یک اول نظریه اعداد گروه ببعی، مبحث قضیه باقیمانده‌چینی

آرین همتی		مهنوش عظیمیان		ارشیا صادقی

منابع رنگی شده لینک های قابل کلیک هستند

چکیده

قضایا و احکام ریاضیات به طور کلی به دو دسته ساختاری و وجودی تقسیم می شوند. عده عظیمی از قضایای پرکاربرد در نظریه‌اعداد از نوع وجودی است که در آن وجود یا عدم وجود عضو یا ساختاری از یک مجموعه با سری معینی از ضوابط مدنظر است. قضیه باقیمانده‌چینی از قضایای پرکاربردی در نظریه‌اعداد و حساب پیمانه ایست که در مورد وجود یک عدد صحیح که در سیستمی از معادلات همنهشتی صدق کند بحث می‌کند. در ادامه با این قضیه و تعمیم های آن و کاربرد های آن در برخی مسائل ساختاری نظریه اعداد آشنا خواهیم شد.

قضیه ۱. برای اعداد صحیح m_1, m_2 که نسبت به هم اولند و اعداد صحیح دلخواه n_1, n_2، عدد صحیح یکتای $0 \leq x < m_1m_2$ وجود دارد که در معادلات همنهشتی زیر به طور همزمان صدق کند :

$$x \overset{m_1}{\equiv} n_1$$

$$x \overset{m_2}{\equiv} n_2$$

اثبات. مجموعه $R = \{tm_1 + n_1 \mid 0 \leq t < m_2\}$ را در نظر بگیرید. ثابت می کنیم این مجموعه یک دستگاه کامل مانده ها به پیمانه m_2 است. برای اثبات این حکم کافیست ثابت کنیم این مجموعه m_2 عضو دارد و هیچ دو عضوی از این مجموعه به پیمانه m_2 همنهشت نیستند. مورد اول از تعریف مجموعه R بدیهیست. برای اثبات مورد دوم داریم :

$$im_1 + n_1 \overset{m_2}{\equiv} jm_1 + n_1 \implies m_2 \mid (i-j)m_1 \quad , \quad \gcd(m_1, m_2) = 1 \implies m_2 \mid i - j$$

$$\implies i - j = 0 \quad \text{یا} \quad \mid i - j \mid \geq m_2$$

که حالت دوم با توجه به شرط $0 \leq t < m_2$ ناممکن است و بنابراین $m_1 = m_2$ که مورد دوم را نیز اثبات می‌کند.
بنابراین مجموعه R یک دستگاه کامل مانده ها به پیمانه m_2 است که اثبات می‌کند دقیقا یک عضو از R وجود دارد که به پیمانه m_2 همنهشت با n_2 است. از طرفی مجموعه R شامل تمام اعداد بازه $[0, m_1m_2)$ است که در معادله همنهشتی اول صادق هستند. این ثابت می‌کند که دستگاه معادلات دقیقا یک جواب صحیح در بازه $[0, m_1m_2)$ دارد که حکم مسئله را به طور کامل ثابت می‌کند.

حال از این قضیه جزئی برای اثبات قضیه باقی‌مانده چینی در یک دستگاه معادلات n تایی استفاده می‌کنیم :

قضیه ۲. برای اعداد صحیح $m_1, m_2, \cdots, m_k$ که دو به دو نسبت به هم اولند و اعداد صحیح و دلخواه $n_1, n_2, \cdots, n_k$، عدد صحیح و یکتای $0 \leq x < m_1m_2\cdots m_k$ وجود دارد که در تمامی معادلات همنهشتی زیر صدق کند :

$$x \overset{m_1}{\equiv} n_1$$

$$x \overset{m_2}{\equiv} n_2$$

$$\vdots$$

$$x \overset{m_k}{\equiv} n_k$$

اثبات. برای اثبات این قضیه از استقرای ریاضی استفاده می‌کنیم : پایه استقرا برای $k = 1, 2$ بدیهیست. برای $k > 2$، بنا بر فرض استقرا عدد یکتای x_0 موجود است که در $k - 1$ رابطه همنهشتی اولیه صدق کند و $x < m_1m_2\cdots m_{k-1}$ صادق باشد. از طرفی می‌دانیم برای هر چنین x_0 طبیعی، عدد $x_0 + t \cdot m_1m_2\cdots m_{k-1}$ نیز در $k - 1$ رابطه اولیه صادق است. بنابراین مجموعه جواب های $k - 1$ معادله همنهشتی اولیه برابر با مجموعه جواب های معادله همنهشتی $x \overset{m_1m_2\cdots m_{k-1}}{\equiv} x_0$ است. از طرفی طبق قضیه 1 می‌دانیم عدد یکتای $0 \leq x < m_1m_2\cdots m_k$ وجود دارد که در هر دو معادله همنهشتی $x \overset{m_1m_2\cdots m_{k-1}}{\equiv} x_0$ و $x \overset{m_k}{\equiv} n_k$ صدق کند. (دقت کنید چون m_i ها دو به دو نسبت به هم اولند، $\gcd(m_1m_2\cdots m_{k-1}, m_k) = 1$ که اجازه استفاده از قضیه 1 را به ما می‌دهد.)

