باقی مانده چینی

قضیه باقیمانده چینی: فرض کنید $m_1, \dots, m_k$ اعدادی طبیعی باشند که دو به دو نسبت به هم اول اند. هم چنین فرض کنید $a_1, a_2, \dots, a_k$ اعدادی صحیح باشند. در این صورت عدد صحیح x وجود دارد که برای هر $1 \leq i \leq k$ داشته باشیم:

$$x \equiv a_i \pmod{m_i}$$

اثبات اول : ابتدا برای $k=2$ حکم را ثابت می کنیم. در این صورت باید ثابت کنیم برای دو عدد a_1, a_2 و دو عدد m_1, m_2 که نسبت به هم اول اند عدد صحیح x وجود دارد که

$$x \equiv a_1 \pmod{m_1}, \qquad x \equiv a_2 \pmod{m_2}$$

قرار می دهیم $x = km_1 + k'm_2$ در این صورت شروط بالا معادل خواهند بود با

$$k'm_2 \equiv a_1 \pmod{m_1}, \qquad km_1 \equiv a_2 \pmod{m_2}$$

یا معادلا :

$$k' \equiv a_1(m_2)^{-1} \pmod{m_1}, \qquad k \equiv a_2(m_1)^{-1} \pmod{m_2}$$

این دو معادله در واقع دو معادله مستقل از هم هستند. کافی است مقادیر k, k' را برابر مقادیر سمت راست آنها قرار دهیم.

در نتیجه برای $k=2$ ثابت شد. برای $k>2$ به عنوان تمرین به استقرا ثابت کنید(قسمت اصلی اثبات $k=2$ بوده است)

اثبات دوم : رجوع به کتاب میرزاخانی-بهشتی زواره

اثبات سوم : مجموعه S متشکل از همه k تایی های به فرم زیر است :

$$(x_1, x_2, \dots, x_k), 0 \leq x_i \leq m_i - 1$$

حال تابع $f:\{0,1,\dots,m_1m_2\dots m_k-1\}\to S$ را این گونه تعریف می کنیم.

$$f(x)=(x_1,x_2,\dots,x_k)\ \ ,x\equiv x_i\ \ (mod\ m_i)$$

در واقع مولفه i برابر با باقیمانده x بر m_i است.

ادعا 1: این تابع یک به یک است.

اثبات ادعا 1: فرض کنیم $f(x)=f(x')$ باشد در این صورت داریم :

$$x\equiv x'\ (mod\ m_i)\to x-x'\equiv 0\ (mod\ m_i)\to m_i|x-x'$$

هم چنین چون m_i ها نسبت به هم اول اند داریم

$$m_1m_2\dots m_k|x-x'\to x=x'$$

در نتیجه اثبات شد که تابع یک به یک است.

ادامه اثبات : دامنه و برد این تابع هم اندازه اند و هر دو اندازه شان $m_1m_2\dots m_k$ است. هر تابع یک به یکی که دامنه و برد آن متناهی و هم اندازه باشد پوشا هم هست (اثبات به عنوان تمرین بر عهده شما). حال $(a_1,a_2,..,a_k)$ را در برد در نظر بگیرید. چون تابع پوشا است عدد x وجود دارد طوری که $f(x)=(a_1,a_2,..,a_k)$ باشد. حال اگر به تعریف f رجوع کنیم برای هر $1\le i\le k$ خواهیم داشت :

$$x\equiv a_i\ \ (mod\ m_i)$$

که دقیقا همان چیزی است که صورت سوال خواسته است. اثبات کامل شد.

بررسی قضیه در حالتی که پیمانه ها نسبت به هم اول نباشند:

مثال نقض :

$$x \equiv 1 \pmod 4 , \qquad x \equiv 2 \pmod 6$$

معادله چپ اشاره دارد که x باید فرد باشد و معادله راست اشاره دارد که x باید زوج باشد که با هم تناقض دارند.

سوالی که مطرح می شود این است که آیا می توان قضیه ای کلی تر از باقیمانده چینی برای مواقعی که پیمانه ها نسبت به هم اول نباشند ارائه داد؟ برای مثال به دستگاه معادله زیر دقت کنید:

$$x \equiv 1 \pmod 4 , \qquad x \equiv 3 \pmod 6$$

این معادله جواب دارد : $x = 9$

برای پیدا کردن قضیه در حالت کلی شرط بدیهی این است که پیمانه ها و a_i نباید تناقض داشته باشند. به طور دقیق تر اگر d عددی طبیعی باشد و $i \neq j$ باشد و $d|m_i \ , d|m_j$ آنگاه داریم

$$x \equiv a_i \pmod{m_i} \ , x \equiv a_j \pmod{m_j} \to x \equiv a_i \pmod d \ , x \equiv a_j \pmod d \to a_i \equiv a_j \pmod d$$

