سایت ویژه ریاضیات www.riazisara.ir

درســـنامه ها و جـــزوه های ریاضـــی

سوالات و پاسخنامه تشریحی کنکور

نمونه سوالات امتحانات ریاضی

نرم افزارهای ریاضیات

و...

فصل چهاردهم
برهان عکس نقیض
Contrapositive Proof
بخش اول
برهان عکس نقیض

در مقابل برهان مستقیم ، به شکل ثانوی یا شکل متناوب آن یعنی برهان عکس نقیض یا به قول اهل منطق ، برهان عکس بر عکس ، می پردازیم. مانند برهان مستقیم ، برهان عکس نقیض برای برهان گزاره های شرطی اگر p پس q بکار برده می شود. اگر چه ممکن است در مواردی بکار بردن برهان مستقیم ممکن باشد ، اما مواردی هم پیش می آید که بکار بردن برهان عکس نقیض ، آسان تر است.

کلمات برهان عکس نقیض Contrapositive Proof با برهان خلف Converse Proof اشتباه نکنید.

۱۴.۱ - برهان عکس نقیض Contrapositive Proof

برای درک این که برهان عکس نقیض کار می کند ، فرض کنید می خواهیم حکم زیر را ثابت کنیم.

حکم : اگر P پس Q .

این یک گزاره شرطی است به شکل $P \Rightarrow Q$

هدف این است که نشان دهیم این گزاره شرطی صحیح است. بخاطر آورید که در بخش ۳.۶ گفتیم $P \Rightarrow Q$ از نظر منطقی معادل $\sim P \Rightarrow \sim Q$ است. برای راحتی شما ، جدول درستی مربوطه را در زیر می آوریم.

P	Q	$\sim Q$	$\sim P$	$P \Rightarrow Q$	$\sim Q \Rightarrow \sim P$
T	T	F	F	**T**	**T**
T	F	T	F	**F**	**F**
F	T	F	T	**T**	**T**
F	F	T	T	**T**	**T**

بر اساس جدول بالا ، $P \Rightarrow Q$ و $\sim P \Rightarrow \sim Q$ دو راه متفاوت برای بیان یک چیز است. عبارت $\sim P \Rightarrow \sim Q$ **شکل عکس بر عکس** $P \Rightarrow Q$ است.

چون $P \Rightarrow Q$ از نظر منطقی معادل $\sim P \Rightarrow \sim Q$ است ، پس برای این که ثابت کنیم $P \Rightarrow Q$ صحیح است ، کافی است ثابت کنیم $\sim P \Rightarrow \sim Q$ صحیح است. اگر می خواستیم برهان مستقیم را بکار بریم که ثابت کنیم $\sim P \Rightarrow \sim Q$ صحیح است ، باید فرض می کردیم $\sim Q$ صحیح است و آنرا

بکار بریم و نتیجه بگیریم $P \sim$ صحیح است. این در حقیقت روش اصلی برهان عکس نقیض است. به صورت زیر خلاصه می کنیم.

حکم اگر P پس Q.
برهان : فرض می کنیم $Q \sim$.
⋮
پس $P \sim$.

پس ترتیب نوشتن برهان عکس نقیض خیلی ساده است. اولین خط برهان جمله فرض می کنیم Q صحیح نیست. آخرین خط جمله لذا P صحیح نیست ، است. بین خط اول و خط آخر ، منطق و تعریف ها را بکار می بریم تا $Q \sim$ را به $P \sim$ تبدیل کنیم.
برای توضیح بیشتر ، حکم زیر را به دو طریق برهان مستقیم و برهان عکس نقیض ، ثابت می کنیم.

حکم فرض کنید $x \in \mathbb{Z}$ باشد. اگر $7x + 9$ زوج باشد ، پس x فرد است.
برهان مستقیم
فرض می کنیم $7x + 9$ زوج باشد.
پس $7x + 9 = 2a$ است، برای یک عدد صحیح a .
از طرفین معادله بالا ، $6x + 9$ کسر می کنیم ، پس $x = 2a - 6x - 9$ بدست می آوریم.
پس $x = 2a - 6x - 9 = 2a - 6x - 10 + 1 = 2(a - 3x - 5) + 1$ بدست آوریم.
در نتیجه $x = 2b + 1$ است. اینجا $b = a - 3x - 5 \in \mathbb{Z}$ است.
پس x فرد است.

برهان عکس نقیض حکم بالا
فرض می کنیم x فرد نیست.
پس x زوج است ، یعنی $x = 2a$ است برای یک عدد صحیح a .
پس $7x + 9 = 7(2a) + 9 = 14a + 8 + 1 = 2(7a + 4) + 1$
پس $7x + 9 = 2b + 1$ است. اینجا b عدد صحیح $7a + 4$ است.
نتیجه می گیریم $7x + 9$ فرد است.
لذا $7x + 9$ زوج نیست.

اگر چه طول هرد دو برهان یکسان است ، ممکن است احساس کنید ، برهان عکس نقیض ، روان تر پیش می رود. زیرا برگرداندن اطلاعات از x به $7x + 9$ آسان تر است.

حکم : اگر $x^2 - 6x + 5$ زوج باشد ، پس x فرد است.

برهان مستقیم مساله ساز است. باید این گونه شروع کنیم که فرض کنیم $x^2 - 6x + 5$ زوج است ، پس $x^2 - 6x + 5 = 2a$ است. سپس باید بگوییم $x = 2b + 1$ است برای $b \in \mathbb{Z}$. اما این

کاملا واضح نیست این کار را چگونه می توان انجام داد. زیرا لازم می شود x را از عبارت درجه دوم کنار بگذاریم. اما، اگر برهان عکس نقیض بکار بریم . کار ما خیلی ساده می شود.