از اثبات حالت دوتایی و چندتایی قضیه باقیمانده‌چینی بنظر می‌رسد که شرط اول بودن دو به دوی m_i ها برای اثبات بیش از اندازه قوی باشد. از این رو یک تعمیم دقیق و شرط دوطرفه برای جواب داشتن یک دستگاه معادلات خطی ارائه می‌دهیم :

قضیه ۳. برای اعداد صحیح و دلخواه (ناصفر) m_1, m_2 و اعداد صحیح دلخواه n_1, n_2، عدد صحیح و یکتای $0 \leq x < \frac{m_1 m_2}{\gcd(m_1,m_2)}$ وجود دارد که در معادلات همنهشتی

$$x \overset{m_1}{\equiv} n_1$$

$$x \overset{m_2}{\equiv} n_2$$

صدق کند، اگر و فقط اگر $\gcd(m_1, m_2) \mid n_1 - n_2$.

اثبات. اثبات گزاره دوم با گزاره اول بدیهیست. داریم :

$$\gcd(m_1, m_2) \mid m_1 \mid x - n_1 \quad , \quad \gcd(m_1, m_2) \mid m_2 \mid x - n_2$$

$$\implies \gcd(m_1, m_2) | (x - n_2) - (x - n_1) = n_1 - n_2$$

اما برای اثبات گزاره اول با استفاده از گزاره دوم، فرض کنید $m_1 = dk_1, m_2 = dk_2$ که در آن $\gcd(m_1, m_2) = d, \gcd(k_1, k_2) = 1$. آنگاه می‌دانیم $d \mid n_1 - n_2$. فرض کنید $n_1 = q_1 d + r, n_2 = q_2 d + r, 0 \leq r < d$. آنگاه معادلات همنهشتی مطلوب ما به صورت زیر خواهند بود :

$$x \overset{dk_1}{\equiv} q_1 d + r \quad , \quad x \overset{dk_2}{\equiv} q_2 d + r$$

$$\implies d \mid dk_1 \mid x - q_1 d - r \implies d \mid x - r \implies x \overset{d}{\equiv} r$$

پس مقدار مطلوب x باید به فرم $td + r$ باشد که در آن $t \in \mathbb{Z}$. حال باید داشته باشیم :

$$td + r \overset{dk_1}{\equiv} q_1 d + r \quad , \quad td + r \overset{dk_2}{\equiv} q_2 d + r$$

$$\iff t \overset{k_1}{\equiv} q_1 \quad , \quad t \overset{k_2}{\equiv} q_2 \quad , \quad \gcd(k_1, k_2) = 1$$

که با توجه به قضیه 1 جوابی یکتا در بازه $0 \leq t < k_1 k_2$ دارد. بنابراین دستگاه معادلات اولیه جوابی یکتا در بازه $r \leq x < dk_1 k_2 + r$ دارد. از طرف دیگر دقت کنید اگر x جوابی برای دستگاه معادلات باشد، آنگاه $x - k_1 k_2$ نیز جوابی برای دستگاه معادلات خواهد بود که نتیجه می‌دهد این دستگاه جوابی یکتا در بازه $0 \leq x < dk_1 k_2$ خواهد داشت که اثبات را کامل می‌کند.

مشابها قضیه را برای تعداد دلخواهی معادله همنهشتی بیان و اثبات می‌کنیم :

قضیه ۴. برای اعداد صحیح و دلخواه (ناصفر) $m_1, m_2, \cdots, m_k$ و اعداد صحیح دلخواه $n_1, n_2, \cdots, n_k$ عدد صحیح x موجود است که در دستگاه معادلات

$$x \overset{m_1}{\equiv} n_1$$

$$x \overset{m_2}{\equiv} n_2$$

$$\vdots$$

$$x \overset{m_k}{\equiv} n_k$$

صدق کند اگر و فقط اگر

$$\forall 1 \leq i < j \leq k \implies \gcd(m_i, m_j) \mid n_i - n_j$$

همچنین در صورت وجود، مقدار x در بازه $\Big[0, \operatorname{lcm}(m_1, m_2, \cdots, m_k)\Big)$ یکتاست.