در نتیجه شرط لازم این است که برای هر i, j داشته باشیم

$$a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$$

قضیه(تعمیم باقیمانده چینی) : فرض کنید $m_1, \dots, m_k$ اعدادی طبیعی باشند و $a_1, a_2, \dots, a_k$ اعدادی صحیح باشند. هم چنین اگر برای هر i, j داریم $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$. در این صورت عدد صحیح x وجود دارد که برای هر $1 \leq i \leq k$ داشته باشیم:

$$x \equiv a_i \pmod{m_i}$$

اثبات: برای اثبات ابتدا به مثالی که پیش تر زدیم رجوع می کنیم :

$$x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 6$$

این دستگاه را می توان به دستگاه های زیر تجزیه کرد(شکست):

$$x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 2, \quad x \equiv 3 \pmod 2$$

در واقع دستگاه را به پیمانه های با توان های اول تجزیه می کنیم. حال توجه کنیم که $x \equiv 1 \pmod 4$ معادله $x \equiv 3 \pmod 2$ را نتیجه می دهد. در نتیجه عملا دو معادله زیر را داریم :

$$x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 2$$

این دو معادله هم در صورت قضیه اصلی باقیمانده چینی صدق می کنند زیرا باقیمانده ها نسبت به هم اول هستند.

حال مساله را در حالت کلی بررسی می کنیم. فرض کنید $[m_1, m_2, .., m_k] = (p_1)^{\alpha_1} \dots (p_t)^{\alpha_t}$ باشد. به سادگی می توان دید با استفاده از تجزیه و حذفی که در مثال بالا مشاهده شد معادله به دشتگاه معادلات زیر تبدیل می شود :

$$x \equiv b_i \pmod{(p_i)^{\alpha_i}}$$

که b_i ها یکی از $\mathrm{a_i}$ ها هستند.

سوال : ثابت کنید اگر $(m,n)=1$ باشد آنگاه $\phi(m)\phi(n)=\phi(mn)$

اثبات : فرض کنید طبق باقیمانده چینی هر زوج (r,s) که $0\le s\le n-1$, $0\le r\le m-1$ که

$$x\equiv r \pmod m\ ,\qquad x\equiv s \pmod n$$

$0\le x\le mn-1$ است. هم چنین اگر $(r,m)=1$, $(s,n)=1$ باشد آنگاه باید $(x,mn)=1$ باشد. در نتیجه هر زوج دلخواه از دستگاه مخفف مانده های m و n متناظر با یک عضو از دستگاه مخفف مانده های mn است. در نتیجه حکم نتیجه می شود.

سوال: آیا این گزاره درست است؟

فرض کنید $\{x^3|x\in\mathbb{Z}\}$ به پیمانه m ، r باقی مانده متمایز و به پیمانه n ، s باقی مانده متمایز را تولید کند.

الف) آیا اگر $(m,n)=1$ باشد می توان نتیجه گرفت که به پیمانه mn دقیقا rs باقی مانده تولید می کند.

ب) در صورتی که ندانیم نسبت به هم اول اند چه حکمی می توان داد؟

حل ب: $m=dm',n=dn'$ و فرض کنید به پیمانه t ، $f(t)$ تا داشته باشه. در نتیجه

$$f(m)=f(d)f(m'),f(n)=f(d)f(n')$$

به نظر نمیرسه چیز خاصی بشه گفت

سوال سطح 1:

سوال)

فرض کنید $m_1, m_2, \dots, m_{2013}$ اعداد طبیعی بزرگتر از 1 باشند . هم چنین $A_1, A_2, \dots, A_{2013}$ مجموعه هایی باشند طوری که برای هر i ، مجموعه A_i زیرمجموعه $\{0,1,2,3,\dots, m_i - 1\}$ است. عددی را عضو A_i به پیمانه m_i می نامیم اگر باقیمانده اش بر m_i عضوی از A_i باشد(برای مثال 7 به پیمانه 5 عضوی از $\{1,2\}$ است چون باقیمانده اش بر 5 برابر 2 است). عدد y را خوب می نامیم اگر برای هر $1 \le i \le 2013$ عضو A_i به پیمانه m_i باشد. ثابت کنید تعداد اعداد طبیعی خوب عضو $\{0,1,2,\dots, M-1\}$ برابر است با:

$$|A_1||A_2|\dots|A_{2013}|$$

که منظور از $|B|$ تعداد اعضای مجموعه B است و $M = m_1 m_2 \dots m_{2013}$

نکته : اگر A_i تک عضوی باشد آنگاه حکم مساله همان باقی مانده چینی خواهد بود.

