعریف: برای هر عدد طبیعی مانند m و هر دو عدد صحیح مانند a, b اگر $m|a-b$ می

گوییم a هم نهشت با b است به سنج یا پیمانه m و می‌نویسیم $a \equiv b \pmod{m}$

$$\forall a, b \in \mathbb{Z} \text{ و } a \equiv b \pmod{m} \Leftrightarrow m|a-b \quad (k \in \mathbb{N}) \Leftrightarrow a-b = mk$$

به بیان دیگر دو عدد a, b را به پیمانه m هم نهشت گوییم هرگاه باقی مانده آن‌ها در

تقسیم بر m یکسان باشد.





تذکر: مجموعه همه اعداد صحیح که باقی مانده تقسیم آنها بر عدد طبیعی m برابر با r می باشد یعنی $A_r = \{x \in \mathbb{Z} / x = mk + r\}$ را کلاس یا دسته هم نهشتی r به پیمانه m می نامیم و با نماد $[r]_m$ نمایش می دهیم.

مثال: دو عدد ۱۱ و ۲۵ در تقسیم بر ۷ هر دو باقی مانده ای برابر ۴ دارند لذا :

$$25 \equiv 11 \pmod{7} \Rightarrow 7 \mid 25 - 11 = 14$$

مثال: $[4]_7 = \{ \dots \text{و } 18 \text{ و } 11 \text{ و } 4 \text{ و } -3 \text{ و } -10 \text{ و } \dots \}$

$$\text{فرم کلی اعضاء مجموعه} = 7k + 4$$

رابطه هم نهشتی در اعداد صحیح :

ویژگی (۱) به دو طرف رابطه هم نهشتی می توان عدد صحیح را اضافه یا از آن کم کرد.

$$a \equiv b \Rightarrow \begin{cases} a + c \equiv b + c \\ a - c \equiv b - c \end{cases}$$

ویژگی (۲) دو طرف رابطه هم نهشتی را می توان در عددی صحیح ضرب کرد.

$$a \equiv b \Rightarrow ac \equiv bc$$





نکته: عکس ویژگی ۲ برقرار نیست.

ویژگی ۳) دو طرف رابطه هم نهشتی را می توان به توان n رساند $n \in \mathbb{N}$

$$a \equiv b \Rightarrow a^n \equiv b^n$$

نکته: عکس رابطه ۳ برقرار نیست. عکس این رابطه یعنی ریشه n ام؟

ویژگی ۴) دو طرف رابطه هم نهشتی را که به پیمانه های یکسان داشته باشند را می توان

با هم جمع یا از هم کم و یا در هم ضرب کرد.

$$a \equiv b \text{ و } c \equiv d \Rightarrow \begin{cases} ac \equiv bd \\ a \pm c \equiv b \pm d \end{cases}$$

تذکر: اگر باقیمانده تقسیم a بر m مساوی با r باشد در اینصورت $a \equiv r$.

مثال: باقی مانده تقسیم عدد $A = (27^7) + 19$ را بر عدد ۱۳ بدست آورید.

پاسخ:

$$27 = 13 \times 2 + 1 \Rightarrow 27 \equiv 1 \Rightarrow (27)^7 \equiv 1^7 \Rightarrow 27^7 \equiv 1$$

$$19 \equiv 6 \Rightarrow 19 \equiv 6 \Rightarrow 19 \equiv 6$$

$$(27)^7 + 19 \equiv 1 + 6 \equiv 7$$





نکته: اگر دو عدد a و b تقسیم بر عدد طبیعی m هم باقیمانده باشند در اینصورت $a \equiv b \pmod{m}$

ویژگی (۵) می توان دو طرف یا یک طرف رابطه هم نهشتی هر مضربی از پیمانه را اضافه یا از آن کم کرد.

$$a \equiv b \pmod{m} \Rightarrow \begin{cases} a + mt \equiv b + mk \\ a - mt \equiv b - mk \end{cases}$$

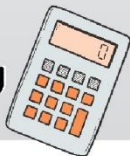
ویژگی (۶) اگر بخواهیم دو طرف یک رابطه هم نهشتی را بر عددی تقسیم کنیم باید آن هم نهشتی را بر m آن عدد و پیمانه تقسیم کنیم.

$$ac \equiv bc \pmod{m} \text{ و } (c, m) = d \Rightarrow a \equiv b \pmod{\frac{m}{d}}$$