حکم : فرض کنید $x \in \mathbb{Z}$ باشد. اگر $x^2 - 6x + 5$ زوج باشد ، پس x فرد است.
برهان از طریق عکس نقیض
فرض می کنیم x فرد نباشد.
پس x زوج است ، و لذا $x = 2a$ است برای یک عدد صحیح a.
پس داریم.

$$x^2-6x+5 = (2a)^2-6(2a)+5 = 4a^2-12a+5 = 4a^2-12a+4+1 = 2(2a^2-6a+2)+1.$$

لذا $x^2 - 6x + 5 = 2b + 1$ است. اینجا b عدد صحیح $2a^2 - 6a + 2$ است.
در نتیجه $x^2 - 6x + 5$ فرد است.
لذا $x^2 - 6x + 5$ زوج نیست.

خلاصه ، چون x فرد نیست $(\sim Q)$ نتیجه می شود $x^2 - 6x + 5$ زوج نباشد $(\sim P)$, پس چون $x^2 - 6x + 5$ زوج است (P) یعنی x فرد است (Q) . پس با اثبات $\sim P \Rightarrow \sim Q$ گزاره $P \Rightarrow Q$ را ثابت کردیم.
مثال دیگر.

حکم : فرض کنید $x, y \in \mathbb{R}$ باشد. اگر $y^3 + yx^2 \leq x^3 + xy^2$ باشد ، پس $y \leq x$ است.
برهان از طریق عکس نقیض
فرض می کنیم $y \leq x$ صحیح نباشد ، پس $y > x$ است.
لذا $y - x > 0$ است. طرفین را در $x^2 + y^2$ که مثبت است ، ضرب می کنیم.

$$\begin{aligned}(y-x)(x^2+y^2) &> 0(x^2+y^2)\\ yx^2+y^3-x^3-xy^2 &> 0\\ y^3+yx^2 &> x^3+xy^2\end{aligned}$$

پس $y^3 + yx^2 > x^3 + xy^2$ است. پس $y^3 + yx^2 \leq x^3 + xy^2$ صحیح نیست.

اثبات اگر P پس Q از طریق عکس نقیض الزاما شامل گزاره های منفی $\sim P$ و $\sim Q$ است. پس در این گونه موارد ، لازم است قواعد دو مورگان را بکار بریم. یک مثال از این نمونه را می آوریم.

حکم : فرض کنید $x, y \in \mathbb{Z}$ باشد. اگر $5|xy$ پس $5|x$ و $5|y$.
برهان از طریق عکس نقیض.

فرض می کنیم $5|x$ **و** $5|y$ صحیح نباشد.

بر اساس قانون دو مورگان $5|x$ **یا** $5|y$ صحیح نیست.

پس $۵|x$ یا $۵|y$ ۰ دو حالت پیش می آید.
حالت اول : فرض می کنیم $۵|x$, پس $x = ۵a$ برای یک $a \in \mathbb{Z}$ ۰
از این موضوع نتیجه می گیریم $xy = ۵(ay)$ یعنی $۵|xy$ ۰
حالت دوم : فرض می کنیم $۵|y$, پس $y = ۵a$ برای یک $a \in \mathbb{Z}$ ۰
از این موضوع نتیجه می گیریم $xy = ۵(ax)$ یعنی $۵|xy$ ۰
حالت های بالا نشان می دهند که $۵|xy$, پس $۵ \nmid xy$ صحیح نیست.

فراموش نشود نماد $\nmid$ یعنی عاد نمی کند.

۱۴.۲ - همنهشتی اعداد صحیح Congruence of Integers

حالا وقت آن فرا رسیده که یک تعریف دیگر معرفی کنیم. الزاما ، مربوط به برهان عکس نقیض نمی‌شود. اما معرفی آن حالا ، به ما کمک می کند که بتوانیم روش های متعدد برهان را در آینده بررسی کنیم. این تعریف جدید در بسیاری از رشته های ریاضی نقش مهمی دارد.

تعریف ۱۴.۲.۱
اگر اعداد صحیح $a,b.c$ و یک $n \in \mathbb{N}$ داشته باشیم ، دو عدد a و b **را به پیمانه n همنهشت یا هم باقیمانده** می گوییم اگر $n|(a-b)$ و آنرا چنین می نویسیم.
$$a \equiv b(mod\ n)$$
اگر a و b به پیمانه n همنهشت نباشند ، می نویسیم $a \not\equiv b(mod\ n)$.

مثال ۱۴.۲.۱

۱) $۹ \equiv ۱(mod\ ۴)$ زیرا $۴|(۹-۱)$
۲) $۶ \equiv ۱۰(mod\ ۴)$ زیرا $۴|(۶-۱۰)$
۳) $۱۴ \not\equiv ۸(mod\ ۴)$ زیرا $۴ \nmid (۱۴-۸)$
۴) $۲۰ \equiv ۴(mod\ ۸)$ زیرا $۸|(۲۰-۴)$
۵) $۱۷ \equiv -۴(mod\ ۳)$ زیرا $۳|(۱۷-(-۴))$

عملا ، $a \equiv b(mod\ n)$ یعنی اگر a و b را بر n تقسیم کنیم ، دارای باقیمانده های مساوی هستند. مثلا ، در بالا دیدیم $۶ \equiv ۱۰(mod\ ۴)$ است. در حقیقت, اگر ۶ را بر ۴ تقسیم کنیم ، خارج قسمت ۱ است وباقیمانده ۲ است. به همین طریق ، اگر ۱۰ را بر ۴ تقسیم کنیم ، خارج قسمت ۲ است و باقیمانده ۲ .

$$۶ \div ۴ = ۴ * ۱ + ۲$$
$$۱۰ \div ۴ = ۴ * ۲ + ۲$$

همچنین دیدیم $۱۴ \not\equiv ۸(mod\ ۴)$ زیرا

$$۱۴ \div ۴ = ۳ * ۴ + ۲$$
$$۸ \div ۴ = ۲ * ۴ + ۰$$

برای این که ببینید این موضوع صحت دارد ، توجه کنید که اگر a و b هنگامی که بر n تقسیم می شوند دارای باقیمانده های مساوی هستند ، فرض کنید $a = kn + r$ و $b = ln + r$ باشد ، برای $k,l \in \mathbb{Z}$ پس داریم $a - b = (kn + r) - (ln + r) = n(k - l)$
حالا $a - b = n(k - l)$ یعنی $n|(a - b)$ ، پس $a \equiv b\ (mod\ n)$.