حل : مشابه با اثبات باقی مانده چینی به عدد x بردار روبرو را متناظر می کنیم : $(x_1, x_2, \dots, x_{2013})$ که x_i باقیمانده x بر m_i است. طبق باقی مانده چینی این تناظریک به یک و پوشا است. یعنی برای هر عدد x دقیقا یک بردار متناظر شده است و هم چنین برای هر بردار دلخواه $(x_1, x_2, \dots, x_{2013})$ ، دقیقا یک عدد $0 \le x < M$ وجود دارد که با آن تناظر پیدا کرده است. حال به سادگی می توان دید که عدد x خوب است اگر و فقط اگر $x_i \in A_i$ باشد. در نتیجه x_i را می توانیم هر کدام از اعضای A_i قرار دهیم و در نتیجه برای x_i به اندازه $|A_i|$ حالت برای انتخاب داریم و طبق اصل ضرب تعداد کل حالات برابر خواهد بود با $|A_1||A_2|\dots|A_{2013}|$. تمام.

سوال)

فرض کنید $p(x)$ چندجمله با ضرایب صحیح باشد و q_1, q_2, q_3 اعداد اول متمایز و x_1, x_2, x_3 اعدادی صحیح باشند طوری که $q_1|p(x_1)$, $q_2|p(x_2)$, $q_3|p(x_3)$. ثابت کنید عدد صحیح y یافت می شود طوری که $q_1q_2q_3|p(y)$

راهنمایی 1: می دانیم یکی از خاصیت های هم نهشتی این است که اگر a, b, m اعدادی صحیح باشند که $a \equiv b \ (mod\ m)$ آنگاه $p(a) \equiv p(b)(mod\ m)$ خواهد بود.

راهنمایی 2: طبق قضیه باقیمانده چینی عدد y یافت می شود که $y \equiv x_1 \ (mod\ q_1)$ و $y \equiv x_2 \ (mod\ q_2)$ و $y \equiv x_3 \ (mod\ q_3)$

اثبات : اولا می دانیم یکی از خاصیت های هم نهشتی این است که اگر a, b, m اعدادی صحیح باشند که $a \equiv b \ (mod\ m)$ آنگاه $p(a) \equiv p(b)(mod\ m)$ خواهد بود.

طبق قضیه باقیمانده چینی عدد y یافت می شود که $y \equiv x_1 \ (mod\ q_1)$ و $y \equiv x_2 \ (mod\ q_2)$ و $y \equiv x_3 \ (mod\ q_3)$ درنتیجه طبق خاصیت بالا داریم $p(y) \equiv p(x_1) \equiv 0 \ (mod\ q_1)$ و $p(y) \equiv p(x_2) \equiv 0 \ (mod\ q_2)$ و $p(y) \equiv p(x_3) \equiv 0(mod\ q_3)$ و در نتیجه $q_1|p(y)$ و $q_2|p(y)$ و $q_3|p(y)$ و در نتیجه $q_1q_2q_3|p(y)$. تمام.

سوال) (المپیاد جهانی 1989 سوال 5)

برگرفته از

http://artofproblemsolving.com/community/c6h62176p3721330

فرض کنید n یک عدد طبیعی است. ثابت کنید n عدد طبیعی متوالی یافت می شود طوری که هیچ کدام توان یک عدد اول نباشند.

راهنمایی 1: اگر عددی دارای حداقل دو عامل اول باشد آنگاه در نتیجه توان کامل یک عدد اول نخواهد بود.

راهنمایی 2: کافی است عدد x را پیدا کنید طوری که برای هر $1 \leq i \leq n$ عدد $x + i$ دارای حداقل دو عامل اول مختلف باشد.

راهنمایی 3 : فرض کنید $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_n$ اعداد اول متمایز باشند. کافی است برای هر $1 \le i \le n$ داشته باشیم

$$x \equiv -i \ (mod\ p_i q_i)$$

حل : فرض کنید $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_n$ اعداد اول متمایز باشند. آنگاه طبق باقی مانده چینی عدد x یافت می شود طوری که $x \equiv -1 \ (mod\ p_1 q_1)$ و $x \equiv -2 \ (mod\ p_2 q_2)$ و ... $x \equiv -n \ (mod\ p_n q_n)$ که نتیجه می شود

$$p_1 q_1 | x+1 \quad p_2 q_2 | x+2 \quad \dots \quad p_n q_n | x+n$$

در نتیجه $x+1, x+2, \dots, x+n$ هر کدام حداقل دو عامل اول دارند و در نتیجه توان کامل یک عدد اول نخواهند بود. تمام.

سوال) (USAMO 2008 سوال اول)

فرض کنید n عددی طبیعی باشد. ثابت کنید n عدد طبیعی بزرگتر از یک $k_1, k_2, \dots, k_n$ وجود دارند که نسبت به هم اول اند و هم چنین $k_0 k_1 \dots k_n + 1 -$ ضرب دو عدد طبیعی متوالی است.

راهنمایی 1: کافی است عدد m پیدا کنید که است $m(m+1)+1$ حداقل n عامل اول داشته باشد.