اثبات. مجددا از استدلال استقرایی ای که در اثبات قضیه 3 استفاده شد بهره می‌بریم. در مورد تعداد جواب دستگاه معادلات هم در گام استقرایی از قضیه ذیل استفاده می‌کنیم :

$$\operatorname{lcm}(m_1, m_2, \cdots, m_i) = \operatorname{lcm}\Big(\operatorname{lcm}(m_1, m_2, \cdots, m_{i-1}), m_i\Big)$$

حال پیش از وارد شدن به بخش مسائل حل نشده درباره قضایای مربوط به باقیمانده چینی، به حل چند مثال با استفاده از این قضیه می‌پردازیم :

مثال ۱. فرض کنید n عددی طبیعی باشد. ثابت کنید n عدد طبیعی متوالی وجود دارد که هیچکدام از آنها خالی از مربع نیستند. (عدد صحیح n را خالی از مربع می‌نامیم اگر بر مربع هیچ عدد طبیعی ای بخش‌پذیر نباشد)

راه حل. فرض کنید $p_1, p_2, \cdots, p_n$ اعداد اول دو به دو متمایز دلخواه باشند. طبق قضیه 2 و با توجه به اینکه هر دو عدد اول متمایز بدیهتا نسبت به هم اولند، می‌توان نتیجه گرفت که عدد صحیح x موجود است که $0 \le x < p_1p_2\cdots p_n$ و همچنین :

$$x \overset{p_1^2}{\equiv} -1$$

$$x \overset{p_2^2}{\equiv} -2$$

$$\dots$$

$$x \overset{p_n^2}{\equiv} -n$$

آنگاه این x مطلوب مسئله خواهد بود زیرا داریم :

$$x \overset{p_1^2}{\equiv} -1 \iff p_1^2 \mid x+1$$

$$x \overset{p_2^2}{\equiv} -1 \iff p_2^2 \mid x+2$$

$$\dots$$

$$x \overset{p_n^2}{\equiv} -1 \iff p_n^2 \mid x+n$$

و بنابراین اعداد $x+1, x+2, \cdots, x+n$، در واقع n عدد متوالی‌اند که هر یک بر مربع یک عدد طبیعی بخش پذیرند و بنابراین خالی از مربع نیستند.

در ادامه به حل تعدادی مثال از المپیادهای مختلف می‌پردازیم که ابتدائاً مسائلی پیچیده هستند اما به راحتی با قضایای باقیمانده چینی قابل حل می‌باشند.

مثال ۲. آیا جایگشتی از اعداد صحیح مثبت مثل $\pi(1), \pi(2), \cdots$ با این خاصیت وجود دارد که به ازای هر مقدار طبیعی $n \ge 1$، مقدار صحیح $\pi(1)+\pi(2)+\cdots+\pi(n)$ بر n بخش‌پذیر باشد؟ (All-Russian olympiad 1995)

راه حل. پاسخ مسئله مثبت است! برای اثبات، از یک استدلال استقرایی استفاده می‌کنیم. برای پایه استقرا کافیست $\pi(1)$ را برابر 1 قرار دهیم. برای اثبات گام استقرایی، فرض کنید دنباله تا k جمله اولیه ($\pi(1), \cdots, \pi(k)$) ساخته شده باشد. حال t را کوچکترین عدد طبیعی در نظر بگیرید که در مجموعه $\{\pi(1), \pi(2), \cdots, \pi(k)\}$ ظاهر نشده است. در این صورت ثابت می‌کنیم s طبیعی و به اندازه دلخواه بزرگ وجود دارد که $s = \pi(k+1)$ و همچنین $t = \pi(k+2)$. برای اثبات، نیاز است دو رابطه ذیل صادق باشند : (برای اختصار و سادگی محاسبات قرار می‌دهیم : $A = \pi(1)+\cdots+\pi(k)$)

$$k+1 \mid \pi(1)+\cdots+\pi(k+1) \quad , \quad k+2 \mid \pi(1)+\cdots+\pi(k+2)$$

$$\iff k+1 \mid A+s \quad , \quad k+2 \mid A+s+t$$

$$\iff s \overset{k+1}{\equiv} -A \quad , \quad s \overset{k+2}{\equiv} -A-t$$

اما واضح است که دو عدد متوالی به هم اولند، بنابراین $\gcd(k+1,k+2)=1$ و بنابراین طبق قضیه 1 عدد صحیح یکتای s موجود است که در نامساوی $0 \le s < (k+1)(k+2)$ صادق باشد و هر دو معادله همنهشتی فوق را نیز برقرار کند. همچنین تمام اعداد به فرم $x+i\cdot(k+1)(k+2)$ که در آن i عددی صحیح و دلخواه است نیز در هر دو معادله صدق خواهند کرد. بنابراین دستگاه جوابهای به اندازه دلخواه بزرگ دارد. حال جوابی از این دستگاه معادلات همنهشتی مثل s انتخاب می‌کنیم به طوری که در مجموعه $\{\pi(1),\cdots,\pi(k)\}$ وجود نداشته باشد و به این صورت حکم استقرا کامل می‌شود.