این بخش را با چند برهان که شامل همنهشتی اعداد صحیح است ، به پایان می رسانیم.

حکم : فرض کنید $a,b \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b(mod\ n)$ باشد ، پس $a^۲ \equiv b^۲(mod\ n)$ است.

برهان مستقیم.

فرض می کنیم $a \equiv b(mod\ n)$ باشد.

بر اساس تعریف همنهشتی اعداد صحیح ، این یعنی $n|(a-b)$.

پس , بر اساس تعریف بخش پذیری ، یک عدد صحیح c وجود دارد بطوری که $a-b=nc$ است.

حالا طرفین این تساوی را در $a+b$ ضرب میی کنیم.

$$\begin{aligned} a-b &= nc \\ (a-b)(a+b) &= nc(a+b) \\ a^2-b^2 &= nc(a+b) \end{aligned}$$

چون $c(a+b) \in \mathbb{Z}$ است ، تساوی بالا به ما می گوید $n|\left(a^۲-b^۲\right)$.

بر اساس تعریف ۱۴.۲.۱ داریم $a^۲ \equiv b^۲(mod\ n)$.

اجازه دهید روی مفهوم حکم بالا کمی دقت کنیم. حکم می گوید $a \equiv b(mod\ n)$ دلالت می کند $a^۲ \equiv b^۲(mod\ n)$. به عبارت دیگر ، می گوید اگر اعداد صحیح a و b هنگام تقسیم بر n دارای باقیمانده های مساوی باشند ، پس $a^۲$ و $b^۲$ هم اگر بر n تقسیم شوند دارای باقیمانده های مساوی هستند. این حکم قول می دهد که این اتفاق برای تمام a,b,n ها رخ می دهد. در مثال ها ، هدف ما بیشتر معطوف است به چگونگی برهان حکم ها ، تا مفهوم حکم ها. اما گاهی هم مفید خواهد بود که هم به مفهوم حکم توجه کنیم و هان به طریق برهان.

حکم : فرض می کنیم $a,b,c \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b(mod\ n)$ باشد ، پس داریم $ac \equiv bc(mod\ n)$.

برهان مستقیم.

فرض می کنیم $a \equiv b(mod\ n)$ باشد. بر اساس تعریف ، داریم $n|(a-b)$. لذا بر اساس تعریف تقسیم پذیری ، یک عدد صحیح k وجود دارد ، بطوری که $a-b=nk$ است. طرفین را در c ضرب می کنیم ، پس داریم $ac-bc=nkc$. پس $ac-bc=n(kc)$ ، اینجا $kc \in \mathbb{Z}$ است. یعنی $n|(ac-bc)$.

بر اساس تعریف همنهشتی اعداد صحیح داریم. $ac \equiv bc(mod\ n)$ است.

در مثال بعدی ، برهان عکس نقیض بهتر به نظر می رسد ، زیرا نماد های $\nmid$ و $\not\equiv$ را حذف می کند.

حکم فرض کنید $a,b \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $۱۲a \not\equiv ۱۲b(mod\ n)$, پس $n \nmid ۱۲$.

برهان عکس نقیض

فرض می کنیم $n|۱۲$, پس یک عدد صحیح c وجود دارد بطوری که $۱۲=nc$ است. حالا ، مطابق زیر دلیل ادامه می دهیم.

$$\begin{aligned} 12 &= nc \\ 12(a-b) &= nc(a-b) \\ 12a-12b &= n(ca-cb) \end{aligned}$$

چون $ca-cb \in \mathbb{Z}$ است ، معادله $12a-12b=n(ca-cb)$ دلالت می کند که $n|(12a-12b)$.

پس در نتیجه $12a \equiv 12b(mod\ n)$.

۱۴.۳ ـ نوشتن دقیق و صحیح Mathematical Writing

به تیتر این بخش و ترجمه انگلیسی آن به فارسی توجه کنید. کلمه Mathematical را ترجمه کرده ایم **دقیق و صحیح.** در حقیقت کار با ریاضیات احتیاج به دقت دارد و همچنین ریاضیات علم دقت است. پس نوشتن ریاضیاتی یعنی نوشتن دقیق و صحیح.

حالا که شروع به نوستن برهان ها کرده ایم ، وقت مناسبی است که روی هنر نوشتن دقت کنیم. بر خلاف منطق و ریاضیات ، که در آنها ، دقیقا تفاوت آشکاری بین صحیح و غلط وجود دارد ، اما تفاوت بین خوب یا بد نوشتن بیشتر بستگی به عقیده اشخاص دارد. یک جمله ممکن است به نظر من یک جمله صحیح باشد ، ولی شما فکر می کنید این جمله من صحیح نیست و یا این که مطلب را واضح و آشکار بیان نمی کند. اما ، چند روش استاندارد وجود دارد که نوشته شما واضح تر شود.

۱ – پایان هر جمله یک نقطه بگذارید ، حتی اگر آن جمله به یک عبارت یا نماد ریاضی ختم شود.

اویلر ثابت کرد که $\sum_{k=1}^{\infty} \frac{1}{k^n} = \prod_{p \in P} \frac{1}{1-\frac{1}{p^2}}$ جمله خوبی نیست ، زیرا ممکن است با جمله بعد از آن اشتباه شود.

اویلر ثابت کرد که $\sum_{k=1}^{\infty} \frac{1}{k^n} = \prod_{p \in P} \frac{1}{1-\frac{1}{p^2}}$. جمله خوبی است ، زیرا با جمله بعدی اشتبا ه نمی شود.

۲ ـ جمله را با یک کلمه شروع کنید ، نه با یک نماد یا عبارت ریاضی.

A یک زیر مجموعه B است. جمله خوبی نیست.

مجموعه A یک زیر مجموعه B است. جمله خوبی است.

a یک عدد صحیح است ، پس $2x + 5$ یک عدد صحیح است. خوب نیست.