راهنمایی 2: طبق باقی مانده چینی و در واقع دقیقا طبق مساله .... باید ثابت کنیم اعداد اول $q_1, q_2, \dots, q_n$ و اعداد $x_1, x_2, \dots, x_n$ یافت می شوند که $x_i(x_i+1)+1 \equiv 0 \ (mod\ q_i)$ باشد.

راهنمایی 3: ثابت کنید مجموعه اعداد $x(x+1)+1, x \in \mathbb{N}$ دارای بی نهایت عامل اول است. یعنی بی نهایت عدد اول p یافت می شود که برای آن عدد طبیعی xوجود دارد که $p | x(x+1)+1$.تمام.

حل: $k_0 k_1 \dots k_n + 1 -$ ضرب دو عدد طبیعی متوالی است اگر و فقط اگر $k_1 \dots k_n + 1 - = m(m+1)$ یا معادلا $k_1 \dots k_n = 1 + m(m+1)$. برای اینکه $k_1, k_2, \dots, k_n$ وجود داشته باشند که نسبت به هم اول باشند کافی است $m(m+1)+1$ حداقل

n عامل اول داشته باشد(*). یعنی باید m ای پیدا کنیم که برای هر $1 \leq i \leq n$ داشته باشیم : $m(m+1)+1 \equiv 0 \ (mod\ q_i)$ که $q_1, q_2, \dots, q_n$ اعدادی اول متمایزی هستند. طبق باقی مانده چینی و در واقع دقیقا طبق مساله .... باید ثابت کنیم اعداد اول $q_1, q_2, \dots, q_n$ و اعداد $x_1, x_2, \dots, x_n$ یافت می شوند که $x_i(x_i+1)+1 \equiv 0 \ (mod\ q_i)$ باشد. فرض کنید چنین x_i هایی را پیدا کرده باشیم. طبق قضیه باقیمانده چینی عدد m یافت می شود که برای هر $1 \leq i \leq n$ داشته باشیم : $m \equiv x_i \ (mod\ q_i)$ به سادگی می توانید متوجه شوید که داریم $m(m+1)+1 \equiv 0 \ (mod\ q_i)$.

ادامه کار را به دو طریق می توان گفت. طریق اول از راه این قضیه است : هر چند جمله غیر ثابت با ضرایب صحیح دارای بی نهایت عامل اول است و این کار را تمام می کند زیرا کافی است این قضیه را برای چند جمله ای $x(x+1)+1$ اعمال کنیم. راه دوم به صورت اثبات مستقیم است. فرض خلف کنید که متناهی عدد اول یافت شوند و آن ها را $r_1, r_2, \dots, r_t$ بنامید. حال بگیرید $M = r_1 r_2 \dots r_t$ و $M(M+1)+1$ نسبت به $r_1, r_2, \dots, r_t$ اول است. در نتیجه عاملی به غیر از $r_1, r_2, \dots, r_t$ دارد. که تناقض است زیرا $r_1, r_2, \dots, r_t$ همه عوامل اول ممکن بوده اند. تمام.

سوال) تغییر یافته سوال پیشنهادی المپیاد جهانی 1972 – لیست بلند

حل: فرض کنید n عدد طبیعی باشد. تعداد اعداد طبیعی حداکثر $2n$ رقمی به صورت $\overline{a_{2n}a_{2n-1}\dots a_1}$ را بیابید طوری که داشته باشیم :

$$\overline{a_{2n}a_{2n-1}\dots a_1} = (\overline{a_n a_{n-1}\dots a_1})^2$$

حل : به سادگی می توان دید شروط مساله معادل است با اینکه

$$\overline{a_n a_{n-1}\dots a_1} \equiv (\overline{a_n a_{n-1}\dots a_1})^2 \ (mod\ 10^n)$$

باشد. فرض کنید $x=\overline{a_n a_{n-1} \dots a_1}$ باشد. در نتیجه شرط مساله معادل است با اینکه $10^n | x(x-1)$ به وضوح $x<10^n$ است.

در نتیجه $10^n \nmid x$ و $10^n \nmid x-1$. در نتیجه با توجه به اینکه $(x, x-1)=1$ است. یکی از دو حالت زیر باید رخ دهد . حالت اول : $2^n | x , 5^n | x-1$ و حالت دوم $5^n | x , 2^n | x-1$ طبق باقیمانده چینی برای هر کدام از حالات دقیقا یک عدد $x<10^n$ با خاصیت مورد نظر یافت می شود . در نتیجه جواب برابر 2 است.

سوال سطح 2:

سوال (قسمتی از راه حل Shortlist 1992 Problem 15)

فرض کنید $A=\{x_1, x_2, \dots, x_m\}$ مجموعه ای از اعداد طبیعی باشد. ثابت کنید عدد طبیعی d وجود دارد طوری که همه اعداد $dx_1 , dx_2, \dots, dx_m$ توان کامل عددی طبیعی باشند.