مثال ۳. فرض کنید f یک چندجمله ای با ضرایب صحیح است که برای برخی a,b های صحیح متمایز داریم : $\gcd(f(a),f(b))=1$. ثابت کنید مجموعه‌ای نامتناهی از اعداد صحیح مثل S موجود است به طوری که برای هر دو عدد متمایز $m,n\in S$ رابطه $\gcd(f(m),f(n))=1$ برقرار باشد.(Poland 2003)

راه حل. فرض کنید مجموعه فوق متناهی باشد. بزرگترین مجموعه‌ای که دارای این خاصیت باشد را S^* می‌نامیم. فرض کنید $S^*=\{s_1,s_2,\cdots,s_k\}$. حال ثابت می‌کنیم می‌توان عضو جدیدی به مجموعه S^* اضافه کرد که فرض خلف را باطل و اثبات مسئله را کامل می‌کند. برای اثبات این حکم، باید عدد طبیعی n را بیابیم به نحوی که برای هر $1\le i\le k$ داشته باشیم $\gcd(f(n),f(s_i))=1$. برای اثبات، از خواص چندجمله‌ای های صحیح‌الضرایب می‌دانیم اگر $n \overset{f(s_i)}{\equiv} n_0 \implies f(n) \overset{f(s_i)}{\equiv} f(n_0)$. بنابراین اگر $\gcd(f(s_i),f(n_0))=1$ باشد، آنگاه $\gcd(f(s_i),f(n_0+tf(s_i))=1$. از همین نکته برای ساخت عضو جدید n استفاده می‌کنیم. چون $f(s_i)$ ها طبق تعریف مجموعه S^* دو به دو نسبت به هم اول هستند، طبق قضیه 2 می‌توان نتیجه گرفت n طبیعی موجود است که داشته باشیم :

$$n \overset{f(s_1)}{\equiv} s_2$$

$$\implies f(n) \overset{f(s_1)}{\equiv} f(s_2)\ ,\ \gcd(f(s_1),f(s_2))=1 \implies \gcd(f(n),f(s_1))=1$$

$$n \overset{f(s_2)}{\equiv} s_3$$

$$\implies f(n) \overset{f(s_2)}{\equiv} f(s_3)\ ,\ \gcd(f(s_2),f(s_3))=1 \implies \gcd(f(n),f(s_2))=1$$

$$\vdots$$

$$n \overset{f(s_k)}{\equiv} s_1$$

$$\implies f(n) \overset{f(s_k)}{\equiv} f(s_1)\ ,\ \gcd(f(s_k),f(s_1))=1 \implies \gcd(f(n),f(s_k))=1$$

حال دقت کنید n می‌تواند طوری انتخاب شود که به اندازه کافی بزرگ باشد. بنابراین نتیجه می‌گیریم $n\notin S^*$ موجود است به طوری که برای هر $1\le i\le k$ داشته باشیم $\gcd(f(s_i),f(n))=1$ که فرض خلف را باطل و اثبات مسئله را کامل می‌کند و در نتیجه مجموعه S نامتناهیست.

مثال ۴. ثابت کنید برای هر $n\in\mathbb{N}$ اعداد طبیعی بزرگتر از 1 مثل $k_0,k_1,\cdots k_n$ وجود دارند که دو به دو نسبت به هم اول باشند و همچنین $k_0k_1\cdots k_n-1$ حاصلضرب دو عدد طبیعی متوالی باشد. (USAMO 2008)

راه حل. مسئله معادل معادله روبرو است : $k_0k_1\cdots k_n=t(t+1)+1$. اگر بتوان ثابت کرد که چندجمله‌ای $t(t+1)+1=t^2+t+1=P(t)$ این خاصیت را دارد که برای هر $d\in\mathbb{N}$، مقدار $t\in\mathbb{N}$ وجود دارد به طوری که $P(t)$ حداقل d عامل اول متمایز داشته باشد، آنگاه اثبات مسئله کامل است.(چرا؟) برای اثبات این حکم، ابتدا از قضیه شور در چندجمله‌های صحیح‌الضرایب بدیهیست که چندجمله‌ای $P(n)$ نامتناهی عامل اول مختلف دارد. حال فرض کنید $p_1,p_2,\cdots,p_d$، تعدادی از این عوامل اول باشند و ثابت می‌کنیم عدد $t_0\in\mathbb{N}$ وجود دارد به نحوی که $p_1p_2\cdots p_d \mid P(t_0)$ و این، اثبات مسئله را کامل می‌کند. برای این امر، دقت کنید چون p_i ها عوامل اولی از چندجمله‌ای $P(n)$ هستند، مقادیر طبیعی $n_1,\cdots,n_d$ باید وجود داشته باشند که داشته باشیم : $\forall 1\le i\le d : p_i \mid P(n_i)$.