چون x یک عدد صحیح است ، پس $2x + 5$ یک عدد صحیح است. خوب است.

$x^2 - x + 2 = 0$ دو ریشه دارد. خوب نیست.

معادله $x^2 - x + 2 = 0$ دو ریشه دارد. خوب است.

۳ ـ نماد ها و عبارت های ریاضی را از کلمات جدا کنید. اگر این کار نکنید ، ممکن است عبارت ها با هم مخلوط شوند و ایجاد ابهام کند.

چون $x^2 - 1 = 0$, $x = 1$, $x = -1$. خوب نیست.

چون $x^2 - 1 = 0$ است ، پس $x = -1$ یا $x = 1$ است.

بر خلاف $A \cup B$, $A \cap B$ مساوی $\emptyset$ است. جمله خیلی بدی است ، اصلا قابل فهم نیست.

بر خلاف $A \cup B$, مجموعه $A \cap B$ مساوی $\emptyset$ است. جمله خوبی است. قابل فهم است.

۴ - از بکار بردن غلط نماد ها دوری کنید. نماد های $=, \leq, \geq, \in, \subseteq$ و غیرو ، کلمات نیستند. بکار بردن این نماد ها در عبارت های ریاضی ، مناسب است ، اما بکار بردن آنها در متن ، صحیح نیست.

چون این دو مجموعه $=$ هستند ، یکی زیر مجموعه دیگری است. خیلی بد.
چون دو مجموعه مساوی هستند ، یکی زیر مجموعه دیگری است.

مجموعه تهی $\subseteq$ یک زیر مجموعه هر مجموعه ای است. بد.
مجموعه تهی یک زیر مجموعه هر مجموعه ای است. خوب.

چون a فرد است و x فرد $\Leftarrow$ $x^۲$ فرد است ، $a^۲$ فرد است. بد.
چون a فرد است و هر عدد فردی مربع شود فرد است ، پس $a^۲$ فرد است. خوب.

۵ - از بکار بردن نماد های غیر ضروری دوری کنید.

هیچ مجموعه X دارای اندازه منفی نیست. بد.
هیچ مجموعه ای دارای اندازه منفی نیست. خوب.

۶ - بهتر است بجای وجه مجهول ، وجه معلوم بکار برید.

مقدار $x = ۳$ از طریق تقسیم طرفین بر ۵ بدست آمده است. بد.
با تقسیم طرفین بر ۵ , مقدار $x = ۳$ بدست می آوریم.

۷ - هر نماد جدید را توضیح دهید. هنگام نوشتن برهان ، باید مفهوم هر نماد جدیدی را که معرفی می کنید ، توضیح دهید.

چون $a|b$, نتیجه می گیریم $b = ac$ است. خواننده نمی فهمد c یک عدد صحیح است یا یک عدد طبیعی و غیرو.
چون $a|b$ نتیجه می گیریم $b = ac$ است ، اینجا c یک عدد صحیح است. حالا خوانند می فهمد عدد c چه نوع عددی است. مثلا ۲ می تواند هم یک عدد صحیح تلقی شود و هم یک عدد طبیعی ، اما ، ۲− عدد طبیعی نیست.

۸ - مواظب بکار بردن ضمیر باشد.
چون $X \subseteq Y$ و $0 < |X|$ می بینیم که آن تهی نیست. واضح نیست کدام مجموعه تهی نیست X یا Y. پس جمله خوبی نیست.
چون $X \subseteq Y$ است ، و $0 < |X|$, می بینیم که Y تهی نیست. حالا خواننده می فهمد کدام مجموعه تهی نیست.

۹ - در بکار بردن حروف ربط چون ، زیرا ، پس , دقت کنید.

چون P, Q با اگر P پس Q فرق دارد.

$x \in \mathbb{N}$ پس $x \in \mathbb{Z}$ خوب نیست.
چون $x \in \mathbb{N}$ پس $x \in \mathbb{Z}$ خوب است.

در خاتمه باید هنگام نوشتن برهان ، از هر گونه ابهام دوری کنید. در بالا فقط نمونه ای بود از بسیار.

۱۴.۴ - الگوریتم اقلیدوس The Euclidian Algorithm

برهان ها و الگوریتم ها به طرق مختلف با هم تداخل دارند. همان طور که خواهیم دید ، شخص می تواند ثابت کند که یک الگوریتم درست کار می کند. از طرف دیگر ، حکم ها و قضیه ها ثابت شده اند تا در الگوریتم ها بکار روند. در این بخش به این موضوع می پردازیم. یعنی الگوریتم معروف اقلیدوس برای پیدا کردن بزرگ ترین مقسوم علیه مشترک دو عدد.

این الگوریتم بنام اقلیدوس نام گذاری شده است. او این الگوریتم را ۲ ۰۰۰ سال پیش به ثبت رسانید.

حکم : اگر a و b اعداد صحیح باشند ، پس $gcd(a,b) = gcd(a-b,b)$.

برهان مستقیم.

فرض می کنیم $a,b \in \mathbb{Z}$ باشند. ابتدا ثابت می کنیم $gcd(a,b) \leq gcd(a-b,b)$ است ، سپس ثابت می کنیم $gcd(a,b) \geq gcd(a-b,b)$ است. این دو با هم نشان می ددهد که $gcd(a,b) = gcd(a-b,b)$ است.

پس اجازه دهید ثابت کنیم $gcd(a,b) \leq gcd(a-b,b)$ است. فرض می کنیم $d = gcd(a,b)$ باشد. چون d مقسوم علیه هم a است و هم b, پس داریم $a = dx$ و $b = dy$ است برای اعداد صحیح x و y. پس $a - b = dx - dy = d(x-y)$, این یعنی d عدد $a-b$ را عاد یا تقسیم می کند. لذا d مقسوم علیه هم $a-b$ است و هم b. اما این d نمی تواند بزرگ تر از بزرگ ترین مقسوم علیه مشترک $a-b$ و b باشد ، که باید بگوییم

$$gcd(a,b) = d \leq gcd(a-b,b)$$

است.