نکته: در واقع قاعده حذف در هم نهشتی ها برای هر عدد که نسبت به پیمانه اول باشند، برقرار است.

$$ac \equiv bc \pmod{m} \text{ و } (c, m) = 1 \Rightarrow a \equiv b \pmod{m}$$





مثال: به ازای کدام مقادیر n از اعداد طبیعی، عدد $2^{10n+2} + 2^{5n+1} - 1$ بر ۱۱

بخش پذیر است؟

پاسخ: توانی از ۲ که نزدیک مضارب ۱۱ باشد 2^5 است.

$$2^5 \equiv -1 \xrightarrow{\text{توان } n} 2^{5n} \equiv (-1)^n \xrightarrow{\times 2} 2^{5n+1} \equiv (-1)^n \times 2$$

اگر دوباره آن را به توان ۲ برسانیم، می شود: $2^{10n+2} \equiv 4$

$$\text{پس شد: } 2^{10n+2} + 2^{5n+1} - 1 \equiv 4 + (-1)^n \times 2 - 1$$

اگر n فرد باشد $4 + (-1)^n \times 2 - 1 = 0$ می شود. یعنی آن عبارت بر ۱۱ بخش-

پذیر است.

کاربردهای هم نهشتی:

((پیدا کردن باقی مانده بر 2^3 و 5^9 و 11^1 بدون انجام عمل تقسیم))

عدد نویسی را بر مبنای ده دهی انجام می دهیم و برای باز کردن یک عدد از توان های

مختلف ۱۰ استفاده می کنیم.





__مثال:

$$1254317 = 7 + 1 \times 10 + 3 \times 10^2 + 4 \times 10^3 + 5 \times 10^4 + 2 \times 10^5 + 1 \times 10^6$$

به طور کلی یک عدد را به صورت $A = \overline{a_n \dots a_2 a_1 a_0}$ در نظر بگیریم. این عدد را می-

توان به صورت زیر بسط داد:

$$A = \overline{a_n \dots a_2 a_1 a_0} = a_0 + 10 a_1 + 10^2 a_2 + \dots + 10^n a_n$$

برای به دست آوردن باقی مانده بر چند عدد خاص، دستورهایی وجود دارد که می توان از آن ها استفاده کرد.

باقی مانده بر ۲ یا ۵ یا ۱۰:

به باز شده عدد $\overline{a_n \dots a_2 a_1 a_0}$ توجه کنید

$$a_0 + \underbrace{10 a_1 + 10^2 a_2 + \dots + 10^n a_n}_{\text{بر } 10^2 \text{ و } 10 \text{ بخش پذیرند}}$$

بنابراین برای پیدا کردن باقی مانده یک عدد بر ۲ یا ۵ یا ۱۰ کافی است به جای کل عدد،

باقی مانده یکان آن را بر عدد خواسته شده به دست آورد.





مثال: $۱۳۷۵ \equiv ? \leftarrow ۷۵۲$

باقی مانده بر ۳ یا ۹:

باز هم عدد $\overline{a_n \dots a_2 a_1 a_0}$ را به صورت زیر باز می کنیم:

$$\begin{aligned} & a_0 + 10a_1 + 10^2a_2 + \dots + 10^na_n \\ &= a_0 + (a_1 + \underline{9a_1}) + (a_2 + \underline{99a_2}) + \dots \end{aligned}$$

جملاتی که زیر آن ها خط کشیده شده است بر ۳ یا ۹ بخش پذیرند بنابراین باقی مانده

آن ها در تقسیم بر ۳ یا ۹ صفر می شود پس باقی مانده کل عدد بر ۳ یا ۹ برابر است با

باقی مانده مجموع جمله های باقی مانده.

$$\overline{a_n \dots a_2 a_1 a_0} \stackrel{۳ \text{ یا } ۹}{\equiv} a_0 + a_1 + a_2 + \dots + a_n$$

مثال: $۱۳۹۸ \equiv ? \leftarrow ۱ + ۳ + ۹ + ۸ \equiv ۰$





باقی مانده بر ۱۱:

باز هم عدد $\overline{a_n \dots a_2 a_1 a}$ را به صورت زیر باز می کنیم

$$\begin{aligned} & a. + 10 a_1 + 10^2 a_2 + \dots + 10^n a_n \\ &= a. + (\underline{11} a_1 - a_1) + (\underline{99} a_2 + a_2) + (\underline{1001} a_3 - a_3) \\ &+ \dots \end{aligned}$$

عددهایی که زیر آن ها خط کشیده شده است بر ۱۱ بخش پذیرند. پس برای به دست

آوردن باقی مانده عددی بر ۱۱ از سمت راست، یک در میان عددی را منفی و مثبت کرده

و باقی مانده را بر ۱۱ به دست می آوریم.