از طرفی از خواص چندجمله‌ای های ضریب صحیح می‌دانیم اگر $p_i \mid P(n_i)$ آنگاه برای هر $s \in \mathbb{N}$ داریم : $p_i \mid P(n_i + sp_i)$. حال با خواص ذکر شده، عدد t_0 را تولید می‌کنیم :
از آنجا که p_i ها اعداد اول متمایزند بدیهیست که دو به دو نسبت به هم اولند. بنابراین طبق قضیه 2 عدد طبیعی t_0 موجود است که داشته باشیم :

$$t_0 \overset{p_1}{\equiv} n_1 \implies p_1 \mid P(t_0)$$

$$t_0 \overset{p_2}{\equiv} n_2 \implies p_2 \mid P(t_0)$$

$$\dots$$

$$t_0 \overset{p_d}{\equiv} n_d \implies p_d \mid P(t_0)$$

و در نتیجه $p_1p_2 \cdots p_d \mid P(t_0)$ که وجود t_0 را اثبات کرده و اثبات مسئله را کامل می‌کند.

مثال ۵. به نقطه ای از صفحه مشبکه صحیح مثل (a, b) قابل رویت می‌گوییم اگر روی پاره خط واصل آن نقطه به مبدا مختصات، هیچ نقطه دیگری وجود نداشته باشد. ثابت کنید برای هر n طبیعی، مربعی با اضلاع موازی با محورهای مختصات وجود دارد که همه نقاط مشبکه درون آن غیرقابل رویت باشند. (Taiwan MO 2002)

راه حل. برای اثبات حکم، لازم است نقطه (a, b) را روی صفحه مختصات به نحوی پیدا کنیم که :

$$\forall 0 \le x \le n, 0 \le y \le n \implies \gcd(a + x, b + y) = 1$$

. از طرفی واضح است یک نقطه غیرقابل رویت است اگر و فقط اگر مولفه های عمودی و افقی آن نقطه نسبت به هم اول باشند. (چرا؟) پس صرفا کافیست کاری کنیم که هر دو عدد دو مجموعه $\{a, a+1, \cdots, a+n\}, \{b, b+1, \cdots, b+n\}$ مقسوم علیه مشترکی بزرگتر از یک داشته باشند. اعداد اول متمایز $\{p_{(0.0)}, p_{(0,1)}, \cdots, p_{0,n)}, p_{(1,0)}, p_{(1,1)}, \cdots, p_{(1.n)}, \cdots\cdots, p_{(n,n)}\}$ را در نظر می‌گیریم و ثابت می‌کنیم می‌توان نقطه (a, b) را طوری انتخاب کرد که داشته باشیم :

$$\forall 0 \le x \le n : p_{(x,0)}p_{(x,1)} \cdots p_{(x,n)} \mid a + x \quad , \quad \forall 0 \le y \le n : p_{(0,y)}p_{(1,y)} \cdots p_{(n,y)} \mid b + y$$

در این صورت برای هر $0 \le x, y \le n$ خواهیم داشت $p_{(x,y)} \mid \gcd(a + x, b + y)$ که خواسته ما را برآورده می‌کند. حال دقت کنید چون p_i ها اعداد اول متمایزند، مجموعه اعداد $\{p_{(x,0)}p_{(x,1)} \cdots p_{(x,n)} \mid \forall 0 \le x \le n\}$ دو به دو نسبت به هم اولند. بنابراین طبق قضیه دو، عدد صحیح a موجود است که داشته باشیم :

$$p_{(0,0)}p_{(0,1)} \cdots p_{(0,n)} \mid a + 0$$

$$p_{(1,0)}p_{(1,1)} \cdots p_{(1,n)} \mid a + 1$$

$$\dots$$

$$p_{(n,0)}p_{(n,1)} \cdots p_{(n,n)} \mid a + n$$

به طریق مشابه عدد صحیح y موجود است که داشته باشیم :

$$\forall 0 \le y \le n : p_{(0,y)}p_{(1,y)} \cdots p_{(n,y} \mid b + y$$

و وجود این مقادیر a, b اثبات مسئله را کامل می‌کند.

مثال ۶. فرض کنید $a, b \in \mathbb{N}$ اعدادی طبیعی باشند به طوری که برای هر $n \in \mathbb{N}$ داشته باشیم $a^n + n \mid b^n + n$. ثابت کنید $a = b$.
(IMO Shortlist 2005)

راه حل. فرض کنید p عددی اول باشد که $p \nmid a$. آنگاه طبق قضیه کوچک فرما داریم $a^{p-1} \overset{p}{\equiv} 1$. حال برای اینکه بتوانیم p را به عامل اولی از $a^n + n$ تبدیل کنیم، n را طوری انتخاب می‌کنیم که $n \overset{p-1}{\equiv} 1$. آنگاه داریم $a^n \overset{p}{\equiv} a^{n(mod)p-1} = a$، بنابراین لازم است $p \mid a+n$. اما چون $\gcd(p, p-1) = 1$ برقرار است، طبق قضیه 1 عدد طبیعی n وجود دارد که در هر دو رابطه همنهشتی زیر صدق کند :

$$n \overset{p}{\equiv} -a$$

$$n \overset{p-1}{\equiv} 1$$

برای این n طبیعی داریم :

$$p \mid a^n + n \mid b^n + n \implies p \mid a^n + n \mid b^n - a^n \implies a^n \overset{p}{\equiv} b^n$$