حالا فرض می کنیم $e = gcd(a-b,b)$ باشد. پس e هم $a-b$ را عاد می کند و هم b. پس $a - b = ex$ است و $b = ey$ است برای اعداد صحیح x و y. پس داریم

$$a = (a-b) + b = ex + ey = e(x+y)$$

پس ، حالا می بینیم e مقسوم علیه هم a است و هم b. اما بزرگ تر از بزرگ ترین مقسوم علیه مسترک $gcd(a-b,b) = e \leq grd(a,b)$ نیست.

این دو برهان های بالا نشان می دهد $gcd(a,b) = gcd(a-b,b)$ است.

این حکم یعنی اگر بخواهیم $gcd(a,b)$ را محاسبه کنیم ، همان پاسخی را بدست می آوریم اگر $gcd(a-b,b)$ محاسبه کنیم. محاسبه اخری آسان تر است ، زیرا شامل اعداد کوچک تر است.

مثلا اگر بخواهیم $gcd(۳۰,۱۲)$ را محاسبه کنیم ، حکم میگوید

$$gcd(۳۰,۱۲) = gcd(۳۰-۱۲,۱۲) = gcd(۱۸,۱۲)$$

است. پس باید $gcd(۱۸,۱۲)$ را محاسبه کنیم. پس مساله را به پیدا کردن $gcd(۱۸,۱۲)$ تقلیل دادیم. پس می توانیم این کار را تکرار کنیم تا

$$gcd(۱۸,۱۲) = gcd(۱۸-۱۲,۱۲) = gcd(۶,۱۲)$$

بدست آوریم. اگر این کار را برای مرتبه سوم تکرار کنیم ،مقدار ۱۲ — ۶ بدست می آوریم. اما می توانیم جای اعداد را عوض کنیم تا $gcd(۶,۱۲) = gcd(۱۲,۶)$ بدست آوریم. حالا حکم را دو مرتبه روی این عبارت آخر

بکار می بریم. تا نتیجه زیر را بدست آوریم.

$$\gcd(12,6) = \gcd(12-6,6) = \gcd(6,6) = \gcd(6-6,6) = \gcd(0,6) = 6.$$

بخاطر بیاورید که $gcd(0,۶) = ۶$ است ، زیرا هر عددی یک مقسوم علیه 0 است. اما بزرگ ترین مقسوم علیه ۶ خود عدد ۶ است. به همین طریق $gcd(0,b) = b$ اگر $b \neq 0$ باشد. با بکار بردن حکم ، چندین مرتبه نتیجه $gcd(۳0,۱۲) = ۶$ به ما داده است.

اجازه دهید به همین طریق $gcd(۳۱0,۹0)$ را محاسبه کنیم. شروع می کنیم به کسر کردن ۹0 از ۳۱0 تا $gcd(۴0,۹0)$ بدست آوریم. در این موقع $۹0 - ۴0$ منفی خواهد بود. پس ترتیب اعداد را عوض می کنیم تا $gcd(۹0,۴0)$ بدست آوریم. این روش را ادامه می دهیم.

$$\begin{aligned}
&\gcd(310,90)\\
=\ &\gcd(220,90)\\
=\ &\gcd(130,90)\\
=\ &\gcd(40,90)
\end{aligned}$$

اعداد را جابجا می کنیم.

$$\begin{aligned}
=\ &\gcd(90,40)\\
=\ &\gcd(50,40)\\
=\ &\gcd(10,40)
\end{aligned}$$

اعداد را جابجا می کنیم.

$$\begin{aligned}
=\ &\gcd(40,10)\\
=\ &\gcd(30,10)\\
=\ &\gcd(20,10)\\
=\ &\gcd(10,10)\\
=\ &\gcd(0,10)\\
=\ &\mathbf{10}
\end{aligned}$$

پس $gcd(۳۱0,۹0) = ۱0$ است.

در نهایت $gcd(0,۱0)$ بدست آوردیم و متوقف شدیم.

الگوریتم اقلیدوس دقیقا این الگو را اجرا می کند ، یعنی b را از a کم می کند تا $a < b$ بشود. سپس a و b را جا بجا می کند ، و این الگو را ادامه می دهد تا $a = 0$ بشود ، در این موقع به $gcd(0,b) = b$ رسیده ایم. این هم الگوریتم.

Algorithm 11: Euclidean Algorithm

Input: Two positive integers a and b.
Output: $\gcd(a,b)$
begin
  while $a \neq 0$ **do**
    if $a < b$ **then**
      $c := a$
      $a := b$
      $b := c$ } ..... swap a and b, so now $a \geq b$
    end
    while $a \geq b$ **do**
      $a := a - b$ ..... keep subtracting b from a until $a < b$
    end
  end
  output b
end

تصور می شود تا کنون بیشتر کلمات انگلیسی الگوریتم بالا را یاد گرفته اید. ترجمه چند کلمه دیگر در ذیل می آوریم تا شما بتدریج بتوانید برنامه های کامپیوتری به زبان انگلیسی بنویسید.

کم کردن ، کسر کردن :Subtract
جا بجا کردن :Swap
ادامه دادن :Continue
عدد صحیح :Integer
مثبت :Positive

حالا یک حکم را در ذیل می آوریم که ثابت می کند ، الگوریتم اقلیدوس پایان می پذیرد. یعنی تا بی نهایت ادامه ندارد.

حکم : اگر اعداد ورودی a و b مثبت باشند ، پس الگوریتم اقلیدوس خاتمه می یابد.
برهان مستقیم.
فرض می کنیم a و b اعداد مثبت باشند.
هنگامی که الگوریتم شروع می شود ، **حلقه مادامی که** اصلی **while loop** اولین تکرار خود را شروع می کند. زیرا $a \neq 0$ است.
اجازه دهید اولین تکرار این حلقه را پی گیری کنیم. اگر $a < b$ پس a و b را جا بجا می شوند.
در هر صورت بعد از فرمان if داریم $a \geq b$.
سپس ، در دومین حلقه مادمی که شروع می کند بطور مکرر b را از a کسر می کند ، تا زمانی که $a \geq b$ است.
چون $a \geq b$ است ، مقدار $a := a - b$ که به a داده می شود ، منفی نیست.