نکته : عدد x را توان کامل عدد طبیعی می نامیم اگر اعداد r, s که $s \geq 2$ یافت شود طوری که $x=r^s$ باشد.

راهنمایی 1: در این سوال هم می توانید با استقرا حکم را ثابت کنید و هم بدون آن . راهنمایی ای که می آید برای راه حل بدون استقرا است. فرض کنید $p_1 < p_2 < \dots < p_m$ اعداد اول باشند. d را طوری انتخاب می کنیم که dx_i توان p_i ام یک عدد باشد.

راهنمایی 2: بگیرید $d=x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$ در این صورت داریم $dx_1=x_1^{1+\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$ اگر داشته باشیم $1+\alpha_1, \alpha_2, \dots, \alpha_m \equiv 0 \ (mod\ p_1)$ آنگاه dx_1 توان p_1 ام یک عدد طبیعی خواهد بود و dx_1 کارش تمام خواهد شد. همین کار را برای $x_2, \dots x_m$هم انجام دهید.

راهنمایی 3: شروط مربوط به α_1 اینها خواهند بود (چرا؟)

$$\alpha_1 \equiv -1 \ (mod\ p_1), \alpha_1 \equiv 0 \ (mod\ p_2), \dots, \alpha_1 \equiv 0 \ (mod\ p_m)$$

حل 1: فرض کنید $p_1 < p_2 < \cdots < p_m$ اعداد اول باشند. d را طوری انتخاب می کنیم که dx_i توان p_i ام یک عدد باشد. توجه کنید که عدد c توان e ام یک عدد است اگر و فقط اگر توان همه عوامل اول آن مضرب e باشد. حال بگیرید

$$d = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$$

در این صورت داریم $dx_1 = x_1^{1+\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$ اگر داشته باشیم $1 + \alpha_1, \alpha_2, \dots, \alpha_m \equiv 0 \ (mod\ p_1)$ آنگاه dx_1 توان p_1 ام یک عدد طبیعی خواهد بود و dx_1 کارش تمام خواهد شد. حال dx_2 . داریم $dx_2 = x_1^{\alpha_1} x_2^{1+\alpha_2} \dots x_m^{\alpha_m}$ اگر داشته باشیم $\alpha_1, 1 + \alpha_2, \dots, \alpha_m \equiv 0 \ (mod\ p_2)$ آنگاه dx_2 توان p_2 ام یک عدد طبیعی خواهد بود و dx_2 کارش تمام خواهد شد. همین شروط را برای dx_3 والی آخر خواهیم داشت. مجموعه همه این شروط مشابه زیر خواهد بود :

شروط مربوط به α_1 :

$$\alpha_1 \equiv -1 \ (mod\ p_1), \alpha_1 \equiv 0 \ (mod\ p_2)\ , \dots\ , \alpha_1 \equiv 0 \ (mod\ p_m)$$

طبق باقی مانده چینی α_1 با این شرایط یافت می شود.

شروط مربوط به α_2 :

$$\alpha_2 \equiv 0 \ (mod\ p_1), \alpha_2 \equiv -1 \ (mod\ p_2)\ , \dots\ , \alpha_2 \equiv 0 \ (mod\ p_m)$$

طبق باقی مانده چینی α_2 با این شرایط یافت می شود. مشابه همین روند را برای $\alpha_3, \dots, \alpha_m$ هم خواهیم داشت که مشابه بالا اعدادی وجود دارند که شروط بالا را ارضا کنند. تمام.

حل از مولف: روی n استقرا می زنیم. برای $n = 1$ کافی است قرار دهید $d = x_1$. حال فرض کنید تا $n = k - 1$ حکم برقرار باشد. حال برای $n = k$: طبق فرض استقرا عدد e یافت می شود طوری که $ex_1, \dots, ex_k$ توان های کامل باشند. فرض کنید ex_i توان y_i ام یک عدد باشد. فرض کنید $T = y_1 y_2 \dots y_k$ باشد. حال بگیرید $d = e * (f)^T$. در این صورت اگر f هر عددی باشد بازهم ex_i توان y_i ام یک عدد خواهد بود(چرا؟). حال y_{k+1} را عددی دلخواه بزرگتر از یک بگیرید که نسبت به T اول باشد. می خواهیم

$dx_{k+1} = de * (f)^T$ توان y_{k+1} ام عددی باشد. ساده ترین کار این است که بگیرید $f = (de)^s$ در این صورت کافی است داشته باشیم $1 + sT \equiv 0 \ (mod \ y_{k+1})$ چون $(T, y_{k+1}) = 1$ چنین عددی یافت می شود و در نتیجه گام استقرا هم کامل شد. تمام.