دقت کنید چون $a^n \overset{p}{\not\equiv} 0$، آنگاه $b^n \overset{p}{\not\equiv} 0$ نیز برقرار است. بنابراین مجددا طبق قضیه کوچک فرما داریم :

$$a^n \overset{p}{\equiv} a \quad , \quad b^n \overset{p}{\equiv} b$$

و بنابراین $p \mid a-b$. اما از آنجا که این رابطه برای هر p اول که عامل اولی از a نباشد برقرار است و تعداد چنین عوامل اولی هم نامتناهی است، $a-b$ اجباراً باید برابر با صفر باشد و این اثبات مسئله را کامل می‌کند.

مثال ۷. آیا تابع $f : \mathbb{N} \to \mathbb{N}$ وجود دارد به طوری که هیچ چندجمله‌ای $P(x)$ موجود نباشد که $\forall i \in \mathbb{N} \implies f(i) = P(i)$ و همچنین برای هر $a, b \in \mathbb{N}$ داشته باشیم $a-b \mid f(a) - f(b)$؟

راه حل. بله، به استقرا این تابع را می‌سازیم. قرار دهید $f(1) = 1$. آنگاه فرض کنید $f(1), f(2), \cdots, f(n-1)$ همگی تعیین شده باشند. x را طوری بیابید که داشته باشیم :

$$n-1 \mid x - f(1) \implies x \overset{n-1}{\equiv} f(1)$$

$$n-2 \mid x - f(2) \implies x \overset{n-2}{\equiv} f(2)$$

$$\vdots$$

$$n-(n-1) \mid x - f(2) \implies x \overset{n-(n-1)}{\equiv} f(n-1)$$

اما طبق قضیه چهار باقیمانده چینی، این دستگاه نامتناهی جواب طبیعی به اندازه کافی بزرگ برای x دارد اگر و فقط اگر برای هر $1 \leq i < j \leq n-1$ داشته باشیم : $\gcd(n-i, n-j) \mid f(i) - f(j)$. اما با توجه به فرض استقرا داریم :

$$\gcd(n-i, n-j) = \gcd((n-i)-(n-j), n-j) = \gcd(j-i, n-j) \mid j-i \mid f(j) - f(i)$$

و بنابراین چنین x ای موجود است و دستگاه جواب دارد. حال با توجه به اینکه دستگاه باقیمانده چینی مذکور نامتناهی جواب در مجموعه اعداد طبیعی دارد، می‌توان مقدار x را طوری انتخاب کرد که در معادلات دستگاه صادق باشد و همچنین داشته باشیم $x - f(n-1) > n^n$. حال قرار دهید $f(n) = x$. این مقدار در تمام شرط های عاد کردن مسئله صادق است. از طرفی تابع ساخته شده برابر با هیچ تابعی از فرم چندجمله‌ای نخواهد بود زیرا برای هر n طبیعی داریم $f(n) - f(n-1) > n^n$ در حالی که اگر $f(n)$ یک چندجمله‌ای باشد، تابع $f(n) - f(n-1)$ خود یک چندجمله‌ای از درجه پایین‌تر خواهد بود در حالی که هیچ چندجمله‌ای $P(x)$ وجود ندارد که داشته باشیم $\forall n \in \mathbb{N} : P(n) > n^n$ و اثبات مسئله کامل است.

مثال ۸. برای هر $a, c \in \mathbb{N}$ و $b \in \mathbb{Z}$ ثابت کنید نامتناهی $x \in \mathbb{N}$ موجود است به طوری که داشته باشیم : $a^x + x \overset{c}{\equiv} b$ (Brazil MO 2005)