پس در پایان اولین تکرار داریم $0 \leq a < b$ ۰
اگر $a = 0$ باشد ، پس دیگر تکراری وجود ندارد و الگوریتم پایان می یابد.
در غیر این صورت در دومین تکرار a و b جا بجا می شوند ، زیرا $a < b$ است.
این کار مقدار b را کم می کند و سبب می شود $a \geq b$ بشود. سپس حلقه مادامی که داخلی مقدار a را کم می کند تا $a < b$ بشود.
اما ، $0 \leq a$ است زیرا عبارت $a := a - b$ فقط هنگامی انجام می شود اگر $a \geq b$ باشد.
پس بعد از دومین تکرار هم a و هم b کاهش می یابند و $0 \leq a < b$ ۰ است.
این روش در تمام تکرار های بعدی ادامه پیدا می کند. تکرار با $0 < a < b$ شروع می شود. سپس a و b جابجا می شوند ، مقدار b کم می شود. سپس a نقصان پیدا می کند تا $0 \leq a < b$ بشود.
پس در هر تکرار بعد از اولین تکرار ، مقدار هم a و هم b کم میشود تا $0 \leq a < b$ بشود.
لذا بعد از تعداد محدودی تکرار ، باید به $a = 0$ برسیم ، که در این موقع الگوریتم پایان می یابد.

توجه داشته باشید که الگوریتم اقلیدوس ، کار را با فقط یک عمل حساب یعنی تفریق انجام می دهد. چون عمل تفریق یک کار آسان است ، الگوریتم اقلیدوس سر راست، سریع با راندمان خوب است.

۱۴.۵- تمرینات فصل چهاردهم

با بکار بردن برهان عکس نقیض ، گزاره های زیر را ثابت کنید. اگر مایل بودید ، می توانید برهان مستقیم را هم اضافه کنید.

۱ - فرض کنید $n \in \mathbb{Z}$ باشد. اگر n^2 زوج باشد ، پس n زوج است.

۲ - فرض کنید $a, b \in \mathbb{Z}$ باشد. اگر $a^2\left(b^2 - 2b\right)$ فرد باشد ، پس a و b فرد هستند.

۳ - فرض کنید $x \in \mathbb{R}$ باشد. اگر $x^2 + 5x < 0$ باشد ، پس $x < 0$ است.

۴ - فرض کنید $a, b \in \mathbb{Z}$ باشد. اگر هم ab و هم $a + b$ زوج باشند ، پس هم a و هم b زوج هستند.

۵ - فرض کنید $n \in \mathbb{Z}$ باشد. اگر $3 \nmid n^2$ پس $3 \nmid n$.

۶ - فرض کنید $x, y \in \mathbb{Z}$ باشد. اگر $x^2(y + 3)$ زوج باشد .پس x زوج است یا y فرد.

۷ - فرض کنید $x \in \mathbb{R}$ باشد. اگر $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$ باشد ، پس $x \geq 0$ است.

۸ - فرض کنید $x \in \mathbb{Z}$ باشد. اگر $x^3 - 1$ زوج باشد ، پس x فرد است.

۹ - اگر n فرد باشد ، پس $8 \mid \left(x^2 - 1\right)$

۱۰ - فرض کنید $a, b \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b (mod\ n)$ و $a = c (mod\ n)$ باشد ، پس $c \equiv b (mod\ n)$ است.

۱۱ - فرض کنید $a, b \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b (mod\ n)$ باشد ، پس $a^3 \equiv b^3 (mod\ n)$ است.

۱۲ - فرض کنید $a, b, c \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b (mod\ n)$ باشد ، پس داریم

$$ca \equiv cb (mod\ n)$$

۱۳ - اگر $n \in \mathbb{N}$ و $2^n - 1$ اول باشد ، پس n اول است.

۱۴ - اگر $a \equiv 0 (mod\ 4)$ یا $a \equiv 1 (mod\ 4)$ باشد ، پس $\binom{a}{2}$ زوج است.

۱۵ - یک الگوریتم بازگشتی بنویسید که $gcd(a, b)$ را محاسبه کند.

پاسخ تمرینات فصل چهاردهم

با بکار بردن برهان عکس نقیض ، گزاره های زیر را ثابت کنید. اگر مایل بودید ، می توانید برهان مستقیم را هم اضافه کنید.

۱ - فرض کنید $n \in \mathbb{Z}$ باشد. اگر $n^۲$ زوج باشد ، پس n زوج است.

برهان عکس نقیض .

فرض می کنیم n زوج نباشد. پس n فرد است ، بطوری که $n = ۲a + ۱$ است برای یک عدد صحیح a, بر اساس تعریف عدد فرد.

پس $n^۲ = (۲a + ۱)^۲ = ۴a^۲ + ۴a + ۱ = ۲(۲a^۲ + ۲a) + ۱$ است.

در نتیجه $n^۲ = ۲b + ۱$ است ، اینجا b عدد صحیح $۲a^۲ + ۲a$ است ، پس $n^۲$ فرد است و لذا $n^۲$ زوج نیست.

۲ - فرض کنید $a, b \in \mathbb{Z}$ باشد. اگر $a^۲(b^۲ - ۲b)$ فرد باشد ، پس a و b فرد هستند.

برهان عکس نقیض.

فرض می کنیم a و b فرد نباشند. پس ، بر اساس قانون دو مورگان ، حد اقل یکی از a یا b زوج است. به این دو حالت جداگانه می پردازیم.

حالت اول : فرض می کنیم a زوج باشد . پس $a = ۲c$ است ، برای یک عدد صحیح c ۰

پس $a^۲(b^۲ - ۲b) = (۲c)^۲(b^۲ - ۲b) = ۲(۲c^۲(b^۲ - ۲b))$ که زوج است.