سوال) (APMO 2009 سوال 4)

(توضیح راه حلش ساده نیست و شاید بهتر باشد در اواسط سطح 2 بیابید) (ایده دارد ولی کلا ساده است)

فرض کنید n عددی طبیعی باشد. ثابت کنید n گویا $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_n}{b_n}$ یافت می شوند طوری که $\forall 1 \le i \le n : (a_i, b_i)$ باشد و این n عدد تشکیل تصاعد حسابی می دهند و هم چنین $2n$ عدد $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ با هم متمایز اند.

راهنمایی 1 : فرض کنید عضو اول و قدر نسبت به ترتیب $\frac{C}{B}$ و$\frac{D}{B}$ باشند. در نتیجه عضو $i + 1$ ام برابر است با $\frac{C+Di}{B}$.

برای متمایز شدن صورت ها کافی است اولا صورت کسر i ام دارای عددی اول باشد که هیچ صورت و مخرج دیگری نداشته باشد و دوما برای اینکه مخرج ها متمایز شوند در کسر i ام دقیقا یک عامل اول یکتا از صورت و مخرج ساده شوند .

راهنمایی 2: اعداد اول متمایز $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_n$ را در نظر بگیرید. فرض کنید $B = p_1 p_2 \dots p_n$ باشد.

شرط اول: برای اینکه بعد از ساده شدن، مخرج های مختلف متمایز باشند کافی است برای هر i فقط p_i از صورت و مخرج ساده شود و $p_i\ ,j \neq i$ ساده نشوند.

شرط دوم : برای اینکه بعد از ساده شدن صورت ها از هم متمایز باشند و هم چنین از مخرج ها متمایز باشند کافی صورت i ام دارای q_i باشد و دارای هیچ کدام از $q_j\ ,j \neq i$ نباشد.

راهنمایی 3: در راهنمایی 2 شروط معادل است با اینکه داشته باشیم $p_i|C + D(j-1) \Leftrightarrow i = j$ و $q_i|C + D(j-1) \Leftrightarrow i = j$

حل: فرض کنید عضو اول و قدر نسبت به ترتیب $\frac{C}{B}$ و$\frac{D}{B}$ باشند. در نتیجه عضو $i+1$ ام برابر است با $\frac{C+Di}{B}$.

اعداد اول متمایز $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_n$ را در نظر بگیرید. فرض کنید $B = p_1 p_2 \dots p_n$ باشد.

شرط اول: برای اینکه بعد از ساده شدن، مخرج های مختلف متمایز باشند کافی است برای هر i فقط p_i از صورت و مخرج ساده شود و $p_i\ ,j \neq i$ ساده نشوند.

شرط دوم : برای اینکه بعد از ساده شدن صورت ها از هم متمایز باشند و هم چنین از مخرج ها متمایز باشند کافی صورت i ام دارای q_i باشد و دارای هیچ کدام از $q_j\ ,j \neq i$ نباشد.

برای شرط اول و دوم باید داشته باشیم $p_i|C + D(j-1) \Leftrightarrow i = j$ و $q_i|C + D(j-1) \Leftrightarrow i = j$. در نتیجه برای مثال برای p_3 باید داشته باشیم :

$$C, C + D, C + 3D, \dots, C + (n-1)D \not\equiv 0 \ (mod\ p_3)\ , C + 2D \equiv 0 \ (mod\ p_3)$$

می توان به سادگی دید باید داشته باشیم $\forall 1 \le i \le n: i \equiv 2 \left(mod\ p_3\right) \Leftrightarrow i = 2$ که معادل با این است که $n-2 < p_3$

باشد . در نتیجه کافی است بگیریم $n < p_2$ باشد.

مشابه همین اوضاع برای p_i ها و q_i های دیگر هم برقرار است و ما به معادلات زیر می رسیم :

$$0 \equiv C\ (mod\ p_1q_1), D \equiv -C\ (mod\ p_2q_2), \dots, (n-1)D \equiv C\ (mod\ p_nq_n)$$

و $\forall 1 \le i \le n: p_i, q_i > n$. حال کافی است قرار دهید $c = p_1q_1$ و طبق باقی مانده چینی عدد D یافت می شود که در معادلات

بالا صدق کند. تمام.

سوال (ELMO 2014 Shortlist N7)

(ایده ای و جالب) (بین سطح دو و سه)

منبع:

http://artofproblemsolving.com/community/c6h599357p3558541

عدد x را قوی می نامیم اگر همه عوامل اول آن بزرگتر از 2014 باشند. سه تایی (a, b, c) از اعداد طبیعی را خوب می نامیم اگر

برای هر عدد قوی n داشته باشیم $n + c | a^n + b^n + n$. همه سه تایی های خوب را بیابید.