راه حل. ابتدا فرض کنید عدد طبیعی n موجود باشد به طوری که $c \mid a^n$. در این صورت هر $x \geq n$ که $x \overset{c}{\equiv} b$ در معادله صادق است و اثبات کامل خواهد بود. در غیر این صورت، حکم را به استقرای قوی روی c اثبات خواهیم کرد. حکم برای $c = 1$ به وضوح درست است. حال فرض کنید حکم برای هر مقدار $c = 1, 2, \cdots, k-1$ صحیح باشد و درستی حکم را برای $c = k$ ثابت می‌کنیم. طبق اصل لانه کبوتری واضح است که دنباله $\{a, a^2, a^2, \cdots\}$ از جایی به بعد به پیمانه k متناوب است و همچنین واضح است که اعضای این دنباله به پیمانه k ناصفرند. بنابراین اعداد طبیعی n_0, r موجودند به طوری که برای هر $n \geq n_0$ داشته باشیم : $\forall k \in \mathbb{N} \implies a^{n_0+kr} \overset{k}{\equiv} a^{n_0+r}$ و همچنین هیچ عددی کمتر از r چنین خاصیتی نداشته باشد. مجدداً واضح است که $r < k$ زیرا اگر داشته باشیم $r \geq k$ آنگاه طبق اصل لانه کبوتری چون اعداد $\{a, a^2, \cdots, a^r\}$ به پیمانه k ناصفرند، دو تا از آنها باید به پیمانه k همنهشت باشند یا به عبارتی : $\exists 1 \leq j < i \leq r : a^i \overset{k}{\equiv} a^j$. اما این معادل این است که برای n های به اندازه کافی بزرگ $a^n = a^{(n-j)+j} \overset{k}{\equiv} a^{(n-j)+i} = a^{n+(i-j)}$ که با توجه به $1 \leq i-j < r$ با فرض اینکه r کوچکترین دوره تناوب است در تناقض خواهد بود. بنابراین می‌دانیم $r < k$. حال کافیست x را طوری انتخاب کنیم که $x \overset{r}{\equiv} i, x \geq n_0$ و همچنین $a^x + x \overset{k}{\equiv} a^i + x \overset{k}{\equiv} b \iff x \overset{k}{\equiv} b - a^i$. (در اینجا $i > n_0$ عددی دلخواه است) اما طبق قضیه سوم باقیمانده چینی، نامتناهی مقدار طبیعی و به اندازه کافی بزرگ x وجود دارد که در دو معادله اخیر صادق باشند اگر و فقط اگر $a^i + i \overset{\gcd(k,r)}{\equiv} b \iff \gcd(k,r) \mid b - a^i - i$.
اما می‌دانیم $\gcd(k,r) < k$ زیرا $\gcd(k,r) \mid k \implies \gcd(k,r) \leq k$ و تنها حالتی که $\gcd(k,r)$ از k کمتر نباشد این است که داشته باشیم $\gcd(k,r) = k$ یا به عبارتی $k \mid r \implies k \leq r$. اما از قبل داشتیم $k > r$ که یک تناقض است و بنابراین $\gcd(k,r) < k$. حال طبق فرض استقرای قوی می‌دانیم مقدار $j \in \mathbb{N}$ موجود است که داشته باشیم $a^j + j \overset{\gcd(k,r)}{\equiv} b$ و با قرار دادن $i = j$ و استفاده از قضیه باقیمانده چینی، درستی حکم برای $c = k$ نیز اثبات می‌شود.

در آخر، تعدادی مسئله حل نشده برای تمرین قرار داده شده است و با کلیک روی منبع سوال می‌توانید به منبع سوال دسترسی پیدا کنید و بعضاً راهنمایی یا راه حل کاملی برای این سوالات پیدا کنید.

تمرین‌های تکمیلی

۱. ثابت کنید برای هر عدد طبیعی n، می‌توان n عدد طبیعی متوالی یافت به طوری که هیچ یک توان کامل یک عدد اول نباشند. (IMO 1989)

۲. فرض کنید $\{s_1, s_2, \cdots, s_{\varphi(n)}\}$ یک دستگاه مخفف مانده ها به پیمانه عدد طبیعی $n > 1$ باشد. تمام اعداد صحیح a را بیابید به طوری که مجموعه $\{s_1 + a, s_2 + a, \cdots, s_{\varphi(n)} + a\}$ نیز یک دستگاه مخفف مانده ها به پیمانه m باشد.

۳. آیا دنباله نامتناهی $\{a_1, a_2, \cdots\}$ از اعداد طبیعی وجود دارد که به ازای هر عدد طبیعی n مجموع هر n جمله متوالی این دنباله بر n^2 بخش پذیر باشد؟ (Baltic Way 2006)

۴. فرض کنید n عددی طبیعی و $\{a_1, a_2, \cdots, a_k\}$ اعدادی طبیعی و متمایز از بازه $[1, n]$ باشند $(k \geq 2)$ به طوری که داشته باشیم :

$$\forall 1 \leq i \leq k-1 \implies n \mid a_i(a_{i+1} - 1)$$

ثابت کنید $n \nmid a_k(a_1 - 1)$. (IMO 2009)

۵. همه سه تایی های اعداد طبیعی مثل (a, b, c) را بیابید به طوری که برای هر $n \in \mathbb{N}$ به طوری که n هیچ عامل اولی کمتر از 2014 نداشته باشد، داشته باشیم : $n + c \mid a^n + b^n + n$. (ELMO Shortlist 2014)

۶. ثابت کنید برای هر $k \in \mathbb{N}$ دنباله حسابی $\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \cdots, \frac{a_k}{b_k}\}$ از اعداد گویا وجود دارد به طوری که برای هر $1 \leq i \leq k$ داشته باشیم $\gcd(a_i, b_i) = 1$ و همچنین اعداد $\{a_1, b_1, a_2, b_2, \cdots, a_k, b_k\}$ دو به دو متمایز باشند. (APMO 2009)