مثال: $2415 \equiv 5 - 1 + 4 - 2 \equiv 6$

معادله هم نهشتی:

تعریف: یک رابطه هم نهشتی همراه با مجهولی چون x به فرم $ax \equiv b$ را یک معادله

هم نهشتی می نامیم و منظور از حل معادله هم نهشتی پیدا کردن همه جواب هایی چون $\in$

$\mathbb{Z}$. x است که در این معادله صدق کند.



پاسخ: اگر آن عدد را ط فرض کنیم باید $۱۳ - ۷۱۳x \equiv ۱۳ \pmod{۳}$ یا $۳x \equiv ۱۳ \pmod{۳}$

قضیه: معادله هم نهشتی $ax \equiv b \pmod{m}$ دارای جواب است اگر و فقط اگر $(a, m) | b$

جواب است.

تعریف: این معادله $ax + by = c$ که x, y در اعداد صحیح جواب های آن هستند و

$a, b, c \in \mathbb{Z}$ صورت را یک معادله سیاله درجه اول یا خطی می‌نامیم.





تبدیل یک معادله سیاله به معادله هم نهشتی:

$$ax + by = c \Rightarrow ax - c = (-b)y \Rightarrow b|ax - c \\ \Rightarrow ax \equiv c \pmod{b} \text{ و } by \equiv c \pmod{a}$$

نکته: با توجه به قضیه قبل نتیجه میگیریم که شرط لازم و کافی برای آنکه معادله سیاله

$$ax + by = c \text{ دارای جواب باشد آن است که } (a, b) | c$$

مثال: تیراندازی به سمت یک هدف شامل دو دایره هم مرکز تیراندازی می کند اگر او

تیر را به دایره با شعاع کوچکتر بزند ۵ امتیاز و اگر به دایره بزرگتر بزند ۳ امتیاز

می گیرد . اگر او کمتر از ۱۵ تیر انداخته و همه تیرها به داخل دایره بزرگتر اصابت

کرده باشد و در پایان ۴۲ امتیاز گرفته باشد، چند حالت برای او در این تیراندازی می تواند

ثبت شود.

$$5x + 3y = 42 \Rightarrow 5x \equiv 42 \pmod{3}$$

$$5x \equiv 42 + 3 \pmod{3} \Rightarrow 5x \equiv 5 \times 9 \pmod{3} \Rightarrow x = 3k + 9, y = -5k - 1$$

$$x, y \in \mathbb{W} \Rightarrow k = \{-1, -2, -3\} \Rightarrow \begin{cases} x = 6 \\ y = 4 \end{cases} \text{ و } \begin{cases} x = 3 \\ y = 9 \end{cases} \text{ و } \begin{cases} x = 0 \\ y = 14 \end{cases}$$

($y=4, x=6$ یعنی تیرانداز ۶ تیر به دایره کوچکتر و ۴ تیر به دایره بزرگتر زده است.)





__مثال: به چند طریق می توان با ۳۷۰۰ ریال ، تمبرهای ۱۵۰ ریالی و ۲۵۰ ریالی خرید.

پاسخ: تعداد تمبرهای ۱۵۰ ریالی را x و تعداد تمبرهای ۲۵۰ ریالی را y نشان می دهیم

$$150x + 250y$$

$$= 3700$$

بر ۵۰ ساده می کنیم

$$\xrightarrow{\text{ساده}} 3x + 5y = 74 \rightarrow 5y \overset{\text{ساده}}{\equiv} 74 \rightarrow 2y \overset{\text{ساده}}{\equiv} 2$$

$$\rightarrow y \overset{\text{ساده}}{\equiv} 1 \Rightarrow y = 3k + 1$$

$$3x + 5(3k + 1) = 74 \Rightarrow 3x + 15k + 5 = 74 \Rightarrow 3x = 69 - 15k$$

$$\Rightarrow x = 23 - 5k$$

$$\begin{cases} x \geq 0 \Rightarrow 23 - 5k \geq 0 \Rightarrow k \leq 4/5 \\ y \geq 0 \Rightarrow 3k + 1 \geq 0 \Rightarrow k \geq -1/3 \end{cases} \Rightarrow k = 0, 1, 2, 3, 4$$