راهنمایی 1: ابتدا به قوی بودن n کار نداشته باشید و صرفا فرض کنید n باید عدد بزرگی باشد. حال فرض کنید عدد اول p عدد

$n + c$ را عاد کند. اگر باقیمانده n بر $p-1$ عدد معلوم باشد آنگاه $p | a^n + b^n + n$ به عبارتی بسیار ساده تر تبدیل خواهد شد.

راهنمایی 2: عدد اول بسیار بزرگ p $(p > a + b + c + abc)$ را در نظر بگیرید. طبق باقیمانده چینی عدد n یافت می شود طوری

که $n \equiv -c\ (mod\ p), n \equiv 1\ (mod\ p-1),$ نتیجه بگیرید اگر n قوی باشد خواهیم داشت $a + b = c$ است. حال باید با

افزودن معادلاتی کار کنید که n حتما قوی شود. پس از آن دسته معادلات دیگری بنویسید و روابط دیگری برای a, b, c به دست آورید.

راهنمایی 3: برای قوی شدن n باید معادلات زیر را در نظر بگیرید

$$n \equiv -c \ (mod\ p), n \equiv 1 \ (mod\ p-1), n \equiv 1 \ \ (\ mod\ q_1 q_2 \dots q_m)$$

هم چنین دسته معادلات دیگری شبیه به این روابط دیگری در مورد a, b, c خواهند داد که باید آن را معرفی کنید. جواب نهایی مساله $(a, b, c) = (1,1,2)$ است.

حل(ویرایش شده حل منبع) : فرض کنید $q_1, q_2, \dots, q_m$ مجموعه اعداد اول کوچکتر از 2014 باشد. عدد اول بسیار بزرگ p ($p > a + b + c + abc$) را در نظر بگیرید. طبق باقیمانده چینی عدد n یافت می شود طوری که

$$n \equiv -c \ (mod\ p), n \equiv 1 \ (mod\ p-1), n \equiv 1 \ \ (\ mod\ q_1 q_2 \dots q_m)$$

توجه کنید که در اینجا $q_1 q_2 \dots q_m$ و $p - 1$ نسبت به هم اول نیستند . اما چون در هر دو باید n در هم نهشتی برابر با 1 شود مشکلی پیش نمی آید (می توانید این را به طور دقیق ثابت کنید؟) . واضح است که n قوی است و

$$p | n + c | a^n + b^n + n$$

در نتیجه $0 \equiv a^n + b^n + n \equiv a + b - c \ (mod\ p)$ و در نتیجه $a + b = c$ است.

مشبها طبق باقیمانده چینی عدد n یافت می شود طوری که

$$n \equiv -c \ (mod\ p), n \equiv -1 \ (mod\ p-1), n \equiv -1 \ \ (\ mod\ q_1 q_2 \dots q_m)$$

واضح است که n قوی است و

$$p|n+c|a^n+b^n+n$$

در نتیجه $0\equiv a^n+b^n+n\equiv a^{-1}+b^{-1}-c\ (mod\ p)$ و در نتیجه $0\equiv b+a-cab\ (mod\ p)$است. در نتیجه $a+b=abc$ است. پیش تر به دست آوردیم $a+b=c$ است. در نتیجه باید داشته باشیم $a=b=1$ است و در نتیجه $c=2$ است. ثابت می کنیم $(a,b,c)=(1,1,2)$ در فرض سوال صدق می کند. این هم به این خاطر است که در این حالت مستقل از اینکه n چه عددی باشد داریم $n+c=n+2|n+2=a^n+b^n+n$.تمام.

سوال سطح 3: سوال های چالش بر انگیز

سوال (ELMO 2013 Problem 3)

این سوال را در لانه کبوتری هم باید قرار داد. چون راه حل با ریشه واحد هم دارد باید در آن فصل هم قرار بگیرد.

منبع :

http://artofproblemsolving.com/community/c6h539544p3152018

(ایده ای و معادل $N4$ المپیاد جهانی) (بسیار زیبا) فرض کنید $m_1,m_2,\dots,m_{2013}$ اعداد طبیعی بزرگتر از 1 باشند . هم چنین $A_1,A_2,\dots,A_{2013}$ مجموعه هایی باشند طوری که برای هر i ، مجموعه A_i زیرمجموعه $\{1,2,3,\dots,m_i-1\}$ است. عددی را عضو A_i به پیمانه m_i می نامیم اگر باقیمانده اش بر m_i عضوی از A_i باشد(برای مثال 7 به پیمانه 5 عضوی از $\{1,2\}$ است چون

باقیمانده اش بر 5 برابر 2 است). عدد y را مستقل می نامیم اگر برای هر $1 \le i \le 2013$ عضو A_i به پیمانه m_i نباشد. ثابت کنید عدد طبیعی و مستقلی وجود دارد که کمتر مساوی عدد زیر باشد :

$$N = (1 + 2|A_1|)(1 + 2|A_2|) \dots (1 + 2|A_{2013}|)$$

که منظور از $|B|$ تعداد اعضای مجموعه B است.