حالت دوم : فرض می کنیم b زوج باشد. پس $b = ۲c$ است برای یک عدد صحیح c ۰

لذا $a^۲(b^۲ - ۲b) = a^۲((۲c)^۲ - ۲(۲c)) = ۲(a^۲(۲c^۲ - ۲c))$ که زوج است.

۳ - فرض کنید $x \in \mathbb{R}$ باشد. اگر $x^۲ + ۵x < ۰$ باشد ، پس $x < ۰$ است.

برهان عکس نقیض .

فرض می کنیم $x < ۰$ نباشد ، پس $x \geq ۰$ است. پس نه $x^۲$ منفی است و نه $۰۵x$

پس $x^۲ + ۵x \geq ۰$ است. لذا $x^۲ + ۵x < ۰$ نیست.

۴ - فرض کنید $a, b \in \mathbb{Z}$ باشد. اگر هم ab و هم $a + b$ زوج باشند ، پس هم a و هم b زوج هستند.

برهان عکس نقیض .

فرض می کنیم صحیح نیست بگوییم هم a زوج است و هم b ۰

پس حد اقل یکی از آنها فرد است. سه حالت وجود دارد.

حالت اول : فرض می کنیم a زوج باشد و b فرد.

پس اعداد صحیح c و d وجود دارند بطوری که $a = ۲c$ و $b = ۲d + ۱$ است.

پس $ab = ۲c(۲d + ۱)$ است که زوج است و $a + b = ۲c + ۲d + ۱ = ۲(c + ۲) + ۱$

است که فرد است.
پس صحیح نیست بگوییم هم ab و هم $a+b$ زوج هستند.
حالت دوم : فرض می کنیم a فرد باشد و b زوج. پس اعداد صحیح c و d وجود دارند ، بطوری که $a=2c+1$ و $b=2d$ است.
پس $ab=(2x+1)(2d)=2\Big(d(2c+1)\Big)$ که زوج است.
و $a+b=2c+1+2d=2(c+d)+1$ که فرد است. پس صحیح نیست بگوییم هم ab و هم $a+b$ زوج هستند.
حالت سوم : فرض می کنیم a فرد باشد و b هم فرد. پس اعداد صحیح c و d وجود دارند ، بطوری که $a=2c+1$ و $b=2d+1$ است.
پس $ab=(2c+1)(2d+1)=4cd+2c+2d+1=2(2cd+c+d)+1$ که فرد است و $a+b=2c+1+2d+1=2(c+d+1)$ که زوج است.
پس صحیح نیست بگوییم هم ab و هم $a+b$ زوج هستند.

۵ - فرض کنید $n\in\mathbb{Z}$ باشد. اگر $3\nmid n^2$ پس $3\nmid n$.
برهان عکس نقیض.
فرض می کنیم صحیح نیست بگوییم $3\nmid n$ پس $3|n$ این یعنی $n=3a$ است برای یک عدد صحیح a. در نتیجه $n^2=9n^2$ است که از آن $n^2=3\Big(3a^2\Big)$ بدست می آوریم. این نشان می دهد که یک عدد صحیح $b=3a^2$ وجود دارد ، بطوری که $n^2=3b$ است ، یعنی $3|n^2$
لذا صحیح نیست بگوییم $3\nmid n^2$

۶ - فرض کنید $x,y\in\mathbb{Z}$ باشد. اگر $x^2(y+3)$ زوج باشد .پس x زوج است یا y فرد.
برهان عکس نقیض.
فرض می کنیم صحیح نیست بگوییم x زوج است یا y فرد.
با استفده از قانون دو مورگان ، این یعنی x زوج نیست و y فرد نیست. ، یعنی باید بگوییم x فرد است و y زوج.
پس اعداد صحیح a و b وجود دارند ، بطوری که $x=2a+1$ و $y=2b$
در نتیجه

$$x^2(y+3)=(2a+1)^2(2b+3)=(4a^2+4a+1)(2b+3)=$$
$$8a^2b+8ab+2b+12a^2+12a+3=8a^2b+8ab+2b+12a^2+12a+2+1=$$
$$2(4a^2b+4ab+b+6a^2+6a+1)+1.$$

این نشان می دهد $x^2(y+3)=2c+1$ است برای
$c=4a^2b+4ab+b+6a^2+1\in\mathbb{Z}$
لذا $x^2(y+3)$ زوج نیست.

۷ - فرض کنید $x \in \mathbb{R}$ باشد. اگر $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$ باشد ، پس $x \geq 0$ است.

برهان عکس نقیض.

فرض می کنیم صحیح نیست بگوییم $x \geq 0$ است. پس $x < 0$ است. یعنی x منفی است. در نتیجه عبارت های x^5 و $7x^3$ و $5x$ همه منفی هستند. پس $x^5 + 7x^3 + 5x < 0$ است. به همین طریق x^4 و x^2 همه مثبت هستند. پس $x^4 + x^2 + 8 > 0$ است.

از این $x^5 + 7x^3 + 5x < x^4 + x^2 + 8$ بدست می آوریم.

پس صحیح نیست بگوییم $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$ است.

۸ - فرض کنید $x \in \mathbb{Z}$ باشد. اگر $x^3 - 1$ زوج باشد ، پس x فرد است.

برهان نقیض عکس.

فرض می کنیم x فرد نیست. پس x زوج است ، لذا $x = 2a$ است برای یک عدد صحیح a.

پس $x^3 - 1 = (2a)^3 - 1 = 8a^3 - 1 = 8a^3 - 2 + 1 = 2(4a^3 - 1) + 1$

$x^3 - 1 = 2b + 1$ است ، اینجا $b = 4a^3 - 1 \in \mathbb{Z}$ است. پس $x^3 - 1$ فرد است. لذا $x^3 - 1$ زوج نیست.

۹ - اگر n فرد باشد ، پس $8 \mid (n^2 - 1)$

برهم مستقیم.