۷. ابوالفضل و علیرضا مشغول انجام یک بازی هستند. مجموعه A با متناهی عضو مفروض است و هر دو بازیکن اعضای این مجموعه را می‌دانند. ابتدا علیرضا یک عضو مثل $a \in A$ را انتخاب می‌کند و ابوالفضل نیز عددی دلخواه مثل b بر می‌گزیند که لزوما عضو A نیست. در نهایت علیرضا تعداد مقسوم‌علیه های عدد ab را به ابوالفضل می‌گوید. ثابت کنید ابوالفضل می‌تواند عددش را طوری انتخاب کند که بتواند عدد انتخاب شده توسط علیرضا (a) را بفهمد.

۸. تمام اعداد طبیعی n را بیابید به طوری که عدد طبیعی m موجود باشد که داشته باشیم : $2^n - 1 \mid m^2 + 9$. (IMO Shortlist 1998)

۹. تمام اعداد $n > 1$ را بیابید به طوری که اعداد طبیعی $b_1, b_2, \cdots, b_n$ وجود داشته باشند که همگی با هم برابر نباشند و همچنین برای هر $k \in \mathbb{N}$ عبارت $(b_1 + k)(b_2 + k) \cdots (b_n + k)$ توان کامل باشد. (ARO 2008)

۱۰. ثابت کنید برای هر $m, n \in \mathbb{N}$ عدد طبیعی k وجود دارد به طوری که $2^k - m$ حداقل n عامل اول متمایز داشته باشد. (China TST 2006)

۱۱. یک مجموعه از اعداد طبیعی را خوش‌بو می‌نامیم اگر حداقل دو عضو داشته باشد و هر عضو آن حداقل یک عامل اول مشترک با حداقل یکی از اعضای دیگر آن داشته باشد. اگر $P(n) = n^2 + n + 1$ آنگاه کوچکترین مقدار طبیعی b را بیابید به طوری که عدد صحیح و نامنفی a وجود داشته باشد چنان‌که مجموعه $\{P(a+1), P(a+2), \cdots, P(a+b)\}$ خوش‌بو باشد. (IMO 2016)

۱۲. فرض کنید $n > 1$ عددی صحیح باشد و k تعداد عوامل اول مختلف n باشد. ثابت کنید عدد صحیح a موجود است به طوری که $1 < a < \frac{n}{k} + 1$ و همچنین $n \mid a^2 - a$. (China TST 2011)

۱۳. طبق موازین اسلامی، "آرین و ارشیا" یک بازی را آغاز کرده‌اند. ارشیا عدد طبیعی $N < 5000$ را انتخاب می‌کند و سپس 20 عدد صحیح $a_1, a_2, \cdots, a_{20}$ را بر می‌گزیند به طوری که برای هر $1 \leq k \leq 20$، داشته باشیم $N \overset{k}{\equiv} a_k$. در یک نوبت، آرین به ارشیا یک مجموعه S شامل اعداد صحیح کوچکتر یا مساوی 20 می‌دهد و ارشیا نیز به آرین مجموعه $\{a_k | k \in S\}$ را بر می‌گرداند. (دقت کنید که ارشیا یک "مجموعه" به آرین تحویل می‌دهد و لذا ترتیب اعضای آن نامشخص است) آرین چه تعداد حرکت لازم است انجام دهد تا بفهمد که عدد انتخابی ارشیا (N) چه بوده است؟ (RMM 2021)

۱۴. فرض کنید $m_1, m_2, \cdots, m_{2013} > 1$ اعدادی طبیعی و دو به دو نسبت به هم اول باشند و $A_1, A_2, \cdots, A_{2013}$ مجموعه هایی باشند (ممکن است بعضی از این مجموعه ها تهی باشند) به طوری که $A_i \subseteq \{1, 2, \cdots, m_i - 1\}$. ثابت کنید عدد طبیعی N موجود است به طوری که داشته باشیم : (ELMO 2013)

$$N \leq (2|A_1|+1)(2|A_2|+1)\cdots(2|A_{2013}|+1) \quad , \quad \forall 1 \leq i \leq 2013 \implies \nexists a \in A_i : m_i \mid N - a$$

.

۱۵. اگر $f : \mathbb{N} \to \mathbb{N}$ یک تابع باشد به طوری که برای هر $m, n \in \mathbb{N}, \gcd(m,n) = 1$ داشته باشیم $\gcd(f(m), f(n)) = 1$ و همچنین برای هر $n \in \mathbb{N}$ داشته باشیم $n \leq f(n) \leq n + 2012$ آنگاه ثابت کنید برای هر $n \in \mathbb{N}, p \in \mathbb{P}$ اگر $p \mid f(n)$ آنگاه $p \mid n$. (USA TSTST 2012)