نکته : شرط مستقل بودن به صورت رسمی می توان اینطور بیان کرد که اگر برای هر $1 \le i \le 2013$ و هر $x \in A_i$ داشته باشیم :

$y \not\equiv x \ (mod\ m_i)$

راهنمایی 1: فرض کنید $M = m_1 m_2 \dots m_{2013}$ باشد. فرض کنید $\{y_1, y_2, \dots, y_s\} \subseteq \{0,1,2, \dots, M-1\}$ که $s \ge N$ مجموعه ای باشند طوری که تفاضل هر دو عضوی از آن مستقل باشد(دو عضو می توانند برابر هم باشند) و هم چنین داشته باشیم $y_1 = 0$. در این صورت به سادگی (به نوعی با استدلال از نوع لانه کبوتری) می توان دید y_i, y_j وجود دارد که $0 < y_i - y_j \le \frac{M}{s} < \frac{\mathrm{M}}{\mathrm{N}}$ باشد و از روی آن حکم مساله نتیجه می شود.

راهنمایی 2: ثابت کنید $B_i \subseteq \{0,1, \dots, m_i\}$ وجود دارد که اولا صفر در آن باشد و ثانیا تفاضل هر دو عضوی از آن، عضو A_i به پیمانه m_i نباشد و $\frac{m_i}{1+2|A_i|} \le |B_i|$

راهنمایی 3: برای اثبات راهنمایی 2 فرض کنید B_i با بیشترین عضو ممکن را انتخاب کرده ایم. در نتیجه اگر عر عضو جدید به آن اضافه کنید خاصیت راهنمایی 2 را نخواهد داشت. از این استفاده کنید و ثابت کنید $\frac{m_i}{1+2|A_i|} \le |B_i|$ است. ادامه کار با باقیمانده چینی خواهد بود.

حل (official solution): فرض کنید $M = m_1 m_2 \dots m_{2013}$ باشد. فرض کنید $\{y_1, y_2, \dots, y_s\} \subseteq \{0,1,2, \dots, M-1\}$ مجموعه ای باشند طوری که تفاضل هر دو عضوی از آن مستقل باشد(دو عضو می توانند برابر هم باشند) و هم چنین داشته باشیم

$y_1 = 0$. در این صورت به سادگی (به نوعی با استدلال از نوع لانه کبوتری) می توان دید y_i, y_j وجود دارد که $0 < y_i - y_j \leq \frac{M}{s}$ باشد. در نتیجه کافی است داشته باشیم $s \geq N$ و از روی آن حکم مساله نتیجه می شود(⁕).

$1 \leq i \leq 2013$ را عددی ثابت بگیرید. فرض کنید $B_i \subseteq \{0,1,\dots,m_i\}$ و با بیشترین عضو ممکن را انتخاب کرده ایم طوری که اولا صفر در آن باشد و ثانیا تفاضل هر دو عضوی از آن، عضو A_i به پیمانه m_i نباشد. فرض کنید $C = \{0,1,\dots,m_i\}\backslash B_i$ باشد. چون B_i بیشترین تعداد اعضای ممکن را دارا است در نتیجه برای هر $x \in C$ باید عدد $y \in B_i$ یافت شود طوری که $x - y \in A_i$ یا $x - y \in -A_i$ (چرا؟) زیرا در غیر این صورت $B_i \cup \{x\}$ مجموعه با تعداد اعضای بیشتری از B_i است و هم چنین عضو A_i به پیمانه m_i نیست(چرا؟). در نتیجه هر عدد در C برابر عضوی از B_i منها یا به علاوه عضوی از A_i خواهد بود. در نتیجه طبق اصل ضرب $|C_i| \leq 2|B_i||A_i|$ (چرا؟) و در نتیجه $m_i = |C_i| + |B_i| \leq |B_i|(1 + 2|A_i|)$ و در نتیجه داریم $\frac{m_i}{1+2|A_i|} \leq |B_i|$ (⁕⁕)

حال همه اعداد در $\{0,1,2,\dots,M-1\}$ را در نظر بگیرید که برای هر $1 \leq i \leq 2013$ عضو B_i به پیمانه m_i باشند. طبق باقیمانده چینی تعداد این اعداد برابر $|B_1||B_2||B_3|\dots|B_{2013}|$ است(چرا؟) که طبق (⁕⁕) مقداری برابر حداقل $\frac{m_1}{1+2|A_1|}.\frac{m_2}{1+2|A_2|}\dots\frac{m_{2013}}{1+2|A_{2013}|} = \frac{M}{N}$ دارد. برای هر دو عدد این چینی، تفاضلشان برای هر $1 \leq i \leq 2013$ عضو A_i به پیمانه m_i نیست(طبق نحوه ساختن B_i). در نتیجه طبق (⁕) حکم نتیجه می‌شود.