فرض می کنیم n فرد باشد ، پس $n = 2a + 1$ است برای یک عدد صحیح a. پس داریم

$n^2 - 1 = (2a + 1)^2 - 1 = 4a^2 + 4a = 4(a^2 + a) = 4a(a + 1)$ تا کنون داریم

$n^2 - 1 = 4a(a + 1)$, اما ، یک فاکتور ۸ می خواهیم ، نه یک فاکتور ۴.

اما توجه کنید که یکی از a یا $a + 1$ باید زوج باشد ، پس عبارت $a(a + 1)$ است. و لذا

$a(a + 1) = 2c$ است ، برای یک عدد صحیح c.

حالا داریم $n^2 - 1 = 4a(a + 1) = 4(2c) = 8c$

اما، $n^2 - 1 = 8c$ یعنی $8 \mid (n^2 - 1)$

۱۰ - فرض کنید $a, b \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b (mod\ n)$ و $a = c (mod\ n)$ باشد ، پس $c \equiv b (mod\ n)$ است.

برهان مستقیم.

فرض می کنیم $a \equiv b (mod\ n)$ و $a = c (mod\ n)$ باشد.

این یعنی $n \mid (a - b)$ و $n \mid (a - c)$

پس اعداد صحیح d و e وجود دارند بطوری که $a - b = nd$ و $a - c = ne$ است.

معادله دوم را از معادله اول کم می کنیم ، پس داریم $c - b = nd - ne$

پس $c-b=n(d-e)$ است و لذا بر اساس تعریف بخش پذیری $n|(c-b)$.
و در نهایت بر اساس تعریف همنهشتی داریم $c \equiv b(mod\ n)$.

۱۱ - فرض کنید $a,b \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b(mod\ n)$ باشد ، پس $a^3 \equiv b^3(mod\ n)$ است.

برهان مشتقیم.

فرض می کنیم $a \equiv b(mod\ n)$ باشد. این یعنی $n|(a-b)$, پس یک عدد صحیح c وجود دارد بطوری که $a-b=nc$ است. پس

$$\begin{aligned} a-b &= nc \\ (a-b)(a^2+ab+b^2) &= nc(a^2+ab+b^2) \\ a^3+a^2b+ab^2-ba^2-ab^2-b^3 &= nc(a^2+ab+b^2) \\ a^3-b^3 &= nc(a^2+ab+b^2). \end{aligned}$$

چون $a^2+ab+b^2 \in \mathbb{Z}$ است ، معادله $a^3-b^3=nc\left(a^2+ab+b^2\right)$ می گوید $n|\left(a^3-b^3\right)$ و لذا $a^3 \equiv b^3(mod\ n)$ است.

۱۲ - فرض کنید $a,b,c \in \mathbb{Z}$ و $n \in \mathbb{N}$ باشد. اگر $a \equiv b(mod\ n)$ باشد ، پس داریم $ca \equiv cb(mod\ n)$.

برهان مستقیم.

فرض می کنیم $a \equiv b(mod\ n)$ باشد. این یعنی $n|(a-b)$, پس یک عدد صحیح d وجود دارد بطوری که $a-b=nd$ است. طرفین را در c ضرب می کنیم تا $ac-bc=ndc$ بدست آید.
در نتیجه یک عدد صحیح $e=dc$ وجود دارد بطوری که $ac-bc=ne$ است ، پس $n|(ac-bc)$ و در نتیجه $ac \equiv bc(mod\ n)$ است.

۱۳ - اگر $n \in \mathbb{N}$ و 2^n-1 اول باشد ، پس n اول است.

برهان عکس نقیض.

فرض می کنیم n اول نباشد. می توان نوشت $n=ab$ است برای اعداد $a,b>1$. پس داریم.

$$2^n-1=$$
$$2^{ab}-1=\left(2^b-1\right)\left(2^{ab-b}+2^{ab-2b}+2^{ab-3b}+\cdots+2^{ab-ab}\right).$$

پس 2^n-1 عدد مرکب است.

۱۴ - اگر $a \equiv 0 (mod\ ۴)$ یا $a \equiv ۱ (mod\ ۴)$ باشد ، پس $\binom{a}{۲}$ زوج است.

برهان مستقیم.

فرض می کنیم $a \equiv 0 (mod\ ۴)$ باشد. پس $\binom{a}{۲} = \frac{a(a-۱)}{۲}$ است. چون $a = ۴k$ است برای یک $k \in \mathbb{N}$, پس داریم $\binom{a}{۲} = \frac{۴k(۴k-۱)}{۲} = ۲k(۴k-۱)$ پس $\binom{a}{۲}$ زوج است. حالا فرض می کنیم $a \equiv ۱ (mod\ ۴)$ باشد. پس $a = ۴k+۱$ است برای یک $k \in \mathbb{N}$ ۰

لذا $\binom{a}{۲} = \frac{(۴k+۱)(۴k)}{۲} = ۲k\,(۴k+۱)$ پس $\binom{n}{۲}$ زوج است. این مساله را ثابت می کند.

۱۵ - یک الگوریتم بازگشتی بنویسید که $gcd(a,b)$ را محاسبه کند.

باز گشتی یعنی از آخر به اول مراجعه می کنیم. مثلا

$$۵! = ۱ * ۲ * ۳ * ۴ * ۵ = ۵ * ۴ * ۳ * ۲ * ۱ = ۱۲۰$$

در الگوریتم باز گشتی از آخر شروع می کنیم و هر دومرتبه به اول الگوریتم بر می گردیم و آنرا صدا می کنیم.

```
Procedure Euclidean(a,b)
begin
    if a < b then
        c := a
        a := b
        b := c
    end
    if a = 0 then
        return b
    else
        return Euclidean(a − b,b)
    end
end
```

ملاحظه می کنید که در حلقه اگر اول متغیر ها را مقدار داده ایم. در حلقه اگر دوم گفته ایم اگر $a = 0$ باشد ، یعنی آخر خط باشیم ، کار تمام است در غیر این صورت بر می گردیم و الگوریتم را صدا می کنیم و دوباره شروع می کنیم. تا عمل پید کردن $gcd(a,b)$ خاتمه پیدا کند.